Apple 플랫폼 보안

2024년 5월

목차

Apple 플랫폼 보안 소개

Apple은 보안을 플랫폼의 핵심으로 설계합니다. Apple은 세계적으로 가장 진보한 모바일 운영 체제를 구축한 경험을 바탕으로 모바일, 시계, 데스크탑 및 홈의 고유한 요구 사항을 해결하는 보안 아키텍처를 만들었습니다.

모든 Apple 기기의 **하드웨어**와 **소프트웨어**, **서비스**는 서로 연동되도록 설계되어 보안성을 극대화하고 투명한 사용자 경험을 제공하는 동시에, 개인정보를 안전하게 보호하는 최종 목표를 달성합니다. 예를 들어 Apple이 설계한 실리콘 칩 및 보안 하드웨어는 주요 보안 기능을 지원합니다. 또한 소프트웨어 보호는 운영 체제 및 타사 앱을 보호하기 위해 기능합니다. 나아가 서비스는 안전하며 시기적절한 소프트웨어 업데이트 메커니즘을 제공하고, 더욱 안전한 앱 생태계로 나아가고, 통신 및 결제를 보호합니다. 결과적으로 Apple 기기는 해당 기기 및 데이터뿐만 아니라 사용자가 로컬에서, 네트워크에서, 그리고 주요 인터넷 서비스에서 행하는 모든 동작을 포함한 전체 생태계를 안전하게 보호합니다.

Apple은 단순하고 직관적이며 기능적인 제품을 설계하는 것만큼이나 안전한 제품을 설계합니다. 하드웨어 기반 기기 암호화와 같은 주요 보안 기능은 실수로 비활성화될 수 없습니다. 또한 Face ID 및 Touch ID와 같은 기능으로 간단하고 직관적으로 기기를 보호할 수 있어 사용자 경험의 수준이 더욱 높아집니다. 나아가 기본적으로 대부분의 보안 기능이 활성화되어 있기 때문에 이용자 또는 IT 부서에서는 추가로 구성을 설정할 필요가 없습니다.

이 문서에서는 보안 기술 및 기능이 Apple 플랫폼에 구현된 방법에 대한 자세한 정보를 제공합니다. 또한 조직이 Apple 플랫폼 보안 기술 및 기능을 조직의 정책 및 절차와 통합하여 해당 조직의 특정 요구 사항에 맞추는 데 도움을 줄 수 있습니다.

이 문서는 다음과 같은 주제로 구성되어 있습니다.

- **하드웨어 보안 및 생체 인증:** Apple Silicon, Secure Enclave, 암호화 엔진, Face ID 및 Touch ID 등 Apple 기기의 보안 기반을 구성하는 실리콘 칩과 하드웨어
- **시스템 보안:** Apple 운영 체제의 안전한 시동, 업데이트 및 지속적인 운영을 위한 통합된 하드웨어 및 소프트웨어 기능
- **암호화 및 데이터 보호:** 기기 분실 또는 도난의 경우 혹은 인증받지 않은 사람 또는 프로세스가 기기를 사용 또는 수정하는 경우에 사용자 데이터를 보호하는 아키텍처와 디자인
- **앱 보안:** 안전한 앱 생태계를 제공하고 앱이 플랫폼 무결성을 해치지 않으면서 안전하게 작동하도록 하는 소프트웨어 및 서비스
- **서비스 보안:** 식별, 암호 관리, 결제, 통신 및 잃어버린 기기 찾기 등을 위한 Apple의 서비스
- **네트워크 보안:** 전송 시 데이터 암호화와 보안 인증을 제공하는 업계 표준 네트워크 프로토콜
- **개발자 키트 보안:** 개인정보 노출 없이 안전하게 집과 건강을 관리하고, Apple 기기와 서비스 기능을 타사 앱으로 확장하기 위한 프레임워크 '키트'
- **보안 기기 관리:** Apple 기기 관리를 허용하고, 인증받지 않은 사람이 기기를 사용할 수 없도록 하며, 기기 분실 또는 도난의 경우 기기를 원격으로 지울 수 있는 방법

보안에 대한 노력

Apple은 고객을 보호하기 위해 최선을 다하고 있습니다. 개인정보 보호 및 보안의 첨단 기술을 통해 개인정보를 보호하고 포괄적인 방법으로 기업 환경에서 기업 데이터를 보호하기 위해 노력합니다. Apple은 Apple 보안 포상금을 제공하여 취약점을 발견하는 연구원의 성과에 대해 보상합니다. 프로그램에 대한 자세한 내용과 포상금 범주는 https://security.apple.com/bounty/ 페이지에서 확인할 수 있습니다.

Apple은 모든 Apple 제품을 지원하기 위한 전용 보안 팀을 유지합니다. 이 팀은 개발 중이거나 출시된 제품에 대한 보안 감사 및 테스트를 제공합니다. 이 팀은 또한 보안 도구와 교육을 제공하고 새로운 보안 문제 리포트 및 위협을 적극적으로 모니터링합니다. Apple은 FIRST(Forum of Incident Response and Security Teams)의 회원입니다.

Apple은 보안 및 개인정보 보호의 한계를 계속해서 극복해 나가고 있습니다. Apple Watch부터 iPhone, iPad 및 Mac의 M 시리즈 칩까지 맞춤형 Apple 실리콘 칩을 활용하여 효율적인 계산뿐 아니라 보안까지 강화합니다. 예를 들어, Apple Silicon은 보안 시동, Face ID 및 Touch ID, 데이터 보호에 대한 기반을 구성합니다. 또한 커널 무결성 보호, 포인터 인증 코드 및 빠른 권한 제한을 포함하는 Apple Silicon으로 구동되는 보안 기능은 일반적인 유형의 공격을 막는 데 도움이 됩니다. 만약 공격자의 코드가 실행되더라도 공격으로 인한 손상을 현저하게 줄입니다.

Apple 플랫폼에 내장된 광범위한 보안 기능을 최대한 활용하기 위해 조직이 IT 및 보안 정책을 검토하여 Apple 플랫폼에서 제공하는 보안 기술 계층을 충분히 활용하도록 권장합니다.

Apple에 문제를 보고하고 보안 알림을 구독하는 것에 대해 알아보려면 보안 또는 개인정보 보호 취약점 신고하기 사이트를 참조하십시오.

Apple은 사용자의 개인정보 보호를 기본적인 인권으로 생각하며, 제품에 다양한 제어 설정 및 옵션을 내장하여 사용자가 앱이 사용할 정보의 내용뿐 아니라 해당 정보를 사용하는 방법과 시점을 결정할 수 있습니다. Apple의 개인정보 보호 접근 방법, Apple 기기에서의 개인정보 보호 제어 및 Apple의 개인정보 처리방침에 관해 더 알아보려면 https://www.apple.com/kr/privacy 페이지를 참조하십시오.

참고: 별도로 명시되지 않은 한, 이 문서에서 다루는 운영 체제 버전은 다음과 같습니다. iOS 17.3, iPadOS 17.3, macOS 14.3, tvOS 17.3 및 watchOS 10.3.

하드웨어 보안 및 생체 인증

하드웨어 보안 개요

소프트웨어의 보안을 유지하려면 보안 기능이 내장된 하드웨어에 소프트웨어를 설치해야 합니다. 이것이 iOS, iPadOS, macOS, tvOS 및 watchOS를 실행하는 Apple 기기에 보안 기능이 담긴 실리콘 칩을 탑재한 이유입니다. 이러한 기능에는 시스템 보안 특성을 제공하는 CPU와 보안 기능을 제공하는 전용 실리콘 칩이 추가로 포함됩니다. 보안 중심 하드웨어는 공격 표면을 최소화하기 위해 제한적이며 별도로 정의된 기능을 지원하는 원칙을 따릅니다. 이러한 구성 요소에는 보안 시동을 위한 하드웨어 신뢰 루트를 형성하는 Boot ROM, 효율적이고 안전한 암호화 및 암호화 해제를 위한 전용 AES 엔진 및 Secure Enclave가 포함됩니다. **Secure Enclave**는 Apple SoC(System on Chip)의 구성 요소로, 최신 iPhone, iPad, Apple Watch, Apple TV, HomePod 기기와 Apple Silicon이 탑재된 Mac 및 Apple T2 보안 칩이 탑재된 Mac에 포함됩니다. Secure Enclave 자체는 SoC와 동일한 설계 원리를 따르며 별도의 Boot ROM 및 AES 엔진을 포함합니다. 또한 Secure Enclave는 유휴 데이터를 암호화하는 데 필요한 키를 안전하게 생성하고 저장하기 위한 기반을 제공하며 Face ID 및 Touch ID의 생체 인증 데이터를 보호하고 평가합니다.

저장 공간 암호화는 빠르고 효율적이어야 합니다. 이와 동시에 암호화 키 관계를 구축하는 데 사용하는 데이터(또는 **키 재료**)를 유출해서는 안 됩니다. AES 하드웨어 엔진은 **파일을 쓰거나 읽을 때** 빠른 인라인 암호화 및 암호화 해제를 수행하여 이 문제를 해결합니다. Secure Enclave의 특수 채널은 이 정보를 응용 프로그램 프로세서(또는 CPU) 또는 전체 운영 체제에 노출하지 않고 AES 엔진에 필요한 키 재료를 제공합니다. 이를 통해 Apple의 데이터 보호와 FileVault 기술이 장기간 사용한 암호화 키를 노출하지 않고 사용자의 파일을 보호할 수 있습니다.

Apple은 보안 시동이 소프트웨어의 최하위 구조가 조작되는 것을 방지하고, 시동 시 Apple에서 신뢰하는 운영 체제 소프트웨어만 로드하도록 설계했습니다. 보안 시동은 **Boot ROM**이라는 변경 불가능 코드가 보안성의 기반을 이룹니다. 이는 Apple SoC 제조 단계에서 구현되며 **하드웨어 신뢰 루트**로 알려져 있습니다. T2 칩이 탑재된 Mac 컴퓨터에서는 T2가 신뢰할 수 있는 macOS 보안 시동의 기반입니다. (T2 칩과 Secure Enclave는 모두 자체적으로 별도의 Boot ROM을 사용하여 자체 보안 시동 프로세스를 실행합니다. 이는 A 시리즈, M1 및 M2 칩이 안전하게 시동되는 방식과 정확히 일치합니다.)

또한 Secure Enclave는 Apple 기기에서 Face ID 및 Touch ID 센서의 얼굴과 지문 데이터를 처리합니다. Secure Enclave는 사용자의 생체 인증 데이터를 노출의 염려 없이 안전하게 보호하면서 보안 인증을 제공합니다. 또한 이를 통해 사용자에게 더 길고 복잡한 암호로 강력한 보안이 제공되며, 접근 또는 구매 시 인증을 신속하게 처리하여 이용이 더 편리해집니다.

Apple SoC 보안

Apple이 설계한 Apple Silicon은 모든 Apple 제품에서 공통 아키텍처를 형성하며 Mac뿐만 아니라 iPhone, iPad, Apple TV 및 Apple Watch의 성능을 향상하고 있습니다. 세계 최고 수준의 Apple Silicon 디자인팀은 10년 이상 Apple SoC(System on Chip)를 구축하고 개선해 왔습니다. 그 결과 모든 기기용으로 설계된 확장 가능한 아키텍처가 보안 기능에 있어서 업계를 선도하게 되었습니다. 이러한 보안 기능에 대한 공통 기반은 소프트웨어와 동작하도록 자체 실리콘 칩을 설계한 회사에서만 가능합니다.

Apple Silicon은 시스템 보안 기능을 사용할 수 있도록 특별히 설계 및 제작되었습니다. 아래에서 자세히 알아보십시오.

기능	A10	A11, S3	A12, A13, A14 S4–S9	A15, A16, A17	M1, M2, M3
커널 무결성 보호	✓	✓	✓	✓	✓
빠른 권한 제한	✗	✓	✓	✓	✓
시스템 보조 프로세서 무결성 보호	✗	✗	✓	✓	✓
포인터 인증 코드	✗	✗	✓	✓	✓
페이지 보호 레이어	✗	✓	✓	✗	✗ 아래의 참고 1 내용 확인.
보안 페이지 테이블 모니터	✗	✗	✗	✓ 아래의 참고 2 내용 확인.	✗

참고 1: PPL(페이지 보호 레이어)는 플랫폼이 **서명되고 신뢰할 수 있는 코드만** 실행하도록 요구합니다. 이는 macOS에 적용되지 않는 보안 모델입니다.

참고 2: 보안 페이지 테이블 모니터(SPTM)는 A15, A16 및 A17에서 지원되며 지원 플랫폼에서 페이지 보호 레이어를 대체합니다.

Apple이 설계한 Apple Silicon은 또한 데이터 보호 기능을 활성화합니다. 아래에서 자세히 알아보십시오.

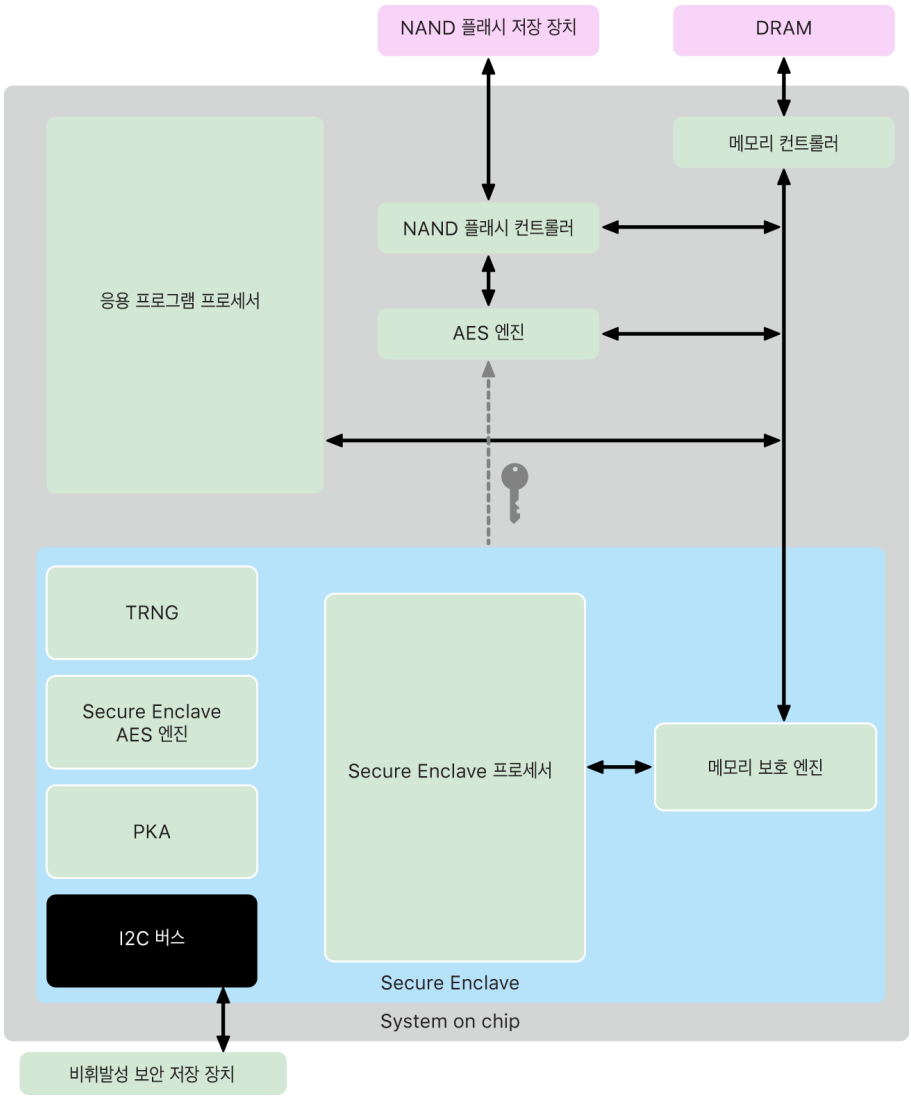
기능	A10, A11 S3	A12–A17 S4–S9 M1, M2, M3
SKP(봉인 키 보호)	✓	✓
복구용 OS - 모든 데이터 보호 클래스가 보호됨	✓	✓
DFU, 진단 및 업데이트의 대체 시동 - 클래스 A, B 및 C 데이터가 보호됨	✗	✓

Secure Enclave

Secure Enclave는 최신 버전의 iPhone, iPad, Mac, Apple TV, Apple Watch, HomePod 모델의 전용 보안 하위 시스템입니다.

개요

Secure Enclave는 Apple SoC(System on Chip)에 통합된 전용 보안 하위 시스템입니다. Secure Enclave는 메인 프로세서와 격리되어 추가적인 보안 계층을 제공하며, 응용 프로그램 프로세서 커널이 손상된 경우에도 민감한 사용자 데이터를 안전하게 보관하도록 설계되었습니다. 이는 하드웨어 신뢰 루트를 확립하기 위한 Boot ROM, 효율적이고 안전한 암호화 작업을 위한 AES 엔진 및 보호된 메모리 등 SoC와 동일한 설계 원리를 따릅니다. Secure Enclave는 저장 장치를 포함하지 않지만 응용 프로그램 프로세서 및 운영 체제에서 사용하는 NAND 플래시 저장 장치와는 별도로 연결된 저장 장치에 정보를 안전하게 저장하는 메커니즘이 있습니다.



Secure Enclave는 하드웨어 기능으로, 다음과 같은 대부분의 iPhone, iPad, Mac, Apple TV, Apple Watch, HomePod 모델에서 제공됩니다.

- iPhone 5s 및 이후 모델
- iPad Air 및 이후 모델
- Apple Silicon이 탑재된 Mac 컴퓨터
- Apple T1 칩 및 Touch Bar가 탑재된 MacBook Pro 컴퓨터(2016년 및 2017년)
- Apple T2 보안 칩이 탑재된 Intel 기반 Mac 컴퓨터
- Apple TV HD 및 이후 모델
- Apple Watch Series 1 및 이후 모델
- HomePod 및 HomePod mini

Secure Enclave 프로세서

Secure Enclave 프로세서는 Secure Enclave에 주요 컴퓨팅 성능을 제공합니다. 가장 강력한 분리를 제공하고자 Secure Enclave 프로세서는 Secure Enclave 전용으로만 사용됩니다. 이를 통해 공격 대상 소프트웨어와 동일한 실행 코어를 공유하는 악성 소프트웨어에 의존하는 사이드 채널 공격을 방지할 수 있습니다.

Secure Enclave 프로세서는 L4 마이크로커널의 Apple 맞춤형 버전을 실행합니다. 또한 느린 클럭 속도에서 효율적으로 작동하도록 설계되어 클럭 및 전력 공격으로부터 보호하는 데 도움이 됩니다. A11 및 S4부터 Secure Enclave 프로세서는 재전송 방지 기능, 보안 시동, 전용 난수 발생기 및 자체 AES 엔진을 갖춘 메모리 보호 엔진 및 암호화된 메모리를 포함합니다.

메모리 보호 엔진

Secure Enclave는 기기의 DRAM 메모리 전용 영역에서 작동합니다. 다중 보호 계층은 Secure Enclave에서 보호하는 메모리를 응용 프로그램 프로세서에서 분리합니다.

기기가 시동되면 Secure Enclave Boot ROM은 메모리 보호 엔진에 대한 임시 메모리 보호 키를 임의로 생성합니다. Secure Enclave가 전용 메모리 영역에 쓸 때마다 메모리 보호 엔진은 AES를 사용하여 Mac XEX(xor-encrypt-xor) 모드에서 메모리 블록을 암호화하고 메모리에 대한 CMAC(암호 기반 메시지 인증 코드) 인증 태그를 계산합니다. 메모리 보호 엔진은 암호화된 메모리와 함께 인증 태그를 저장합니다. Secure Enclave가 메모리를 읽을 때 메모리 보호 엔진은 인증 태그를 확인합니다. 인증 태그가 일치하면 메모리 보호 엔진이 메모리 블록을 암호화 해제합니다. 태그가 일치하지 않는 경우 메모리 보호 엔진은 Secure Enclave에 오류 신호를 보냅니다. 메모리 인증 오류가 발생하면 Secure Enclave는 시스템이 재시동될 때까지 요청 수락을 중단합니다.

Apple A11 및 S4 SoC부터, 메모리 보호 엔진은 Secure Enclave 메모리에 재전송 보호 기능을 추가합니다. 메모리 보호 엔진은 보안에 중요한 데이터의 재전송을 방지하기 위해 인증 태그와 함께 메모리 블록에 대한 **재전송 방지 값**이라고 불리는 고유한 일회성 숫자를 저장합니다. 재전송 방지 값은 CMAC 인증 태그에 대한 추가적인 트윅으로 사용됩니다. 모든 메모리 블록에 대한 재전송 방지 값은 Secure Enclave 내의 전용 SRAM에 뿌리를 둔 무결성 트리로 보호됩니다. 쓰기의 경우 메모리 보호 엔진은 재전송 방지 값 및 무결성 트리의 각 수준을 SRAM까지 **업데이트**합니다. 읽기의 경우 메모리 보호 엔진은 재전송 방지 값 및 무결성 트리의 각 수준을 SRAM까지 **확인**합니다. 재전송 방지 값 불일치는 인증 태그 불일치와 유사하게 처리됩니다.

Apple A14 및 M1 이상의 SoC에서 메모리 보호 엔진은 두 개의 임시 메모리 보호 키를 지원합니다. 첫 번째는 Secure Enclave의 비공개 데이터에 사용되며 두 번째는 Secure Neural Engine과 공유되는 데이터에 사용됩니다.

메모리 보호 엔진은 Secure Enclave에 대해 인라인으로 투명하게 작동합니다. Secure Enclave는 암호화되지 않은 일반 DRAM처럼 메모리를 읽고 쓰지만, Secure Enclave 외부의 관찰자는 암호화되고 인증된 메모리 버전만 볼 수 있습니다. 이로 인해 성능이 저하되거나 소프트웨어를 복잡하게 만들지 않고도 강력한 메모리 보호 기능이 제공됩니다.

Secure Enclave Boot ROM

Secure Enclave에는 전용 Secure Enclave Boot ROM이 포함되어 있습니다. 응용 프로그램 프로세서 Boot ROM과 마찬가지로 Secure Enclave Boot ROM은 Secure Enclave에 대해 하드웨어 신뢰 루트를 구축하는 변경 불가능 코드입니다.

시스템을 시작할 때 iBoot는 Secure Enclave에 전용 메모리 영역을 할당합니다. 메모리를 사용하기 전에 Secure Enclave Boot ROM은 메모리 보호 엔진을 초기화하여 Secure Enclave로 보호된 메모리에 대한 암호화 보호를 제공합니다.

그러면 응용 프로그램 프로세서가 Secure Enclave Boot ROM에 sepOS 이미지를 전송합니다. sepOS 이미지를 Secure Enclave로 보호된 메모리에 복사하고 나면 Secure Enclave Boot ROM은 이미지의 암호화 해시 및 서명을 확인하여 sepOS가 기기에서 실행되도록 인증되었는지 확인합니다. sepOS 이미지가 기기에서 실행되도록 올바르게 서명된 경우 Secure Enclave Boot ROM은 sepOS에 제어 권한을 넘겨줍니다. 서명이 유효하지 않은 경우 Secure Enclave Boot ROM은 다음 칩이 재설정될 때까지 Secure Enclave를 더 이상 사용할 수 없도록 합니다.

Apple A10 및 이후에 출시된 SoC에서 Secure Enclave Boot ROM은 sepOS의 해시를 이 용도로만 사용되는 레지스터에 잠급니다. 공개 키 액셀러레이터는 OS 바운드(Operating-System-Bound) 키에 이 해시를 사용합니다.

Secure Enclave 시동 모니터

Apple A13 및 이후에 출시된 SoC에서 Secure Enclave에는 시동 모니터가 포함되어 시동된 sepOS의 해시에 더 강력한 무결성을 보장합니다.

시스템을 시동할 때 Secure Enclave 프로세서의 SCIP(시스템 보조 프로세서 무결성 보호) 구성은 Secure Enclave 프로세서가 Secure Enclave Boot ROM 이외의 코드를 실행하는 것을 방지합니다. 시동 모니터는 Secure Enclave가 SCIP 구성을 직접 수정하지 못하도록 합니다. Secure Enclave Boot ROM은 로드된 sepOS의 크기 및 주소를 포함한 요청을 시동 모니터에 전송하여 로드된 sepOS를 실행할 수 있게 합니다. 시동 모니터가 요청을 받으면 Secure Enclave 프로세서를 재설정하고 로드된 sepOS를 해시한 다음, 로드된 sepOS의 실행을 허용하도록 SCIP 설정을 업데이트하고 새로 로드된 코드 내에서 실행을 시작합니다. 시스템이 계속 시동되면서 새로운 코드가 실행될 때마다 동일한 프로세스가 사용됩니다. 시동 모니터는 시동 프로세스의 실행 중인 해시를 매번 업데이트합니다. 또한, 시동 모니터는 실행 중인 해시에 중요한 보안 매개 변수를 포함합니다.

시동이 완료되면 시동 모니터가 실행 중인 해시를 종결하고 이를 공개 키 액셀러레이터로 전송하여 OS 바운드 키에 사용합니다. 이 프로세스는 Secure Enclave Boot ROM에 취약점이 있더라도 운영 체제 키 바인딩을 우회할 수 없도록 설계되었습니다.

참난수 발생기

참난수 발생기(TRNG)는 안전한 임의 데이터를 생성하는 데 사용됩니다. Secure Enclave는 임의 암호화 키, 임의 키 시드 또는 기타 엔트로피를 생성할 때마다 TRNG를 사용합니다. TRNG는 CTR_DRBG(카운터 모드에서 블록 암호를 기반으로 하는 알고리즘)로 후처리된 다수의 링 오실레이터를 기반으로 합니다.

루트 암호화 키

Secure Enclave에는 UID(고유 ID) 루트 암호화 키가 포함되어 있습니다. UID는 개별 기기마다 고유하며 기기의 다른 식별자와 관련이 없습니다.

임의로 생성된 UID는 제조 시 SoC에 결합됩니다. A9 SoC부터 UID는 제조 중 Secure Enclave TRNG에 의해 생성되며, Secure Enclave에서 완전히 실행되는 소프트웨어 프로세스를 사용하여 퓨즈에 기록됩니다. 이 프로세스는 UID가 제조 중 기기 외부에서 보이지 않도록 하기 때문에 Apple 또는 Apple의 공급업체가 접근하거나 저장하는 데 사용할 수 없습니다.

sepOS는 UID를 사용하여 기기 고유의 기밀 정보를 보호합니다. UID로 데이터를 특정 기기와 연결하여 암호화할 수 있습니다. 예를 들면, 파일 시스템을 보호하는 키 계층에 UID가 포함되어 있어 내부 SSD 저장 공간을 물리적으로 다른 기기로 옮기는 경우 해당 파일에 접근할 수 없습니다. 그 외에 보호되는 기기별 특정 기밀에는 Face ID 및 Touch ID 데이터가 포함됩니다. Mac에서는 AES 엔진에 연결된 전체 내부 저장 공간만 이 수준의 암호화를 받습니다. 예를 들어, USB로 연결된 외장 저장 장치나 Mac Pro(2019년)에 추가된 PCIe 기반 저장 공간은 이러한 방식으로 암호화되지 않습니다.

또한 Secure Enclave에는 지정된 SoC를 사용하는 모든 기기에서 공동으로 사용하는 기기 GID(그룹 ID)를 지닙니다 (예 : Apple A15 SoC를 사용하는 모든 기기는 동일한 GID를 공유).

또한 UID와 GID는 JTAG(Joint Test Action Group) 또는 다른 디버그 인터페이스를 통해서는 사용할 수 없습니다.

Secure Enclave AES 엔진

Secure Enclave AES 엔진은 AES 암호에 기반한 대칭 암호화를 수행하는 데 사용되는 하드웨어 블록입니다. AES 엔진은 타이밍 및 정적 전력 분석(SPA)을 사용하여 정보 유출을 방지하도록 설계되어 있습니다. A9 SoC부터, AES 엔진에 동적 전력 분석(DPA) 대응책도 포함됩니다.

AES 엔진은 하드웨어 및 소프트웨어 키를 지원합니다. 하드웨어 키는 Secure Enclave의 UID 또는 GID에서 파생됩니다. 이러한 키는 AES 엔진 내에 있으며 sepOS 소프트웨어에서도 보이지 않도록 설계되었습니다. 소프트웨어는 하드웨어 키로 암호화 및 암호화 해제 작업을 요청할 수 있지만 키를 추출할 수는 없습니다.

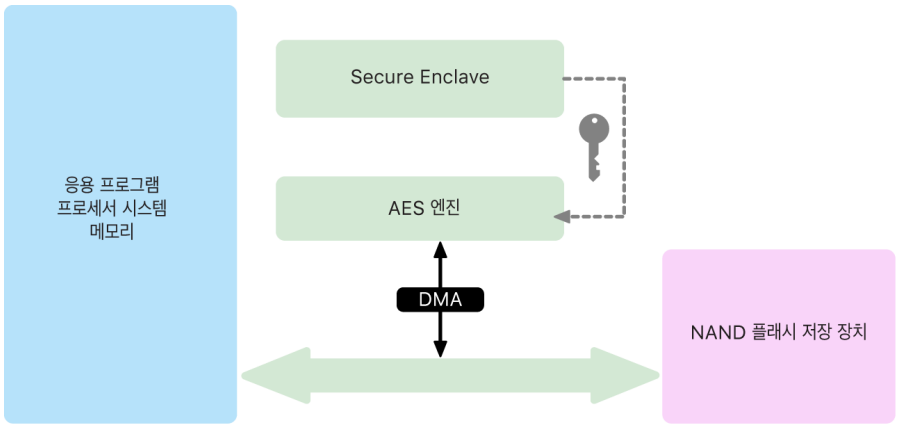
Apple A10 이상 SoC에서 AES 엔진은 UID 또는 GID에서 파생된 키를 다양화하는 잠금식 시드 비트를 포함합니다. 이를 통해 기기 작동 모드에 따라 데이터 접근이 조정되도록 할 수 있습니다. 예를 들어 잠금식 시드 비트는 DFU(기기 펌웨어 업데이트) 모드에서 시동할 때 암호로 보호된 데이터에 대한 접근을 거부하는 데 사용됩니다. 자세한 내용은 암호를 참조하십시오.

AES 엔진

Secure Enclave를 사용하는 모든 Apple 기기에는 전용 AES256 암호화 엔진('AES 엔진')이 NAND(비휘발성) 플래시 저장 장치와 메인 시스템 메모리 사이의 DMA(직접 메모리 접근) 경로에 내장되어 있어 매우 효율적인 파일 암호화를 가능하게 합니다. A9 또는 이상 버전의 A 시리즈 프로세서에서 플래시 저장 장치 보조 시스템은 분리된 버스에 위치해 있으며, 이 버스는 DMA 암호화 엔진을 통해 사용자 데이터가 포함되어 있는 메모리에만 접근할 수 있습니다.

시동 시 sepOS는 TRNG를 사용하여 임시 래핑 키를 생성합니다. Secure Enclave는 전용 와이어를 통해 이 키를 AES 엔진으로 전송하여 Secure Enclave 외부의 모든 소프트웨어에서 접근하는 것을 방지합니다. 그러면 sepOS는 임시 래핑 키를 통해 응용 프로그램 프로세서 파일 시스템 드라이버에서 사용할 파일 키를 래핑할 수 있습니다. 파일 시스템 드라이버가 파일을 읽거나 쓸 때, 래핑된 키를 AES 엔진으로 전송하여 키를 래핑 해제합니다. AES 엔진은 래핑되지 않은 키를 소프트웨어에 노출하지 않습니다.

참고: AES 엔진은 Secure Enclave 및 Secure Enclave AES 엔진과는 별개의 구성 요소이지만 그 작동은 아래와 같이 Secure Enclave와 밀접하게 연결되어 있습니다.



공개 키 액셀러레이터

PKA(공개 키 액셀러레이터)는 비대칭형 암호화 작업을 수행하는 데 사용되는 하드웨어 블록입니다. PKA는 RSA 및 ECC(Elliptic Curve 암호화) 서명 및 암호화 알고리즘을 지원합니다. PKA는 타이밍, SPA 및 DPA와 같은 사이드 채널 공격을 통한 정보 유출을 방지하도록 설계되었습니다.

PKA는 소프트웨어 및 하드웨어 키를 지원합니다. 하드웨어 키는 Secure Enclave의 UID 또는 GID에서 파생됩니다. 이러한 키는 PKA 내에 있으며, sepOS 소프트웨어에서도 보이지 않도록 설계되었습니다.

A13 SoC부터, PKA 암호화 구현은 공식 검증 기법을 활용하여 수학적으로 정확하다는 사실이 입증되었습니다.

Apple A10 및 이후에 출시된 SoC에서 PKA는 SKP(봉인 키 보호)라고 하는 OS 바운드 키를 지원합니다. 이러한 키는 기기의 UID와 기기에서 실행 중인 sepOS 해시의 조합을 사용하여 생성됩니다. 해시는 Secure Enclave Boot ROM 또는 Apple A13 및 이후에 출시된 SoC의 Secure Enclave 시동 모니터에 의해 제공됩니다. 이러한 키는 특정 Apple 서비스에 요청할 때 sepOS 버전을 확인하는 데에도 사용되며, 사용자 인증 없이 시스템에 중요한 변경이 있을 경우 키 재료에 대한 접근을 방지하여 암호로 보호된 데이터의 보안을 향상시키는 데에도 사용됩니다.

비휘발성 보안 저장 장치

Secure Enclave에는 전용 비휘발성 보안 저장 장치가 탑재되어 있습니다. 비휘발성 보안 저장 장치는 전용 I2C 버스를 사용하여 Secure Enclave에 연결되므로, Secure Enclave에서만 접근할 수 있습니다. 모든 사용자 데이터 암호화 키는 Secure Enclave의 비휘발성 저장 장치에 저장된 엔트로피에 뿌리를 두고 있습니다.

A12, S4 및 이후에 출시된 SoC를 사용하는 기기의 경우, Secure Enclave가 엔트로피 저장 장치의 보안 저장 장치 구성 요소와 연결됩니다. 보안 저장 장치 구성 요소는 변경이 불가능한 ROM 코드, 하드웨어 무작위 번호 발생기, 기기별 고유 암호화 키, 암호화 엔진 및 물리적 변형 감지 기능을 사용하여 자체 설계되었습니다. Secure Enclave 및 보안 저장 장치 구성 요소는 엔트로피에 대한 단독 접근을 제공하는 암호화되고 인증된 프로토콜을 사용하여 통신합니다.

2020년 가을 이후 처음 출시된 기기에는 2세대 보안 저장 장치 구성 요소가 탑재되어 있습니다. 2세대 보안 저장 장치 구성 요소는 카운터 록박스를 추가합니다. 각 카운터 록박스는 128비트 솔트, 128비트 암호 검증자, 8비트 카운터 및 8비트 최대 시도 값을 저장합니다. 카운터 록박스로의 접근은 암호화되고 인증된 프로토콜을 통해 이루어집니다.

카운터 록박스는 암호로 보호된 사용자 데이터를 잠금 해제하는 데 필요한 엔트로피를 보관합니다. 사용자 데이터에 접근하려면 페어링된 Secure Enclave가 사용자의 암호와 Secure Enclave의 UID에서 올바른 암호 엔트로피 값을 추출해야 합니다. 페어링된 Secure Enclave 이외의 소스에서 전송된 잠금 해제 시도를 사용하여 사용자의 암호를 학습할 수 없습니다. 암호 입력 시도 횟수 제한을 초과한 경우(예: iPhone에서 10회), 암호로 보호된 데이터는 보안 저장 장치 구성 요소에 의해 완전히 지워집니다.

Secure Enclave는 카운터 록박스를 생성하기 위해 보안 저장 장치 구성 요소에 암호 엔트로피 값 및 최대 시도 값을 전송합니다. 보안 저장 장치 구성 요소는 난수 발생기를 사용하여 솔트 값을 생성합니다. 그런 다음 제공된 암호 엔트로피, 보안 저장 장치 구성 요소의 고유한 암호화 키 및 솔트 값으로부터 암호 검증자 값과 록박스 엔트로피 값을 파생합니다. 보안 저장 장치 구성 요소는 0의 카운트, 제공된 최대 시도 값, 파생된 암호 검증자 값 및 솔트 값으로 카운터 록박스를 초기화합니다. 그런 다음 보안 저장 장치 구성 요소는 생성된 록박스 엔트로피 값을 Secure Enclave로 반환합니다.

나중에 카운터 록박스에서 록박스 엔트로피 값을 검색하기 위해 Secure Enclave가 보안 저장 장치 구성 요소에 암호 엔트로피를 보냅니다. 보안 저장 장치 구성 요소는 우선 록박스의 카운터를 증가시킵니다. 증가된 카운터가 최대 시도 값을 초과하면 보안 저장 장치 구성 요소가 카운터 록박스를 완전히 지웁니다. 최대 시도 수에 도달하지 않은 경우, 보안 저장 장치 구성 요소는 카운터 록박스를 만드는 데 사용된 것과 동일한 알고리즘을 사용하여 암호 검증자 값과 록박스 엔트로피 값을 파생하려고 시도합니다. 파생된 암호 검증자 값이 저장된 암호 검증자 값과 일치하는 경우, 보안 저장 장치 구성 요소는 록박스 엔트로피 값을 Secure Enclave로 반환하고 카운터를 0으로 재설정합니다.

암호로 보호된 데이터에 접근하는 데 사용되는 키는 카운터 록박스에 저장된 엔트로피에 있습니다. 자세한 내용은 데이터 보호 개요를 참조하십시오.

비휘발성 보안 저장 장치는 Secure Enclave의 재전송 방지 서비스를 위해 사용됩니다. Secure Enclave의 재전송 방지 서비스는 재전송 방지 경계를 표시하는 이벤트를 통해 데이터를 폐기하는 데 사용됩니다. 이는 다음을 포함하지만 이에 국한되지는 않습니다.

- 암호 변경
- Face ID 또는 Touch ID 활성화 또는 비활성화
- Face ID 얼굴 또는 Touch ID 지문 추가 또는 삭제
- Face ID 또는 Touch ID 재설정
- Apple Pay 카드 추가 또는 삭제
- 모든 콘텐츠 및 설정 지우기

보안 저장 장치 구성 요소가 없는 아키텍처에서는 EEPROM(전기적으로 지울 수 있는 프로그래밍 가능 읽기 전용 메모리)을 활용하여 Secure Enclave에 보안 저장 장치 서비스를 제공합니다. 보안 저장 장치 구성 요소와 마찬가지로 EEPROM은 Secure Enclave에서만 연결 및 접근할 수 있지만 전용 하드웨어 보안 기능을 포함하지 않으며, 엔트로피(물리적 연결에서 벗어난) 또는 카운터 록박스 기능에 대한 독점 접근을 보장하지 않습니다.

보안 뉴럴 엔진

Face ID(Touch ID 제외)를 지원하는 기기에서 보안 뉴럴 엔진은 2D 이미지와 심도 맵을 사용자 얼굴의 수학적 표현으로 변환합니다.

A11부터 A13 SoC에서 보안 뉴럴 엔진은 Secure Enclave에 통합됩니다. 보안 뉴럴 엔진은 DMA(직접 메모리 접근)를 사용하여 뛰어난 성능을 제공합니다. sepOS 커널의 통제하에 IOMMU(입력/출력 메모리 관리 유닛)는 직접 접근을 인증된 메모리 영역으로 제한합니다.

A14 및 M1 제품군부터, 보안 뉴럴 엔진은 응용 프로그램 프로세서의 뉴럴 엔진에 보안 모드로 구현되었습니다. 전용 하드웨어 보안 컨트롤러가 응용 프로그램 프로세서와 Secure Enclave 작업 간을 전환하며, 전환할 때마다 뉴럴 엔진 상태를 재설정하여 Face ID 데이터를 안전하게 보호합니다. 전용 엔진에서 메모리 암호화, 인증 및 접근 제어를 적용하며, 동시에 별도의 암호화 키와 메모리 범위를 사용하여 보안 뉴럴 엔진을 인증된 메모리 영역으로 제한합니다.

전원 및 클럭 모니터

모든 전자 기기는 제한된 전압 및 주파수 포락선 내에서 작동하도록 설계됩니다. 이 범위 밖에서 작동하면 전자 장치가 오작동할 수 있으며 보안 제어를 우회할 수 있습니다. Secure Enclave는 모니터링 회로가 있는 설계를 통해 전압과 주파수가 안전한 범위 내에 유지되도록 보장합니다. 이러한 모니터링 회로는 나머지 Secure Enclave보다 훨씬 폭넓은 작동 포락선을 갖추도록 설계되었습니다. 모니터에서 불법적인 작동점을 감지하면 Secure Enclave의 클럭은 자동으로 작동을 중단하며, 다음번에 SoC가 재설정되고 나서야 재시동됩니다.

Secure Enclave 기능 요약

참고: 2020년 가을에 처음 출시된 A12, A13, S4 및 S5 제품에는 2세대 보안 저장 장치 구성 요소가 있는 반면, SoC를 기반으로 하는 이전 제품에는 1세대 보안 저장 장치 구성 요소가 있습니다.

SoC	메모리 보호 엔진	보안 저장 장치	AES 엔진	PKA
A8	암호화 및 인증	EEPROM	있음	없음
A9	암호화 및 인증	EEPROM	DPA 보호	있음
A10	암호화 및 인증	EEPROM	DPA 보호 및 잠금식 시드 비트	OS 바운드 키
A11	암호화, 인증 및 재전송 방지	EEPROM	DPA 보호 및 잠금식 시드 비트	OS 바운드 키
A12(2020년 가을 전 출시된 Apple 기기)	암호화, 인증 및 재전송 방지	보안 저장 장치 구성 요소 1세대	DPA 보호 및 잠금식 시드 비트	OS 바운드 키
A12(2020년 가을 후 출시된 Apple 기기)	암호화, 인증 및 재전송 방지	보안 저장 장치 구성 요소 2세대	DPA 보호 및 잠금식 시드 비트	OS 바운드 키
A13(2020년 가을 전 출시된 Apple 기기)	암호화, 인증 및 재전송 방지	보안 저장 장치 구성 요소 1세대	DPA 보호 및 잠금식 시드 비트	OS 바운드 키 및 시동 모니터
A13(2020년 가을 후 출시된 Apple 기기)	암호화, 인증 및 재전송 방지	보안 저장 장치 구성 요소 2세대	DPA 보호 및 잠금식 시드 비트	OS 바운드 키 및 시동 모니터
A14–A17	암호화, 인증 및 재전송 방지	보안 저장 장치 구성 요소 2세대	DPA 보호 및 잠금식 시드 비트	OS 바운드 키 및 시동 모니터
S3	암호화 및 인증	EEPROM	DPA 보호 및 잠금식 시드 비트	있음
S4	암호화, 인증 및 재전송 방지	보안 저장 장치 구성 요소 1세대	DPA 보호 및 잠금식 시드 비트	OS 바운드 키
S5(2020년 가을 전 출시된 Apple 기기)	암호화, 인증 및 재전송 방지	보안 저장 장치 구성 요소 1세대	DPA 보호 및 잠금식 시드 비트	OS 바운드 키
S5(2020년 가을 후 출시된 Apple 기기)	암호화, 인증 및 재전송 방지	보안 저장 장치 구성 요소 2세대	DPA 보호 및 잠금식 시드 비트	OS 바운드 키
S6–S9	암호화, 인증 및 재전송 방지	보안 저장 장치 구성 요소 2세대	DPA 보호 및 잠금식 시드 비트	OS 바운드 키
T2	암호화 및 인증	EEPROM	DPA 보호 및 잠금식 시드 비트	OS 바운드 키
M1, M2, M3	암호화, 인증 및 재전송 방지	보안 저장 장치 구성 요소 2세대	DPA 보호 및 잠금식 시드 비트	OS 바운드 키 및 시동 모니터

Face ID 및 Touch ID

Face ID 및 Touch ID 보안

암호는 Apple 기기의 보안에 중추적인 역할을 하지만, 동시에 사용자는 하루에 수백 번 이상 기기에 편리하게 접근할 수 있기를 원합니다. 생체 인증을 사용하면 복잡한 암호만큼 강력한 보안을 유지할 수 있으며, 수동으로 암호를 입력하지 않아도 되기 때문에 오히려 더욱 안전한 동시에 손가락을 대고 있거나 기기를 보기만 해도 빠르게 잠금을 해제할 수 있어 편리합니다. Face ID 및 Touch ID는 암호를 대신하지 않지만, 대부분의 상황에서 빠르고 편리한 접근을 도와줍니다.

Apple의 생체 인증 보안 아키텍처는 생체 인증 센서 및 Secure Enclave 간의 엄격한 역할 구분 및 보안 연결에 의존합니다. 생체 인증 센서는 생체 인증 이미지를 캡처하고 안전하게 Secure Enclave로 전송합니다. 등록하는 동안 Secure Enclave는 해당 Face ID 및 Touch ID 템플릿 데이터를 처리, 암호화 및 저장합니다. 인식하는 동안 Secure Enclave는 생체 인증 센서에서 수신하는 데이터를 저장된 템플릿과 비교하여 기기를 잠금 해제할지 결정하거나 인식한 데이터가 일치하는지 응답합니다(Apple Pay, 앱 내 및 기타 Face ID 및 Touch ID 사용처). 생체 인증 보안 아키텍처는 iPhone, iPad 및 다양한 Mac 컴퓨터와 같이 생체 인증 센서 및 Secure Enclave 모두를 포함하는 기기를 지원하며 물리적으로 생체 인증 센서를 주변기기로 분리하고 Apple Silicon이 탑재된 Mac의 Secure Enclave와 안전하게 페어링하는 기능도 지원합니다.

Face ID 보안

Face ID를 통해 지원되는 Apple 기기를 주시하기만 하면 안전하게 잠금을 해제할 수 있습니다. Face ID는 고급 기술을 사용하는 TrueDepth 카메라 시스템을 통해 활성화되는 직관적이고 안전한 인증 방식을 제공하여, 사용자 얼굴의 기하학적 구조를 정확히 매핑합니다. Face ID는 신경망을 통해 화면 주시 여부, 사용자 일치 여부, 스푸핑 방지 여부를 확인하므로, 지원되는 기기를 마스크를 쓴 상태로 사용하더라도 사용자는 휴대폰을 보는 것만으로 잠금을 해제할 수 있습니다. Face ID는 사용자의 외모 변화에 자동으로 적응하며 사용자의 생체 데이터 보안 및 개인정보를 안전하게 보호합니다.

Face ID는 사용자가 카메라를 주시하고 있는지 확인하도록 설계되었고, 오인식률이 낮은 강력한 인증 방식을 제공하며, 디지털 스푸핑 및 물리적 스푸핑을 줄입니다.

TrueDepth 카메라는 사용자가 Face ID를 지원하는 Apple 기기를 들어 올리거나 화면을 탭하여 깨울 때 자동으로 사용자의 얼굴을 인식하며, 해당 기기가 수신 알림을 표시하기 위해 인증을 시도하거나 Face ID 지원 앱에서 Face ID 인증을 요청하는 경우에도 자동으로 사용자의 얼굴을 인식합니다. 얼굴이 감지되면 Face ID는 사용자가 눈을 뜨고 있는지와 기기를 응시하는지를 감지하여 사용자가 카메라를 보고 있으며 잠금을 해제하려는 것인지 확인합니다. Face ID의 사용자 확인은 VoiceOver가 켜져 있는 경우 비활성화되며, 필요한 경우 개별적으로 비활성화할 수 있어 보다 나은 접근성을 제공합니다. 마스크를 쓴 상태로 Face ID를 사용할 경우, 항상 주시 감지가 필요합니다.

TrueDepth 카메라는 얼굴이 카메라를 응시하는 것을 확인한 다음, 수천 개의 적외선 점을 투사하고 인식하여 2D 적외선 이미지에 따라 얼굴의 심도 맵을 형성합니다. 이 데이터는 디지털 서명되고 Secure Enclave에 전송되는 연속된 2D 이미지 및 심도 맵을 생성하는 데 사용됩니다. TrueDepth 카메라는 디지털 및 물리적 스푸핑에 대응하기 위해 2D 이미지와 심도 맵 캡처 내용의 순서를 무작위로 지정하며, 기기별로 특정한 무작위 패턴을 투사합니다. Secure Enclave 내에서 보호되는 보안 뉴럴 엔진의 일부는 이 데이터를 변형시켜 수학적으로 표현해내어 등록된 얼굴 데이터와 비교합니다. 등록된 얼굴 데이터는 다양한 각도에서 캡처된 사용자 얼굴에 대한 수학적 표현 그 자체입니다.

Touch ID 보안

Touch ID는 더 빠르고 간편하게, 또한 안전하게 지원되는 Apple 기기에 접근할 수 있는 지문 인식 시스템입니다. Touch ID 기술은 모든 각도의 지문 데이터를 읽고 센서를 사용할 때마다 추가로 겹쳐지는 노드를 확인하여 지문 지도를 계속 확장시키는 방법으로 계속해서 사용자의 지문을 학습합니다.

Touch ID 센서가 탑재된 Apple 기기는 지문을 사용해 잠금을 해제할 수 있습니다. 기기를 시동하거나, 재시동하거나, 로그아웃(Mac의 경우)할 경우에는 아직 기기 암호나 사용자 암호가 사용되므로 Touch ID가 이들의 용도를 완전히 대체하지는 않습니다. 일부 앱에서 Touch ID를 기기 암호나 사용자 암호 대신 사용할 수도 있습니다(예: 메모 앱에서 암호로 보호되는 메모를 잠금 해제하거나, 키체인으로 보호되는 웹 사이트의 잠금을 해제하거나, 지원되는 앱 암호의 잠금을 해제하는 경우). 하지만 기기 암호 또는 사용자 암호는 일부 경우에 항상 요구됩니다(예: 기존의 기기 암호나 사용자 암호를 변경하거나, 기존에 등록된 지문을 제거하고 새로운 지문을 등록하는 경우).

손가락 접촉을 감지한 지문 센서는 고급 이미지 처리 배열을 동작시켜 손가락을 스캔하고, 스캔한 내용을 Secure Enclave로 전송합니다. 이 연결을 보호하는 데 사용되는 채널은 기기에 Secure Enclave와 함께 Touch ID 센서가 탑재되어 있는지 또는 각자 주변기기로 분리되어 있는지에 따라 다릅니다.

지문 스캔은 분석을 위해 벡터화되는 동시에 Secure Enclave의 암호화된 메모리에 임시로 저장되며, 분석이 끝난 뒤에는 폐기됩니다. 해당 분석 단계에서는 피하 융선 흐름 각도 매핑을 사용합니다. 이 기술은 사용자의 실제 지문을 복원하는 데 필요한 '손가락 상세 데이터'를 폐기하는 손실 프로세스입니다. 등록하는 동안 노드 지도는 암호화된 포맷으로 저장되며 신원 정보의 유출 없이 Secure Enclave에서만 이후의 인식용으로 비교하기 위해 템플릿 형식으로 읽습니다. 이 데이터는 절대 기기 밖으로 유출될 수 없습니다. Apple에 전송되지도 않으며, 기기 백업에 포함되지도 않습니다.

내장 Touch ID 채널 보안

Secure Enclave와 내장 Touch ID 센서 간의 통신은 SPI(직렬 주변기기 인터페이스) 버스를 통해 이루어집니다. 프로세서는 데이터를 Secure Enclave로 전달할 수는 있지만, 읽을 수는 없습니다. 제조 과정 중에 모든 Touch ID 센서와 그에 해당하는 Secure Enclave용으로 권한이 설정된 공유 키를 사용하여 양도받은 세션 키로 통신을 암호화 및 인증합니다. 모든 Touch ID 센서의 공유 키는 강력하고 무작위적이며 서로 다릅니다. 세션 키 교환은 통신하는 양측에서 제공하는 임의 키를 사용한 AES 키 래핑으로 이루어집니다. 임의 키는 세션 키를 설정하고 AES-CCM을 통해 인증 및 기밀성을 한꺼번에 제공하는 전송 암호화를 사용합니다.

Touch ID가 탑재된 Magic Keyboard

Touch ID가 탑재된 Magic Keyboard 및 Touch ID와 숫자 키패드가 탑재된 Magic Keyboard는 Apple Silicon이 탑재된 Mac에 사용할 수 있는 Touch ID 보안을 제공하는 외장 키보드입니다. Touch ID가 탑재된 Magic Keyboard는 생체 인증 센서의 역할을 수행하지만 생체 인증 템플릿을 저장하거나, 생체 인증 인식을 수행하거나 또는 보안 정책을 시행(예: 잠금 해제 없이 48시간이 지나면 암호를 입력해야 함)하지 않습니다. Touch ID가 탑재된 Magic Keyboard의 Touch ID 센서는 Mac의 Secure Enclave와 안전하게 페어링되어야 사용이 가능하며 Secure Enclave는 내장 Touch ID 센서의 경우처럼 등록 및 인식 작업을 수행하며 보안 정책을 시행하는 역할을 합니다. Mac과 함께 제공되는 Touch ID가 탑재된 Magic Keyboard의 경우 Apple에서 페어링 프로세스를 제조 과정에서 수행합니다. 필요한 경우 사용자가 페어링 작업을 수행할 수도 있습니다. Touch ID가 탑재된 Magic Keyboard는 한 번에 한 대의 Mac에만 안전하게 페어링될 수 있지만 Mac은 최대 5개의 Touch ID가 탑재된 Magic Keyboard와 보안 페어링을 유지할 수 있습니다.

Touch ID가 탑재된 Magic Keyboard 및 내장 Touch ID 센서는 서로 호환됩니다. Mac에 내장된 Touch ID 센서에 등록된 손가락을 Touch ID가 탑재된 Magic Keyboard에 가져다 대거나 그 반대의 경우에도 Mac의 Secure Enclave에서 손가락을 올바르게 인식합니다.

보안 페어링 및 Mac Secure Enclave와 Touch ID가 탑재된 Magic Keyboard 간의 통신을 위해 해당 키보드는 증명을 제공하는 PKA(공개 키 액셀러레이터) 하드웨어 블록과 필요한 암호화 프로세스를 수행하는 하드웨어 기반 키를 포함하고 있습니다.

보안 페어링

Touch ID가 탑재된 Magic Keyboard를 Touch ID 작업에 사용하려면 먼저 Mac과 안전하게 페어링해야 합니다. 페어링하려면 Mac의 Secure Enclave와 Touch ID가 탑재된 Magic Keyboard의 PKA 블록에서 신뢰하는 Apple CA가 루트인 공개 키를 교환하고 하드웨어 기반 증명 키 및 임시 ECDH를 사용하여 서로의 신원을 인증합니다. Mac에서 이 데이터는 Secure Enclave가 보호하며 Touch ID가 탑재된 Magic Keyboard에서는 PKA 블록이 보호합니다. 보안 페어링을 완료하면 Mac과 Touch ID가 탑재된 Magic Keyboard 간에 통신된 모든 Touch ID 데이터는 저장된 신원을 기반으로 NIST P-256 곡선을 사용하여, 키 길이가 256비트인 AES-GCM 및 임시 ECDH 키를 통해 암호화됩니다. 무선 모드에서의 키보드 사용에 관한 자세한 정보는 Bluetooth 보안을 참조하십시오.

페어링에 대한 보안 의사

새로운 지문을 등록하는 작업처럼 처음으로 Touch ID 작업을 수행하려면 사용자는 Mac과 Touch ID가 탑재된 Magic Keyboard를 사용하려는 의사를 물리적으로 확인해야 합니다. 물리적 의사는 사용자 인터페이스에서 표시하는 경우 Mac의 전원 버튼을 두 번 눌러 확인하거나 이전에 Mac에 등록되어 있던 지문을 올바르게 인식하는 것으로 확인할 수 있습니다. 자세한 내용은 Secure Enclave에 대한 보안 의사 및 연결를 참조하십시오.

Apple Pay 결제는 Touch ID를 인식하거나 또는 macOS 사용자 암호를 입력하고 Touch ID가 탑재된 Magic Keyboard의 Touch ID 버튼을 두 번 누르면 승인됩니다. 후자의 경우 사용자는 Touch ID를 인식하지 않고도 물리적 의사를 확인할 수 있습니다.

Touch ID가 탑재된 Magic Keyboard 채널 보안

Touch ID가 탑재된 Magic Keyboard의 Touch ID 센서와 페어링된 Mac의 Secure Enclave 간의 보안 통신 채널을 위해 다음과 같은 사항이 요구됩니다.

- Touch ID가 탑재된 Magic Keyboard의 PKA 블록 및 Secure Enclave 간의 보안 페어링(위 참조)
- Touch ID 센서가 탑재된 Magic Keyboard와 PKA 블록 간의 보안 채널

Touch ID 센서가 탑재된 Magic Keyboard와 PKA 블록 간의 보안 채널은 서로 간에 공유된 고유 키를 사용하여 제조 과정에서 구축합니다. (이는 Touch ID가 내장된 Mac 컴퓨터에서 Mac의 Secure Enclave와 내장 센서 간 보안 채널을 생성하기 위해 사용된 기술과 동일합니다.)

Face ID, Touch ID, 암호

Face ID 또는 Touch ID를 사용하려면 먼저 기기에서 잠금 해제에 사용할 암호를 설정해야 합니다. Face ID 또는 Touch ID가 일치하는 데이터를 감지하면 기기는 암호를 묻지 않고 잠금을 해제합니다. 이 기능으로 사용자는 길고 복잡한 암호를 자주 입력할 필요 없이 더 실용적으로 사용할 수 있습니다. Face ID 및 Touch ID는 암호를 대신하지는 않지만, 안전하고 빠르게 기기에 접근할 수 있도록 지원합니다. 강력한 암호는 iPhone, iPad, Mac 또는 Apple Watch가 해당 사용자의 데이터를 암호로 보호하는 방식의 토대가 되기 때문에 중요합니다.

기기에 암호가 필요한 경우

언제든지 Face ID 또는 Touch ID 대신 암호를 사용할 수 있지만, 생체 인증은 사용할 수 없는 경우가 있습니다. 보안에 민감한 다음과 같은 작업을 할 때에는 항상 암호를 입력해야 합니다.

- 소프트웨어 업데이트하기
- 기기 지우기
- 암호 설정 보기 또는 변경하기
- 구성 프로파일 설치하기
- Mac의 시스템 설정(macOS 13 이상)에서 개인정보 보호 및 보안 패널 잠금 해제하기
- Mac의 시스템 환경설정(macOS 12 또는 이전 버전)에서 보안 및 개인정보 보호 패널 잠금 해제하기
- Mac의 시스템 설정(macOS 13 이상)에서 사용자 및 그룹 패널 잠금 해제하기(FileVault가 켜진 경우)
- Mac의 시스템 환경설정(macOS 12 또는 이전 버전)에서 사용자 및 그룹 패널 잠금 해제하기(FileVault가 켜진 경우)

또한 기기가 다음 상태 중 하나인 경우 암호를 입력해야 합니다.

- 기기가 방금 켜졌거나 재시동된 경우.
- 사용자가 Mac 계정에서 로그아웃하거나 아직 로그인하지 않은 경우.
- 사용자가 48시간 이상 기기를 잠금 해제하지 않은 경우.
- 사용자가 156시간(6.5일) 동안 암호를 사용하여 기기를 잠금 해제하지 않았고, 4시간 동안 생체 인증을 사용하여 기기를 잠금 해제하지 않은 경우.
- 기기가 원격 잠금 명령을 받은 경우.
- 사용자가 볼륨 버튼 한쪽과 잠자기/깨우기 버튼을 동시에 2초 동안 길게 누른 다음 취소를 눌러 전원 종료나 긴급 구조 요청에서 빠져나온 경우.
- 생체 인증을 5회 실패한 경우(단, 편리한 사용을 위해 생체 인증에 실패한 횟수가 이보다 적더라도 기기에서 암호를 사용할 것을 제안할 수 있음).

iPhone에서 '마스크를 쓴 상태로 Face ID 사용'을 활성화할 경우, 사용자가 다음을 수행한 후 6.5시간 동안 사용할 수 있습니다.

- 마스크 착용 여부와 관계없이 성공적인 Face ID 일치
- 기기 암호 확인
- Apple Watch를 사용한 기기 잠금 해제

이 중 어떤 동작을 수행해도 6.5시간을 추가적으로 연장합니다.

iPhone이나 iPad에서 Face ID 또는 Touch ID가 활성화되어 있으면 잠자기/깨우기 버튼을 누르는 즉시 기기가 잠기며, 기기가 잠자기 상태에 진입할 때에도 잠깁니다. 기기를 깨울 때마다 Face ID 및 Touch ID는 일치하는 데이터(아니면 암호 입력 선택 가능)를 요구합니다.

전 세계 인구 중 무작위의 사람이 Face ID를 사용하여 사용자의 iPhone, iPad를 잠금 해제할 수 있는 확률은 마스크를 쓴 상태로 Face ID를 사용할 경우를 포함하여 1/1,000,000입니다. Touch ID가 탑재되거나 Magic Keyboard와 연결된 사용자의 iPhone, iPad, Mac 모델의 경우 1/50,000입니다. 지문 또는 얼굴을 여러 개 등록하면 이 확률이 높아집니다(지문을 5개 등록한 경우 1/10,000, 얼굴을 2개 등록한 경우 1/500,000). 보안을 강화하기 위해 Face ID 및 Touch ID 데이터 일치 시도에 다섯 번 실패하면 사용자 기기 또는 계정 접근 시 암호가 요구됩니다. 다음의 경우 Face ID가 오인식될 가능성이 높아집니다.

- 사용자와 닮은 형제나 자매, 쌍둥이
- 13세 미만의 어린이(뚜렷한 얼굴 특징이 완전히 발달되지 않았을 수 있기 때문)

이 두 상황에서 마스크를 쓴 상태로 Face ID를 사용할 경우, 오인식률이 더욱 높아집니다. 오인식이 우려된다면 Apple에서는 인증에 암호를 사용할 것을 권장합니다.

얼굴 인식 보안

얼굴 인식은 이를 목적으로 특수하게 훈련된 신경망을 사용한 Secure Enclave 내에서 수행됩니다. Apple은 참가자들의 사전 동의하에 수행된 연구에서 수집한 IR(적외선) 및 심도 이미지를 포함하여 십억 장이 넘는 이미지를 사용하여 얼굴 인식 신경망을 개발했습니다. Apple은 전 세계에서 온 참가자들과 작업하여 성별, 나이, 인종 및 기타 요소를 대표하는 그룹을 구성했습니다. 이 연구는 다양한 사용자들에게 높은 수준의 정확성을 제공하기 위해 확장되었습니다. Face ID는 모자, 스카프, 안경, 콘택트 렌즈 및 여러 선글라스 종류를 구분하도록 설계되었습니다. Face ID는 iPhone 12 및 이후 모델, 그리고 iOS 15.4 이상 버전의 iPhone 기기에서 마스크를 쓴 상태로 잠금 해제를 지원합니다. 나아가 실내와 실외, 심지어는 완전한 어둠 속에서도 인식하도록 설계되었습니다. 스푸핑을 발견하고 대응하도록 훈련된 추가 신경망은 사진이나 마스크로 사용자의 기기를 잠금 해제하려는 시도로부터 방어합니다. Face ID 데이터는 사용자 얼굴의 수학적 표현을 포함하여 암호화되어 있으며 Secure Enclave에만 이를 사용할 수 있습니다. 이 데이터는 절대 기기 밖으로 유출될 수 없습니다. Apple에 전송되지도 않으며, 기기 백업에 포함되지도 않습니다. 정상 작동 중에 다음의 Face ID 데이터가 저장되며, Secure Enclave용으로만 암호화됩니다.

- 등록하는 동안 산출된 사용자 얼굴의 수학적 표현
- Face ID에서 추후 얼굴 인식을 보완하는 데 유용할 것으로 판단한 경우, 잠금 해제를 시도하는 동안 산출된 사용자 얼굴의 수학적 표현

정상 작동 중 캡처된 얼굴 이미지는 저장되지 않으며, Face ID 등록 또는 등록된 Face ID 데이터와의 비교를 위한 수학적 표현이 산출된 후 즉시 폐기됩니다.

Face ID 인식률 개선

인식 성능을 향상하고, 자연스럽게 변해가는 사용자의 얼굴과 외모에 적응하기 위해 Face ID는 저장된 수학적 표현을 계속해서 보완합니다. 인식에 성공하면 Face ID는 새로 계산된 수학적 표현의 품질이 양호할 경우 이 데이터를 일정한 횟수만큼 인식에 사용한 다음 폐기할 수 있습니다. 반대로 Face ID가 얼굴 인식을 실패했지만 특정 기준값보다 인식 품질이 높고, 인식에 실패한 뒤 사용자가 즉시 암호를 입력한 경우 Face ID는 사용자 얼굴을 다시 캡처한 다음, 등록된 Face ID 데이터에 새로 산출된 수학적 표현을 보완합니다. 이 새로운 Face ID 데이터는 사용자가 얼굴 인식을 중단하거나 일정한 인식 횟수를 채우면 폐기되며, Face ID 재설정 옵션을 선택해도 폐기됩니다. 이러한 보완 작업은 오인식률은 최소화하면서 Face ID가 사용자의 헤어 스타일이나 메이크업이 크게 변화하더라도 사용자를 인식할 수 있도록 합니다.

Face ID 및 Touch ID의 용도

기기 또는 사용자 계정 잠금 해제

Face ID 또는 Touch ID가 비활성화된 상태에서 기기 또는 계정이 잠기게 되면 Secure Enclave에서 보관하던 최상위 클래스의 데이터 보호 키가 폐기됩니다. 해당 클래스에 있는 파일 및 키체인 항목은 사용자가 암호를 입력하여 기기 또는 계정을 잠금 해제해야만 접근할 수 있습니다.

하지만 Face ID 또는 Touch ID가 켜져 있는 경우에는 기기나 계정이 잠기더라도 해당 키가 폐기되지 않습니다. 대신에 Secure Enclave 내의 Face ID 또는 Touch ID 보조 시스템에 할당된 키가 해당 키를 래핑합니다. 사용자가 기기나 계정의 잠금을 해제하려 할 때 기기가 일치하는 데이터를 감지하면 데이터 보호 키를 래핑 해제하기 위한 키가 제공되며 기기 또는 계정이 잠금 해제됩니다. 이 프로세스는 데이터 보호와 Face ID 또는 Touch ID 보조 시스템의 조합을 통해 기기를 잠금 해제하기 때문에 더욱 안전합니다.

기기를 재시동하면 Face ID 또는 Touch ID가 기기나 계정의 잠금을 해제하는 데 필요한 키는 손실되고, 암호 입력을 요구하는 조건이 충족되면 Secure Enclave에서 폐기합니다.

Apple Pay를 통한 안전한 구매

또한, 사용자는 Face ID 또는 Touch ID를 Apple Pay와 함께 사용하여 매장, 앱, 웹에서 간편하고 안전하게 구매할 수 있습니다.

- **매장에서 Face ID 사용하기:** Face ID로 매장 내 결제를 승인하려면 먼저 측면 버튼을 이중 클릭하여 결제 의사를 밝혀야 합니다. 이러한 이중 클릭은 Secure Enclave에 직접 연결된 물리적인 제스처를 사용하여 사용자의 의사를 파악하며, 악의적인 과정으로 인한 위조를 막을 수 있습니다. 그런 다음 Face ID를 사용하여 인증한 다음 기기를 비접촉식 결제 리더기 가까이에 댑니다. Face ID로 인증하고 나서 재인증을 통해 다른 Apple Pay 결제 방법을 선택할 수 있으며, 이 경우 측면 버튼을 다시 이중 클릭할 필요는 없습니다.
- **앱 및 웹에서 Face ID 사용하기:** 앱 및 웹에서 결제하려면 측면 버튼을 이중 클릭하여 결제 의사를 표시한 다음, Face ID로 인증하여 결제를 승인합니다. 측면 버튼을 클릭한 후 60초 이내에 Apple Pay 거래가 완료되지 않으면, 측면 버튼을 다시 이중 클릭하여 결제 의사를 재확인해야 합니다.
- **Touch ID 사용하기:** Touch ID의 경우 사용자의 지문과 완벽하게 일치하도록 결합된 Touch ID 센서를 활성화하는 제스처를 통해 결제 의사를 확인합니다.

시스템 제공 API 사용

타사 앱은 시스템이 제공하는 API를 사용하여 사용자에게 Face ID, Touch ID 또는 암호로 인증하도록 요청할 수 있습니다. Touch ID를 지원하는 앱은 별다른 변경 사항 없이 Face ID를 자동으로 지원합니다. Face ID 또는 Touch ID를 사용할 때 해당 앱은 인증 성공 여부만을 전달받기 때문에 등록된 사용자의 Face ID, Touch ID 또는 데이터에 접근할 수 없습니다.

키체인 항목 보호

Face ID 또는 Touch ID를 통해 키체인 항목도 보호하여 데이터가 일치하거나 기기의 암호 또는 계정 암호가 입력된 경우에만 Secure Enclave에서 항목을 해제할 수 있습니다. 앱 개발자는 사용자에게 키체인 항목을 잠금 해제하기 위해 Touch ID, Face ID 또는 암호를 요구하기 전에 사용자가 암호를 설정했는지 확인하는 API를 보유하고 있습니다. 앱 개발자는 다음의 모든 작업을 수행할 수 있습니다.

- 인증 API 작업으로 앱 암호 또는 기기 암호만 확인하는 결과가 되지 않도록 요구할 수 있습니다. 작업 시 사용자 등록 여부를 쿼리하고, 보안에 민감한 앱에서 Face ID 또는 Touch ID를 보조 수단으로 사용하게 합니다.
- Face ID 또는 Touch ID로 보호될 수 있는 Secure Enclave 내부 ECC(Elliptic Curve 암호화) 키를 생성하고 사용할 수 있습니다. 해당 키를 사용한 작업은 사용을 승인받은 후에 Secure Enclave 내부에서 항상 이루어집니다.

구매 및 구매 승인

사용자가 Face ID 또는 Touch ID를 통해 iTunes Store, App Store, Apple Books 등에서 구매를 승인하도록 구성하면 Apple ID 암호를 입력할 필요가 없습니다. 구매가 이루어지면 Secure Enclave에서 생체 인증이 일어났는지 확인한 다음, 매장 요청을 서명하는 데 사용된 ECC 키를 해제합니다.

Secure Enclave에 대한 보안 의사 및 연결

보안 의사는 운영 체제 또는 응용 프로그램 프로세서와의 상호 작용 없이도 사용자의 의사를 확인하는 방법을 제공합니다. 연결 방식은 다음과 같은 기기에서 사용 가능한 물리적 버튼과 Secure Enclave와의 물리적 링크입니다.

- iPhone X 및 이후 모델
- Apple Watch Series 1 및 이후 모델
- iPad Pro(모든 모델)
- iPad Air(2020년)
- Apple Silicon이 탑재된 Mac 컴퓨터

이 링크를 통해 사용자는 자신의 의사를 확인하여 소프트웨어가 루트 권한으로 실행되는 경우나 커널이 스푸핑할 수 없는 경우에도 설계된 그대로 작업을 완료할 수 있습니다.

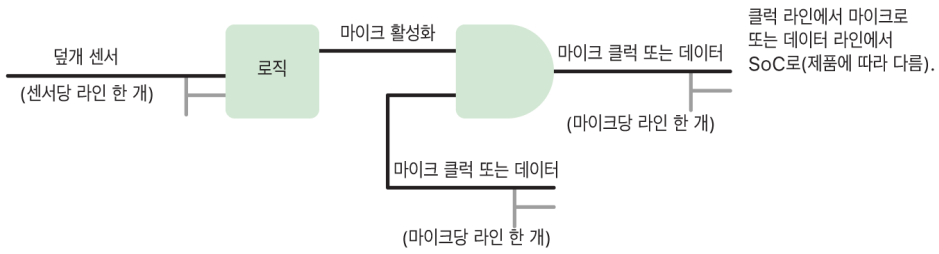
이 기능은 Apple Pay 결제 진행 중에 사용자 의사를 확인하는 데 사용되며 Touch ID가 탑재된 Magic Keyboard와 Apple Silicon이 탑재된 Mac 간의 페어링을 완료하는 데도 사용됩니다. 사용자 인터페이스에서 요청하는 경우 적절한 버튼(Face ID)을 두 번 누르거나 지문(Touch ID)을 스캔하면 사용자 의사를 확인하는 신호가 전송됩니다. 자세한 내용은 Apple Pay를 통한 안전한 구매를 참조하십시오. Apple T2 보안 칩이 탑재되어 있고 Touch Bar가 없는 MacBook 모델에서는 Secure Enclave 및 T2 펌웨어 기반의 유사한 매커니즘을 지원합니다.

하드웨어 마이크 연결 해제

Apple T2 보안 칩이 탑재된 Intel 기반 Mac 노트북 및 Apple Silicon 기반 Mac 노트북에는 덮개가 닫히면 항상 마이크를 비활성화하는 하드웨어 연결 해제 기능이 있습니다. T2 칩이 탑재된 모든 MacBook Pro 13 및 MacBook Air 13 노트북, T2 칩이 탑재된 모든 MacBook(2019년 및 이후 모델) 노트북, 그리고 Apple Silicon이 탑재된 Mac 노트북에서 이러한 연결 해제는 하드웨어만으로 구현됩니다. 이 연결 해제 기능은 덮개가 닫힌 상태에서 소프트웨어가 마이크에 연결되는 것을 방지하도록 설계되었으며, 이는 macOS에서 루트 또는 커널 권한이 있거나 소프트웨어가 T2 칩 또는 기타 펌웨어에서 구동되더라도 마찬가지입니다. (카메라는 하드웨어에서 분리되지 않는데, 이는 덮개를 닫으면 카메라 시야가 완전히 차단되기 때문입니다.)

2020년부터 iPad 모델에도 하드웨어 마이크 연결 해제 기능이 탑재되었습니다. MFi를 준수하는 케이스(Apple에서 판매하는 케이스 포함)가 iPad에 탑재되어 있고 덮개가 닫힌 상태인 경우 마이크가 하드웨어에서 연결 해제됩니다. 이는 iPadOS 또는 어떤 기기 펌웨어의 루트 권한 또는 커널 권한을 가지고 있더라도 소프트웨어에서 마이크 오디오 데이터를 사용하지 못하도록 하기 위한 것입니다.

이 섹션에서 보호는 다음 회로도에 따라 하드웨어 로직으로 직접 구현됩니다.



하드웨어 마이크 컷오프가 있는 각 제품에서 하나 이상의 덮개 센서가 상호 작용의 일부 물리적 성질(예: 홀 효과 센서 또는 힌지 앵글 센서)을 사용하여 덮개 또는 케이스가 물리적으로 닫히는 것을 감지합니다. 교정이 필요한 센서의 경우 기기 생산 과정에서 매개 변수가 설정되며, 교정 과정에는 센서의 민감한 매개 변수에 대한 후속 변경에 따른 비가역 하드웨어 잠금이 포함됩니다. 이러한 센서는 재프로그래밍이 불가능한 일련의 단순한 하드웨어 로직을 거치는 직접 하드웨어 신호를 발산합니다. 이 로직은 마이크 기능을 해제하기 전에 디바운스, 자기 이력 현상 및 최대 500ms의 지연을 제공합니다. 제품에 따라 마이크와 SoC(System on Chip) 간에 데이터를 전송하는 라인을 비활성화하거나 마이크 모듈을 활성화하는 입력 라인(예: 클럭 라인 또는 유사한 효과 제어) 중 하나를 비활성화하는 방법으로 신호를 구현할 수 있습니다.

여분의 전원으로 익스프레스 카드 사용

iPhone에 배터리 잔량이 부족하여 iOS가 실행 중이 아닌 경우에도 익스프레스 카드 거래를 위한 배터리 잔량이 남아 있을 수 있습니다. 지원되는 iPhone 기기는 다음 카드를 사용하여 자동으로 이 기능을 지원합니다.

- 익스프레스 승차 카드로 지정된 교통 카드 또는 지불
- 익스프레스 모드가 켜져 있는 접근 카드

측면 버튼을 누르면 배터리 아이콘에 전원이 부족함을 나타내고 익스프레스 카드를 사용할 수 있다는 텍스트가 표시됩니다. 거래가 햅틱 알림으로만 표시되는 것을 제외하고(겉으로 보이는 알림 없음) NFC 컨트롤러가 iOS가 실행 중일 때와 동일하게 익스프레스 카드 거래를 수행합니다. iPhone SE 2세대에서는 완료된 거래가 화면에 표시되는 데 몇 초가 소요될 수 있습니다. 이 기능은 표준 사용자가 전원을 끈 경우에는 사용할 수 없습니다.

시스템 보안

시스템 보안 개요

Apple 하드웨어의 고유한 기능을 토대로 시스템 보안은 사용성을 손상시키지 않고 Apple 기기의 시스템 리소스 접근을 제어합니다. 시스템 보안은 시동 프로세스, 소프트웨어 업데이트 및 컴퓨터 시스템 리소스(예:CPU, 메모리, 디스크, 소프트웨어 프로그램, 저장된 데이터) 보호를 포함합니다.

Apple 운영 체제는 최신 버전에 가까울수록 보안성이 강력합니다. Apple 보안에서는 시동 시 악성 코드 감염으로부터 시스템을 보호하는 **보안 시동**이 중요한 역할을 차지합니다. 보안 시동은 실리콘에서 시작하여 소프트웨어를 통해 신뢰 체인을 구축합니다. 각 단계는 제어 권한을 넘기기 전에 다음 단계가 제대로 작동하는지 확인합니다. 이 보안 모델은 Apple 기기의 기본 시동뿐만 아니라 Apple 기기에서 다양한 복구 및 시기적절한 업데이트 모드를 지원합니다. Secure Enclave와 같은 하위 구성 요소도 자체 보안 시동을 수행하여 Apple에서 확인된 코드만 시동하도록 합니다. 업데이트 시스템은 다운그레이드 공격을 방지하기 위해 설계되었기 때문에 공격자가 사용자 데이터를 도용하기 위한 방편으로 침해 방법을 파악하고 있는 이전 버전의 운영 체제로 기기를 되돌릴 수 없습니다.

또한, Apple 기기는 시동 및 런타임 보호 기능을 포함하고 있어서 계속 작동하는 중에도 무결성을 유지할 수 있습니다. iPhone, iPad, Apple Silicon이 탑재된 Mac, Apple Watch, Apple TV, 및 HomePod에서 Apple이 설계한 실리콘은 운영 체제 무결성을 보호하기 위한 공통 아키텍처를 제공합니다. 또한 macOS는 모든 Mac 하드웨어 플랫폼에서 지원되는 기능뿐만 아니라 다양한 컴퓨팅 모델을 지원하는 확장되고 구성 가능한 일련의 보호 기능을 제공합니다.

보안 시동

iPhone 및 iPad 기기용 시동 프로세스

시동 프로세스의 모든 단계에서는 무결성 확인 활성화를 위해 Apple이 암호화하여 서명한 구성요소가 포함됩니다. 또한 신뢰 체인을 확인한 이후에만 다음 단계를 진행할 수 있습니다. 신뢰 체인의 구성요소에는 부트로더, 커널, 커널 확장 프로그램 및 셀룰러 베이스밴드 펌웨어가 포함됩니다. 이러한 보안 시동 체인은 소프트웨어의 최하위 구조가 조작되지 않았는지 확인하도록 설계되었습니다.

iPhone 및 iPad 기기가 켜질 때 기기의 응용 프로그램 프로세서가 Boot ROM이라는 읽기 전용 메모리에 저장된 코드를 즉시 실행합니다. 이 변경 불가능 코드(**하드웨어 신뢰 루트**라고 함)는 칩 제조 단계에서 저장되어 절대적인 신뢰를 받습니다. 이 Boot ROM 코드에는 Apple 루트 CA(인증 기관) 공개 키가 포함되어 있으며, 이 키를 사용하여 iBoot 부트로더를 로드하기 전에 Apple이 서명했는지를 확인합니다. 위의 단계가 신뢰 체인의 첫 번째 단계로서 이와 같이 각 단계에서 다음 단계의 Apple 서명을 확인합니다. iBoot가 작업을 완료하면 iOS 또는 iPadOS 커널을 확인하고 실행합니다. A9 또는 이전 버전의 A 시리즈 프로세서를 사용하는 기기에서는 Boot ROM에서 저레벨 부트로더(LLB) 단계를 추가로 로드하고 확인한 다음 iBoot를 로드하고 확인합니다.

다음의 단계를 로드하거나 확인하는 데 실패하는 경우, 하드웨어에 따라 다르게 처리됩니다.

- **Boot ROM이 LLB를 로드할 수 없는 경우(이전 기기):** DFU(기기 펌웨어 업그레이드) 모드
- **LLB 또는 iBoot:** 복구 모드

둘 중 어떤 경우든 USB를 통해 기기를 Finder(macOS 10.15 이상) 또는 iTunes(macOS 10.14 또는 이전 버전)에 연결하여 초기 설정으로 복구해야 합니다.

BPR(Boot Progress Register)은 Secure Enclave에서 여러 가지 모드의 사용자 데이터에 접근을 제한하는 데 사용되며 다음 모드로 들어가기 전에 업데이트됩니다.

- **DFU 모드:** Apple A12 또는 이후에 출시된 SoC를 사용하는 기기는 Boot ROM을 통해 설정됨
- **복구 모드:** Apple A10, S2 또는 이후에 출시된 SoC를 사용하는 기기는 iBoot를 통해 설정됨

셀룰러 접속이 가능한 기기에서는 셀룰러 베이스밴드 하위 시스템이 서명된 소프트웨어 및 베이스밴드 프로세서에서 확인한 키로 추가적인 보안 시동을 수행합니다.

Secure Enclave는 또한 보안 시동을 수행하여 Apple이 해당 소프트웨어(sepOS)를 검증하고 서명했는지 확인합니다.

메모리 안전 iBoot 구현

iOS 14 및 iPadOS 14 이상에서 Apple은 보안을 향상하기 위해 iBoot 부트로더를 구축하는 데 사용되는 C 컴파일러 도구 체인에 변화를 주었습니다. 개선된 도구 체인은 코드를 구현하여 C 프로그램에서 일반적으로 발생하는 메모리 및 유형 안전성 문제를 방지합니다. 예를 들어, 다음 클래스에 있는 대부분의 취약점을 방지합니다.

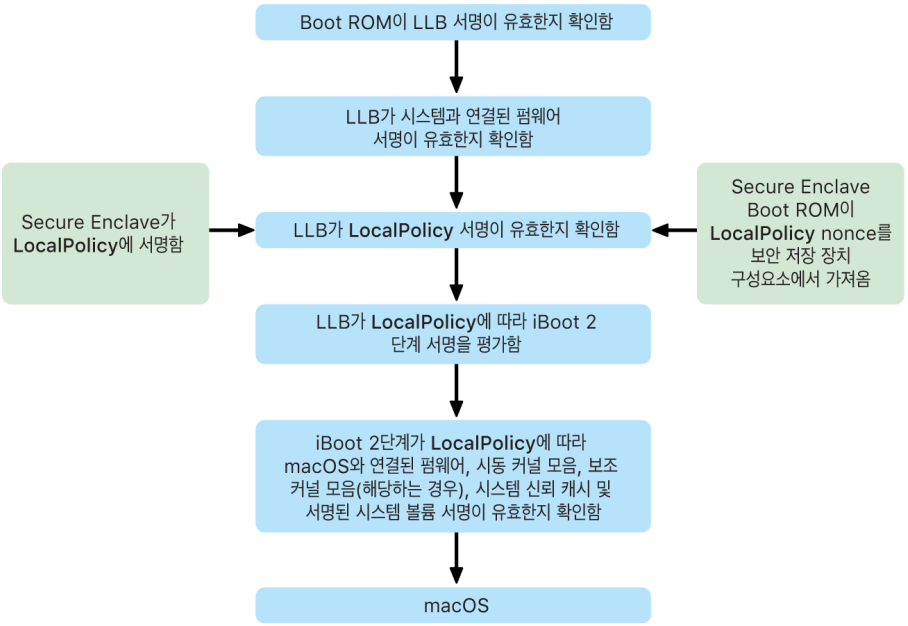
- 버퍼 오버플로: 모든 포인터가 메모리에 접근할 때 확인된 범위 정보를 전달하도록 보장하여 해결
- 히프 공격: 히프 데이터를 메타데이터에서 분리하고 더블 프리 오류와 같은 오류 조건을 정확하게 탐지하여 해결
- 유형 혼동: 포인터 캐스트 작업 도중 모든 포인터가 확인된 런타임 유형 정보를 전달하도록 보장하여 해결
- use-after-free 문제로 인한 유형 혼동: 정적 유형별로 모든 동적 메모리 할당을 분리하여 해결

이 기술은 A13 Bionic 칩 및 이후 모델이 탑재된 iPhone과 A14 Bionic 칩 및 이후 모델이 탑재된 iPad에서 지원됩니다.

Apple Silicon이 탑재된 Mac 컴퓨터

Apple Silicon이 탑재된 Mac의 시동 프로세스

Apple Silicon이 탑재된 Mac이 켜져 있으면 Mac은 iPhone 및 iPad와 매우 유사한 시동 프로세스를 수행합니다.



이 칩은 신뢰 체인의 첫 번째 단계에 Boot ROM에서 코드를 실행합니다. Apple Silicon이 탑재된 Mac의 macOS 보안 시동은 운영 체제 코드 자체뿐만 아니라 인증된 사용자가 구성한 보안 정책 및 KEXT(지원되지만 권장되지는 않음)도 확인합니다.

LLB(저레벨 부트로더를 의미함)가 실행되면 서명을 확인하고 저장 장치, 디스플레이, 시스템 관리, Thunderbolt 컨트롤러와 같은 내부 SoC 코어에 대한 시스템 페어링 펌웨어를 로드합니다. 또한 LLB는 Secure Enclave 프로세서가 서명한 파일인 LocalPolicy의 로드도 담당합니다. LocalPolicy 파일은 시스템 시동 및 런타임 보안 정책과 관련하여 사용자가 선택한 구성을 설명합니다. LocalPolicy는 다른 모든 시동 개체와 동일한 데이터 구조 형식을 띠지만, 소프트웨어 업데이트처럼 Apple 중앙 서버에서 서명되는 것이 아니라 특정 컴퓨터의 Secure Enclave 내에서만 지원되는 개인 키를 통해 로컬로 서명됩니다.

이전 LocalPolicy의 재전송을 방지하기 위해 LLB는 Secure Enclave에 연결된 보안 저장 장치 구성 요소에서 재전송 방지 값을 찾습니다. 이를 위해 Secure Enclave Boot ROM을 사용하며 LocalPolicy의 재전송 방지 값이 보안 저장 장치 구성 요소의 재전송 방지 값과 일치하는지 확인합니다. 이를 통해 보안 업그레이드 후 더 낮은 보안 수준으로 구성되었을 수 있던 이전 LocalPolicy가 시스템에 재적용되지 않도록 합니다. 그 결과 Apple Silicon이 탑재된 Mac의 보안 시동은 운영 체제 버전의 롤백뿐만 아니라 보안 정책의 다운그레이드로부터 보호하는 데 도움이 됩니다.

LocalPolicy 파일은 운영 체제가 완전 보안, 부분 보안 또는 최소 보안 중 어떤 모드로 구성될지를 결정합니다.

- **완전 보안:** 시스템은 iOS 및 iPadOS와 같이 작동하며, 설치 시 지원되는 가장 최신 소프트웨어의 시동만을 허용합니다.
- **부분 보안:** LLB는 운영 체제와 함께 제공되는 '전역' 서명을 신뢰하도록 지정됩니다. 이를 통해 시스템은 이전 macOS 버전을 실행할 수 있게 됩니다. 이전 macOS 버전은 불가피하게 패치되지 않은 취약성을 내포하며, 이 모드가 **부분 보안**으로 설명되는 것도 이와 같은 이유에서입니다. 이는 시동 KEXT(커널 확장 프로그램)를 지원하는 데 필요한 정책 수준이기도 합니다.
- **최소 보안:** iBoot 이상에 대해 전역 서명 확인을 사용한다는 점에서 시스템이 부분 보안처럼 작동하지만, 이 모드는 LocalPolicy에 서명하는 데 사용된 동일한 키로 Secure Enclave에서 서명하는 일부 시동 개체를 허용해야 함을 iBoot에 알립니다. 이 정책 수준은 사용자가 자신의 사용자 설정 XNU 커널을 빌드하고, 서명하고, 시동할 수 있도록 지원합니다.

선택한 운영 체제가 완전 보안에서 실행된다고 LocalPolicy가 LLB에 표시하면 LLB는 iBoot의 개인 맞춤화된 서명을 평가합니다. 부분 보안 또는 최소 보안에서 실행 중인 경우 전역 서명을 평가합니다. 서명 확인에 오류가 있으면 시스템이 복구용 OS로 시동되어 복구 옵션을 제공합니다.

LLB에서 iBoot로 전달되고 나면 보안 뉴럴 엔진, 항상 켬 프로세스용 펌웨어 및 기타 펌웨어처럼 macOS와 페어링된 펌웨어가 로드됩니다. iBoot는 LLB에서 넘겨받은 LocalPolicy 관련 정보도 확인합니다. LocalPolicy에서 AuxKC(보조 커널 모음)가 있어야 한다고 표시되면 iBoot는 파일 시스템에서 AuxKC를 찾아 LocalPolicy와 동일한 키로 Secure Enclave에서 서명했는지 확인하고 해당 해시가 LocalPolicy에 저장된 해시와 일치하는지 검증합니다. AuxKC가 확인되면 iBoot는 이를 시동 커널 모음의 메모리에 저장한 후, SCIP(시스템 보조 프로세서 무결성 보호)로 시동 커널 모음과 AuxKC를 아우르는 전체 메모리 영역을 잠급니다. 정책에 AuxKC가 있어야 하지만 찾을 수 없다고 표시되는 경우 시스템은 AuxKC 없이 계속 macOS로 시동됩니다. 또한 iBoot는 SSV(서명된 시스템 볼륨) 루트 해시를 확인하여 커널이 마운트할 파일 시스템의 전체 무결성이 검증되었는지 확인합니다.

Apple Silicon이 탑재된 Mac의 시동 모드

Apple Silicon이 탑재된 Mac에서는 아래에서 설명하는 시동 모드를 제공합니다.

모드	키 조합	설명
macOS	종료 상태에서 전원 버튼을 길게 눌렀다가 **놓으십시오**.	1. Boot ROM에서 LLB로 전달됩니다. 2. LLB 가 선택한 macOS에 대하여 시스템과 연결된 펌웨어 및 LocalPolicy를 로드합니다. 3. LLB가 macOS로 시동 중이라는 표시를 BPR(Boot Progress Register)에서 잠그고, iBoot로 전달합니다. 4. iBoot가 macOS와 연결된 펌웨어, 정적 신뢰 캐시, 기기 트리, 시동 커널 모음을 로드합니다. 5. LocalPolicy가 허용하는 경우 iBoot에서 타사 KEXT의 AuxKC(보조 커널 모음)를 로드합니다. 6. LocalPolicy가 이를 비활성화하지 않은 경우 iBoot는 서명된 시스템 볼륨의 루트 서명 해시를 확인합니다.
페어링된 복구용 OS	종료 상태에서 전원 버튼을 **길게** 누르십시오.	1. Boot ROM에서 LLB로 전달됩니다. 2. LLB가 시스템과 연결된 펌웨어와 복구용 OS에 대한 LocalPolicy를 로드합니다. 3. LLB가 페어링된 복구용 OS로 시동 중이라는 표시를 Boot Progress Register에서 잠그고, 페어링된 복구용 OS를 위해 iBoot로 전달합니다. 4. iBoot가 macOS와 연결된 펌웨어, 신뢰 캐시, 기기 트리, 시동 커널 모음을 로드합니다. 5. 페어링된 복구용 OS가 시동에 실패하면 폴백 복구용 OS로 시동을 시도합니다.
폴백 복구용 OS	종료 상태에서 전원 버튼을 **길게 두 번 누르십시오**.	1. Boot ROM에서 LLB로 전달됩니다. 2. LLB가 시스템과 연결된 펌웨어와 복구용 OS에 대한 LocalPolicy를 로드합니다. 3. LLB가 페어링된 복구용 OS로 시동 중이라는 표시를 Boot Progress Register에서 잠그고, 복구용 OS를 위해 iBoot로 전달합니다. 4. iBoot가 macOS와 연결된 펌웨어, 신뢰 캐시, 기기 트리, 시동 커널 모음을 로드합니다.
안전 모드	앞서 언급한 대로 복구용 OS로 시동되면 **Shift** 키를 누른 상태로 시동 볼륨을 선택합니다.	1. 앞서 언급한 대로 복구용 OS로 시동합니다. 2. Shift 키를 누른 상태로 볼륨을 선택하면 BootPicker 응용 프로그램이 평소와 같이 해당 macOS의 시동을 승인하는 동시에 iBoot에서 다음 시동 시 AuxKC를 로드하지 않도록 하는 `nvram` 변수를 설정합니다. 3. 시스템이 재시동되어 선택한 볼륨으로 시동되지만, iBoot는 AuxKC를 로드하지 않습니다.

페어링된 복구용 OS 제한 사항

macOS 12.0.1 이상에서, 모든 새로운 macOS는 설치될 경우 해당하는 APFS 볼륨 그룹에 페어링된 버전의 복구용 OS를 설치합니다. 이는 Intel 기반 Mac 컴퓨터 사용자에게 익숙하지만, Apple Silicon이 탑재된 Mac은 추가적인 보안 및 호환성 보증을 제공합니다. 이제 모든 macOS 설치에는 페어링된 지정 복구용 OS가 있어 페어링된 지정 복구용 OS만이 보안을 다운그레이드하는 작업을 수행하도록 합니다. 이를 통해 새로운 버전의 macOS 설치가 이전 버전의 macOS로 인해 변조를 일으키는 등의 문제를 방지합니다.

페어링 제한 사항은 다음과 같이 시행됩니다.

- 모든 macOS 11 설치는 복구용 OS에 페어링됩니다. 만약 macOS 11 설치가 기본값으로 시동하도록 선택되었을 경우, 복구용 OS는 Apple Silicon이 탑재된 Mac을 시동 시 전원 키를 길게 눌러 시동됩니다. 복구용 OS는 모든 macOS 11 설치의 보안 설정을 다운그레이드할 수 있지만, macOS 12.0.1 설치에서는 불가능합니다.
- macOS 12.0.1 이상 버전 설치가 기본값으로 시동하도록 선택되었을 경우, 페어링된 복구용 OS는 Mac 시동 시 전원 키를 길게 눌러 시동됩니다. 페어링된 복구용 OS는 모든 macOS 설치의 보안 설정을 다운그레이드할 수 있지만, 기타 macOS 설치에서는 불가능합니다.

모든 macOS 설치에서 페어링된 복구용 OS로 시동하려면, 시스템 설정에서 일반 > 시동 디스크를 사용하거나 (macOS 13 이상), 시스템 환경설정에서 시동 디스크를 사용하거나(macOS 12 또는 이전 버전) 복구용 OS를 시동한 다음 Option 키를 누른 상태로 볼륨을 선택하여 해당 설치를 기본값으로 선택해야 합니다.

참고: 폴백 복구용 OS는 macOS 설치에서 다운그레이드를 실행할 수 없습니다.

Apple Silicon이 탑재된 Mac의 시동 디스크 보안 정책 제어

개요

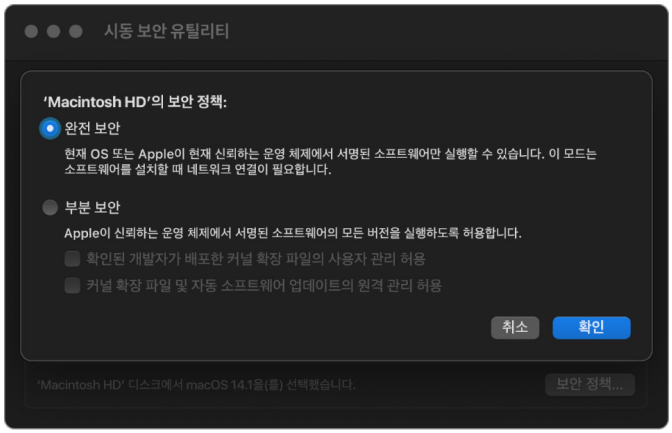
Intel 기반 Mac 컴퓨터의 보안 정책과 달리 Apple Silicon이 탑재된 Mac 컴퓨터의 보안 정책은 설치된 각 운영 체제에 대한 것입니다. 이는 버전과 보안 정책이 다른 여러 개의 설치된 macOS 인스턴스가 동일한 Mac에서 지원됨을 의미합니다. 이러한 이유로 **운영 체제 선택기**가 시동 보안 유틸리티에 추가되었습니다.

Apple Silicon이 탑재된 Mac에서 시스템 보안 유틸리티는 KEXT 시동 또는 SIP(시스템 무결성 보호) 구성과 같은 macOS 사용자 구성 보안의 전반적인 상태를 나타냅니다. 보안 설정 변경 시 보안이 크게 약화되거나 시스템이 쉽게 손상될 수 있는 경우, 변경을 하기 위해 사용자가 전원 버튼을 길게 눌러 복구용 OS에 진입해야 합니다(악성 소프트웨어는 신호를 발생시키지 못하고 물리적 접근 권한이 있는 사람만 가능). 이로 인해 Apple Silicon 기반 Mac도 펌웨어 암호를 요구(또는 지원)하지 않으며, 모든 주요 변경 사항은 이미 사용자 인증에 의해 게이트화됩니다. SIP에 대한 자세한 내용은 시스템 무결성 보호를 참조하십시오.

완전 보안 및 부분 보안은 복구용 OS에서 시동 보안 유틸리티를 사용하여 설정할 수 있습니다. 그러나 최소 보안의 경우 Mac의 보안이 급격히 약화되는 위험을 감수하는 사용자가 설정하도록 명령어 라인 도구에서만 접근 가능합니다.

완전 보안 정책

완전 보안은 기본 설정이며 iOS 및 iPadOS처럼 작동합니다. 소프트웨어가 다운로드되고 설치될 준비를 마쳤을 때 macOS는 소프트웨어와 함께 제공되는 전역 서명을 사용하는 대신 iOS 및 iPadOS에 사용되는 것과 동일한 Apple 서명 서버와 통신하여 새로운 '개인 맞춤화된' 서명을 요청합니다. 이러한 경우에 서명 요청의 일부로서 Apple CPU에 특정된 고유 ID인 ECID(Exclusive Chip Identification)가 포함된 서명이 개인 맞춤화됩니다. 서명 서버에서 돌려주는 해당 서명은 고유하며 특정 Apple CPU에서만 사용할 수 있습니다. 완전 보안 정책이 적용되면 Boot ROM 및 LLB는 지정된 서명이 Apple에서 서명했을 뿐 아니라 특정 Mac에 대해서도 서명되어 결국 해당 버전의 macOS를 해당하는 Mac에 연결하도록 보장합니다.

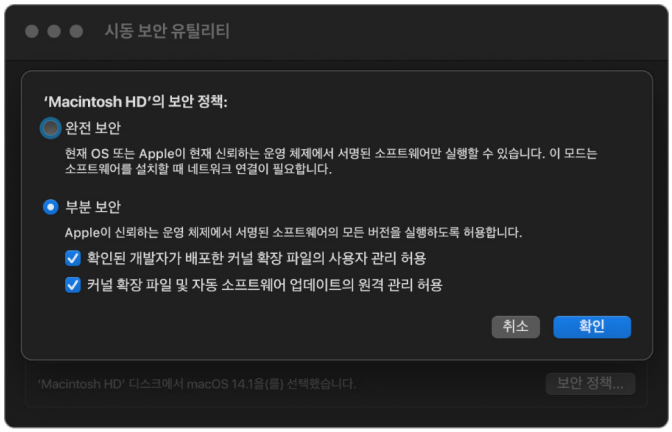


또한 온라인 서명 서버를 사용하면 롤백 공격에 대해 일반적인 전역 서명 방식보다 더 강력한 보호 기능이 제공됩니다. 전역 서명 시스템에서 보안 에포크는 여러 차례 롤링되었을 수 있지만 최신 펌웨어를 본 적 없는 시스템은 이에 대해 알 수 없습니다. 예를 들어, 현재 보안 에포크 1에 있다고 생각하는 컴퓨터는 실제로는 현재 보안 에포크가 5인 경우에도 보안 에포크 2의 소프트웨어를 허용합니다. Apple Silicon 온라인 서명 시스템에서 서명 서버는 최신 보안 에포크를 제외한 모든 보안 에포크의 소프트웨어에 대한 서명 생성을 거부할 수 있습니다.

또한, 보안 에포크를 변경하고 나서 공격자가 취약점을 발견하면 시스템 A의 이전 에포크에서 취약한 소프트웨어를 선택하여 시스템 B를 공격하는 데 적용할 수 없습니다. 이전 에포크에서의 취약한 소프트웨어가 시스템 A로 개인 맞춤화되었다는 점은 소프트웨어가 전송되어 시스템 B를 공격하는 데 사용되는 것을 방지합니다. 이러한 모든 메커니즘은 함께 작동하여 공격자가 최신 소프트웨어가 제공하는 보호 기능을 우회하기 위해 취약한 소프트웨어를 의도적으로 Mac에 배치할 수 없도록 합니다. 하지만 Mac 관리자의 사용자 이름과 암호를 알고 있는 사용자는 언제든지 사용 목적에 가장 적합한 보안 정책을 선택할 수 있습니다.

부분 보안 정책

부분 보안은 T2 칩이 탑재된 Intel 기반 Mac 컴퓨터의 중간 보안과 유사하게 동작하며, 여기서 공급업체(이 경우 Apple)는 코드의 디지털 서명을 생성하여 코드가 해당 공급업체에서 제공한 것임을 확고히 합니다. 이를 통해 공격자가 서명되지 않은 코드를 삽입하지 못하도록 방지합니다. 이 서명은 현재 부분 보안 정책이 설정되어 있는 Mac이면 모든 Mac에서 언제든지 사용할 수 있기 때문에, Apple에서는 이를 '전역' 서명이라고 부릅니다. 무단으로 운영 체제를 변경하여 사용자 데이터에 접근할 수 없게 되더라도 부분 보안 자체는 롤백 공격에 대한 보호 기능을 제공하지 않습니다. 자세한 내용은 Apple Silicon이 탑재된 Mac의 커널 확장 프로그램를 참조하십시오.

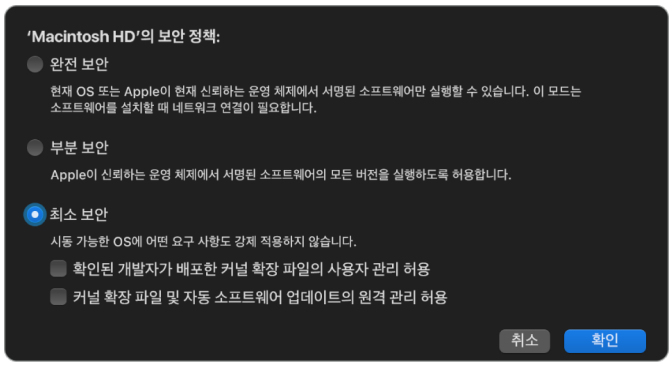


사용자가 이전 macOS 버전을 실행하도록 하는 것 외에도 부분 보안은 타사 KEXT(커널 확장 프로그램) 도입과 같이 사용자의 시스템 보안이 취약해지는 작업에 필요합니다. KEXT는 커널과 동일한 권한을 가지고 있어 타사 KEXT에 취약성이 있을 경우 운영 체제가 완전히 손상될 수 있습니다. 이런 이유로 추후 Apple Silicon이 탑재된 Mac 컴퓨터의 macOS에서 KEXT 지원이 제거되기 전에 개발자들이 시스템 확장 프로그램을 채택할 것을 강력히 권장합니다. 타사 KEXT를 활성화한 경우에도 요청 시 KEXT가 커널에 로드되지 않습니다. 그 대신 KEXT는 해시가 LocalPolicy에 저장되는 AuxKC(보조 커널 모음)로 병합되므로 재시동이 필요합니다. AuxKC 생성에 관한 자세한 내용은 macOS에서 안전하게 커널 확장하기를 참조하십시오.

최소 보안 정책

최소 보안은 Mac을 아주 불안정한 상태로 만드는 위험을 감수하는 사용자를 위한 모드입니다. 이 모드는 T2 칩이 탑재된 Intel 기반 Mac의 보안 없음 모드와는 다릅니다. 최소 보안에서 서명 확인은 여전히 전체 보안 시동 체인을 따라 수행됩니다. 단, 정책을 최소 보안으로 설정하면 사용자 설정된 XNU 커널에서 구축된 사용자 생성 시동 커널 모음처럼 로컬로 Secure Enclave 서명된 시동 개체를 허용해야 한다고 iBoot에 신호를 보냅니다. 이런 식으로 최소 보안은 임의의 '완전히 신뢰할 수 없는 운영 체제' 커널을 실행하는 아키텍처 기능을 제공합니다. 사용자 설정된 시동 커널 모음 또는 완전히 신뢰할 수 없는 운영 체제가 시스템에 로드된 경우 일부 암호화 키는 사용할 수 없게 됩니다. 이는 완전히 신뢰할 수 없는 운영 체제가 신뢰하는 운영 체제의 데이터에 접근하지 못하도록 하기 위한 것입니다.

중요사항: Apple은 사용자 설정 XNU 커널을 제공하거나 지원하지 않습니다.



최소 보안이 T2 칩이 탑재된 Intel 기반 Mac 컴퓨터의 보안 없음과는 다른 점이 또 있습니다. 바로 과거에 독립적으로 제어할 수 있었던 일부 보안 다운그레이드의 전제 조건이라는 점입니다. 특히 Apple Silicon이 탑재된 Mac에서 SIP(시스템 무결성 보호)를 비활성화하려면 시스템을 최소 보안으로 설정하고 있음을 사용자가 인식해야 합니다. 이는 SIP를 비활성화하면 시스템이 커널로 인해 훨씬 쉽게 손상될 수 있는 상태로 전환되기 때문입니다. 특히 Apple Silicon이 탑재된 Mac에서 SIP를 비활성화하면 AuxKC 생성 시간 동안 KEXT 서명 실행이 비활성화되므로, 커널 메모리에 임의의 KEXT가 로드될 수 있습니다. Apple Silicon이 탑재된 Mac에서는 정책 저장소가 NVRAM에서 LocalPolicy로 옮겨져 또다른 SIP 개선이 이루어졌습니다. 따라서 이제는 SIP를 비활성화하려는 경우 전원 버튼을 길게 누르면 실행되는 복구용 OS에서 LocalPolicy 서명 키에 접근할 수 있는 사용자의 인증이 필요합니다. 이를 통해 소프트웨어만 노리는 공격이 훨씬 어려워졌으며, 실제 공격자도 SIP를 비활성화하기가 상당히 까다로워졌습니다.

시동 보안 유틸리티 앱에서 최소 보안으로 다운그레이드할 수 없습니다. 사용자는 복구용 OS 터미널에서 `csrutil`(SIP 비활성화를 위한)과 같은 명령어 라인 도구를 실행해야만 다운그레이드할 수 있습니다. 사용자가 다운그레이드를 마치면 발생 사실이 시동 보안 유틸리티에 반영되고 사용자는 손쉽게 더 안전한 보안 모드로 설정할 수 있습니다.

참고: Apple Silicon이 탑재된 Mac은 기술적으로 모든 시동이 로컬에서 수행되기 때문에 특정 미디어 시동 정책을 요구하거나 지원하지 않습니다. 사용자가 외부 미디어에서 시동하기로 선택한 경우 먼저 복구용 OS에서 인증된 재시동을 사용하여 해당 운영 체제 버전을 개인 맞춤화해야 합니다. 이러한 재시동은 외부 미디어에 저장된 운영 체제에서 신뢰하는 시동을 수행하는 데 사용되는 내부 드라이브에 LocalPolicy 파일을 생성합니다. 즉, 외부 미디어에서 시동할 구성은 항상 운영 체제별로 명시적으로 활성화되고 이미 사용자 인증을 요구하므로 추가적인 보안 구성이 필요하지 않습니다.

LocalPolicy 서명 키 생성 및 관리

생성

제조 과정에서 macOS를 처음 설치하거나 테더링된 제거 및 설치가 수행된 경우, Mac은 임시 복원 RAM 디스크의 코드를 실행해 기본 상태로 복원합니다. 이 과정에서 복원 환경은 새로운 공개 키와 개인 키 한 쌍을 생성하며 이는 Secure Enclave에 보관됩니다. 해당 개인 키는 **OIK(소유자 신원 키)**라고 합니다. 이미 존재하는 OIK는 이 과정에서 제거됩니다. 복원 환경은 또한 활성화 잠금에 사용된 키인 **UIK(사용자 신원 키)**를 초기화합니다. 해당 과정 중 Apple Silicon이 탑재된 Mac에서 독특한 부분은 활성화 잠금에 UIK 인증서가 요구되는 경우로, LocalPolicy에서 필요한 일련의 제약이 검증 시 시행되는 것을 포함합니다. 기기에서 활성화 잠금에 UIK를 인증할 수 없는 경우(예: 기기가 현재 나의 Mac 찾기 계정에 연결되어 있고 분실한 것으로 알려짐), 로컬 정책 생성을 더 이상 진행할 수 없습니다. 기기가 **ucrt(사용자 신원 인증서)**를 발행한 경우, 해당 ucrt는 X.509 v3 확장 프로그램에서 서버에서 요구하는 정책 제약 및 사용자 요청 정책 제한을 포함합니다.

활성화 잠금/`ucrt`를 성공적으로 불러온 경우, 이는 서버 쪽의 데이터베이스에 저장되며 기기에도 반환됩니다. 기기에서 ucrt를 보유한 후에는 OIK에 대응하는 공개 키 인증 요청이 **BAA(기본 증명 인증 기관)** 서버로 전송됩니다. BAA는 BAA 접근 가능 데이터베이스에 저장된 ucrt의 공개 키를 사용하여 OIK 인증 요청을 확인합니다. BAA가 인증을 확인할 수 있는 경우 BAA가 서명하고 ucrt에 저장된 제약을 포함하는 **OIC(소유자 신원 인증서)**를 반환하며 공개 키를 인증합니다. 해당 OIC는 Secure Enclave로 다시 전송됩니다. 그때부터 Secure Enclave가 새로운 LocalPolicy에 서명할 때마다 Image4에 OIC를 연결합니다. LLB에는 BAA 루트 인증서에 대한 신뢰가 내장되어 있으며 이로 인해 OIC를 신뢰하고 전반적인 LocalPolicy 서명을 신뢰하게 됩니다.

RemotePolicy 제약

로컬 정책뿐 아니라 모든 Image4 파일은 Image4 매니페스트 평가에 제약이 있습니다. 이러한 제약은 리프 인증서의 OID(특수 개체 식별자)를 사용하여 인코딩됩니다. Image4 확인 보관함은 서명 평가 중 인증서에서 특수 인증서 제약 OID를 검색한 다음, 명시된 제약을 기계적으로 평가합니다. 제약의 형식은 다음과 같습니다.

- X는 반드시 존재함
- X는 반드시 존재하지 않음
- X는 반드시 특별한 값을 가짐

예를 들어, '개인 맞춤화된' 서명의 경우 인증서 제약에는 'ECID가 반드시 존재함'이 포함되며, '전역' 서명의 경우 'ECID가 반드시 존재하지 않음'이 포함됩니다. 이러한 제약은 주어진 키로 서명된 모든 Image4 파일이 특정 요건을 준수하여 잘못 서명된 Image4 매니페스트가 생성되지 않도록 합니다.

각 LocalPolicy의 측면에서는 Image4 인증서 제약을 **RemotePolicy**라고 합니다. 다른 시동 환경의 LocalPolicies에 다른 RemotePolicy가 존재할 수 있습니다. RemotePolicy는 복구용 OS LocalPolicy를 제한하는 데 사용되어 복구용 OS가 시동될 때 완전 보안을 사용하여 시동되는 것처럼만 동작하도록 할 수 있습니다. 이로 인해 정책을 변경할 수 있는 장소로서 복구용 OS 시동 환경의 무결성에 대한 신뢰도가 높아집니다. RemotePolicy는 LocalPolicy가 생성된 Mac의 ECID와 해당 Mac의 보안 저장 장치 구성 요소에 저장된 특정 Remote Policy nonce 해시(`rpnh`)를 포함하도록 제한합니다. `rpnh`, 즉 RemotePolicy는 나의 Mac 찾기 및 활성화 잠금에 등록, 등록 해제, 원격 잠금, 원격으로 지우기 등과 같은 작업이 수행될 경우에만 변경됩니다. Remote Policy 제약은 UIK(사용자 신원 키) 인증 시 확정되고 지정되며 발급된 ucrt(사용자 신원 인증서)로 로그인합니다. ECID, ChipID 및 BoardID와 같은 일부 Remote Policy 제약은 서버에서 결정합니다. 이는 한 기기에서 다른 기기에 대해 LocalPolicy 파일을 서명하는 것을 방지하기 위한 것입니다. 기기는 다른 Remote Policy 제약을 지정하여 현재 OIK 접근에 필요한 로컬 인증 및 기기가 활성화 잠금 상태인 계정의 원격 인증을 제공하지 않고도 로컬 정책의 보안 다운그레이드를 방지할 수 있습니다.

Apple Silicon이 탑재된 Mac용 LocalPolicy 파일의 콘텐츠

LocalPolicy는 Secure Enclave로 서명된 Image4 파일입니다. Image4는 ASN.1(Abstract Syntax Notation One) DER로 인코딩된 데이터 구조 형식이며, Apple 플랫폼에서 보안 시동 체인 개체 정보를 설명하는 데 사용됩니다. Image4 기반 보안 시동 모델에서 보안 정책은 Apple 중앙 서명 서버에 서명을 요청하여 실행된 소프트웨어 설치 시 요청됩니다. 정책에서 허용 가능한 경우 서명 서버는 서명된 Image4 파일을 반환하며, 여기에는 여러 가지 4CC(4자리 코드) 배열이 포함됩니다. Boot ROM 또는 LLB와 같은 소프트웨어는 시동 시 이렇게 서명된 Image4 파일 및 4CC를 평가합니다.

운영 체제 간 소유권 이전

OIK(소유자 신원 키) 접근을 '소유권'이라고 합니다. 소유권은 정책이나 소프트웨어 변경 후 사용자가 LocalPolicy에 재서명하는 데에 필요합니다. OIK는 SKP(봉인 키 보호)에서 설명된 것과 같은 키 계층으로 보호되며 이때 OIK는 VEK(볼륨 암호화 키)와 같은 KEK(키 암호화 키)로 보호됩니다. 이는 일반적으로 사용자 암호와 운영 체제 및 정책 측정으로 보호된다는 뜻입니다. Mac의 운영 체제에는 단 하나의 OIK가 있습니다. 그리하여 두 번째 운영 체제를 설치하는 경우 해당 운영 체제의 사용자에게 소유권을 이전하기 위해서는 첫 번째 운영 체제의 사용자로부터 명시적인 동의가 필요합니다. 하지만 설치 프로그램이 첫 번째 운영 체제를 통해 실행되는 동안 두 번째 운영 체제의 사용자는 아직 존재하지 않습니다. 해당 운영 체제가 시동되고 설정 지원이 실행되어야 운영 체제의 사용자가 생성됩니다. 그러므로 Apple Silicon이 탑재된 Mac에 두 번째 운영 체제를 설치할 때 두 가지의 새로운 작업이 필요합니다.

- 두 번째 운영 체제에 LocalPolicy 생성하기
- 소유권 이전을 위한 '사용자 설치' 준비하기

설치 지원을 실행하고 두 번째 여유 볼륨에 설치를 진행하면 메시지가 나타나 현재 볼륨의 사용자를 복제하여 두 번째 볼륨의 첫 번째 사용자로 지정할지 묻습니다. 사용자가 이를 수락하면 실제로는 KEK(선택된 사용자 암호 및 하드웨어 키에서 파생)에서 생성된 '사용자 설치'가 OIK를 암호화하는 데에 사용됩니다. 동시에 OIK는 두 번째 운영 체제로 전달됩니다. 그러면 두 번째 운영 체제의 설치 지원에서 사용자의 암호를 사용해 새로운 운영 체제의 Secure Enclave에 있는 OIK에 접근할지 묻는 메시지가 나타납니다. 사용자가 해당 사용자를 복제하지 않도록 선택해도 사용자 설치가 동일한 방법으로 생성되지만 사용자의 암호 대신 빈 암호가 사용됩니다. 이 두 번째 흐름은 특정 시스템 관리 시나리오를 위한 것입니다. 그러나 여러 볼륨에 설치를 하거나 가장 안전한 방법으로 소유권 이전을 수행하려는 사용자는 항상 첫 번째 운영 체제에서 두 번째 운영 체제로 사용자 복제하기를 선택해야 합니다.

Apple Silicon이 탑재된 Mac의 LocalPolicy

Apple Silicon이 탑재된 Mac 컴퓨터의 경우, 로컬 보안 정책 제어는 Secure Enclave에서 실행되는 응용 프로그램에 위임되어 왔습니다. 이 소프트웨어는 사용자의 자격 증명과 기본 CPU의 시동 모드를 활용하여 보안 정책을 변경할 수 있는 사용자와 시동 환경을 결정합니다. 이렇게 하면 악성 소프트웨어가 사용자에 대한 보안 정책 제어 권한을 다운그레이드하여 더 많은 권한을 얻지 못하도록 방지할 수 있습니다.

LocalPolicy 매니페스트 속성

LocalPolicy 파일에는 특정 Apple CHIP(칩)을 지칭하는 BORD(보드 또는 모델 ID) 또는 ECID(Exclusive Chip Identification) 같이 대부분의 Image4 파일에서 찾아볼 수 있는 일부 아키텍처 4CC가 포함됩니다. 단, 다음의 4CC에서는 사용자 구성이 가능한 보안 정책에만 초점을 맞춥니다.

참고: Apple은 **1TR(페어링 One True recoveryOS)** 용어를 사용하여 물리적 전원 버튼을 한 번 길게 눌러 실행되는 페어링된 복구용 OS로 시동할 수 있음을 나타냅니다. 이는 NVRAM을 사용하여 실행하거나, 두 번 길게 눌러 실행하거나, 시동 시 오류가 발생할 경우 시행되는 일반적인 복구용 OS 시동과는 다릅니다. 특정한 종류의 물리적 버튼을 누르면 macOS에 침입하는 소프트웨어 전용 공격자가 시동 환경에 접근할 수 없어져 신뢰도가 높아집니다.

lpnh(LocalPolicy nonce 해시)

- **유형:** OctetString(48)
- **변경 가능한 환경:** 1TR, 복구용 OS, macOS
- **설명:** `lpnh`는 LocalPolicy의 재전송 방지에 사용됩니다. 이 해시는 보안 저장 장치 구성 요소에 저장되는 LPN(LocalPolicy nonce)의 SHA384 해시이며, Secure Enclave Boot ROM 또는 Secure Enclave를 통해 접근할 수 있습니다. 원시 재전송 방지 값은 응용 프로그램 프로세서에 공개되지 않으며, sepOS에만 표시됩니다. LLB가 공격자가 캡처한 이전 LocalPolicy가 유효하다고 믿게 만들려면 공격자는 보안 저장 장치 구성 요소에 값을 넣어야 하며, 이 칩은 재전송하려는 LocalPolicy에 있는 `lpnh`값과 동일하게 해시되어야 합니다. 소프트웨어 업데이트 중 두 개가 동시에 유효한 경우를 제외하면 일반적으로 시스템에는 유효한 LPN이 하나 있어 업데이트 오류 발생 시 이전 소프트웨어를 다시 시동할 수 있습니다. 모든 운영 체제의 LocalPolicy가 변경되면 정책 전부가 보안 저장 장치 구성 요소에 있는 새로운 LPN에 해당하는 최신 **lpnh** 값으로 다시 서명됩니다. 이러한 변화는 사용자가 각각 새로운 LocalPolicy로 보안 설정을 변경하거나 최신 운영 체제를 생성하는 경우 일어납니다.

rpnh(RemotePolicy nonce 해시)

- **유형:** OctetString(48)
- **변경 가능한 환경:** 1TR, 복구용 OS, macOS
- **설명:** 이 `rpnh`는 `lpnh`와 같은 방식으로 동작하지만, 나의 찾기 등록 상태가 변경될 때처럼 RemotePolicy가 업데이트되어야만 업데이트됩니다. 이러한 변화는 사용자가 Mac에서 나의 찾기 상태를 변경하는 경우 일어납니다.

ronh(복구용 OS nonce 해시)

- **유형:** OctetString(48)
- **변경 가능한 환경:** 1TR, 복구용 OS, macOS
- **설명:** 이 `ronh`는 lpnh와 같은 방식으로 동작하지만, 시스템 복구용 OS의 LocalPolicy에서만 찾을 수 있습니다. 이 해시는 소프트웨어 업데이트 등 시스템 복구용 OS가 업데이트될 때 업데이트됩니다. `lpnh` 및 `rpnh`와는 별도의 재전송 방지 값이 사용되므로 나의 찾기를 통해 기기가 비활성화 상태가 되면 기존의 운영 체제는 비활성화되지만(보안 저장 장치 구성 요소에서 LPN 및 RPN 제거) 시스템 복구용 OS는 계속 시동 가능한 상태로 남습니다. 이러한 방법으로 소유자가 나의 찾기 계정에 사용되는 iCloud 암호를 넣음으로써 운영 체제 통제권을 증명하면 해당 운영 체제가 재활성화될 수 있습니다. 이러한 변화는 사용자가 시스템 복구용 OS를 업데이트하거나 새로운 운영 체제를 생성하는 경우 일어납니다.

nsih(다음 단계 Image4 매니페스트 해시)

- **유형:** OctetString(48)
- **변경 가능한 환경:** 1TR, 복구용 OS, macOS
- **설명: nsih** 필드는 시동된 macOS를 설명하는 Image4 매니페스트 데이터 구조의 SHA384 해시를 나타냅니다. macOS Image4 매니페스트는 iBoot, 정적 신뢰 캐시, 기기 트리, 시동 커널 모음, SSV(서명된 시스템 볼륨) 루트 해시 등 모든 시동 개체에 대한 측정값을 포함합니다. LLB가 지정된 macOS를 시동하도록 설정되면 iBoot에 연결된 macOS Image4 매니페스트 해시가 LocalPolicy의 `nsih` 필드에 캡처된 것과 일치됩니다. 이러한 방식으로 `nsih`는 직접 LocalPolicy를 생성한 운영 체제에 대한 사용자의 의도를 담아냅니다. 사용자는 소프트웨어 업데이트를 수행할 때 `nsih` 값을 절대적으로 변경하게 됩니다.

spih(Cryptex1 Image4 매니페스트 해시)

- **유형:** OctetString(48)
- **변경 가능한 환경:** 1TR, 복구용 OS, macOS
- **설명:** `spih` 필드는 Cryptex1 Image4 매니페스트 데이터 구조의 SHA384 해시를 나타냅니다. Cryptex1 Image4 매니페스트는 cryptex, 해당 파일 시스템 봉인 및 관련 신뢰 캐시의 측정값을 포함합니다. macOS를 시동하면 XNU 커널 및 페이지 보호 레이어에서 Cryptex1 Image4 매니페스트 해시가 LocalPolicy의 `spih` 필드에서 iBoot가 발급한 것과 일치하는지 확인합니다. 사용자는 신속 보안 대응을 설치하거나 소프트웨어 업데이트를 수행할 때 `spih` 값을 절대적으로 변경할 수 있습니다. Cryptex1 Image4 매니페스트 해시는 다음 단계 Image4 매니페스트 해시와 별도로 업데이트될 수 있습니다.

stng(Cryptex1 생성)

- **유형:** 64비트 부호 없는 정수
- **변경 가능한 환경:** 1TR, 복구용 OS, macOS
- **설명:** `stng` 필드는 Cryptex1 Image4 매니페스트 해시가 LocalPolicy에서 마지막으로 업데이트되었을 때 나타나는 카운터 값입니다. 페이지 보호 레이어가 Incoming Cryptex 적용을 위한 로컬 정책을 평가하는 동안 `lpnh` 대신 재전송 방지 값을 제공합니다. 사용자는 신속 보안 대응 또는 소프트웨어 업데이트를 설치할 때 `stng` 값을 절대적으로 증가할 수 있습니다.

auxp(AuxKC(보조 커널 모음) 정책 해시)

- **유형:** OctetString(48)
- **변경 가능한 환경:** macOS
- **설명:** `auxp`는 UAKL(사용자 승인 KEXT 목록) 정책의 SHA384 해시입니다. 이는 사용자 인증 KEXT만 AuxKC에 포함되도록 AuxKC 생성 시 사용됩니다. 이 필드를 설정하려면 `smb2`가 전제되어야 합니다. 사용자가 시스템 설정의 개인정보 보호 및 보안(macOS 13 이상) 또는 시스템 환경설정의 보안 및 개인 정보 보호 패널(macOS 12 또는 이전 버전)에서 KEXT를 승인하여 UAKL을 수정하면 `auxp` 값을 절대적으로 변경할 수 있습니다.

auxi(AuxKC(보조 커널 모음) Image4 매니페스트 해시)

- **유형:** OctetString(48)
- **변경 가능한 환경:** macOS
- **설명:** 시스템에서 UAKL 해시가 LocalPolicy의 `auxp` 필드에서 찾은 값과 일치함을 확인한 후에 LocalPolicy 서명을 담당하는 Secure Enclave 프로세서 응용 프로그램에서 AuxKC에 서명하도록 요청합니다. 그 다음에는 AuxKC Image4 매니페스트 서명의 SHA384 해시가 LocalPolicy에 배치되어 시동 시 이전에 서명된 AuxKC가 뒤섞이고 이를 운영 체제와 일치시킬 가능성을 피할 수 있습니다. iBoot가 LocalPolicy에서 `auxi` 필드를 발견한 경우 저장 장치에서 AuxKC를 로드하고 서명을 검증하려고 시도합니다. AuxKC에 연결된 Image4 매니페스트의 해시가 `auxi` 필드에서 찾은 값과 일치하는지 확인합니다. 어떤 이유로든 AuxKC가 로드되지 않은 경우 시스템은 해당 시동 개체 없이 계속해서 시동되므로, 타사 KEXT가 로드되지 않습니다. `auxp` 필드는 LocalPolicy에서 auxi 필드를 설정하는 데 필요한 전제 조건입니다. 사용자가 시스템 설정의 개인정보 보호 및 보안(macOS 13 이상) 또는 시스템 환경설정의 보안 및 개인 정보 보호 패널(macOS 12 또는 이전 버전)에서 KEXT를 승인하여 UAKL을 수정하면 `auxi` 값을 절대적으로 변경할 수 있습니다.

auxr(AuxKC(보조 커널 모음) 영수증 해시)

- **유형:** OctetString(48)
- **변경 가능한 환경:** macOS
- **설명:** `auxr`은 AuxKC에 포함된 정확한 KEXT 집합을 나타내는 AuxKC 영수증의 SHA384 해시입니다. AuxKC 영수증은 UAKL의 하위 집합이 될 수 있는데, KEXT가 사용자 승인을 받았더라도 공격에 사용된 것으로 밝혀지면 AuxKC에서 제외될 수 있기 때문입니다. 더욱이 사용자 커널 경계를 무너뜨리는 데 사용될 수 있는 일부 KEXT는 기능 저하를 초래하여 Apple Pay를 사용하지 못하거나 4K 및 HDR 콘텐츠를 재생할 수 없는 결과를 낳을 수 있습니다. 이러한 기능을 이용하기를 원하는 사용자는 AuxKC를 보다 제한적으로 포함하도록 선택할 수 있습니다. `auxp` 필드는 LocalPolicy에서 `auxr` 필드를 설정하는 데 필요한 전제 조건입니다. 사용자가 시스템 설정의 개인정보 보호 및 보안(macOS 13 이상) 또는 시스템 환경설정의 보안 및 개인 정보 보호 패널(macOS 12 또는 이전 버전)에서 새로운 AuxKC를 구축하면 `auxr` 값을 절대적으로 변경할 수 있습니다.

coih(CustomOS Image4 매니페스트 해시)

- **유형:** OctetString(48)
- **변경 가능한 환경:** 1TR
- **설명:** `coih`는 CustomOS Image4 매니페스트의 SHA384 해시입니다. 해당 매니페스트의 페이로드는 XNU 커널이 아닌 iBoot에서 제어 권한 전송에 사용합니다. 사용자가 1TR에서 `kmutil configure-boot` 명령어 라인 도구를 사용하면 `coih` 값이 절대적으로 변경됩니다.

vuid(APFS 볼륨 그룹 UUID)

- **유형:** OctetString(16)
- **변경 가능한 환경:** 1TR, 복구용 OS, macOS
- **설명:** `vuid`는 커널이 루트로 사용해야 하는 볼륨 그룹을 나타냅니다. 이 필드는 주로 정보를 제공하며 보안 제약에 사용되지 않습니다. 사용자가 새로운 운영 체제 설치를 생성하면 `vuid`가 절대적으로 설정됩니다.

kuid(KEK(Key encryption key) 그룹 UUID)

- **유형:** OctetString(16)
- **변경 가능한 환경:** 1TR, 복구용 OS, macOS
- **설명:** `kuid`는 시동된 볼륨을 가리킵니다. 키 암호화 키는 일반적으로 데이터 보호에 사용됩니다. 각 LocalPolicy에서는 LocalPolicy 서명 키를 보호하는 데 사용됩니다. 사용자가 새로운 운영 체제 설치를 생성하면 `kuid`가 절대적으로 설정됩니다.

PROT(페어링된 복구용 OS 신뢰하는 시동 정책 측정)

- **유형:** OctetString(48)
- **변경 가능한 환경:** 1TR, 복구용 OS, macOS
- **설명:** 페어링된 복구용 OS 신뢰하는 시동 정책 측정(TBPM)은 LocalPolicy의 Image4 매니페스트에 대한 특수 반복적 SHA384 해시 계산입니다. `lpnh`와 같은 재전송 방지 값은 자주 업데이트될 것이므로 시간 경과에 따른 일관된 측정을 위해 재전송 방지 값은 제외됩니다. 각 macOS LocalPolicy에서만 찾을 수 있는 `prot` 필드는 macOS LocalPolicy에 부합하는 복구용 OS LocalPolicy를 나타내는 페어링을 제공합니다.

hrlp(Secure Enclave 서명 복구용 OS LocalPolicy 존재)

- **유형:** 불리언
- **변경 가능한 환경:** 1TR, 복구용 OS, macOS
- **설명:** `hrlp`는 위의 `prot` 값이 Secure Enclave로 서명된 복구용 OS LocalPolicy의 측정값인지를 나타냅니다. 그렇지 않은 경우 복구용 OS LocalPolicy는 macOS Image4 파일과 같은 것에 서명하는 Apple 온라인 서명 서버에 의해 서명됩니다.

LOVE(Local Operating System Version)

- **유형:** 불리언
- **변경 가능한 환경:** 1TR, 복구용 OS, macOS
- **설명:** `love`는 LocalPolicy가 생성된 OS 버전을 나타냅니다. 버전은 LocalPolicy 생성 중 다음 상태 매니페스트에서 가져오고, 복구용 OS 페어링 제한 사항을 시행하는 데 사용됩니다.

smb0(보안 멀티 시동)

- **유형:** 불리언
- **변경 가능한 환경:** 1TR, 복구용 OS
- **설명:** `smb0`이 존재하고 참일 경우 LLB는 다음 단계 Image4 매니페스트가 개인 맞춤화된 서명을 필요로 하지 않고 전역적으로 서명되도록 허용합니다. 사용자는 시동 보안 유틸리티 또는 `bputil`으로 이 필드를 변경하여 부분 보안으로 다운그레이드할 수 있습니다.

smb1(보안 멀티 시동)

- **유형:** 불리언
- **변경 가능한 환경:** 1TR
- **설명:** `smb1`이 존재하고 참일 경우 iBoot는 사용자 설정 커널 모음과 같은 개체가 LocalPolicy와 동일한 키를 사용하여 Secure Enclave로 서명되도록 허용합니다. `smb0`이 있어야 `smb1`이 존재할 수 있습니다. 사용자는 `csrutil` 또는 `bputil`과 같은 명령어 라인 도구로 이 필드를 변경하여 최소 보안으로 다운그레이드할 수 있습니다.

smb2(보안 멀티 시동)

- **유형:** 불리언
- **변경 가능한 환경:** 1TR
- **설명:** `smb2`가 존재하고 참일 경우 iBoot는 보조 커널 모음이 LocalPolicy와 동일한 키를 사용하여 Secure Enclave로 서명되도록 허용합니다. `smb0`이 있어야 `smb2`이 존재할 수 있습니다. 사용자는 시동 보안 유틸리티 또는 `bputil`으로 이 필드를 변경하여 부분 보안으로 다운그레이드하고 타사 KEXT를 활성화할 수 있습니다.

smb3(보안 멀티 시동)

- **유형:** 불리언
- **변경 가능한 환경:** 1TR
- **설명:** `smb3`가 존재하고 참일 경우 기기의 사용자는 시스템에 대한 MDM(모바일 기기 관리) 제어를 사용하도록 선택합니다. 이 필드가 있으면 LocalPolicy를 제어하는 Secure Enclave 프로세서 응용 프로그램이 로컬 사용자 인증을 필요로 하는 대신 MDM 인증을 허용합니다. 사용자는 시동 보안 유틸리티 또는 `bputil`으로 이 필드를 변경하여 타사 KEXT와 소프트웨어 업데이트에 대한 관리되는 제어를 활성화할 수 있습니다. (macOS 11.2 이상 버전의 경우 MDM에서는 현재 보안 모드가 완전 보안일 경우 최신 macOS 버전으로 업데이트하는 작업도 수행할 수 있습니다.)

smb4(보안 멀티 시동)

- **유형:** 불리언
- **변경 가능한 환경:** macOS
- **설명:** `smb4`가 존재하고 참일 경우 기기는 Apple School Manager, Apple Business Manager 또는 Apple Business Essential을 통해 운영 체제에 대한 MDM 제어를 사용하도록 설정됩니다. 이 필드가 있으면 LocalPolicy를 제어하는 Secure Enclave 응용 프로그램이 로컬 사용자 인증을 필요로 하는 대신 MDM 인증을 허용합니다. 이 필드는 MDM 솔루션에서 기기의 일련 번호가 세 서비스 중 하나에 표시된 것을 감지하면 변경될 수 있습니다.

sip0(시스템 무결성 보호)

- **유형:** 64비트 부호 없는 정수
- **변경 가능한 환경:** 1TR
- **설명:** `sip0`는 이전에 NVRAM에 저장된 기존 SIP(시스템 무결성 보호) 정책 비트를 보유합니다. 새로운 SIP 정책 비트가 LLB가 아닌 macOS에서만 사용되는 경우 아래처럼 LocalPolicy 필드를 사용하는 대신 여기에 추가됩니다. 사용자는 1TR에서 `csrutil`을 통해 SIP를 비활성화하고 최소 보안으로 다운그레이드하여 이 필드를 변경할 수 있습니다.

sip1(시스템 무결성 보호)

- **유형:** 불리언
- **변경 가능한 환경:** 1TR
- **설명:** `sip1`이 존재하고 참일 경우 iBoot는 SSV 루트 해시를 확인할 수 있도록 실패를 허용합니다. 사용자는 1TR에서 `csrutil` 또는 `bputil`을 사용하여 이 필드를 변경할 수 있습니다.

sip2(시스템 무결성 보호)

- **유형:** 불리언
- **변경 가능한 환경:** 1TR
- **설명:** sip2가 존재하고 참일 경우 iBoot는 커널 메모리를 쓸 수 없음으로 표시하는 **CTRR(구성 가능한 텍스트 읽기 전용 영역)** 하드웨어 레지스터를 잠그지 않습니다. 사용자는 1TR에서 `csrutil` 또는 `bputil`을 사용하여 이 필드를 변경할 수 있습니다.

sip3(시스템 무결성 보호)

- **유형:** 불리언
- **변경 가능한 환경:** 1TR
- **설명:** 이 `sip3`가 존재하고 참일 경우 iBoot는 boot-args NVRAM 변수에 대해 내장 허용 목록을 실행하지 않으며, 그렇지 않으면 커널에 전달된 옵션이 필터링됩니다. 사용자는 1TR에서 `csrutil` 또는 `bputil`을 사용하여 이 필드를 변경할 수 있습니다.

인증서 및 RemotePolicy

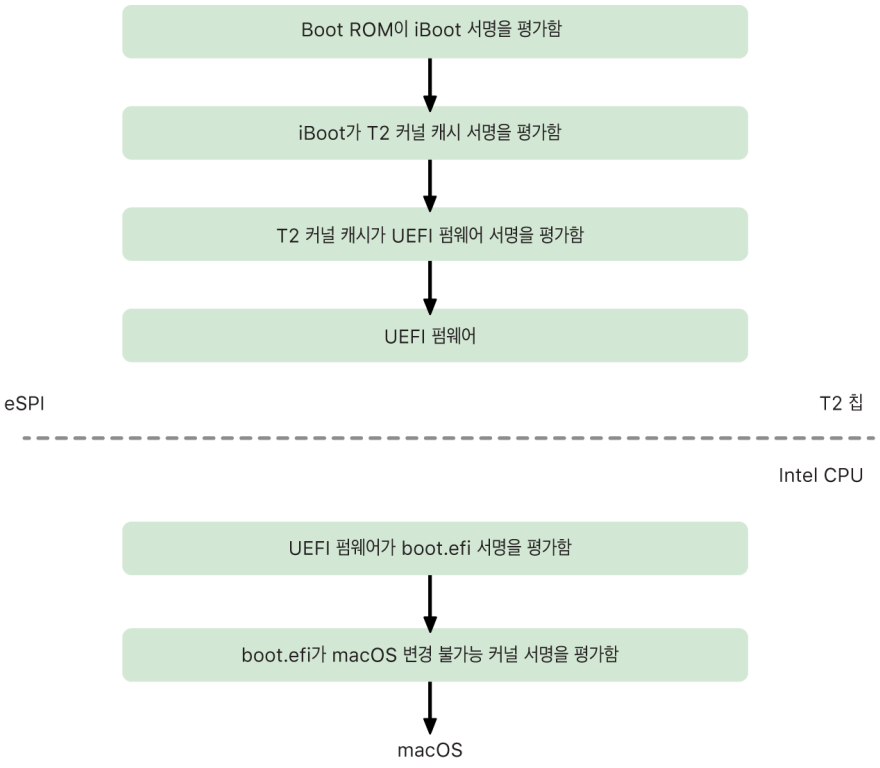
LocalPolicy 서명 키 생성 및 관리에서 설명한 대로 LocalPolicy Image4는 OIC(소유자 신원 증명서) 및 임베디드 RemotePolicy도 포함합니다.

Intel 기반 Mac 컴퓨터

Intel 기반 Mac의 시동 프로세스

Apple T2 보안 칩이 탑재된 Intel 기반 Mac 컴퓨터

Apple T2 보안 칩이 탑재된 Intel 기반 Mac 컴퓨터가 켜져 있는 경우, 칩은 iPhone, iPad 및 Apple Silicon이 탑재된 Mac과 동일한 방식으로 Boot ROM에서 보안 시동을 수행합니다. 이는 iBoot 부트로더를 확인하며 신뢰 체인의 첫 번째 단계입니다. iBoot는 T2 칩의 커널 및 커널 확장 프로그램 코드를 확인한 후, Intel UEFI 펌웨어를 검증합니다. UEFI 펌웨어 및 관련 서명은 T2 칩에서만 처음 사용할 수 있습니다.



확인이 끝나면 UEFI 펌웨어 이미지는 T2 칩 메모리의 일부에 매핑됩니다. 이 메모리는 eSPI(향상된 직렬 주변기기 인터페이스)를 통해 Intel CPU에서 사용할 수 있습니다. Intel CPU가 처음 시동될 때 무결성 검사를 완료하고 메모리 매핑된 T2 칩의 펌웨어 사본에서 eSPI를 통해 UEFI 펌웨어를 가져옵니다.

UEFI 펌웨어는 macOS 부트로더인 boot.efi에 대한 서명을 평가하며, Intel CPU에서 신뢰 체인의 평가가 계속됩니다. Intel에 있는 macOS 보안 시동 서명은 iOS, iPadOS 및 T2 칩 보안 시동에 사용되는 것과 동일한 Image4 형식으로 저장되며, Image4 파일을 구문 분석하는 코드는 현재 iOS 및 iPadOS 보안 시동 구현과 동일하게 강화된 코드입니다. Boot.efi는 immutablekernel이라는 새로운 파일의 서명을 확인합니다. 보안 시동이 활성화되면 immutablekernel 파일은 macOS를 시동하는 데 필요한 전체 Apple 커널 확장 프로그램 세트를 나타냅니다. 보안 시동 정책은 immutablekernel에 대한 전달로 종료되며, 그 후에는 macOS 보안 정책(시스템 무결성 보호 및 서명된 커널 확장 프로그램 등)이 적용됩니다.

이 프로세스에서 실패하거나 오류가 발생하면 Mac이 복구 모드, Apple T2 보안 칩 복구 모드 또는 Apple T2 보안 칩 DFU(기기 펌웨어 업그레이드) 모드로 진입합니다.

T2 칩이 탑재된 Intel 기반 Mac의 Microsoft Windows

기본적으로 보안 시동을 지원하는 Intel 기반 Mac은 Apple이 서명한 콘텐츠만 신뢰합니다. 하지만 Boot Camp 설치 보안을 향상시키기 위해 Apple은 Windows에서도 보안 시동을 지원합니다. UEFi(Unified Extensible Firmware Interface) 펌웨어는 Microsoft 부트로더 인증에 사용되는 Microsoft Windows Production CA 2011 인증서 사본을 포함합니다.

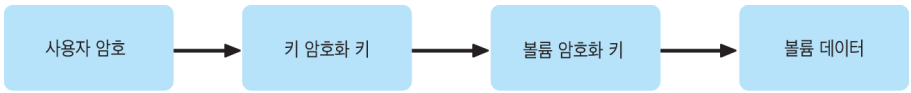
참고: 현재 Microsoft 파트너가 서명한 코드 검증을 허용하는 Microsoft Corporation UEFI CA 2011에 대한 신뢰는 제공되지 않습니다. 이 UEFI CA는 일반적으로 변형된 Linux와 같은 다른 운영 체제에 대한 부트로더의 신뢰성을 확인하는 데 사용됩니다.

Windows의 보안 시동 지원은 기본적으로 활성화되어 있지 않으며 대신 BCA(Boot Camp 지원)를 사용하여 활성화됩니다. 사용자가 BCA를 실행하면 macOS는 시동 중에 Microsoft 자사 서명 코드를 신뢰하도록 재구성됩니다. BCA가 완료된 후 보안 시동 중에 macOS가 Apple 자사 신뢰 평가를 통과하지 못하면 UEFI 펌웨어는 UEFI 보안 시동 형식에 따라 개체 신뢰도 평가를 시도합니다. 신뢰도 평가에 성공하면 Mac은 계속해서 Windows를 시동합니다. 실패하는 경우 Mac은 복구용 OS로 진입하고 신뢰도 평가에 실패했음을 사용자에게 알립니다.

T2 칩이 탑재되지 않은 Intel 기반 Mac 컴퓨터

T2 칩이 탑재되지 않은 Intel 기반 Mac은 보안 시동을 지원하지 않습니다. 따라서 UEFi(Unified Extensible Firmware Interface) 펌웨어는 확인 없이 파일 시스템에서 macOS 시동 프로그램(boot.efi)을 로드하고 시동 프로그램은 확인 없이 파일 시스템에서 커널(prelinkedkernel)을 로드합니다. 부트 체인의 무결성을 보호하기 위해 사용자는 다음의 보안 메커니즘을 모두 활성화해야 합니다.

- **시스템 무결성 보호(SIP):** 이 기능은 기본적으로 활성화되며, 실행 중인 macOS 내의 악의적 쓰기로부터 시동 프로그램과 커널을 보호합니다.
- **FileVault:** 이는 사용자 또는 MDM(모바일 기기 관리) 관리자에 의한 두 가지 방법으로 활성화할 수 있습니다. 이를 통해 실제 공격자가 대상 디스크 모드를 사용하여 시동 프로그램에 덮어쓰는 것을 막습니다.
- **펌웨어 암호:** 이는 사용자 또는 MDM 관리자가 활성화할 수 있습니다. 이를 통해 실제 공격자가 복구용 OS, 단일 사용자 모드 또는 대상 디스크 모드와 같은 대체 시동 모드를 실행하여 시동 프로그램을 덮어쓰는 것을 막습니다. 또한 공격자가 시동 프로그램을 덮어쓰는 코드를 실행해 대체 미디어에서 시동하는 행위를 방지합니다.



Apple T2 보안 칩이 탑재된 Intel 기반 Mac 컴퓨터의 시동 모드

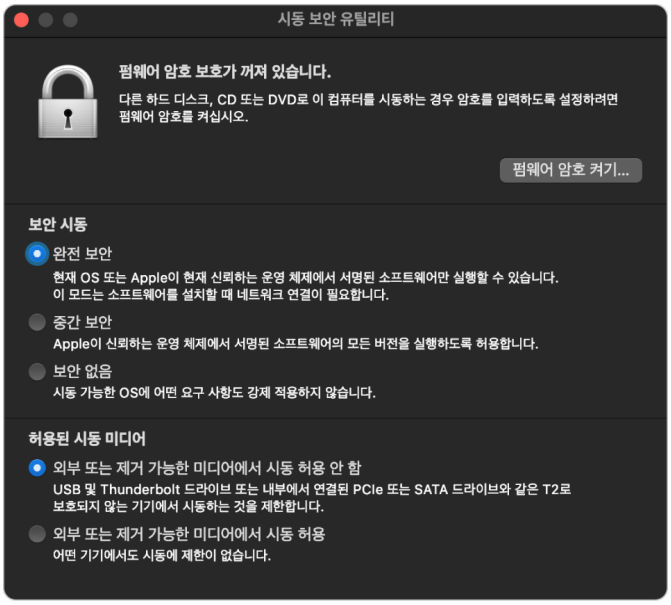
Apple T2 보안 칩이 탑재된 Intel 기반 Mac에는 UEFI 펌웨어 또는 시동 프로그램이 인식하는 키 조합을 눌러 시동 시 진입할 수 있는 다양한 시동 모드가 있습니다. 단일 사용자 모드와 같은 일부 시동 모드는 시동 보안 유틸리티에서 보안 정책을 보안 없음으로 변경하지 않으면 사용할 수 없습니다.

모드	키 조합	설명
macOS 시동	없음	UEFI 펌웨어는 macOS 커널로 전달하는 macOS 시동 프로그램(UEFI 응용 프로그램)으로 전달됩니다. FileVault가 활성화된 Mac의 표준 시동에서 macOS 시동 프로그램은 암호를 가져와 저장 공간의 암호화를 해제하는 로그인 윈도우 인터페이스를 표시합니다.
시동 관리자	Option (⌥)	UEFI 펌웨어는 내장 UEFI 응용 프로그램을 실행하여 사용자에게 시동 기기 선택 인터페이스를 표시합니다.
TDM(대상 디스크 모드)	T	UEFI 펌웨어는 FireWire, Thunderbolt, USB 또는 이 세 가지의 조합(Mac 모델에 따라 상이)을 통해 가공되지 않은 블록 기반 저장 장치로서의 내장 저장 장치를 노출하는 내장 UEFI 응용 프로그램을 실행합니다.
단일 사용자 모드	Command (⌘)-S	macOS 커널이 launchd의 인수 벡터에 –s 플래그를 전달하면 launchd가 콘솔 앱의 tty에 단일 사용자 셸을 생성합니다. **참고:** 사용자가 셸을 종료하면 macOS는 로그인 윈도우로 시동을 계속합니다.
복구용 OS	Command (⌘)-R	UEFI 펌웨어는 내장 저장 장치의 서명된 디스크 이미지(.dmg) 파일에서 최소한의 macOS를 로드합니다.
인터넷 복구용 OS	Option (⌥)-Command (⌘)-R	서명된 디스크 이미지는 HTTP를 사용하여 인터넷에서 다운로드됩니다.
진단	D	UEFI 펌웨어는 내장 저장 장치의 서명된 디스크 이미지 파일에서 최소한의 UEFI 진단 환경을 로드합니다.
인터넷 진단	Option (⌥)-D	서명된 디스크 이미지는 HTTP를 사용하여 인터넷에서 다운로드됩니다.
Windows 시동	없음	Boot Camp를 사용하여 Windows를 설치한 경우, UEFI 펌웨어는 Windows 시동 프로그램으로 전달되고 Windows 시동 프로그램은 Windows 커널로 전달됩니다.

Apple T2 보안 칩이 탑재된 Mac의 시동 보안 유틸리티

개요

Apple T2 보안 칩이 탑재된 Intel 기반 Mac의 경우 시동 보안 유틸리티가 다수의 보안 정책 설정을 처리합니다. 이 유틸리티에 접근하려면 복구용 OS로 시동하고 유틸리티 메뉴에서 시동 보안 유틸리티를 선택합니다. 이 유틸리티는 지원되는 보안 설정을 보호하여 공격자가 쉽게 조작하지 못하도록 합니다.



중요한 정책을 변경하려면 복구 모드에서도 인증이 필요합니다. 시동 보안 유틸리티를 처음 열면 현재 시동된 복구용 OS와 연결된 기본 macOS 설치에서 관리자 암호를 입력하라는 메시지가 사용자에게 표시됩니다. 관리자가 없는 경우, 관리자를 생성한 다음 정책을 변경할 수 있습니다. T2 칩은 Mac 컴퓨터가 현재 복구용 OS로 시동할 것과, 이러한 정책 변경을 적용하기 전에 Secure Enclave가 지원하는 자격 증명을 사용하여 인증할 것을 요구합니다. 보안 정책을 변경하려면 복구용 OS에 필요한 다음 두 가지 절대적 조건이 지켜져야 합니다.

- 다른 기기의 파티션에는 내장 저장 장치에 연결된 Secure Enclave가 지원하는 자격 증명이 없기 때문에, macOS 복구가 T2 칩에 직접 연결된 저장 장치에서 시동되어야 합니다.
- macOS 복구를 APFS 기반 볼륨에 보관해야 하며, 이는 드라이브의 ‘Preboot’ APFS 볼륨에 있는 Secure Enclave로 전송된 ‘복구에서 인증’ 자격 증명을 저장만 할 수 있는 기능이 지원되기 때문입니다. HFS 플러스 포맷의 볼륨은 보안 시동을 사용할 수 없습니다.

이 정책은 T2 칩이 탑재된 Intel 기반 Mac 컴퓨터의 시동 보안 유틸리티에만 표시됩니다. 대부분의 활용 사례에서는 보안 시동 정책 변경을 요구해서는 안 되지만, 근본적으로 사용자는 기기 설정을 제어할 수 있으며 필요에 따라 Mac에서 보안 시동 기능을 비활성화하거나 다운그레이드할 수 있습니다.

이 앱 내에서 변경되는 보안 시동 정책은 Intel 프로세서에서 검증하는 신뢰 체인 평가에만 적용됩니다. ‘T2 칩의 보안 시동’ 옵션은 항상 유효합니다.

보안 시동 정책은 완전 보안, 중간 보안 및 보안 없음의 세 가지 설정으로 구성할 수 있습니다. 보안 없음 설정은 Intel 프로세서에서 보안 시동 평가를 완전히 비활성화하고 사용자가 원하는 대로 시동할 수 있도록 합니다.

완전 보안 시동 정책

완전 보안은 기본 시동 정책이며 iOS 및 iPadOS 또는 Apple Silicon이 탑재된 Mac의 완전 보안과 유사하게 작동합니다. 소프트웨어를 다운로드하고 설치할 준비가 되었을 때 서명 요청의 일부로서 T2 칩에 특정된 고유 ID인 ECID(Exclusive Chip Identification)가 포함된 서명으로 개인 맞춤화됩니다. 서명 서버에서 돌려주는 해당 서명은 고유하며 특정 T2 칩에서만 사용할 수 있습니다. UEFi(Unified Extensible Firmware Interface) 펌웨어는 완전 보안 정책이 적용되면 지정된 서명이 Apple에서 서명했을 뿐 아니라 특정 Mac에 대해서도 서명되어 결국 해당 버전의 macOS를 해당하는 Mac에 연결하도록 합니다. 이렇게 하면 Apple Silicon이 탑재된 Mac의 완전 보안에 대해 설명된 대로 롤백 공격을 방지할 수 있습니다.

중간 보안 시동 정책

중간 보안 시동 정책은 공급업체에서 제공한 코드임을 밝히기 위해 공급업체(이 경우 Apple)가 코드에 대한 디지털 서명을 생성하는 기존 UEFI 보안 시동과 다소 유사합니다. 이러한 방식으로 공격자가 서명되지 않은 코드를 삽입하는 것을 방지합니다. 이 서명은 현재 중간 보안 정책이 설정되어 있는 Mac 컴퓨터에 대해 모든 Mac에서 언제든지 사용할 수 있기 때문에, 이를 '전역' 서명이라고 부릅니다. iOS, iPadOS, T2 칩 모두 전역 서명을 자체 지원하지 않습니다. 이 설정은 롤백 공격 방지를 시도하지 않습니다.

미디어 시동 정책

미디어 시동 정책은 T2 칩이 탑재된 Intel 기반 Mac 컴퓨터에만 존재하며 보안 시동 정책과는 독립적입니다. 따라서 이 정책으로 인해 사용자가 보안 시동을 비활성화하더라도 Mac을 시동하기 위해 T2 칩에 직접 연결된 저장 장치가 아닌 다른 장치에서의 시동을 방지하는 기본 동작이 변경되지는 않습니다. (미디어 시동 정책은 Apple Silicon이 탑재된 Mac에서 필요하지 않습니다. 자세한 내용은 시동 디스크 보안 정책 제어를 참조하십시오.)

Intel 기반 Mac의 펌웨어 암호 보호

Apple T2 보안 칩이 탑재된 Intel 기반 Mac 컴퓨터의 macOS는 특정 Mac에서 의도하지 않은 펌웨어 설정 변경을 방지하기 위해 펌웨어 암호 사용을 지원합니다. 펌웨어 암호는 복구용 OS나 단일 사용자 모드로의 시동, 인증되지 않은 볼륨에서의 시동 또는 대상 디스크 모드로의 시동과 같은 대체 시동 모드가 선택되는 것을 방지합니다.

참고: Apple Silicon이 탑재된 Mac에서는 펌웨어 암호가 필요하지 않습니다. 이는 제한된 주요 펌웨어 기능이 복구용 OS로 이동되었고, FileVault가 활성화된 경우 복구용 OS는 주요 기능에 도달하기 전에 사용자 인증이 필요하기 때문입니다.

T2 칩이 **탑재되지 않은** Intel 기반 Mac에서는 복구용 OS 펌웨어 암호 유틸리티에서, T2 칩이 **탑재된** Intel 기반 Mac에서는 시동 보안 유틸리티에서 가장 기본적인 펌웨어 암호 모드에 접근할 수 있습니다. macOS의 `firmwarepasswd` 명령어 라인 도구에서 고급 옵션(시동할 때마다 암호를 묻는 기능 등)을 사용할 수 있습니다.

T2 칩이 탑재되지 않은 Intel 기반 Mac 컴퓨터에서 물리적으로 존재하는 공격자로부터의 공격 위험을 줄이려면 펌웨어 암호를 설정하는 것이 특히 중요합니다. 펌웨어 암호는 공격자가 복구용 OS로 시동하는 것을 중지시켜 SIP(시스템 무결성 보호)를 비활성화하지 못하도록 합니다. 또한, 대체 미디어의 시동을 제한하여 공격자가 다른 운영 체제에서 권한 코드를 실행하여 주변기기 펌웨어를 공격할 수 없습니다.

암호를 잊어버린 사용자에게 도움을 주기 위해 펌웨어 암호 재설정 메커니즘이 존재합니다. 사용자가 시동할 때 키 조합을 누르면 AppleCare에 제공되는 모델별 문자열이 표시됩니다. AppleCare는 URI(Uniform Resource Identifier)에서 서명을 확인한 리소스에 디지털로 서명합니다. 서명이 유효하고 특정 Mac에 대한 콘텐츠인 경우, UEFI 펌웨어는 펌웨어 암호를 제거합니다.

소프트웨어적인 방법으로 본인 외에는 누구도 펌웨어 암호를 제거하는 것을 원하지 않는 사용자를 위해 macOS 10.15 버전의 `firmwarepasswd` 명령어 라인 도구에 `–disable–reset–capability` 옵션이 추가되었습니다. 이 옵션을 설정하기에 앞서, 암호를 잊어서 제거해야 하는 경우가 발생하면 사용자는 이에 필요한 로직 보드 교체 비용을 본인이 부담해야 한다는 점을 알고 있어야 합니다. 조직이 외부 공격자 및 직원으로부터 Mac 컴퓨터를 보호하려면, 조직 소유 시스템에서 펌웨어 암호를 설정해야 합니다. 이는 기기에서 다음 중 하나의 방법으로 수행할 수 있습니다.

- 권한 설정 시 `firmwarepasswd` 명령어 라인 도구를 수동으로 사용
- `firmwarepasswd` 명령어 라인 도구를 사용하는 타사 관리 도구 사용
- MDM(모바일 기기 관리) 사용

Intel 기반 Mac용 복구용 OS 및 진단 환경

복구용 OS

복구용 OS는 주요 macOS와 완전히 별개이며 전체 콘텐츠는 BaseSystem.dmg라는 디스크 이미지 파일에 저장됩니다. BaseSystem.dmg의 무결성을 확인하는 데 사용되는 관련 BaseSystem.chunklist도 있습니다. chunklist는 BaseSystem.dmg의 10MB 청크용 일련의 해시입니다. UEFi(Unified Extensible Firmware Interface) 펌웨어는 chunklist 파일의 서명을 평가한 다음, BaseSystem.dmg에서 하나의 청크에 대한 해시를 하나씩 평가합니다. 이를 통해 각 해시가 chunklist에 있는 서명된 콘텐츠와 일치하는지 확인합니다. 이 해시 중 하나라도 일치하지 않으면 로컬 복구용 OS에서의 시동이 중단되고 UEFI 펌웨어가 대신 인터넷 복구용 OS에서 시동을 시도합니다.

확인이 성공적으로 완료되면 UEFI 펌웨어는 BaseSystem.dmg를 RAM 디스크로 마운트하고 그 안에 포함된 boot.efi 파일을 실행합니다. UEFI 펌웨어가 boot.efi에 대한 특정 검사를 수행하거나 boot.efi가 커널을 검사할 필요는 없는데, 이는 이러한 요소가 하위 집합에 불과한 운영 체제의 전체 콘텐츠에 대한 무결성 확인을 이미 완료했기 때문입니다.

Apple 진단

로컬 진단 환경을 시동하는 절차는 대부분 복구용 OS를 실행하는 절차와 동일합니다. AppleDiagnostics.dmg 및 AppleDiagnostics.chunklist 파일은 각자 별도로 사용되지만, 확인되는 방식은 BaseSystem 파일과 동일합니다. UEFI 펌웨어는 boot.efi를 실행하는 대신 디스크 이미지(.dmg 파일) 내부에서 diags.efi라는 이름의 파일을 실행합니다. 이 파일은 하드웨어에 접속하고 하드웨어의 오류를 확인할 수 있는 다양한 기타 UEFI 드라이버를 호출하는 역할을 합니다.

인터넷 복구용 OS 및 진단 환경

로컬 복구 또는 진단 환경을 실행할 때 오류가 발생하는 경우 UEFI 펌웨어는 대안으로 인터넷에서 이미지 다운로드를 시도합니다. 또한, 사용자는 시동 시 보관된 특수 키 시퀀스를 사용하여 인터넷에서 이미지를 가져오도록 특별히 요청할 수 있습니다. 디스크 이미지 및 OS 복구 서버에서 다운로드한 chunklist의 무결성 확인은 저장 장치에서 검색된 이미지와 동일한 방법으로 수행됩니다.

HTTP를 사용하여 OS 복구 서버에 연결하는 동안 앞에서 설명한 대로 다운로드한 전체 콘텐츠의 무결성이 확인됩니다. 따라서 네트워크를 제어하는 공격자의 조작 공격으로부터 보호됩니다. 개별 청크가 무결성 확인에 실패하는 경우 OS 복구 서버에서 무결성 확인을 11회 다시 요청한 다음, 오류를 표시합니다.

2011년형 Mac 컴퓨터에 인터넷 복구와 진단 모드를 추가한 것은 UEFI 펌웨어에서 한층 복잡한 HTTPS 기능을 구현하여 펌웨어의 공격 표면이 늘어나도록 하기보다는 더 간단한 HTTP 전송을 이용하고 chunklist 메커니즘을 통해 콘텐츠 인증을 처리하는 것이 더 효과적이라는 판단을 내렸기 때문입니다.

서명된 시스템 볼륨 보안

macOS 10.15에서 Apple은 시스템 콘텐츠 전용으로 격리된 읽기 전용 시스템 볼륨을 도입했습니다. macOS 11 이상 버전은 **SSV(서명된 시스템 볼륨)**가 있는 시스템 콘텐츠에 강력한 암호화 보호 기능을 추가합니다. SSV는 런타임 시 시스템 콘텐츠의 무결성을 확인하고 Apple의 암호 서명이 유효하지 않은 데이터(코드 및 비코드 포함)를 거부하는 커널 메커니즘을 특징으로 합니다. iOS 15 및 iPadOS 15부터, iPhone 또는 iPad의 시스템 볼륨은 서명된 시스템 볼륨의 암호화 보호 또한 받습니다.

SSV는 운영 체제의 일부인 Apple 소프트웨어의 변조를 방지할 뿐 아니라 macOS 소프트웨어 업데이트의 신뢰성과 안전성을 높입니다. 한편 SSV는 APFS(Apple 파일 시스템) 스냅샷을 활용하므로, 업데이트를 수행할 수 없는 경우 이전 시스템 버전을 다시 설치하지 않고 복원할 수 있습니다.

SSV의 도입 이후 APFS는 내장 저장 장치의 비암호화 체크섬을 통해 파일 시스템 메타데이터 무결성을 제공해 왔습니다. SSV는 암호화 해시를 추가하고 파일 데이터의 모든 바이트를 포함하도록 이를 확장하여 무결성 메커니즘을 강화합니다. 파일 시스템 메타데이터 등 내장 저장 장치의 데이터는 읽기 경로에서 암호로 해시되며, 이후 해당 해시와 파일 시스템 메타데이터의 예상 값이 비교됩니다. 불일치가 있을 경우 시스템은 데이터가 변조되었다고 가정하고 요청한 소프트웨어에 데이터를 반환하지 않습니다.

각 SSV SHA256 해시는 그 자체로 해시되는 기본 파일 시스템 메타데이터 트리에 저장됩니다. 또한 트리의 각 노드는 반복적으로 해당 하위 항목 해시(바이너리 해시(Merkle) 트리와 유사함)의 무결성을 확인하므로 **SEAL**이라고 하는 루트 노드의 해시 값은 SSV 데이터의 모든 바이트를 포함합니다. 이는 암호화 서명이 시스템 볼륨 전체에 적용됨을 뜻합니다.

macOS 설치 및 업데이트가 진행되는 동안 SEAL은 기기 내 파일 시스템에서 다시 산출되며, 이 값은 Apple에서 서명한 측정 값을 기준으로 확인을 거칩니다. Apple Silicon이 탑재된 Mac의 부트로더는 제어 권한을 커널로 이전하기 전에 해당 SEAL을 확인합니다. Apple T2 보안 칩이 탑재된 Intel 기반 Mac에서 부트로더는 측정값과 서명을 커널로 전달한 다음, 루트 파일 시스템에 마운트하기 전에 직접 SEAL을 확인합니다. 두 경우 모두 확인에 실패하면 시동 프로세스가 중단되고 사용자에게 macOS를 다시 설치하라는 메시지가 표시됩니다. 사용자가 더 낮은 수준의 보안 모드에 진입하도록 설정하고 서명된 시스템 볼륨을 별도로 비활성화하도록 선택하지 않는 한 이 프로세스는 시동 시마다 반복됩니다.

iOS 및 iPadOS 소프트웨어 업데이트 중에 시스템 볼륨은 비슷한 방법으로 준비되고 다시 산출됩니다. iOS 및 iPadOS 부트로더는 기기가 커널을 시작하도록 허용하기 전에 SEAL이 그대로 유지되었는지와 Apple이 서명한 값과 일치하는지를 확인합니다. 시동 시 불일치가 있을 경우, 사용자에게 기기의 시스템 소프트웨어를 업데이트하도록 요청합니다. 사용자는 iOS 및 iPadOS에서 서명된 시스템 볼륨의 보호를 해제할 수 없습니다.

SSV 및 코드 서명

코드 서명은 계속해서 사용되며 커널에서 시행됩니다. 서명된 시스템 볼륨은 내장 저장 장치에서 바이트를 전혀 읽을 수 없는 경우를 보호합니다. 반대로, 코드 서명은 Mach 개체가 실행 가능한 것으로 메모리 매핑될 때 보호 기능을 제공합니다. SSV 및 코드 서명 모두 읽기 및 실행 경로 전체에서 실행 가능한 코드를 보호한다는 공통점이 있습니다.

SSV 및 FileVault

macOS 11 이상에서는 SSV가 시스템 콘텐츠에 대한 동급의 유휴 상태 보호 기능을 제공하여 시스템 볼륨이 더 이상 암호화될 필요가 없도록 합니다. 유휴 상태에서 파일 시스템이 변경되면 파일 시스템에서 읽어 들일 때 이를 탐지합니다. 사용자가 FileVault를 켠 경우 데이터 볼륨에 있는 사용자의 콘텐츠는 여전히 사용자가 지정한 비밀 키로 암호화됩니다.

사용자가 SSV를 비활성화하기로 선택한 경우 시스템이 유휴 상태일 때 변조에 취약해지며, 공격자는 이러한 공격으로 다음에 시스템이 시동될 때 암호화된 사용자 데이터를 추출할 수 있게 됩니다. 따라서 FileVault를 켠 경우 사용자는 시스템에서 SSV를 비활성화할 수 없습니다. 두 볼륨에서 유휴 상태 보호 기능은 일관되게 활성화하거나 비활성화해야 합니다.

macOS 10.15 또는 이전 버전에서 FileVault는 사용자 지정 비밀로 보호되는 키로 사용자 및 시스템 콘텐츠를 암호화하여 유휴 상태인 운영 체제 소프트웨어를 보호합니다. 이로써 기기에 물리적 접근이 가능한 공격자가 시스템 소프트웨어를 포함하는 파일 시스템에 접근하거나 실제로 이를 수정하는 것을 방지합니다.

SSV와 Apple T2 보안 칩이 탑재된 Mac

Apple T2 보안 칩이 탑재된 Mac에서 macOS만이 자체적으로 SSV의 보호를 받습니다. T2 칩에서 실행되고 macOS를 확인하는 소프트웨어는 보안 시동의 보호를 받지 않습니다.

보안 소프트웨어 업데이트

보안은 하나의 과정이기 때문에 초기 설치된 운영 체제 버전을 안정적으로 시동하는 것만으로는 충분하지 않습니다. 최신 보안 업데이트를 빠르고 안전하게 받을 수 있는 메커니즘도 있어야 합니다. Apple은 정기적으로 소프트웨어 업데이트를 출시하여 새로운 보안 문제를 해결합니다. iPhone 및 iPad 기기 사용자는 기기에서 업데이트 알림을 받습니다. Mac 사용자는 시스템 설정(macOS 13 이상) 또는 시스템 환경설정(macOS 12 또는 이전 버전)에서 사용 가능한 업데이트를 확인할 수 있습니다. 업데이트는 무선으로 제공되므로 최신 보안 수정 사항을 빠르게 적용할 수 있습니다.

업데이트 프로세스 보안

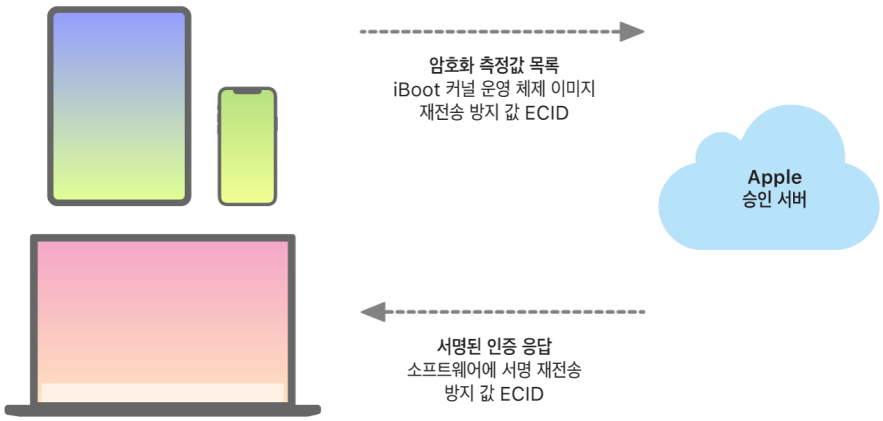
업데이트 프로세스는 시동을 안전하게 하고 Apple이 서명한 코드만 설치하도록 고안된 동일한 하드웨어 기반 신뢰 루트를 사용합니다. 업데이트 프로세스는 또한 시스템 소프트웨어 승인을 사용하여 Apple이 유효하게 서명한 운영 체제 버전의 합법적인 사본만 iPhone 및 iPad 기기 또는 시동 보안 유틸리티의 보안 시동 정책이 완전 보안 설정으로 구성된 Mac 컴퓨터에 설치될 수 있도록 확인합니다. 이러한 보안 프로세스를 적용해 Apple은 알려진 취약성이 있는 이전 운영 체제 버전에 서명을 중지하여 다운그레이드 공격을 방지할 수 있습니다.

더 높은 수준의 소프트웨어 업데이트 보안을 위해 업데이트할 기기가 Mac에 물리적으로 연결되어 있으면 iOS 또는 iPadOS의 전체 사본이 다운로드되고 설치됩니다. OTA(Over The Air) 소프트웨어 업데이트의 경우 운영 체제 전체를 다운로드하지 않고 **업데이트 완료에 필요한 구성요소만을 다운로드**하므로 네트워크 효율성이 개선됩니다. 또한, 소프트웨어 업데이트가 macOS 10.13 이상 버전이 설치되어 있고 콘텐츠 캐싱이 켜져 있는 Mac에 캐시될 수 있어 iPhone 및 iPad 기기는 필요한 업데이트를 인터넷에서 다시 다운로드할 필요가 없습니다. 하지만 업데이트를 완료하기 위해서는 Apple 서버에 접속해야 합니다.

개인 맞춤형 업데이트 프로세스

업그레이드 및 업데이트 도중 Apple 설치 승인 서버에서 특정 정보를 사용할 수 있으며 설치해야 할 설치 번들의 각 부분(예: iBoot, 커널, 운영 체제 이미지)의 암호화 측정값 목록, 재전송 방지 무작위 값 및 기기 고유 ECID(Exclusive Chip Identification)를 포함합니다.

승인 서버가 제공된 암호화 측정값 목록을 확인하여 허용된 설치 버전을 찾아 일치하는 버전을 찾으면 해당 암호화 측정값에 ECID를 추가하고 결과를 서명합니다. 그리고 업그레이드 프로세스의 일부로서 서버가 서명된 데이터 전체를 기기에 전송합니다. ECID를 추가하게 되면 업데이트를 요청하는 기기에 대한 승인이 '개인 맞춤화'됩니다. 확인된 암호화 측정값에 대해서만 서명하고 인증하여 Apple이 제공하는 방식대로 서버에서 업데이트를 진행합니다.



시동 시의 신뢰 체인 평가를 통해 Apple의 서명을 확인하고 저장 장치에서 불러온 항목의 암호화 측정값 및 기기의 ECID가 서명에서 명시한 것과 일치하는지 확인합니다. 이러한 과정은 개인 맞춤화를 지원하는 기기에서 특정 기기를 대상으로 인증이 이뤄지고 하나의 기기에 있는 이전 버전의 운영 체제 또는 펌웨어가 다른 기기로 복사되지 않도록 합니다. 재전송 방지 값은 공격자가 서버 응답을 저장하지 못하도록 하여 기기 변조 또는 시스템 소프트웨어 수정을 방지합니다.

개인 맞춤화 프로세스는 Apple T2 보안 칩이 탑재된 Intel 기반 Mac을 포함하여 Apple이 설계한 실리콘으로 모든 기기를 업데이트하기 때문에 항상 Apple로의 네트워크 연결이 필요합니다.

또한, Secure Enclave를 사용하는 기기에서 마찬가지로 하드웨어가 시스템 소프트웨어 승인을 사용하여 소프트웨어 무결성을 확인하고 다운그레이드 설치를 방지합니다.

운영 체제 무결성

Apple의 운영 체제 소프트웨어는 보안을 핵심으로 설계되었습니다. 여기에는 보안 시동을 활성화하기 위한 하드웨어 신뢰 루트와 함께 빠르고 안전한 보안 소프트웨어 업데이트 프로세스도 포함됩니다. 또한 Apple 운영 체제는 시스템이 실행될 때 악용되는 것을 방지하기 위한 목적으로 제작된 실리콘 기반 하드웨어 기능을 활용합니다. 이러한 런타임 기능은 신뢰하는 코드가 실행될 때의 무결성을 보호합니다. 간단히 말해서 Apple의 운영 체제 소프트웨어는 악성 앱, 웹 또는 다른 채널을 통해 발생하는 공격과 그러한 기술의 악용을 완화하는 데 도움이 됩니다. 여기에 나열된 보호 기능은 Apple이 설계한 SoC 지원 기기에서 사용할 수 있습니다. 여기에는 iOS, iPadOS, tvOS, watchOS 및 Apple Silicon이 탑재된 Mac의 macOS가 포함됩니다.

기능	A10	A11, S3	A12, A13, A14 S4–S9	A15, A16, A17	M1, M2, M3
커널 무결성 보호	✓	✓	✓	✓	✓
빠른 권한 제한	✗	✓	✓	✓	✓
시스템 보조 프로세서 무결성 보호	✗	✗	✓	✓	✓
포인터 인증 코드	✗	✗	✓	✓	✓
페이지 보호 레이어	✗	✓	✓	✓	✗ 아래의 참고 1 내용 확인.
보안 페이지 테이블 모니터	✗	✗	✗	✓ 아래의 참고 2 내용 확인.	✗

참고 1: PPL(페이지 보호 레이어)는 플랫폼이 **서명되고 신뢰할 수 있는 코드만** 실행하도록 요구합니다. 이는 macOS에 적용되지 않는 보안 모델입니다.

참고 2: 보안 페이지 테이블 모니터(SPTM)는 A15, A16 및 A17에서 지원되며 지원 플랫폼에서 페이지 보호 레이어를 대체합니다.

커널 무결성 보호

운영 체제 커널 초기화가 완료되면 커널 및 드라이버 코드 수정을 방지하기 위해 커널 무결성 보호(KIP)가 활성화됩니다. 메모리 컨트롤러는 iBoot가 커널 및 커널 확장 프로그램을 로드하는 데 사용하는 보호된 물리적 메모리 영역을 제공합니다. 시동이 완료되면 메모리 컨트롤러는 보호되는 물리적 메모리 영역에 쓰기를 거부합니다. 보호되는 메모리 영역 외부에 있는 물리적 메모리의 권한 코드 매핑을 방지하고 커널 메모리 영역 내에서 물리적 메모리의 쓰기 가능한 매핑을 방지하도록 응용 프로그램 프로세서의 MMU(메모리 관리 유닛)가 구성됩니다.

재구성을 방지하기 위해 시동 프로세스가 완료된 후 KIP를 활성화하는 데 사용된 하드웨어가 잠깁니다.

빠른 권한 제한

Apple A11 Bionic 및 S3 SoC부터는 새로운 하드웨어 프리미티브가 도입되었습니다. 빠른 권한 제한인 이 프리미티브에는 스레드당 권한을 빠르게 제한하는 CPU 레지스터가 포함되어 있습니다. 빠른 권한 제한(또는 APRR 레지스터)으로 지원되는 운영 체제는 시스템 호출 및 페이지 테이블 워크 또는 플러시 비용을 들이지 않고 메모리에서 실행 권한을 제거할 수 있습니다. 이러한 레지스터는 웹에서 발생하는 공격, 특히 런타임 동안 컴파일된 코드(Just In Time compiled)에 대해 한 단계 더 추가된 보완 기능을 제공합니다. 메모리는 메모리를 읽거나 기록할 때와 동시에 효과적으로 실행될 수 없기 때문입니다.

시스템 보조 프로세서 무결성 보호

보조 프로세서 펌웨어는 Secure Enclave, 이미지 센서 프로세서 및 동작 인식 보조 프로세서와 같은 여러 중요한 시스템 작업을 처리합니다. 따라서 보조 프로세서 펌웨어의 보안은 전체 시스템 보안의 핵심입니다. Apple은 보조 프로세서 펌웨어가 변경되는 것을 방지하기 위해 **시스템 보조 프로세서 무결성 보호(SCIP)**라는 메커니즘을 사용합니다.

SCIP는 다음과 같은 점에서 커널 무결성 보호(KIP)와 매우 유사합니다. 시동 시 iBoot는 각 보조 프로세서의 펌웨어를 KIP 영역과 별도로 구분되는 영역인 보호되는 메모리 영역으로 로드합니다. iBoot는 각 보조 프로세서의 메모리 유닛을 구성하여 다음을 방지합니다.

- 보호되는 메모리 영역의 해당 부분 외부에서 실행 가능한 매핑
- 보호되는 메모리 영역의 해당 부분 내부에서 쓰기 가능한 매핑

또한 시동 시 Secure Enclave에 대한 SCIP를 구성하기 위해 Secure Enclave 운영 체제가 사용됩니다. 시동 프로세스가 완료되면 SCIP를 활성화하는 데 사용된 하드웨어가 잠깁니다. 이는 재구성을 방지하기 위한 것입니다.

포인터 인증 코드

PAC(포인터 인증 코드)는 메모리 손상 버그 악용으로부터 보호하기 위해 사용됩니다. 시스템 소프트웨어와 내장 앱은 PAC를 사용하여 함수 포인터와 반환 주소(코드 포인터)의 수정을 방지합니다. PAC는 5개의 128비트 비밀 값을 사용하여 커널 지침 및 데이터에 서명하고, 각 사용자 공간 프로세스는 고유한 B 키를 지닙니다. 항목은 아래와 같이 암호로 솔트되고 서명됩니다.

항목	키	솔트
함수 반환 주소	IB	저장 장치 주소
함수 포인터	IA	0
블록 호출 함수	IA	저장 장치 주소
Objective-C 메소드 캐시	IB	저장 장치 주소 + 클래스 + 선택자
C++ V-Table 엔트리	IA	저장 장치 주소 + 해시(훼손된 메소드 이름)
계산된 Goto 레이블	IA	해시(함수 이름)
커널 스레드 상태	GA	•
사용자 스레드 상태 레지스터	IA	저장 장치 주소
C++ V-Table 포인터	DA	0

서명 값은 64비트 포인터의 상단에 있는 사용되지 않은 패딩 비트에 저장됩니다. 서명은 사용 전에 확인되며, 패딩은 작동하는 포인터 주소를 확인하기 위해 복원됩니다. 확인에 실패하면 작업이 중단됩니다. 이 확인 과정은 스택에 저장된 함수 반환 주소를 조작하는 방식으로 기기를 악의적으로 속여 기존 코드를 실행하게끔 시도하는 ROP(Return Oriented Programming) 공격과 같은 여러 공격을 감행하기 어렵게 만듭니다.

페이지 보호 레이어

iOS, iPadOS 및 watchOS의 PPL(페이지 보호 레이어)은 코드 서명 확인이 완료된 후 사용자 공간 코드가 수정되지 않도록 방지하기 위해 설계되었습니다. 커널 무결성 보호 및 빠른 권한 제한에 기반하여, PPL은 페이지 테이블 권한 오버라이드를 관리하여 PPL만 사용자 코드 및 페이지 테이블을 포함하는 보호된 페이지를 변경할 수 있도록 합니다. 이 시스템은 침해된 커널이 있더라도 시스템 전반 코드 무결성 시행을 지원하여 공격 표면을 크게 줄입니다. PPL은 실행된 모든 코드가 반드시 서명되어야 하는 시스템에서만 적용할 수 있기 때문에 이 보호 기능은 macOS에서는 제공되지 않습니다.

보안 페이지 테이블 모니터 및 신뢰하는 실행 모니터

보안 페이지 테이블 모니터(SPTM) 및 신뢰하는 실행 모니터(TXM)를 함께 사용하면 공격자가 커널 쓰기 기능을 가지고 있고 제어 흐름 보호를 우회할 수 있는 경우에도 사용자와 커널 프로세스 둘 다의 페이지 테이블이 수정되지 않도록 보호할 수 있습니다. SPTM은 커널보다 높은 권한 수준을 활용하고 코드 실행을 관리하는 정책을 실제로 시행하기 위해 낮은 권한을 가진 TXM을 활용하여 이를 수행합니다. 이 시스템은 이러한 권리 분리 및 권한 간 신뢰 관리에 의해 TXM 손상이 자동으로 SPTM 우회로 이어지지 않도록 설계되었습니다. A15, A16 및 A17 SOC에서 SPTM(TXM과 조합)은 PPL을 대체하여, 시동 초기에도 커널 신뢰에 의존하지 않는 더 작은 공격 표면을 제공합니다. 또한 SPTM은 PPL이 활용하는 빠른 권한 제한을 발전시킨 새로운 실리콘 프리미티브에 의존합니다.

안전하게 데이터 연결 활성화하기

iPhone 및 iPad 기기와 Mac 컴퓨터에서 최근에 데이터 연결이 설정되지 않은 경우 Thunderbolt, USB, Lightning, Smart Connector 또는 SD Extended Capacity 'SDXC' 카드 인터페이스(macOS 13.3 이상)를 통한 데이터 연결을 활성화하려면 사용자는 Face ID, Touch ID 또는 암호를 사용해야 합니다. 이를 통해 악성 충전기 등의 기기가 물리적으로 연결되었을 때 공격 표면을 줄일 수 있으며, 적절한 제한 시간 내에 다른 액세서리를 계속 사용할 수 있습니다. iPhone 또는 iPad가 잠기거나 액세서리의 데이터 연결이 중단된 지 한 시간 이상이 지나면 기기의 잠금이 해제될 때까지 기기는 새로운 데이터 연결을 허용하지 않습니다. 이 한 시간 동안에는, 이전에 잠금 해제 상태의 기기에 연결된 적이 있는 액세서리의 데이터 연결만 허용됩니다. 이렇게 연결된 액세서리는 마지막으로 연결된 날로부터 30일 동안 저장됩니다. 이 시간 동안 알 수 없는 액세서리를 사용하여 데이터 연결을 열려고 시도하는 경우, 해당 기기가 다시 잠금 해제되기 전까지 이러한 연결을 통한 모든 액세서리 데이터 연결이 비활성화됩니다. 이 시간 동안에는 다음이 해당됩니다.

- Mac 또는 PC, 액세서리, CarPlay 유선 환경에 자주 연결하는 사용자가 기기를 연결할 때마다 암호를 입력하지 않아도 됩니다.
- 액세서리 생태계는 데이터 연결을 구축하기 전에 액세서리를 식별하는 신뢰할 수 있는 암호화 방식을 제공하지 않기 때문에 이 시간이 필요합니다.

또한 액세서리로 데이터 연결이 구축된 지 3일이 지난 경우, 기기가 잠기는 즉시 새로운 데이터 연결을 허용하지 않습니다. 이는 이러한 액세서리를 자주 사용하지 않는 사용자를 더 잘 보호하기 위함입니다. 기기에서 생체 인증을 다시 활성화하기 위해 암호를 입력해야 하는 경우에는 항상 이러한 데이터 연결도 비활성화됩니다.

사용자는 설정에서 다시 활성화 시에 항상 데이터 연결을 켜도록 선택할 수 있습니다(일부 보조 기기는 자동으로 이렇게 설정됨).

iPhone 및 iPad의 액세서리 확인하기

Made for iPhone, iPad(MFi) 라이선스 프로그램은 심사를 통과한 액세서리 생산 업체에게 iPod 액세서리 프로토콜(iAP) 및 필수 지원 하드웨어 구성요소에 대한 권한을 부여합니다.

MFi 액세서리가 iPhone 또는 iPad와 통신하는 경우 해당 액세서리는 심사를 통과했다는 점을 Apple에 증명해야 합니다. (액세서리와 기기 간 연결은 Thunderbolt, Lightning, Bluetooth 또는 특정 기기의 경우 USB-C를 사용합니다.) 액세서리는 기기에 Apple에서 제공한 인증서를 승인 증명 자료로 전송하고 기기는 이를 확인합니다. 그리고 기기가 보내는 확인 요청에 액세서리는 서명된 응답을 보내야만 합니다. 이 프로세스는 전적으로 Apple이 액세서리 생산 업체에 제공하는 커스텀 IC(집적 회로)에 의해 처리되며 액세서리 자체에서는 이 과정을 인지하지 못합니다.

확인된 MFi 액세서리는 여러 전송 방식과 기능에 대한 접근을 요청할 수 있습니다. 예를 들어, Thunderbolt 케이블을 통한 디지털 오디오 스트림 또는 Bluetooth를 통해 제공되는 위치 정보 등이 있습니다. 인증 IC는 승인된 MFi 액세서리만 기기에 대한 전체 접근 권한을 갖도록 지원하기 위해 설계되었습니다. 액세서리가 인증을 지원하지 않으면 액세서리는 시리얼(UART) 오디오 재생 제어의 일부 및 아날로그 오디오에 접근할 수 있는 권한만을 가지도록 제한됩니다.

AirPlay도 인증 IC를 사용해 수신 기기가 Apple의 승인을 받았는지 확인합니다. AirPlay 오디오 및 CarPlay 비디오 스트림은 CTR(카운터) 모드의 AES128을 사용해 액세서리와 기기간의 통신을 암호화하는 MFi-SAP(보안 연계 프로토콜)을 사용합니다. ECDH 키 교환(Curve25519)을 사용하여 임시 키가 교환되고 인증 IC의 1024비트 RSA 키를 STS(Station-to-Station) 프로토콜의 부분으로 사용해 서명됩니다.

메시지 앱 및 IDS용 BlastDoor

iOS, iPadOS, macOS 및 watchOS는 **BlastDoor**라는 보안 경감 매커니즘을 포함합니다. 이는 iOS 14 및 관련 릴리즈에서 처음 도입되었습니다. BlastDoor의 목표는 공격자를 가둬서 공격자가 메시지 앱 및 Apple IDS(Identity Service)를 악용하려고 할 때 복잡성을 높여 시스템을 보호하는 것입니다. BlastDoor는 메지시 앱, IDS 및 기타 경로로 들어오는 신뢰할 수 없는 데이터를 격리, 분석, 트랜스코딩 및 확인하여 공격을 방지하도록 지원합니다.

이를 위해 BlastDoor는 샌드박스 제한 및 출력에 대한 메모리 안전 검증을 적용하여 공격자가 운영 체제의 다른 부분에 도달하기 위해 처리해야 하는 어려운 장애물을 생성합니다. 이는 사용자를 공격으로부터, 특히 사용자 상호 작용이 필요 없는 '제로 클릭' 공격에서 보호하기 위한 능력을 크게 향상하도록 설계되었습니다.

마지막으로, 메시지 앱은 '알고 있는 발신자'와 '알 수 없는 발신자'의 트래픽을 다르게 처리하여 각 그룹에 서로 다른 기능 세트를 제공하고 '알고 있는 발신자'와 '알 수 없는 발신자'의 데이터를 구별된 BlastDoor 인스턴스로 보냅니다.

Apple 기기용 차단 모드 보안

차단 모드는 사용자의 신원이나 활동으로 인해 표적화된 용병 스파이웨어와 같은 가장 정교한 디지털 위협의 개인적 표적이 될 수 있는 극소수의 개인을 위해 설계된 선택적이고 극단적인 보호 기능입니다. 대부분의 사람은 이러한 공격 유형의 대상이 되지 않습니다.

차단 모드가 켜져 있을 때 기기는 평소와 같은 방식으로 작동하지 않습니다. 악용될 수 있는 공격 표면을 줄이기 위해 특정 앱, 웹 사이트 및 기능이 엄격히 제한되어 보안을 지키며, 일부 경험은 아예 사용할 수 없을 수도 있습니다.

차단 모드는 iOS 16, iPadOS 16, macOS 13 및 watchOS 10 이상에서 사용 가능합니다. 추가 보호 기능은 iOS 17, iPadOS 17, macOS 14 및 watchOS 10.1 이상의 업데이트에서 사용 가능합니다. 차단 모드의 추가 기능을 사용하려면 기기를 최신 운영 체제로 업데이트해야 합니다. 자세한 내용은 Apple 지원 문서 차단 모드에 관하여를 참조하십시오.

차단 모드는 보안을 향상하는 대신 기능, 성능 또는 둘 모두를 저하시킵니다. 이는 다음과 같은 항목에 영향을 미칩니다.

- 백그라운드 서비스
- 연결성
- 기기 관리
- FaceTime
- GameCenter
- Mail
- 메시지 앱
- 사진 앱
- Safari
- 시스템 설정
- WebKit

추가 macOS 시스템 보안 기능

추가 macOS 시스템 보안 기능

macOS는 더 광범위한 하드웨어 세트(예 : Intel 기반 CPU, Apple T2 보안 칩이 탑재된 Intel 기반 CPU 및 Apple Silicon 기반 SoC)에서 작동하며 다양한 범용 컴퓨팅 사용 사례를 지원합니다. 일부 사용자들은 기본적으로 미리 설치된 앱이나 App Store에서 다운받을 수 있는 앱만 사용하는 반면, 커널 해커는 가장 높은 신뢰 단계에서와 실행 코드를 실행하고 테스트하기 위해 기본적으로 모든 플랫폼 보호를 비활성화합니다. 대부분의 사용자는 그 중간 정도에 있으며, 이들 중 다수는 다양한 방법으로 접근해야 하는 주변기기와 소프트웨어를 가지고 있습니다. Apple은 하드웨어, 소프트웨어 및 서비스에 대한 통합적 접근 방식으로 macOS 플랫폼을 설계했습니다. 이는 설계에 의한 보안을 제공하고 구성, 배포 및 관리가 간단하면서도 사용자가 기대하는 구성 가능성은 유지하는 플랫폼입니다. macOS에는 IT 전문가가 기업 데이터를 보호하고 안전한 기업 네트워크 환경 내에서 통합하는 데 필요한 주요 보안 기술이 포함되어 있습니다.

다음 기능은 macOS 사용자의 다양한 요구 사항을 지원하고 보호합니다. 그 기능은 다음과 같습니다.

- 서명된 시스템 볼륨 보안
- 시스템 무결성 보호
- 신뢰 캐시
- 주변기기 보호
- Apple Silicon이 탑재된 Mac용 Rosetta 2(자동 변환) 지원 및 보안
- DMA 지원 및 보호
- KEXT(커널 확장 프로그램) 지원 및 보안
- 옵션 ROM 지원 및 보안
- Intel 기반 Mac 컴퓨터용 UEFI 펌웨어 보안

시스템 무결성 보호

macOS는 커널 권한을 활용하여 **시스템 무결성 보호(SIP)** 기능으로 중요한 시스템 파일의 쓰기 가능성을 제한합니다. 이 기능은 Apple Silicon이 탑재된 Mac에서 사용 가능한 하드웨어 기반 커널 무결성 보호(KIP)와는 별개로 추가되었으며, 메모리에서 커널 수정을 보호합니다. 강제적 접근 제어 기술을 활용하여 샌드박스 및 Data Vault를 포함한 여러 커널 수준 보호 기능을 제공합니다.

강제적 접근 제어

macOS는 개발자가 만든 보안 제한을 덮어쓸 수 없는 정책인 강제적 접근 제어를 사용합니다. 이 방식은 사용자가 자신의 환경설정에 따라 보안 정책을 덮어쓸 수 있는 임의 접근 제어와는 다릅니다.

강제적 접근 제어는 사용자에게 보이지는 않지만 샌드박스, 유해 콘텐츠 차단, 관리되는 환경설정, 확장 프로그램 및 시스템 무결성 보호를 비롯한 여러 가지 중요한 기능을 지원하는 기본 기술입니다.

시스템 무결성 보호

시스템 무결성 보호는 악성 코드가 구성요소를 수정하지 못하도록 특정 중요 파일 시스템 위치에서 구성요소를 읽기 전용으로 제한합니다. 시스템 무결성 보호는 사용자가 OS X 10.11 이상으로 업그레이드하는 경우 기본적으로 켜지는 컴퓨터별 설정입니다. Intel 기반 Mac에서 이를 비활성화하면 물리적 저장 장치의 모든 파티션에 대한 보호 기능이 제거됩니다. macOS는 프로세스가 샌드박스되어 실행되는지 아니면 관리자 권한을 가지고 실행되는지와 상관없이 시스템에서 실행 중인 모든 프로세스에 이 보안 정책을 적용합니다.

신뢰 캐시

보안 시동 체인에 포함된 개체 중 하나는 정적 신뢰 캐시로, 서명된 시스템 볼륨에 마스터되는 모든 Mach-O 바이너리의 신뢰하는 레코드입니다. 각 Mach-O는 코드 디렉토리 해시로 표현됩니다. 효율적인 검색을 위해 이러한 해시는 신뢰 캐시에 넣기 전에 정렬됩니다. 코드 디렉토리는 `codesign(1)`에 의해 수행된 서명 작업의 결과입니다. 신뢰 캐시를 실행하려면 SIP을 활성화해야 합니다. Apple Silicon이 탑재된 Mac에서 신뢰 캐시 실행을 비활성화하려면 보안 시동이 최소 보안으로 구성되어야 합니다.

바이너리가 실행되면 새로운 프로세스 생성 또는 기존 프로세스에 실행 코드를 매핑하는 작업의 일부로서 해당 코드 디렉토리가 추출되고 해시됩니다. 결과 해시가 신뢰 캐시에서 발견되는 경우, 바이너리에 대해 생성된 실행 가능한 매핑에 플랫폼 권한이 부여됩니다. 즉, 서명의 진위 여부에 대한 추가 확인 없이 권한을 소유하고 이행할 수 있습니다. 이는 바이너리에 서명하는 Apple 인증서를 통해 플랫폼 권한이 운영 체제 콘텐츠에 전달되는 Intel 기반 Mac과는 대조적입니다. (이 인증서는 바이너리가 소유하는 권한을 제한하지 않음.)

비플랫폼 바이너리(예 : 공증된 타사 코드)를 실행하려면 유효한 인증서 체인이 있어야 하며, Apple Developer Program에서 개발자에게 발급한 서명 프로파일에 의해 소유할 수 있는 권한이 제한됩니다.

macOS에 포함된 모든 바이너리는 **플랫폼 식별자**로 서명됩니다. Apple Silicon이 탑재된 Mac에서 이 식별자는 Apple에서 바이너리에 서명한 경우에도, 실행하려면 해당 코드 디렉토리 해시가 신뢰 캐시에 있어야 한다는 것을 나타내는 데 사용됩니다. Intel 기반 Mac에서 플랫폼 식별자는 이전 릴리즈의 macOS에서 바이너리의 해지를 수행합니다. 이는 최신 버전에서 바이너리가 실행되지 않도록 방지하는 데 사용됩니다.

정적 신뢰 캐시는 주어진 macOS 버전에 바이너리 세트를 완전히 잠급니다. 이러한 동작으로 공격자가 이점을 얻을 수 있도록 이전 운영 체제에서 합법적으로 Apple이 서명한 바이너리가 새로운 운영 체제에 도입되는 것을 방지할 수 있습니다.

운영 체제 외부에 제공된 플랫폼 코드

Apple은 플랫폼 식별자로 서명되지 않은 일부 바이너리(예: Xcode 및 개발 도구 스택)를 제공합니다. 그러한 경우에도 Apple Silicon이 탑재된 Mac 및 T2 칩이 탑재된 Mac에서 플랫폼 권한으로 바이너리를 실행하도록 허용됩니다. 이 플랫폼 소프트웨어는 macOS와 별도로 제공되기 때문에 정적 신뢰 캐시에 의해 부과되는 해지 동작에 영향을 받지 않습니다.

로드 가능한 신뢰 캐시

Apple은 **로드 가능한 신뢰 캐시**가 있는 특정 소프트웨어 패키지를 제공합니다. 이러한 캐시는 정적 신뢰 캐시와 동일한 데이터 구조를 갖습니다. 하지만 정적 신뢰 캐시는 하나뿐이며, 커널의 초기 초기화가 완료된 후 해당 콘텐츠가 항상 읽기 전용 범위로 잠기도록 보장하지만 로드 가능한 신뢰 캐시가 런타임 동안 시스템에 추가됩니다.

이러한 신뢰 캐시는 시동 펌웨어를 인증하는 동일 메커니즘(Apple이 신뢰하는 서명 서비스를 사용하여 개인 맞춤화)을 통하거나 전역 서명된 개체(대상체의 서명이 특정 기기에 바인딩하지 않음)로 인증됩니다.

개인 맞춤화된 신뢰 캐시의 예로 Apple Silicon이 탑재된 Mac에서 현장 진단을 수행하는 데 사용되는 디스크 이미지와 함께 제공되는 캐시가 있습니다. 이 신뢰 캐시는 디스크 이미지와 함께 개인 맞춤화되며 진단 모드로 시동되는 동안 대상 Mac 컴퓨터의 커널에 로드됩니다. 신뢰 캐시는 디스크 이미지 내의 소프트웨어를 플랫폼 권한으로 실행할 수 있도록 합니다.

전역 서명된 신뢰 캐시의 예시가 macOS 소프트웨어 업데이트와 함께 제공됩니다. 이 신뢰 캐시는 소프트웨어 업데이트(**업데이트 브레인**) 내의 코드 청크가 플랫폼 권한으로 실행되는 것을 허용합니다. 업데이트 브레인은 호스트 시스템이 여러 버전에서 일관된 방식으로 수행할 용량이 부족한 소프트웨어 업데이트를 준비하는 모든 작업을 수행합니다.

Mac 컴퓨터의 주변기기 프로세서 보안

현대 컴퓨팅 시스템에는 네트워킹, 그래픽, 전원 관리 등과 같은 작업을 전담하는 다양한 내장 주변기기 프로세서가 있습니다. 일반적으로 이러한 주변기기 프로세서는 단일 목적으로 구성되며, 기본 CPU보다 훨씬 덜 강력합니다. 충분한 보안을 구현하지 않는 내장 주변 기기는 공격자가 더욱 쉽게 악용할 수 있는 대상이 되며, 공격자는 이를 통해 계속하여 운영 체제를 감염시킬 수 있습니다. 주변기기 프로세서 펌웨어를 감염시킨 후 공격자는 기본 CPU의 소프트웨어를 공격 대상으로 삼거나 중요한 데이터를 직접 캡처할 수 있습니다(예: 이더넷 기기는 암호화되지 않은 패킷의 콘텐츠를 볼 수 있음).

가능한 경우 Apple은 필요한 주변기기 프로세서 수를 줄이고 펌웨어가 필요한 설계를 피하고자 노력합니다. 하지만 자체 펌웨어와 함께 별도의 프로세서가 필요한 경우에는 공격자가 해당 프로세서를 계속 감염시킬 수 없도록 조치하고 있습니다. 이는 다음 두 가지 중 하나의 방법으로 프로세서를 검증하여 가능합니다.

- 시동 시 기본 CPU에서 확인된 펌웨어를 다운로드하도록 프로세서 실행하기
- Mac 시동 시마다 주변 기기 프로세서 펌웨어를 검증하기 위해 주변 기기 프로세서가 자체 보안 시동 체인을 구현하도록 하기

Apple은 공급 업체와 협력하여 구현을 검사하고 다음과 같은 원하는 속성을 포함하도록 설계를 개선합니다.

- 최소 암호화 강도 보장
- 알려진 불량 펌웨어의 강력한 폐기 보장
- 디버그 인터페이스 비활성화
- Apple이 제어하는 HSM(하드웨어 보안 모듈)에 저장된 암호화 키를 사용하여 펌웨어에 서명하기

최근 몇 년 동안 Apple은 일부 외부 공급업체와 협력하여 Apple Silicon에서 사용하는 것과 동일한 'Image4' 데이터 구조, 확인 코드 및 서명 인프라를 적용했습니다.

저장 장치가 필요 없는 작업이나 저장 장치 + 보안 시동이 모두 옵션이 아닌 경우, 영구 저장 장치를 업데이트하기 전에 펌웨어 업데이트를 암호화하여 서명하고 검증해야 합니다.

Apple Silicon이 탑재된 Mac의 Rosetta 2

Apple Silicon이 탑재된 Mac은 **Rosetta 2**라는 변환 메커니즘을 사용하여 x86_64 명령 세트에 대해 컴파일된 코드를 실행할 수 있습니다. Just In Time 및 Ahead Of Time라는 두 가지 유형의 변환이 있습니다.

Just In Time 변환

JIT(Just In Time) 변환 파이프라인, x86_64 Mach 개체는 이미지 실행 경로의 초기에 확인됩니다. 이러한 이미지가 발견되면 커널은 동적 링크 에디터인 `dyld(1)`가 아닌 특수 Rosetta 변환 스텁으로 제어 권한을 전송합니다. 그러면 변환 스텁은 이미지 실행 도중 x86_64 페이지를 변환합니다. 이러한 변환은 전적으로 프로세스 내에서 이루어집니다. 커널은 페이지 오류 발생에 따라 바이너리에 첨부된 코드 서명에 대해 각 x86_64 페이지의 코드 해시를 계속 확인합니다. 해시 불일치가 발생하는 경우 커널은 해당 프로세스에 적절한 교정 정책을 시행합니다.

Ahead Of Time 변환

AOT(Ahead Of Time) 변환 경로인 x86_64 바이너리는 시스템이 해당 코드의 반응성에 대해 최적이라고 판단될 때 저장 장치에서 읽히게 됩니다. 변환된 아티팩트는 특수한 유형의 Mach 개체 파일로 저장 장치에 기록됩니다. 해당 파일은 실행 가능 이미지와 유사하지만 다른 이미지의 변환된 결과물임을 뜻하는 정보가 있습니다.

이 모델에서 AOT 아티팩트는 모든 ID 정보를 원본 x86_64 실행 가능 이미지에서 파생합니다. 이 바인딩을 시행하기 위해 권한이 있는 사용자 공간 항목은 Secure Enclave에서 관리하는 기기별 키를 사용하여 변환 아티팩트에 서명합니다. 이 키는 제한된 권한을 사용하여 식별되는 권한이 있는 사용자 공간 항목에만 공개됩니다. 변환 아티팩트에 대해 생성된 코드 디렉토리에는 원본 x86_64 실행 가능 이미지의 코드 디렉토리 해시가 포함됩니다. 변환 아티팩트 자체에 있는 서명을 **보조 서명**이라고 합니다.

AOT 파이프 라인은 커널은 동적 링크 에디터인 `dyld(1)`가 아닌 Rosetta 런타임으로 제어를 전송하면서 JIT 파이프 라인과 유사하게 시작됩니다. 하지만 Rosetta 런타임은 IPC(프로세스 간 통신) 쿼리를 Rosetta 시스템 서비스로 전송하여 현재 실행 가능 이미지에 대해 사용 가능한 AOT 변환이 있는지 묻습니다. 있는 경우, Rosetta 서비스는 해당 변환에 대한 핸들을 제공하며, 프로세스에 매핑되고 실행됩니다. 실행 중에 커널은 기기별 서명 키에 루트된 서명으로 인증된 변환 아티팩트의 코드 디렉토리 해시를 시행합니다. 원본 x86_64 이미지의 코드 디렉토리 해시는 이 프로세스와 관련이 없습니다.

변환된 아티팩트는 Rosetta 서비스를 제외한 어떤 항목도 런타임에 접근할 수 없는 Data Vault에 저장됩니다. Rosetta 서비스는 읽기 전용 파일 설명자를 개별 변환 아티팩트에 배포하여 캐시에 대한 접근을 관리합니다. 이는 AOT 아티팩트 캐시에 대한 접근을 제한합니다. 이 서비스의 프로세스 간 통신 및 종속 풋프린트는 공격 표면을 제한하기 위해 의도적으로 매우 좁게 유지됩니다.

원본 x86_64 이미지의 코드 디렉토리 해시가 AOT 변환 아티팩트의 서명으로 인코딩된 해시와 일치하지 않는 경우, 이 결과는 잘못된 코드 서명으로 간주되어 적절한 시행 조치가 취해집니다.

원격 프로세스가 AOT로 변환된 실행 파일의 권한 또는 기타 코드 ID 속성을 커널에 쿼리하는 경우, 원본 x86_64 이미지의 ID 속성이 반환됩니다.

정적 신뢰 캐시 콘텐츠

macOS 11 이상은 x86_64 및 arm64 컴퓨터 코드 슬라이스를 포함하는 Mach ‘fat’ 바이너리와 함께 제공됩니다. Apple Silicon이 탑재된 Mac에서 사용자는 다양한 이유로 Rosetta 파이프라인을 통해 시스템 바이너리의 x86_64 슬라이스를 실행하도록 결정할 수 있습니다. 예를 들면 기본 arm64 변형이 없는 플러그인을 로드하기 위한 이유가 있습니다. 이러한 접근을 지원하기 위해 일반적으로 macOS와 함께 제공되는 정적 신뢰 캐시에는 Mach 개체 파일당 3개의 코드 디렉토리 해시가 포함되어 있습니다.

- arm64 슬라이스의 코드 디렉토리 해시
- x86_64 슬라이스의 코드 디렉토리 해시
- x86_64 슬라이스 AOT 변환의 코드 디렉토리 해시

Rosetta AOT 변환 절차는 변환이 수행된 시기 또는 수행된 기기와 상관없이 주어진 입력에 대해 동일한 출력을 재현한다는 면에서 결정론적입니다.

macOS 빌드 도중 모든 Mach 개체 파일은 빌드 중인 macOS 버전과 관련된 Rosetta AOT 변환 파이프라인을 통해 실행되며 결과 코드 디렉토리 해시는 신뢰 캐시에 기록됩니다. 실제 변환된 제품은 효율성을 이유로 운영 체제와 함께 제공되지 않으며 사용자가 요청하는 경우 재구성됩니다.

Apple Silicon이 탑재된 Mac에서 x86_64 이미지가 실행될 때 해당 이미지의 코드 디렉토리 해시가 정적 신뢰 캐시에 있는 경우, 결과 AOT 아티팩트의 코드 디렉토리 해시 **또한** 정적 신뢰 캐시에 있을 것으로 예상됩니다. 이러한 제품은 서명 기관이 Apple 보안 시동 체인에 뿌리를 두고 있기 때문에 기기별 키로 서명되지 않습니다.

서명되지 않은 x86_64 코드

Apple Silicon이 탑재된 Mac은 유효한 서명이 첨부되지 않으면 기본 arm64 코드 실행을 허용하지 않습니다. 이 서명은 비대칭 키 쌍의 감춰진 절반에서 실제 신원을 가지고 있지 않은 ‘임시’ 코드 서명 (`codesign(1)`와 비교 시)처럼 간단할 수 있습니다(단순히 바이너리의 인증되지 않은 측정임).

바이너리 호환성을 위해 변환된 x86_64 코드는 서명 정보가 전혀 없어도 Rosetta를 통해 실행되도록 허용됩니다. 기기별 Secure Enclave 서명 절차를 통해 이 코드에 특정 ID가 전달되지 않으며 Intel 기반 Mac에서 실행되는 서명되지 않은 기본 코드와 정확히 동일한 제한으로 실행됩니다.

Mac 컴퓨터의 직접 메모리 접근 보호

PCIe, FireWire, Thunderbolt 및 USB 등 고속 인터페이스의 높은 처리량을 처리하려면 컴퓨터가 주변기기로부터 DMA(직접 메모리 접근)를 지원해야 합니다. 즉, CPU를 계속 사용하지 않고도 RAM을 읽고 쓸 수 있어야 합니다. 2012년부터 Mac 컴퓨터는 DMA를 보호하기 위한 수많은 기술을 구현하여 모든 PC에 가장 우수하며 종합적인 DMA 보호 기능을 제공합니다.

Apple Silicon이 탑재된 Mac의 직접 메모리 접근 보호

Apple SoC(System on Chip)는 PCIe 및 Thunderbolt 포트를 비롯하여 시스템의 각 DMA 에이전트에 대해 IOMMU(입력/출력 메모리 관리 유닛)를 포함합니다. 각 IOMMU는 주소 변환표 집합을 보유하여 DMA 요청을 변환하므로, PCIe 또는 Thunderbolt로 연결된 주변기기는 사용 목적과 명백히 매핑되는 메모리에만 접근할 수 있습니다. 주변기기는 커널이나 펌웨어처럼 시스템의 다른 부분에 속한 메모리 또는 다른 주변기기에 할당된 메모리에 접근할 수 없습니다. 한 IOMMU에서 주변기기가 사용 목적에 매핑되지 않은 메모리에 접근하려는 시도를 감지하면 커널 패닉을 일으킵니다.

Intel 기반 Mac용 직접 메모리 접근 보호

Intel 기반 Mac 컴퓨터에 Intel Virtualization Technology for Directed I/O(VT-d)가 적용되어 있으면 IOMMU를 초기화하여 DMA 재매핑 및 인터럽트 재매핑을 가능케 하므로, 시동 프로세스의 극초기 단계에서 다양한 종류의 보안 취약성을 완화합니다. Apple IOMMU 하드웨어는 기본 거부 정책으로 작동을 시작하여 시스템 전원이 켜지는 순간 자동으로 주변기기의 DMA 요청을 차단합니다. 소프트웨어를 사용한 초기화 후 IOMMU는 주변기기 사용 목적과 명백히 매핑된 메모리 영역으로 해당 기기의 DMA 요청을 허용하기 시작합니다.

참고: 각 IOMMU가 그 주변기기에 대한 MSI를 처리하기 때문에 Apple Silicon이 탑재된 Mac에서는 PCIe에 대한 인터럽트 재매핑이 필요하지 않습니다.

macOS 11부터 Apple T2 보안 칩이 탑재된 모든 Mac 컴퓨터는 UEFI 드라이버를 실행하며, 이러한 드라이버가 외부 기기와 페어링될 때 제한된 ring 3 환경에서 DMA를 제공합니다. 이 속성은 시동 시 악성 기기가 예기치 못한 방법으로 UEFI 드라이버와 통신할 경우 발생할 수 있는 보안 취약성을 완화하는 데 도움이 됩니다. 특히 DMA 버퍼의 드라이버 처리 시 취약성의 영향을 줄여줍니다.

macOS에서 안전하게 커널 확장하기

macOS 11부터, 타사 KEXT(커널 확장 프로그램)를 활성화한 경우 요청 시 KEXT가 커널에 로드되지 않습니다. 대신 KEXT가 시동 프로세스 동안 로드되는 **AuxKC(보조 커널 모음)**에 병합됩니다. Apple Silicon이 탑재된 Mac에서 AuxKC의 측정값은 LocalPolicy로 서명되며, 이전 하드웨어의 경우 AuxKC가 데이터 볼륨에 남아있게 됩니다. AuxKC를 다시 빌드하려면 변경 사항을 커널에 로드하기 위해 사용자의 승인 및 macOS 재시동이 필요하며 보안 시동을 부분 보안으로 구성해야 합니다.

중요사항: macOS에서 KEXT는 더 이상 권장되지 않습니다. KEXT는 운영 체제의 무결성과 신뢰성을 위협하기 때문에 Apple은 사용자가 커널 확장이 필요 없는 솔루션을 우선적으로 선택하기를 추천합니다.

Apple Silicon이 탑재된 Mac의 커널 확장 프로그램

Apple Silicon이 탑재된 Mac에서 커널 확장 프로그램을 사용하도록 설정하려면 시동 시 전원 버튼을 눌러 1TR(One True Recovery) 모드에 진입한 다음, 부분 보안으로 다운그레이드하고 체크상자를 선택하여 KEXT를 확실하게 활성화해야 합니다. 또한, 이 작업을 수행하려면 관리자 암호를 입력하여 다운그레이드를 승인해야 합니다. 1TR 및 암호 요구 사항이 조합되어 macOS 내에서 출발하는 소프트웨어 전용 공격자가 macOS에 KEXT를 심고 이를 악용하여 커널 권한을 얻기가 어려워집니다.

사용자가 KEXT를 로드하도록 승인한 후에 앞서 언급한 사용자 승인 커널 확장 프로그램 로딩 흐름이 KEXT 설치를 승인하는 데 사용됩니다. 이 흐름에 사용되는 승인은 LocalPolicy에서 UAKL(사용자 승인 KEXT 목록)의 SHA384 해시를 캡처하는 데 활용되기도 합니다. 그러면 `kmd`(커널 관리 데몬)가 UAKL에서 찾은 KEXT만 검증하고 AuxKC에 포함시킵니다.

- SIP(시스템 무결성 보호)가 활성화된 경우 각 KEXT의 서명이 확인되고 나서 AuxKC에 포함됩니다.
- SIP가 비활성화되면 KEXT 서명은 실행되지 않습니다.

이 방식은 Apple Developer Program의 일원이 아닌 개발자 또는 사용자가 서명되지 않은 KEXT를 테스트할 수 있는 최소 보안 흐름을 허용합니다.

AuxKC가 생성되면 AuxKC 측정값이 Secure Enclave로 보내져 서명되어 시동 시 iBoot에서 평가할 수 있는 Image4 데이터 구조에 포함됩니다. AuxKC 구조의 일부로 KEXT 영수증도 함께 생성됩니다. 이 영수증은 AuxKC에 실제로 포함되는 KEXT 목록을 포함하는데, 금지된 KEXT가 발생하면 이 집합이 UAKL의 하위 집합이 될 수 있기 때문입니다. AuxKC Image4 데이터 구조의 SHA384 해시와 KEXT 영수증은 LocalPolicy에 포함됩니다. AuxKC Image4 해시는 시동 시 iBoot가 시행하는 추가적인 확인에 사용되어 최신 LocalPolicy로 이전 Secure Enclave에서 서명한 AuxKC Image4 파일을 시동할 가능성이 없는지 확인합니다. KEXT 영수증은 Apple Pay와 같은 하위 시스템에서 사용되어 현재 로드된 KEXT 중에 macOS의 신뢰성을 훼손하여 KEXT가 있는지 파악합니다. 만약 있다면 Apple Pay 기능이 비활성화됩니다.

시스템 확장 프로그램

macOS 10.15 버전은 개발자가 커널 수준이 아닌 사용자 공간에서 실행되는 시스템 확장 프로그램을 설치하고 관리하여 macOS의 기능을 확장할 수 있도록 합니다. 시스템 확장 프로그램은 사용자 공간에서 실행되어 macOS의 안정성과 보안을 향상합니다. KEXT에는 기본적으로 전체 운영 체제에 대한 전체 접근 권한이 있지만 사용자 공간에서 실행되는 확장 프로그램의 경우 지정된 기능을 수행하는 데 필요한 권한만 부여됩니다.

개발자는 KEXT를 작성할 필요 없이 DriverKit, EndpointSecurity 및 NetworkExtension을 포함한 프레임워크를 사용하여 USB 및 휴먼 인터페이스 드라이버, 엔드포인트 보안 도구(데이터 손실 방지 또는 기타 엔드포인트 에이전트 등), VPN 및 네트워크 도구에 쓰기를 수행할 수 있습니다. 이러한 API 사용에 장점이 있거나, 해당 API로 전환하고 커널 확장 프로그램에서 벗어날 수 있는 강력한 로드맵이 있는 경우에만 타사 보안 에이전트를 사용해야 합니다.

사용자 승인 커널 확장 프로그램 로딩

보안을 향상하기 위해 macOS 10.13 버전이 설치되어 있거나, 설치한 후에 커널 확장 프로그램을 로드할 때 사용자 동의가 필요합니다. 이 프로세스를 **사용자 승인 커널 확장 프로그램 로딩(User-Approved Kernel Extension Loading)**이라고 합니다. 커널 확장 프로그램을 승인하려면 관리자 권한이 필요합니다. 다음과 같은 경우에는 커널 확장 프로그램 승인이 필요하지 않습니다.

- macOS 10.12 또는 이전 버전을 실행하는 Mac에 커널 확장 프로그램이 설치된 경우
- 이전에 승인된 확장 프로그램을 대치하는 경우
- Mac이 복구용 OS에서 시동될 때 사용 가능한 `spctl` 명령어 라인 도구를 사용하여 사용자 동의 없이 로드를 허용한 경우
- MDM(모바일 기기 관리) 구성을 사용하여 로드를 허용한 경우

  macOS 10.13.2부터, 사용자는 MDM을 사용하여 사용자 동의 없이 로드되는 커널 확장 프로그램 목록을 지정할 수 있습니다. 이 옵션을 사용하려면 Apple School Manager, Apple Business Manager 또는 사용자가 수행한 MDM 등록을 통해 MDM에 등록된 macOS 10.13.2 버전을 실행하는 Mac이 필요합니다.

macOS의 옵션 ROM 보안

참고: Apple Silicon이 탑재된 Mac에서는 현재 옵션 ROM이 지원되지 않습니다.

Apple T2 보안 칩이 탑재된 Mac의 옵션 ROM 보안

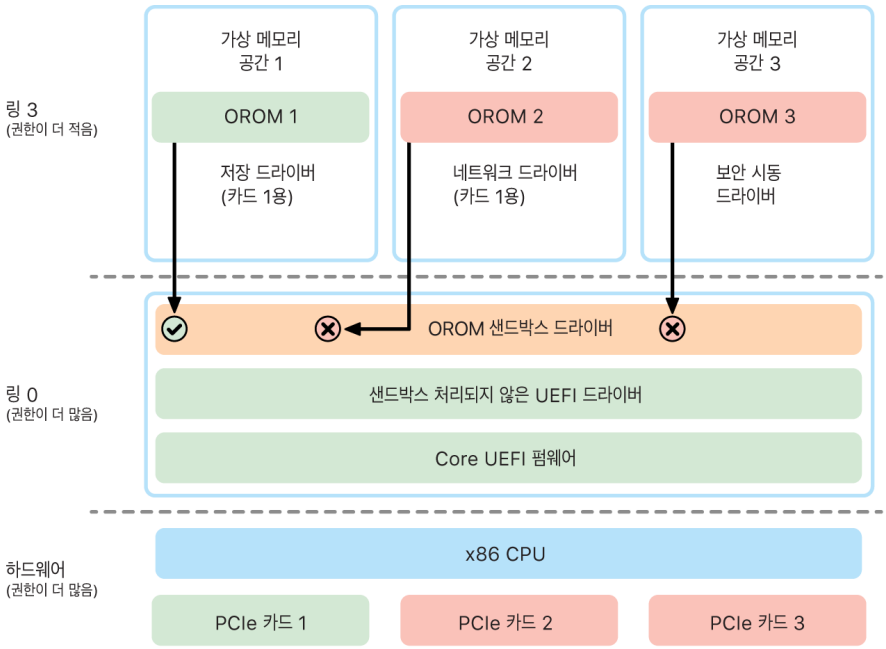
Thunderbolt 및 PCIe 기기는 물리적으로 기기에 탑재된 '옵션 ROM'(OROM)을 지닐 수 있습니다. (이는 일반적으로 실제 ROM은 아니며, 펌웨어를 저장하는 다시 쓰기가 가능한 칩입니다.) UEFI 기반 시스템에서 해당 펌웨어는 일반적으로 UEFI 드라이버이며 UEFI 펌웨어에서 읽고 실행합니다. 실행된 코드는 검색된 하드웨어를 초기화하고 구성하여 나머지 펌웨어에서 하드웨어를 사용할 수 있도록 합니다. 이 기능은 전문화된 타사 하드웨어가 초기 시동 단계(예: 외부 RAID 어레이에서 시동) 동안 로드 및 작동하는 데 필요합니다.

하지만 OROM은 일반적으로 다시 쓰기가 가능하기 때문에 공격자가 합법적인 주변기기의 OROM을 덮어쓰면 공격자의 코드가 시동 프로세스 초기에 실행되며, 실행 환경을 조작하여 이후에 로드된 소프트웨어의 무결성을 위반할 수 있습니다. 마찬가지로 공격자가 시스템에 자체 악성 기기를 도입하면 악성 코드가 실행될 수도 있습니다.

2011년 이후 판매된 macOS 10.12.3 버전이 설치된 Mac 컴퓨터의 경우 특수 키 조합을 누르지 않는 한 Mac이 시동될 때 기본적으로 OROM을 실행하지 않도록 동작이 변경되었습니다. 이 키 조합은 macOS 시동 과정에 악의적인 OROM이 실수로 유입되는 것을 방지합니다. 사용자가 펌웨어 암호를 설정하면 키 조합을 누르는 경우에도 OROM을 실행할 수 없도록 펌웨어 암호 유틸리티의 기본 동작도 변경되었습니다. 이는 의도적으로 악성 OROM을 도입하는 실제 공격자로부터 보호합니다. 펌웨어 암호가 설정되어 있는 동안에도 OROM을 실행해야 하는 사용자의 경우 macOS의 `firmwarepasswd` 명령어 라인 도구를 사용하여 기본값이 아닌 옵션을 구성할 수 있습니다.

OROM 샌드박스 보안

macOS 10.15 버전에서 UEFI 펌웨어는 OROM 샌드박스 및 이로부터의 권한 취소 메커니즘을 포함하도록 업데이트되었습니다. UEFI 펌웨어는 일반적으로 OROM을 포함한 모든 코드를 'ring 0'이라는 CPU 최대 권한 레벨에서 실행하며, 모든 코드 및 데이터를 위한 단일 공유 가상 메모리 공간을 보유합니다. ring 0은 macOS 커널이 실행되는 권한 수준이며, 더 낮은 권한 수준인 ring 3에서는 앱이 실행됩니다. OROM 샌드박스는 커널처럼 가상 메모리 분리를 사용하고 OROM을 ring 3으로 실행하여 OROM의 권한을 취소했습니다.



샌드박스는 OROM이 호출할 수 있는 인터페이스(커널의 시스템 호출 필터링과 흡사)와 OROM이 등록할 수 있는 기기 유형(앱 승인과 흡사)을 상당히 제한합니다. 이러한 설계의 장점은 악성 OROM이 'ring 0' 메모리 내부의 어디에서도 더 이상 직접 쓰기를 할 수 없다는 것입니다. 대신에 해당 OROM은 매우 좁고 잘 정의된 샌드박스 인터페이스에 제한됩니다. 이 제한된 인터페이스는 공격 표면을 크게 줄이며 공격자가 어쩔 수 없이 먼저 샌드박스에서 벗어나 권한 수준을 높일 수밖에 없도록 합니다.

Intel 기반 Mac의 UEFI 펌웨어 보안

Apple T2 보안 칩이 탑재된 Intel 기반 Mac은 UEFI(Intel) 펌웨어를 사용하여 보안 기능을 제공합니다.

개요

2006년부터 Intel 기반 CPU가 탑재된 Mac 컴퓨터는 EFI(확장 펌웨어 인터페이스) 개발 키트(EDK) 버전1 또는 버전2 기반의 Intel 펌웨어를 사용합니다. EDK2 기반 코드는 UEFi(Unified Extensible Firmware Interface) 사양을 준수합니다. 이 섹션에서 **UEFI 펌웨어**는 Intel 펌웨어를 말합니다. UEFI 펌웨어는 Intel 칩에서 실행되는 첫 번째 코드입니다.

Apple T2 보안 칩이 탑재되지 않은 Intel 기반 Mac의 경우 UEFI 펌웨어의 신뢰 루트는 펌웨어가 저장된 칩입니다. UEFI 펌웨어 업데이트는 저장 장치에 업데이트하기 전에 Apple에서 디지털로 서명하고 펌웨어에 의해 확인됩니다. 롤백 공격을 방지하려면 항상 기존 버전보다 최신 버전인 업데이트가 있어야 합니다. 하지만 Mac에 물리적으로 접근할 수 있는 공격자는 하드웨어를 사용하여 펌웨어 저장 장치 칩에 접근하고 악성 콘텐츠를 포함하도록 칩을 업데이트할 가능성이 있습니다. 마찬가지로 UEFI 펌웨어의 초기 시동 프로세스에서 취약점이 발견되면(저장 장치 칩에 쓰기 제한을 적용하기 전) UEFI 펌웨어가 지속적으로 감염될 수 있습니다. 이는 T2 칩이 탑재되지 않은 모든 Intel 기반 Mac 컴퓨터에 존재하며 대부분의 Intel 기반 PC에서 흔히 나타나는 하드웨어 구조적인 제한입니다.

UEFI 펌웨어를 파괴하는 물리적 공격을 방지하기 위해 Mac 컴퓨터는 T2 칩의 UEFI 펌웨어에 대한 신뢰 루트로 재설계되었습니다. 이 섹션 후반부의 Intel 기반 Mac의 시동 프로세스에서 설명한 것처럼 이러한 Mac 컴퓨터에서는 T2 펌웨어 자체가 UEFI 펌웨어의 신뢰 루트입니다.

Intel 관리 엔진(ME) 하위 구성요소

Intel 관리 엔진(ME) 펌웨어는 UEFI 펌웨어 내에 저장되는 하위 구성 요소 중 하나입니다. 별도의 프로세서이자 Intel 칩 내의 하위 시스템인 ME는 Intel 기반 그래픽만을 사용하는 Mac에서 오디오 및 비디오 저작권 보호에 주로 사용됩니다. Intel 기반 Mac은 구성 요소가 대다수 제거된 커스텀 ME 펌웨어를 실행하여 이러한 하위 구성 요소의 공격 표면을 줄입니다. 그로 인해 만들어진 Mac ME 펌웨어는 Intel이 만든 기본 최소 빌드보다 더 작기 때문에 과거에 보안 연구가들이 공개 공격의 대상으로 간주한 많은 구성 요소들이 더 이상 존재하지 않습니다.

SMM(시스템 관리 모드)

Intel 프로세서에는 정상 작동과는 다른 특수 실행 모드가 있습니다. 이는 **SMM(시스템 관리 모드)**으로 불리며 원래 전원 관리 등 시간에 민감한 작업을 처리하기 위해 도입되었습니다. 하지만 Mac 컴퓨터는 역사적으로 **SMC(시스템 관리 컨트롤러)**라는 별개의 마이크로 컨트롤러를 사용하여 이러한 작업을 수행해왔습니다. SMC는 T2 칩에 통합되어 더 이상 별개의 마이크로 컨트롤러가 아닙니다.

watchOS의 시스템 보안

Apple Watch는 iOS에서 사용하는 것과 동일한 하드웨어 기반 플랫폼 보안 기술을 다수 사용합니다. 예를 들어, Apple Watch에서는 다음과 같은 보안 기술을 제공합니다:

- 보안 시동 및 보안 소프트웨어 업데이트 수행
- 운영 체제 무결성 유지
- 데이터 보안(기기 내 데이터 및 페어링된 iPhone과의 통신 또는 인터넷 통신에서의 데이터 모두)

지원되는 기술에는 시스템 보안(예: KIP, SKP 및 SCIP)에 나열된 기술뿐만 아니라 데이터 보호, 키체인 및 네트워크 기술이 포함됩니다.

watchOS 업데이트하기

watchOS를 밤사이 업데이트하도록 구성할 수 있습니다. Apple Watch 암호가 저장되고 업데이트 도중 사용되는 방식에 대한 자세한 내용은 Keybag을 참조하십시오.

손목 인식

손목 인식이 활성화되어 있는 경우, 해당 기기를 손목에서 제거하면 잠시 후에 자동으로 잠깁니다. 손목 인식이 비활성화되어 있는 경우, 제어 센터는 Apple Watch 잠금 옵션을 제공합니다. Apple Watch가 잠기면 Apple Watch에 암호를 입력해야만 Apple Pay를 사용할 수 있습니다. 손목 인식은 iPhone의 Apple Watch 앱을 사용해 끌 수 있습니다. 이 설정은 또한 MDM(모바일 기기 관리) 솔루션을 사용해 강제로 적용할 수 있습니다.

활성화 잠금

iPhone에 나의 찾기가 켜져 있는 경우 해당 iPhone과 페어링된 Apple Watch도 활성화 잠금을 사용할 수 있습니다. 활성화 잠금은 Apple Watch를 분실 또는 도난당했을 때 다른 사람이 사용하거나 판매하기 어렵게 만듭니다. 활성화 잠금은 페어링된 Apple Watch를 연결 해제, 삭제, 재활성화할 경우 사용자의 Apple ID 및 암호를 요구합니다.

iPhone의 보안 페어링

Apple Watch는 동시에 하나의 iPhone과만 페어링할 수 있습니다. Apple Watch의 페어링이 해제되면 iPhone은 해당 Apple Watch에서 모든 콘텐츠와 데이터를 지우라는 명령을 전달합니다.

Apple Watch와 iPhone 간의 페어링은 대역 외 프로세스에서 공개 키, 그리고 이어지는 BLE(Bluetooth® Low Energy) 링크 공유 비밀을 교환하여 보호됩니다. Apple Watch는 iPhone에서 카메라를 사용해 캡처할 수 있는 움직이는 패턴을 표시합니다. 이 패턴은 BLE 4.1 대역 외(OOB) 페어링에 사용되는 암호화된 비밀을 포함하고 있습니다. 필요한 경우 표준 BLE 패스키 엔트리가 폴백 페어링 방식으로 사용됩니다.

BLE 세션이 구축되어 Bluetooth 핵심 표준에서 지원하는 강력한 보안 프로토콜로 암호화되고 나면 iPhone 및 Apple Watch는 다음을 통해 키를 교환합니다.

- iMessage 보안 개요에서 설명한 바와 같이 Apple IDS(Identity Service)에서 채택한 프로세스를 사용합니다.
- IKEv2/IPsec를 통한 키 교환을 사용합니다. 최초의 키 교환은 Bluetooth 세션 키(페어링 시나리오의 경우) 또는 IDS 키(운영 체제 업데이트 시나리오의 경우)로 인증됩니다. 각 기기는 256비트 Ed25519의 공개 및 개인 키 쌍을 무작위로 생성하며, 최초 키 교환 프로세스에서는 공개 키가 교환됩니다. watchOS 10 이상을 실행 중인 Apple Watch가 처음 페어링되면 개인 키는 Secure Enclave에 루팅됩니다.

  iCloud 백업을 동일한 iPhone에 복구하는 사용자는 마이그레이션하지 않아도 기존 Apple Watch 페어링을 보존하기 때문에 iOS 17 이상을 실행 중인 iPhone에서 개인 키는 Secure Enclave에 루팅되지 않습니다.

참고: 키 교환 및 암호화에 사용되는 메커니즘은 iPhone 및 Apple Watch의 운영 체제 버전에 따라 달라집니다. iOS 13 이상 버전이 설치된 iPhone 기기가 watchOS 6 이상 버전을 실행하는 Apple Watch와 페어링된 경우 IKEv2/IPsec만을 사용하여 키를 교환하고 암호화합니다.

키가 교환되면 다음이 이루어집니다.

- Bluetooth 세션 키가 폐기되고, iPhone 및 Apple Watch 간 모든 통신이 앞서 나열된 방법(별도의 암호화 단계를 제공하는 암호화된 Bluetooth, Wi-Fi 및 셀룰러 링크) 중 하나를 통해 암호화됩니다.
- (IKEv2/IPsec에만 해당) 시스템 키체인에 키가 저장되어 향후 기기 간 IKEv2/IPsec 세션을 인증할 때 사용됩니다. watchOS 8 이상이 설치된 Apple Watch Series 4 및 이후 모델과 페어링된 iOS 15 이상의 iPhone 기기에서 앞으로 있을 기기 간 통신은 AES-256-GCM을 통해 암호화되며 무결성이 보호됩니다. (256비트 키가 포함된 ChaCha20-Poly1305는 이전에 출시된 기기 또는 이전 운영 체제 버전이 설치된 기기에서 사용됩니다.)

Bluetooth LE 기기 주소는 누군가가 영구 식별자를 브로드캐스트하는 경우 기기가 로컬로 추적되는 위험을 줄이기 위해 15분 간격으로 교체됩니다.

스트리밍 데이터가 필요한 앱을 지원하기 위해 FaceTime 보안에 설명된 방식을 통해 암호화가 제공됩니다. 암호화는 인터넷에 직접 연결하거나 페어링된 iPhone에서 제공하는 Apple IDS(Identity Service)를 이용합니다.

Apple Watch는 파일 및 키체인 항목의 하드웨어 암호화된 저장 장치 및 클래스 기반 보호를 구현합니다. 또한, 키체인 항목에 대해서는 접근이 제어되는 Keybag이 사용됩니다. Apple Watch와 iPhone 간의 통신에 사용되는 키 역시 클래스 기반의 보호를 사용합니다. 자세한 내용은 데이터 보호용 Keybag를 참조하십시오.

자동 잠금 해제 및 Apple Watch

다양한 Apple 기기를 사용할 때 더욱 편리하도록 일부 기기는 특정 상황에서 자동으로 잠금 해제될 수 있습니다. 자동 잠금 해제는 다음과 같은 세 가지 사용 사례가 있습니다.

- iPhone으로 Apple Watch를 잠금 해제할 수 있습니다.
- Apple Watch로 Mac을 잠금 해제할 수 있습니다.
- 사용자의 코와 입이 가려진 상태임을 인식한 경우 Apple Watch로 iPhone을 잠금 해제할 수 있습니다.

세 가지 사용 사례 모두 동일한 기반이 있습니다. 공통으로 인증된 STS(Station-to-Station) 프로토콜이 있고 기능 활성화 당시에 장기 키를 교환했다는 것과 잠금 해제 요청시마다 고유의 임시 세션 키를 교환한다는 것입니다. 기본 통신 채널에 상관 없이 STS 터널은 각 기기의 Secure Enclave 간에 직접 교환하며 모든 암호화 자료는 보안 도메인에 보관합니다(Secure Enclave가 없는 Mac 컴퓨터의 경우 커널에서 STS 터널을 제거하기 때문에 예외임).

잠금 해제

전체 잠금 해제 시퀀스는 두 단계로 구분할 수 있습니다. 먼저 잠금 해제되는 기기('대상 기기')에서 암호화된 잠금 해제 비밀을 생성하고 잠금 해제를 수행하는 기기('수행 기기')로 전송합니다. 그런 다음, 수행 기기에서 이전에 생성한 비밀을 사용하여 잠금 해제를 수행합니다.

자동 잠금 해제를 활성화하려면 BLE 연결을 통해 두 기기를 서로 연결합니다. 그러면 대상 기기에서 임의로 생성한 32바이트 잠금 해제 비밀이 STS 터널을 통해 수행 기기로 전송됩니다. 다음에 생체 인증 또는 암호로 잠금 해제하는 경우 대상 기기에서 암호 파생 키(PDK)를 잠금 해제 비밀로 래핑하고 대상 기기의 메모리에서 잠금 해제 비밀을 폐기합니다.

잠금 해제를 수행하려면 두 기기는 새로운 BLE 연결을 시작한 다음 피어 투 피어 Wi-Fi를 사용하여 서로 간의 거리를 안전하게 대략적으로 계산합니다. 두 기기가 특정 범위 내에 있고 필수 보안 정책이 충족되는 경우 수행 기기에서 잠금 해제 비밀을 STS 터널을 통해 대상 기기로 전송합니다. 그런 다음, 대상 기기는 새로운 32바이트 잠금 해제 비밀을 생성하고 수행 기기로 반환합니다. 수행 기기에서 전송한 현재 잠금 해제 비밀이 성공적으로 잠금 해제 기록의 암호화를 해제하면 대상 기기가 잠금 해제되며 PDK가 새로운 잠금 해제 비밀로 다시 래핑됩니다. 마지막으로 새로운 잠금 해제 비밀 및 PDK가 대상 기기의 메모리에서 폐기됩니다.

Apple Watch 자동 잠금 해제 보안 정책

편리성을 위해 Apple Watch는 초기 시동 이후에 암호를 먼저 입력할 필요 없이 iPhone으로 직접 Apple Watch를 잠금 해제할 수 있습니다. 이를 위해 임의의 잠금 해제 비밀(기능을 활성화하고 처음으로 수행하는 잠금 해제 시퀀스 중에 생성됨)을 사용하여 장기 에스크로 레코드를 생성합니다. 이 에스크로 레코드는 Apple Watch keybag에 보관됩니다. 에스크로 레코드 비밀은 iPhone 키체인에 보관되며 Apple Watch를 재시동할 때마다 새로운 세션을 부트스트랩하는 데 사용됩니다.

iPhone 자동 잠금 해제 보안 정책

Apple Watch을 통한 iPhone 자동 잠금 해제에는 추가 보안 정책이 적용됩니다. Apple Watch는 Apple Pay 또는 앱 인증과 같은 작업에 iPhone의 Face ID를 대체할 수 없습니다. Apple Watch가 페어링된 iPhone을 성공적으로 잠금 해제하면 Apple Watch에서 알림을 표시하고 관련 햅틱을 재생합니다. 사용자가 알림 화면의 iPhone 잠금 버튼을 탭하면 Apple Watch가 BLE를 통해 잠금 명령을 iPhone을 전송합니다. iPhone이 잠금 명령을 받으면 iPhone은 기기를 잠그고 Face ID를 비활성화하고 Apple Watch를 통한 잠금 해제도 비활성화합니다. 다음번 iPhone 잠금 해제는 iPhone 암호로 수행해야 합니다.

Apple Watch로 페어링된 iPhone을 성공적으로 잠금 해제(기능이 활성화된 경우)하려면 다음과 같은 조건이 충족되어야 합니다.

- 연결된 Apple Watch를 손목에 착용하고 잠금 해제한 상태에서 최소한 한 번은 iPhone을 다른 방식으로 잠금 해제해야 합니다.
- 센서가 사용자의 코와 입이 가려져 있다는 것을 인식할 수 있어야 합니다.
- 두 기기의 범위는 2~3미터 이하여야 합니다.
- Apple Watch가 취침 시간 모드가 아니어야 합니다.
- Apple Watch 또는 iPhone이 최근에 잠금 해제된 적이 있거나 Apple Watch에서 착용자의 활동을 인식할 수 있는 물리적인 움직임을 감지(예: 사용자가 수면 중이 아닌 상태)해야 합니다.
- iPhone이 지난 6.5시간 동안 최소한 한 번은 잠금 해제되었어야 합니다.
- Face ID로 iPhone의 기기 잠금 해제를 수행하는 것이 가능한 상태여야 합니다. (자세한 내용은 Face ID, Touch ID, 암호를 참조하십시오.)

macOS에서 Apple Watch를 통한 승인

Apple Watch에서 자동 잠금 해제가 활성화되면 Apple Watch를 다음 위치에서 또는 Touch ID와 함께 사용하여 다음으로부터 인증 및 인증 메시지를 승인할 수 있습니다.

- 인증을 요청한 macOS 및 Apple 앱
- 인증을 요청한 타사 앱
- 저장된 Safari 암호
- 보안 메모

Wi-Fi, 셀룰러, iCloud 및 Gmail의 안전한 사용

Apple Watch가 Bluetooth 범위 안에 있지 않다면 Wi-Fi 또는 셀룰러를 대신 사용할 수 있습니다. Apple Watch는 페어링된 iPhone에서 이전에 접속한 Wi-Fi 네트워크에 자동으로 연결되며 해당 네트워크의 자격 증명은 두 기기가 범위 내에 있는 동안 Apple Watch에 동기화됩니다. 그런 다음 이 자동 연결 동작은 Apple Watch 설정 앱의 Wi-Fi 섹션에 있는 각 네트워크를 기반으로 구성됩니다. 두 기기에서 이전에 연결된 적이 없는 Wi-Fi 네트워크는 Apple Watch 설정 앱의 Wi-Fi 섹션에서 수동으로 연결할 수 있습니다.

Apple Watch 및 iPhone이 서로 범위 밖에 있는 경우 페어링된 iPhone과 인터넷으로 메일 데이터를 동기화하지 않고 Apple Watch가 iCloud 및 Gmail 서버에 직접 연결하여 메일을 가져옵니다. Gmail 계정의 경우 사용자는 iPhone에서 Watch 앱을 열고 Mail 섹션에서 Google에 인증해야 합니다. Google에서 받은 OAuth 토큰은 Apple IDS(Identity Service)를 통해 암호화 포맷으로 Apple Watch로 전송되기 때문에 메일을 가져오는 데 사용할 수 있습니다. 이 OAuth 토큰은 연결된 iPhone에서 Gmail 서버에 연결하는 데 사용되지 않습니다.

난수 발생

CPRNG(의사 난수 발생기)는 보안 소프트웨어의 중요한 구성 요소입니다. 이를 위해 Apple은 iOS, iPadOS, macOS, tvOS 및 watchOS 커널에서 실행되는 신뢰하는 소프트웨어 CPRNG를 지원합니다. 이는 시스템에서 raw 엔트로피를 집계하고 커널과 사용자 공간 모두에서 안전한 무작위 번호를 소비자에게 제공하는 것을 담당합니다.

엔트로피 소스

커널 CPRNG는 기기를 시동하는 동안과 기기의 수명 주기에 걸쳐 여러 엔트로피 소스에서 시드됩니다. 이는 다음을 포함합니다(가능 여부에 따라).

- Secure Enclave 하드웨어 TRNG
- 시동 중에 수집된 타이밍 기반 지터
- 하드웨어 인터럽트에서 수집된 엔트로피
- 시동 과정에 걸쳐 엔트로피를 유지하는 데 사용되는 시드 파일
- Intel 임의 명령(예 : RDSEED 및 RDRAND(Intel 기반 Mac에만 해당))

커널 CPRNG

커널 CPRNG는 256비트 보안 수준을 대상으로 하는 Fortuna 파생 설계입니다. 다음과 같은 API를 통해 사용자 공간 소비자에게 고품질의 무작위 번호를 제공합니다.

- `getentropy`(2) 시스템 호출
- 임의의 기기(/dev/random)

커널 CPRNG는 임의의 기기에 쓰기를 통해 사용자 제공 엔트로피를 수용합니다.

Apple 보안 리서치 기기

Apple 보안 리서치 기기는 보안 전문가가 iPhone의 플랫폼 보안 기능을 해치거나 비활성화하지 않고 iOS에 대한 연구를 수행할 수 있도록 특별히 결합된 iPhone입니다. 이 기기를 사용하면 연구원이 플랫폼과 동등한 권한으로 실행되는 콘텐츠를 사이드 로드할 수 있게 하여 생산 기기를 보다 밀접하게 모델링하는 플랫폼에 대한 연구를 수행할 수 있습니다.

사용자 기기가 보안 리서치 기기 실행 정책의 영향을 받지 않도록 하기 위해 정책 변경 사항이 iBoot와 시동 커널 모음의 변형에 구현됩니다. 이는 사용자 하드웨어에서 시동할 수 없습니다. 리서치 iBoot는 새로운 결합 상태를 확인하며, 비연구용 결합 하드웨어에서 실행 중인 경우 패닉 루프에 진입합니다.

cryptex 하위 시스템을 통해 전문가는 개인 맞춤화된 신뢰 캐시와 상응하는 콘텐츠를 포함한 디스크 이미지를 로드할 수 있게 됩니다. 사용자 기기에서 이러한 하위 시스템이 실행되지 않도록 하고자 다음과 같이 여러 심층적인 방어 조치가 구현되었습니다.

- `launchd`가 일반 고객 기기를 감지할 수 없는 경우 `cryptexd` launchd 속성 목록을 로드하지 않습니다.
- `cryptexd`가 일반 고객 기기를 감지할 경우 중단됩니다.
- `AppleImage4`는 일반 고객 기기의 리서치 cryptex를 확인하는 데 사용되는 재전송 방지 값을 공급하지 않습니다.
- 서명 서버는 명시적인 허용 목록에 없는 기기의 cryptex 디스크 이미지를 개인 맞춤화하지 않습니다.

보안 전문가의 개인정보를 지키기 위해 실행 파일 또는 커널 캐시와 보안 리서치 기기 식별자의 측정값(예: 해시)은 개인 맞춤화가 이루어지는 동안에만 Apple에 전송됩니다. Apple에서는 기기에 로드되는 cryptex의 내용을 수신하지 않습니다.

악의적인 인물이 리서치 기기를 사용자 기기로 위장하여 대상을 속이고 일상 용도로 사용하는 것을 피하기 위해 보안 리서치 기기에는 다음과 같은 차이점이 있습니다.

- 보안 리서치 기기는 Lightning 케이블 또는 Qi 호환 충전기 등으로 충전하는 동안에만 시동됩니다. 시동하는 동안 기기가 충전되지 않으면 복구 모드에 들어갑니다. 사용자가 충전을 시작하고 기기를 재시동하면 정상적으로 시동됩니다. XNU가 시작되는 대로 기기를 충전할 필요 없이 계속해서 사용할 수 있습니다.
- **보안 리서치 기기**라는 단어가 iBoot 시동 중에 Apple 로고 아래에 표시됩니다.
- 상세 모드에서 XNU 커널이 시동됩니다.
- 기기 측면에 다음과 같이 메시지가 새겨져 있습니다. ‘Property of Apple. Confidential and Proprietary. Call +1 877 595 1125.’

다음은 소프트웨어에서 구현되는 추가적인 조치로 시동 후 나타납니다.

- 기기 설정 중에 표시되는 **보안 리서치 기기**라는 단어
- 잠금 화면과 설정 앱에 나타나는 **보안 리서치 기기**라는 단어

보안 리서치 기기는 전문가에게 사용자 기기에서 사용할 수 없는 다음과 같은 기능을 제공합니다.

- Apple 운영 체제 구성요소와 동일한 권한 수준에서 임의의 권한을 가진 기기에 실행 코드 사이드 로드
- 시동 시 서비스 시작
- 재시동 후에도 콘텐츠 유지
- `research.com.apple.license-to-operate` 권한을 사용하여 시스템 프로세스를 포함한 시스템의 모든 기타 프로세스를 디버그하기 위한 프로세스 허용.

  `research.` 네임스페이스는 AppleMobileFileIntegrity 커널 확장 프로그램의 RESEARCH 변형에 의해서만 적용되며 이 권한의 모든 프로세스는 서명 확인 중 고객 기기에서 제거됩니다.
- 사용자 설정 커널 캐시 개인 맞춤화 및 복구하기

암호화 및 데이터 보호

암호화 및 데이터 보호 개요

보안 시동 체인, 시스템 보안, 앱 보안 기능은 신뢰하는 코드와 앱만 기기에서 실행되도록 확인합니다. Apple 기기에는 기기가 분실되거나 신뢰할 수 없는 코드를 실행하는 등, 보안 인프라의 일부가 손상된 경우에도 사용자 데이터를 보호하기 위한 추가 암호화 기술이 적용되어 있습니다. 이를 통해 사용자 및 IT 관리자 모두가 개인과 기업의 정보를 보호할 수 있으며, 기기를 분실하거나 도난당한 경우에도 기기를 원격으로 즉시 지울 수 있는 방법이 제공된다는 장점이 있습니다.

iPhone 및 iPad 기기는 **데이터 보호**라는 파일 암호화 기법을 사용하며, Intel 기반 Mac은 **FileVault**라는 볼륨 암호화 기술로 데이터를 보호합니다. Apple Silicon이 탑재된 Mac은 두 가지 사항에 주의하여 데이터 보호를 지원하는 하이브리드 모델을 사용합니다. 가장 낮은 보호 수준인 클래스 D는 지원되지 않으며 기본 수준인 클래스 C는 볼륨 키를 사용하여 Intel 기반 Mac에서의 FileVault처럼 작동합니다. 모든 경우에 키 관리 계층은 Secure Enclave의 전용 실리콘 칩에 뿌리를 두고 있으며, 전용 AES 엔진이 회선 속도의 암호화를 지원하고, 장기간 사용한 암호화 키를 커널 운영 체제 또는 CPU에 노출되지 않도록 합니다(해당 암호화 키가 손상되었을 가능성이 있는 경우). (T1이 있거나 Secure Enclave가 없는 Intel 기반 Mac은 전용 실리콘을 사용하여 FileVault 암호화 키를 보호하지 않습니다.)

데이터 무단 접근 방지를 위해 데이터 보호 및 FileVault를 사용하는 것 외에도 Apple은 **운영 체제 커널**을 사용하여 보호 및 보안을 시행합니다. 커널은 샌드박스 앱에 접근 권한 제어를 사용하여 앱이 접근할 수 있는 데이터를 제한하며, **Data Vault**라는 메커니즘을 사용하여 앱의 요청을 제한하는 대신 요청을 보내는 다른 모든 앱이 특정 앱의 데이터에 접근하는 것을 방지합니다.

암호

Apple은 사용자의 데이터를 악의적인 공격에서 보호하기 위해 iOS, iPadOS 및 macOS에서 암호를 사용합니다. 암호가 길면 길수록 강력하고 무작위 대입 공격을 방지할 확률이 높아집니다. 공격을 더욱 효과적으로 방지하기 위해 Apple은 iOS 및 iPadOS에서 시간 지연 기능을 실행하고 Mac에서는 암호 입력 시도 횟수를 제한합니다.

iOS 및 iPadOS에서 기기 암호를 설정할 경우, 사용자는 자동으로 데이터 보호를 활성화합니다. 데이터 보호는 Apple Silicon이 탑재된 Mac, Apple TV 및 Apple Watch와 같이 다른 Apple SoC(system on chip) 기기에서도 활성화됩니다. Apple은 macOS에서 내장 볼륨 암호화 프로그램 **FileVault**를 사용합니다.

강력한 암호가 보안을 강화하는 방법

iOS 및 iPadOS는 6자리, 4자리, 또는 임의의 길이의 알파벳 숫자 암호를 지원합니다. 또한 암호는 기기를 잠금 해제하는 것 외에도 특정 암호화 키에 대한 엔트로피를 제공합니다. 이를 통해 해커가 기기의 소유권을 획득하여도 암호 없이는 특정 보호 클래스에 있는 데이터에 접근할 수가 없습니다.

암호는 기기의 UID와 연결되어 무작위 대입 공격은 이미 공격이 진행 중인 기기에서만 발생합니다. 하지만 반복 횟수가 늘어나면 입력 속도가 점점 느려집니다. 반복 횟수는 시도 한 번에 약 80밀리초가 소요되도록 보정되었기 때문입니다. 즉, 6자리의 영문 소문자와 숫자로 이루어지는 알파벳 숫자 암호 조합을 모두 시도하려면 5년 6개월 이상이 걸립니다.

사용자 암호가 강력해질수록 암호화 키도 강력해집니다. 또한 Face ID 및 Touch ID를 사용하여 사용자는 더욱 강력한 암호를 설정할 수 있습니다. 강력한 암호를 통해 데이터 보호에 사용되어 암호화 키를 보호하는 엔트로피 규모의 효율성이 증가하는 동시에, 기기의 잠금을 하루에 여러 차례 해제할 때의 사용자 경험에 부정적인 영향을 미치지 않습니다.

숫자로만 이루어진 긴 암호가 입력될 경우 잠금 화면에 전체 키보드 대신 숫자 키패드가 표시됩니다. 비슷한 수준의 보안을 제공하는 짧은 알파벳-숫자 암호보다는 긴 숫자 암호가 더 입력하기 편할 수 있습니다.

설정 > 'Touch ID 및 암호' 또는 'Face ID 및 암호'의 암호 옵션에서 '사용자 지정 알파벳 숫자 코드'를 선택하면 긴 알파벳-숫자 암호를 설정할 수 있습니다.

점진적 시간 지연이 무작위 대입 공격을 무효화하는 방법

iOS, iPadOS 및 macOS에서 무작위 암호 대입 공격의 추가 방지책으로는 아래의 표에 나타난 대로, 암호 또는 PIN 입력을 실패한 경우(기기 및 기기 상태에 따라 다름) 암호 입력을 점진적으로 지연시키는 시간 지연 기능이 있습니다.

시도 횟수	3	4	5	6	7	8	9	10 이상
iOS 및 iPadOS 잠금 화면	없음	1분	5분	15분	1시간	3시간	8시간	기기가 비활성화되었고 Mac 또는 PC에 연결해야 함
watchOS 잠금 화면	없음	1분	5분	15분	1시간	3시간	8시간	기기가 비활성화되었고 iPhone에 연결해야 함
macOS 로그인 윈도우 및 잠금 화면	없음	1분	5분	15분	1시간	3시간	8시간	8시간
macOS 복구 모드	없음	1분	5분	15분	1시간	3시간	8시간	아래의 'macOS에서 점진적 시간 지연이 무작위 대입 공격을 무효화하는 방법' 참조
복구 키가 있는 FileVault (개인, 기관 또는 iCloud)	없음	1분	5분	15분	1시간	3시간	8시간	아래의 'macOS에서 점진적 시간 지연이 무작위 대입 공격을 무효화하는 방법' 참조
macOS 원격 잠금 PIN 코드	1분	5분	15분	30분	1시간	1시간	1시간	1시간

iPhone 또는 iPad에서 데이터 지우기 옵션이 켜진 경우(설정 > [Face ID] 또는 [Touch ID] 및 암호), 10번 연속으로 잘못된 암호를 입력하면 모든 콘텐츠와 설정이 저장 공간에서 제거됩니다. 올바르지 않은 동일한 암호를 연속으로 입력한 경우 이 제한 횟수에 포함되지 않습니다. 이 설정은 이 기능을 지원하는 MDM(모바일 기기 관리) 솔루션과 Microsoft Exchange ActiveSync을 통해 관리 정책으로 사용할 수 있으며, 한계값을 더 낮출 수도 있습니다.

Secure Enclave를 사용하는 기기에서는 Secure Enclave가 시간 지연을 시행합니다. 덕분에 시간 지연 도중 기기가 재시동되어도 시간 지연은 계속되며 타이머가 현재 단계에 맞춰 다시 시작됩니다.

macOS에서 점진적 시간 지연이 무작위 대입 공격을 무효화하는 방법

무작위 대입 공격을 방지하기 위해 Mac이 시동될 때 로그인 윈도우에서 10회를 초과하여 암호 입력을 시도할 수 없으며, 특정 횟수만큼 올바르지 않은 암호를 입력한 뒤에는 점점 늘어나는 시간 지연이 발생합니다. 이러한 지연 시간은 Secure Enclave를 통해 강제로 적용됩니다. 지연 시간 도중 Mac이 재시동되어도 지연은 계속되며, 타이머가 현재 단계에 맞춰 다시 시작됩니다.

악성 코드가 사용자의 암호에 공격을 시도해 영구적인 데이터 손상을 유발하는 것을 방지하기 위해 사용자가 Mac에 올바르게 로그인한 후에는 이러한 제한이 적용되지 않지만, 재시동한 다음에는 다시 적용됩니다. 10회의 입력 기회가 모두 소진될 경우, 복구용 OS로 재시동한 다음 10회 더 입력을 시도할 수 있습니다. 이 입력 기회 또한 모두 소진될 경우 FileVault 복구 과정(iCloud 복구, FileVault 복구 키, 기관 키)마다 추가로 10회의 입력을 시도할 수 있으며, 최대 30회까지 시도할 수 있습니다. 이 추가 입력 기회도 모두 소진될 경우, Secure Enclave는 더 이상 볼륨의 암호화를 해제하거나 암호를 검증하려는 요청을 처리하지 않으며, 드라이브의 데이터는 복구할 수 없게 됩니다.

기업용 설정에서 데이터를 보호하려면, IT 부서에서 MDM 솔루션을 사용하여 FileVault 구성 정책을 정의하고 적용해야 합니다. 조직에서는 기관 복구 키 또는 개인 복구 키(MDM에 저장해 에스크로 가능)를 사용하거나, 둘을 조합해 사용하는 등 몇 가지 방법을 사용해 암호화 볼륨을 관리할 수 있습니다. MDM에서 키 순환도 정책으로 설정할 수 있습니다.

Apple T2 보안 칩이 탑재된 Mac에서는 암호가 유사한 역할을 하지만, 생성된 키가 데이터 보호 대신 FileVault 암호화에 사용된다는 점이 다릅니다. macOS에서는 다음과 같은 암호 복구 옵션 또한 제공됩니다.

- iCloud 복구
- FileVault 복구
- FileVault 기관 키

데이터 보호

데이터 보호 개요

Apple은 데이터 보호라는 기술을 사용하여 iPhone, iPad, Apple Watch, Apple TV 및 Apple Silicon이 탑재된 Mac 컴퓨터와 같은 Apple SoC 기기의 플래시 저장 장치에 저장된 데이터를 안전하게 보호합니다. 데이터 보호는 통화 수신과 같은 일반적인 이벤트에 기기가 응답하는 것을 허용하는 동시에 사용자 데이터에 대해서는 높은 수준의 암호화를 제공합니다. 기본적으로 데이터 보호는 메시지, Mail, 캘린더, 연락처, 사진 등 특정 시스템 앱의 데이터 값과 건강 데이터 값에 사용됩니다. 타사 앱은 자동으로 이 보호 기능을 받습니다.

구현

데이터 보호는 키 계층을 구성하고 관리하는 방식으로 구현되며, Apple 기기에 내장된 하드웨어 암호화 기술을 기반으로 합니다. 데이터 보호는 각각의 파일을 클래스에 할당하는 파일별 기준으로 제어되며, 클래스 키가 잠금 해제되었는지에 따라 접근성이 결정됩니다. APFS(Apple 파일 시스템)로 파일 시스템이 키를 익스텐트 단위로 더욱 세분화할 수 있습니다(파일 일부가 다른 키를 가진 경우).

데이터 볼륨에 파일이 생성될 때마다 데이터 보호는 256비트 키(**파일별 키**)를 새로 생성하며 하드웨어 AES 엔진에 전달합니다. AES 엔진은 이 키를 사용해 플래시 저장 공간에 작성되는 파일을 암호화합니다. A14부터 A17 기기 및 M1부터 M3 기기에서 암호화는 XTS 모드에서 AES-256을 사용하여 256비트 파일별 키가 키 파생 함수(NIST Special Publication 800-108)를 거치며 256비트 트윅과 256비트 암호 키를 파생합니다. A9부터 A13 기기 및 S5부터 S9 기기에서 암호화는 XTS 모드에서 AES128을 사용하며, 256비트 파일별 키가 분리되어 128비트 트윅과 128비트 암호 키를 제공합니다.

Apple Silicon이 탑재된 Mac에서는 기본적으로 클래스 C의 데이터 보호(데이터 보호 클래스 참조)를 제공하지만, 익스텐트별 또는 파일별 키를 사용하는 대신 볼륨 키를 사용하며 사용자 데이터에 FileVault 보안 모델을 재생성하게 됩니다. 암호를 사용하여 암호화 키 계층 구조를 완전히 보호하기 위해서 사용자는 계속 FileVault를 선택해야 합니다. 개발자는 파일별 또는 익스텐트별 키를 사용하는 상위 보호 클래스를 선택할 수도 있습니다.

Apple 기기의 데이터 보호

데이터 보호를 제공하는 Apple 기기에서는 각 파일이 고유한 파일별 또는 익스텐트별 키로 보호됩니다. NIST AED 키 래핑 알고리즘을 사용하여 래핑된 해당 키는 파일 접근 방식에 따라 여러 클래스 키 중 하나로 다시 래핑됩니다. 래핑된 파일별 키는 파일의 메타데이터에 저장됩니다.

APFS 포맷을 사용하는 기기는 파일 복제(쓰기 시 복사 기술을 사용하는 제로 코스트 사본)를 지원할 수 있습니다. 파일이 복제되면 복제 데이터의 절반은 새로운 키를 얻어서 들어오는 쓰기 내용을 받으므로, 새로운 데이터는 새로운 키로 미디어에 기록됩니다. 시간이 지날수록 파일은 각기 다른 키에 매핑되는 다양한 익스텐트(또는 조각)로 구성됩니다. 하지만 파일을 구성하는 모든 익스텐트는 동일한 클래스 키로 보호됩니다.

파일을 열면 파일 시스템 키로 메타데이터의 암호화가 해제되고 래핑된 파일별 키와 키를 보호하는 클래스 이름이 공개됩니다. 파일별(또는 익스텐트별) 키는 클래스 키를 통해 래핑이 해제되고 하드웨어 AES 엔진에 공급됩니다. AES 엔진은 파일을 플래시 저장 공간에서 읽은 상태 그대로 암호화를 해제합니다. 래핑된 파일 키에 대한 처리는 모두 Secure Enclave에서 수행됩니다. 또한 파일 키는 절대로 응용 프로그램 프로세서에 직접 노출되지 않습니다. 시동 시 Secure Enclave는 AES 엔진과 임시 키를 교환합니다. Secure Enclave가 파일의 키를 래핑 해제하면 임시 키가 파일의 키를 다시 래핑하여 응용 프로그램 프로세서로 다시 보냅니다.

데이터 볼륨 파일 시스템에 있는 모든 파일의 메타데이터는 임의 볼륨 키로 암호화되어 있습니다. 임의 볼륨 키는 운영 체제가 처음으로 설치되거나 사용자가 기기의 데이터를 지운 경우에 생성됩니다. 이 키는 장기 보관용 Secure Enclave에만 알려지는 키 래핑 키로 암호화 및 래핑됩니다. 키 래핑 키는 사용자가 기기를 지울 때마다 변경됩니다. A9 이상의 SoC에서 Secure Enclave는 재전송 방지 시스템으로 보조하는 엔트로피에 의존하여 삭제 가능성을 확보하고, 다른 자산과 더불어 키 래핑 키를 보호합니다. 자세한 내용은 비휘발성 보안 저장 장치를 참조하십시오.

파일별 또는 익스텐트별 키와 같이 데이터 볼륨의 메타데이터 키는 응용 프로그램 프로세서에 직접 노출되지 않습니다. Secure Enclave는 부트별 버전의 임시값을 대신 제공합니다. 저장 시 암호화된 파일 시스템 키는 삭제할 수 있는 저장 장치(Effaceable Storage)에 저장된 '삭제할 수 있는 키' 또는 Secure Enclave 재전송 방지 메커니즘에 의해 보호되는 미디어 키 래핑 키를 사용하여 추가 래핑됩니다. 이 키는 데이터 기밀을 추가적으로 제공하지 않습니다. 대신에 키는 요청 시에 빠르게 삭제됩니다(사용자가 모든 콘텐츠 및 설정 지우기 옵션을 사용하거나, 사용자 또는 관리자가 MDM(모바일 기기 관리) 솔루션, Microsoft Exchange ActiveSync 또는 iCloud에서 원격 지우기 명령을 사용하여 삭제할 수 있습니다). 이러한 방식으로 키를 삭제하는 경우 모든 파일이 암호화되어 접근할 수 없습니다.

파일의 콘텐츠는 하나 이상의 파일별(또는 익스텐트별) 키로 암호화됩니다. 파일별 키는 클래스 키로 래핑되어 파일의 메타데이터에 저장됩니다. 또한 메타데이터는 파일 시스템 키로 암호화됩니다. 클래스 키는 주로 하드웨어 UID로 보호되지만 일부 클래스의 경우 사용자의 암호로 보호됩니다. 이러한 보안 계층을 통해 유연성과 성능이 개선될 수 있습니다. 예를 들어 파일의 클래스를 변경하는 경우에는 파일별 키만 다시 래핑하면 되고, 암호를 변경하는 경우에는 클래스 키만 다시 래핑하면 됩니다.

데이터 보호 클래스

데이터 보호를 지원하는 기기에서 새로운 파일이 생성되면 그 파일을 생성한 앱이 파일에 클래스를 할당합니다. 데이터 접근 시기를 결정하는 정책은 클래스마다 다릅니다. 기본 클래스와 정책은 다음 섹션에서 설명합니다. Apple Silicon 기반 Mac 컴퓨터는 클래스 D를 지원하지 않습니다. 클래스 D는 보호 기능이 없으며 로그인 및 로그아웃시 보안 경계가 설정됩니다 (iPhone 및 iPad에서처럼 잠금 또는 잠금 해제하는 방식이 아님).

클래스	보호 유형
클래스 A: Complete Protection	NSFileProtectionComplete
클래스 B: Protected Unless Open	NSFileProtectionCompleteUnlessOpen
클래스 C: Protected Until First User Authentication **참고:** macOS는 볼륨 키를 사용하여 FileVault 보호 특성을 다시 생성함.	NSFileProtectionCompleteUntilFirstUserAuthentication
클래스 D: No Protection **참고:** macOS에서 지원되지 않음.	NSFileProtectionNone

Complete Protection

NSFileProtectionComplete: 이 클래스 키는 사용자 암호 및 기기 UID에서 파생된 키로 보호됩니다. 사용자가 기기를 잠그고 잠시 후(암호 요구가 '즉시'로 설정되어 있는 경우 10초), 암호화가 해제된 클래스 키는 폐기되고, 사용자가 암호를 다시 입력하거나 Face ID 및 Touch ID를 사용하여 기기를 잠금 해제(로그인)하기 전까지 이 클래스에 있는 모든 데이터에 접근할 수 없도록 렌더링합니다.

macOS에서 사용자가 로그아웃하고 잠시 후, 암호화가 해제된 클래스 키는 폐기되고 사용자가 암호를 다시 입력하거나 Touch ID를 사용하여 기기에 로그인하기 전까지 이 클래스에 있는 모든 데이터에 접근할 수 없도록 렌더링합니다.

Protected Unless Open

NSFileProtectionCompleteUnlessOpen: 일부 파일은 기기가 잠금 상태이거나 사용자가 로그아웃했을 때에도 쓸 수 있어야 합니다. 좋은 예로는 이메일 첨부 파일을 백그라운드에서 다운로드하는 상황입니다. 이 작업은 비대칭 타원곡선 암호화(Curve25519를 통한 ECDH)를 통해 실행됩니다. 일반적으로 파일별 키는 NIST SP 800-56A에 서술된 단일 패스 디피-헬만 키 합의(Diffie-Hellman Key Agreement)를 사용해 파생된 키로 보호됩니다.

해당 합의로 파생된 임시 공개 키는 래핑된 파일별 키와 함께 저장됩니다. KDF는 NIST SP 800-56A의 5.8.1에 서술된 연속 키 유도 함수(Concatenation Key Derivation Function)(승인된 대안 1)입니다. 여기서 AlgorithmID는 생략됩니다. PartyUInfo는 임시 공개 키이며 PartyVInfo는 정적 공개 키입니다. SHA256은 해시 함수로 사용됩니다. 파일을 닫으면 바로 파일별 키는 메모리에서 지워집니다. 파일을 다시 열려면 Protected Unless Open 클래스의 개인 키 및 파일의 임시 공개 키를 사용해 공유 비밀이 다시 생성됩니다. 이 개인 키와 임시 공개 키를 사용하여 파일별 키의 래핑을 해제한 다음 파일의 암호화도 해제합니다.

macOS에서 시스템의 모든 사용자가 로그인되어 있거나 인증되어 있는 동안에는 NSFileProtectionCompleteUnlessOpen의 비공개 영역에 접근할 수 있습니다.

Protected Until First User Authentication

NSFileProtectionCompleteUntilFirstUserAuthentication: 이 클래스는 기기가 잠기거나 사용자가 로그아웃하더라도 암호화가 해제된 클래스 키가 메모리에서 삭제되지 않는다는 점을 제외하면 Complete Protection 과 같은 방식으로 동작합니다. 이 클래스의 보호 방식은 데스크탑 풀 볼륨 암호화(Full-Volume Encryption)와 비슷한 특징을 가지고 있으며 재시동과 관련된 공격으로부터 데이터를 보호합니다. 데이터 보호 클래스에 할당되지 않은 모든 타사 앱 데이터는 기본으로 이 클래스에 할당됩니다.

macOS에서 이 클래스는 볼륨이 마운트되어 있는 동안 접근할 수 있는 볼륨 키를 사용하며 FileVault처럼 작동합니다.

No Protection

NSFileProtectionNone: 이 클래스 키는 UID로만 보호되며 삭제할 수 있는 저장 장치(Effaceable Storage)에 보관됩니다. 이 클래스에 있는 파일을 암호화 해제하는 데 필요한 모든 키는 기기에 저장되어 있기 때문에 암호화는 빠른 원격 지우기의 이점만 제공합니다. 파일에 데이터 보호 클래스가 할당되지 않더라도 iOS 및 iPadOS 기기의 다른 모든 데이터와 마찬가지로 암호화된 형태로 보관됩니다.

macOS에서 지원되지 않습니다.

참고: macOS에서 시동된 운영 체제가 아닌 볼륨의 경우, 볼륨이 마운트되어 있는 동안에는 모든 데이터 보호 클래스에 접근할 수 있습니다. 기본 데이터 보호 클래스는 NSFileProtectionCompleteUntilFirstUserAuthentication 입니다. 익스텐트별 키 기능은 Rosetta 2 및 기본 앱에서 사용할 수 있습니다.

데이터 보호용 Keybag

파일 및 키체인 데이터 보호 클래스의 키는 iOS, iPadOS, tvOS 및 watchOS의 Keybag에서 수집하고 관리합니다. 이러한 운영 체제는 user, device, backup, escrow 및 iCloud Backup 등의 Keybag을 사용합니다.

User keybag

User keybag은 기기의 일반적인 작업에 사용되는 래핑된 클래스 키가 저장되는 곳입니다. 예를 들어 암호가 입력되면 User keybag에서 **NSFileProtectionComplete** 키가 로드되어 래핑이 해제됩니다. No Protection 클래스에 저장된 바이너리 속성 목록(.plist) 파일입니다.

A9 이전에 출시된 SoC가 탑재된 기기의 경우, .plist 파일 콘텐츠는 삭제할 수 있는 저장 장치(Effaceable Storage)에 보관된 키로 암호화됩니다. Keybag에 전방 보안성을 제공하기 위해 사용자가 암호를 변경할 때마다 이 키는 지워졌다가 다시 생성됩니다.

A9 이상의 SoC가 탑재된 기기에서는 .plist 파일에 Secure Enclave로 제어되는 재전송 방지 값으로 보호되는 잠금 장치에 저장되는 Keybag을 나타내는 키가 포함됩니다.

Secure Enclave는 User keybag을 관리하며 기기의 잠금 상태에 대한 쿼리를 받습니다. User keybag의 모든 클래스 키가 접근 가능한 상태이며 이상 없이 래핑이 해제된 경우에만 Secure Enclave에서 기기가 잠금 해제되었음을 보고합니다.

Device keybag

Device keybag은 기기별로 특정한 데이터를 다루는 작업에 사용되는 래핑된 클래스 키를 저장하는 데 사용됩니다. 공용으로 사용하도록 구성된 iPadOS 기기는 어느 사용자도 로그인하지 않은 상태에서 자격 증명에 접근해야 하는 경우가 가끔 있습니다. 따라서 사용자의 암호로 보호되지 않는 Keybag이 필요합니다.

iOS 및 iPadOS에서는 파일 시스템 콘텐츠를 사용자별로 암호화하여 구분하는 기능은 지원하지 않으며, 시스템이 Device keybag에서 클래스 키를 사용해 파일별 키를 래핑합니다. 하지만 키체인은 User keybag에서 클래스 키를 사용하여 사용자 키체인의 항목을 보호합니다. 단일 사용자용으로 구성(기본 구성)된 iPhone 및 iPad 기기에서 Device keybag과 User keybag은 동일한 하나의 개체이며, 사용자의 암호로 보호됩니다.

Backup keybag

Backup keybag은 Finder(macOS 10.15 이상 버전) 또는 iTunes(macOS 10.14 또는 이전 버전)에서 암호화된 백업 데이터가 만들어질 때 생성되고 기기가 백업된 컴퓨터에 저장됩니다. 새로운 일련의 키와 함께 새로운 Keybag이 생성되며, 백업된 데이터는 이 새로운 키로 다시 암호화됩니다. 위에서 설명한 것처럼 이동할 수 없는 키체인 항목은 UID에서 파생된 키로 래핑된 상태라 원래 백업된 기기에는 복원할 수 있지만 다른 기기에서는 접근할 수 없습니다.

암호 세트로 보호되는 keybag은 키 파생 함수 PBKDF2의 1,000만 회 반복을 통해 실행됩니다. 반복 횟수가 크지만 특정 기기에 연관되지 않아 이론상으로는 동시에 다수의 컴퓨터에 가하는 무작위 대입 공격이 Backup keybag을 공격할 수 있습니다. 하지만 강력한 암호로 이러한 위협을 완화할 수 있습니다.

사용자가 백업 데이터를 암호화하지 않기로 선택하면 해당 파일들은 데이터 보호 클래스와 무관하게 암호화가 수행되지 않지만 키체인은 UID에서 파생된 키로 계속 보호됩니다. 따라서 키체인 항목은 백업 암호가 설정된 경우에만 새로운 기기로 마이그레이션됩니다.

Escrow keybag

Escrow keybag은 USB 및 MDM(모바일 기기 관리)을 통해 Finder(macOS 10.15 이상) 또는 iTunes(macOS 10.14 및 이전 버전)와 동기화하는 데 사용됩니다. 이 Keybag은 사용자에게 암호 입력을 요청하지 않고도 Finder 또는 iTunes에서 백업과 동기화를 수행할 수 있게 해 주며, MDM 솔루션에서 사용자의 암호를 원격으로 지울 수 있게 해 줍니다. Finder 또는 iTunes를 통해 동기화할 때 사용되는 컴퓨터에 저장되거나, 기기를 원격으로 관리하는 MDM 솔루션에 저장되기도 합니다.

Escrow keybag은 모든 데이터 클래스에 접근해야 할 수 있는 기기 동기화 과정에서 사용자 경험을 향상합니다. 암호로 잠긴 기기가 Finder 또는 iTunes에 처음으로 연결되면 사용자에게 암호를 입력하라는 대화상자가 나타납니다. 이후 기기에서 사용하는 것과 동일한 클래스 키가 포함된 Escrow keybag이 기기를 통해 생성되고 새로 생성된 키로 보호합니다. Escrow keybag 및 이를 보호하는 키는 기기와 호스트 또는 기기와 서버 사이에서 Protected Until First User Authentication 클래스에 있는 기기에 저장된 데이터와 함께 분리됩니다. 이런 이유로 재시동 후 처음으로 Finder 또는 iTunes에 연결하고 백업을 할 때 암호를 입력해야 합니다.

OTA(Over-The-Air) 소프트웨어 업데이트의 경우, 업데이트를 시작할 때 사용자에게 암호를 입력하라는 대화상자가 나타납니다. 이는 업데이트 후에 User keybag을 잠금 해제하는 일회성 잠금 해제 토큰을 안전하게 만드는 데 사용됩니다. 사용자의 암호를 입력하지 않으면 이 토큰을 생성할 수 없으며, 사용자의 암호가 변경되면 이전에 생성된 모든 토큰은 무효화됩니다.

일회성 잠금 해제 토큰은 소프트웨어 업데이트의 자동 또는 수동 설치 모두에 필요합니다. 해당 토큰은 Secure Enclave 내 모노토닉 카운터의 현재 값, Keybag의 UUID, Secure Enclave의 UID에서 파생된 키로 암호화됩니다.

A9 이상 SoC에서 일회성 잠금 해제 토큰은 더 이상 카운터 또는 삭제할 수 있는 저장 장치(Effaceable Storage)에 의존하지 않습니다. 대신 Secure Enclave에서 제어하는 재전송 방지 값으로 보호됩니다.

수동 소프트웨어 업데이트용 일회성 잠금 해제 토큰은 20분이 지나면 만료됩니다. iOS 13 및 iPadOS 13.1 이상에서 토큰은 Secure Enclave에 의해 보호되는 잠금 장치에 저장됩니다. iOS 13 이전 버전에서는 이 토큰이 Secure Enclave에서 내보내져 삭제할 수 있는 저장 장치(Effaceable Storage)에 작성되었거나 Secure Enclave 재전송 방지 메커니즘에 의해 보호되었습니다. 기기가 20분 내에 재시동되지 않으면 정책 타이머가 카운터를 증가시켰습니다.

자동 소프트웨어 업데이트는 시스템에서 사용 가능한 업데이트를 감지했고 다음 중 하나에 해당되는 경우에 발생합니다.

- 자동 업데이트가 iOS 12 이상에서 구성된 경우.
- 사용자가 업데이트 알림을 받았을 때 나중에 설치를 선택한 경우.

사용자가 암호를 입력한 후 일회성 잠금 해제 토큰이 생성되며 최대 8시간 동안 Secure Enclave에서 유효합니다. 업데이트가 아직 수행되지 않은 경우, 이 일회성 잠금 해제 토큰은 모든 잠금마다 제거되고 이후에 잠금 해제를 할 때마다 다시 생성됩니다. 잠금 해제를 할 때마다 8시간 윈도우를 다시 시작합니다. 8시간이 지나면 정책 타이머가 일회성 잠금 해제 토큰을 무효화합니다.

iCloud Backup keybag

iCloud Backup keybag은 Backup keybag과 유사합니다. 이 keybag에 있는 모든 클래스 키는 비대칭(Protected Unless Open Data Protection 클래스와 같이 Curve25519를 사용함)입니다. 비대칭 Keybag은 iCloud 키체인 복구를 위해 백업된 키체인을 보호하는 데도 사용됩니다.

대체 시동 모드에서의 보호 키

데이터 보호는 인증에 성공한 후, 그리고 인증된 사용자에게만 사용자 데이터에 대한 접근 권한을 제공하도록 설계되었습니다. 데이터 보호 클래스는 기기가 잠겨 있어도(단, 첫 잠금 해제 후) 일부 데이터를 읽고 쓸 수 있는 기능 등 다양한 활용 사례를 지원하도록 설계되었습니다. DFU(기기 펌웨어 업데이트) 모드, 복구 모드, Apple 진단에 사용되는 것과 같은 대체 시동 모드 또는 소프트웨어 업데이트 중에 사용자 데이터에 대한 접근으로부터 보호하기 위해 추가 단계가 수행됩니다. 이러한 기능은 하드웨어와 소프트웨어 기능을 결합한 것으로 Apple이 설계한 Silicon의 발전에 따라 확장되었습니다.

기능	A10	A11–A17 S3–S9 M1, M2, M3
복구: 모든 데이터 보호 클래스가 보호됨	✓	✓
DFU 모드, 복구 및 소프트웨어 업데이트의 대체 시동 모드: 클래스 A, B 및 C 데이터가 보호됨	✗	✓

Secure Enclave AES 엔진은 잠글 수 있는 소프트웨어 시드 비트를 포함합니다. UID에서 키가 생성될 때 추가적인 키 계층을 생성하기 위해 이러한 시드 비트가 키 유도 함수에 포함됩니다. 시드 비트 사용 방법은 SoC(systems on chip)에 따라 다음과 같이 달라집니다.

- Apple A10 및 S3 SoC부터, 시드 비트는 사용자의 암호로 보호된 키를 구분하는 용도로만 사용됩니다. 시드 비트는 사용자의 암호를 요구하는 키(데이터 보호 클래스 A, 클래스 B 및 클래스 C 포함)에 설정되어 있으며 사용자의 암호를 요구하지 않는 키(파일 시스템 메타데이터 키 및 클래스 D 키 포함)의 경우 설정되어 있지 않습니다.
- A10 이상이 탑재된 기기에 iOS 13 이상 및 iPadOS 13.1 이상 버전이 설치된 경우, 기기를 진단 모드에서 시동하면 모든 사용자 데이터가 암호화 방식으로 렌더링되어 접근이 불가능합니다. 이는 설정을 통해 미디어 키에 대한 접근 권한을 관리하는 시드 비트를 추가로 활용하여 구현되고, 미디어 키 자체는 데이터 보호로 암호화된 데이터 볼륨에 포함된 모든 파일의 메타데이터와 콘텐츠에 접근하는 데 필요합니다. 이 보호는 사용자의 암호를 요구하는 파일 외에도 클래스 A, B, C, D의 모든 클래스로 보호되는 파일에 적용됩니다.
- A12 SoC의 경우 응용 프로그램 프로세서가 DFU(기기 펌웨어 업그레이드) 모드 또는 복구 모드로 들어가면 Secure Enclave Boot ROM이 암호 시드 비트를 잠급니다. 암호 시드 비트가 잠기면 변경 작업은 허용되지 않습니다. 이는 사용자의 암호로 보호되는 데이터에 대한 접근을 방지하기 위해 설계된 것입니다.

DFU 모드에 들어간 기기를 복원하면 수정되지 않은 상태의 Apple 서명 코드만 있는 정상 상태로 기기가 돌아갑니다. DFU 모드는 수동으로 들어갈 수 있습니다.

기기에서 DFU 모드로 진입하는 방법에 대해서는 다음 Apple 지원 문서를 참조하십시오.

기기	Apple 지원 문서
iPhone, iPad	iPhone 암호를 잊어버린 경우
Apple TV	Apple TV에 경고 기호가 표시되는 경우
Apple Silicon이 탑재된 Mac	Mac 펌웨어를 되살리거나 복원하는 방법

공격에 대한 사용자 데이터 보호

사용자 데이터를 추출하려는 공격자는 종종 여러 기술을 시도합니다. 암호화된 데이터를 다른 매체로 추출하여 무작위 대입 공격을 하거나 운영 체제 버전을 조작하거나, 공격을 쉽게 하기 위해 기기의 보안 정책을 변경하거나 약화시킵니다. 기기에서 데이터를 공격하려면 종종 Thunderbolt, Lightning 또는 USB-C와 같은 물리적 인터페이스를 사용하여 기기와 통신해야 할 수 있습니다. Apple 기기는 이러한 공격을 방지하는 데 도움이 되는 기능을 포함하고 있습니다.

Apple 기기는 암호화 자료를 기기 외부에서 사용할 수 없도록 렌더링하거나 적합한 사용자 인증 없이 운영 체제 버전 또는 보안 설정을 조작하는 경우에 사용되는 **SKP(봉인 키 보호)**라는 기술을 지원합니다. 이 기능은 Secure Enclave에서 제공되지 **않으며**, 대신 Secure Enclave와 독립적인 사용자 데이터 암호화 해제에 필요한 키에 추가 보호 계층을 제공하기 위해 하위 계층에 있는 하드웨어 레지스터에서 지원됩니다.

참고: SKP는 Apple이 설계한 SoC가 있는 기기에서만 사용할 수 있습니다.

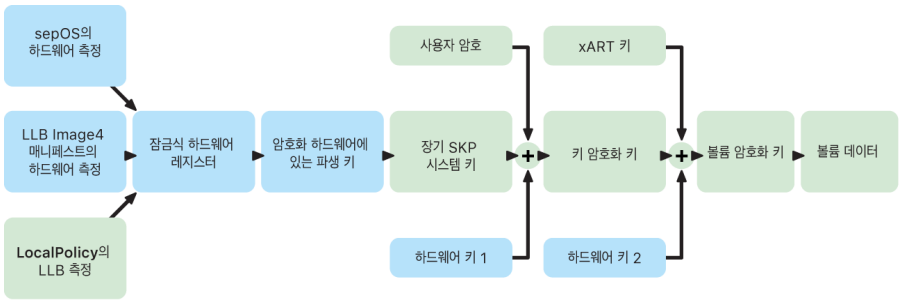
기능	A11–A17 S3–S9 M1, M2, M3
봉인 키 보호	✓

또한 iPhone 및 iPad 기기를 해당 기기가 여전히 인증된 소유자의 물리적 통제하에 있음을 나타내는 가능성이 더 높은 조건에서만 데이터 연결을 활성화하도록 구성할 수도 있습니다.

SKP(봉인 키 보호)

데이터 보호를 지원하는 Apple 기기에서 KEK(키 암호화 키)는 시스템의 소프트웨어 측정값으로 보호되거나 봉인되며 Secure Enclave에서만 사용할 수 있는 UID에 연결됩니다. Apple Silicon이 탑재된 Mac에서 macOS는 다른 플랫폼에서 지원되지 않는 중요한 보안 정책 변경(예: 보안 시동 또는 SIP 비활성화)을 지원하기 때문에 시스템의 보안 정책에 대한 정보를 통합하여 KEK의 보호를 한층 강화합니다. Apple Silicon이 탑재된 Mac 시스템에서 FileVault는 데이터 보호(클래스 C)를 사용하여 구현되므로 이 보호에는 FileVault 키가 포함됩니다.

사용자 암호, 장기 SKP 키 및 하드웨어 키 1(Secure Enclave의 UID)를 연결하여 파생된 키는 **암호 파생 키**라고 합니다. 이 키는 지원되는 모든 플랫폼의 User keybag과 KEK(macOS만 해당)를 보호하고 Apple Watch와 같이 다른 기기에서 생체 인식 잠금 해제 또는 자동 잠금 해제를 활성화하는 데 사용됩니다.



Secure Enclave 시동 모니터는 로드된 Secure Enclave OS의 측정값을 캡처합니다. 응용 프로그램 프로세서 Boot ROM에서 LLB에 연결된 Image4 매니페스트를 측정할 때 해당 매니페스트는 로드된 다른 모든 시스템 쌍 펌웨어의 측정값도 포함합니다. LocalPolicy는 로드된 macOS에 대한 핵심 보안 구성을 포함합니다. 또한 LocalPolicy는 macOS Image4 매니페스트의 해시인 `nsih` 필드를 포함합니다. macOS Image4 매니페스트는 모든 macOS 쌍 펌웨어 및 부트 커널 모음 또는 SSV(서명된 시스템 볼륨) 루트 해시와 같은 핵심 macOS 시동 개체의 측정값을 포함합니다.

위에서 측정한 펌웨어, 소프트웨어 또는 보안 구성 요소를 공격자가 예기치 않게 변경할 수 있는 경우, 하드웨어 레지스터에 저장된 측정값을 수정합니다. 측정값이 수정되면 키 계층의 봉인을 효과적으로 해제하며 암호화 하드웨어 파생 **SMRK(시스템 측정 루트 키)**가 다른 값으로 유도됩니다. 이는 **SMDK(시스템 측정 장치 키)**에 접근할 수 없도록 만들고, 이에 따라 KEK를 유발하여 데이터에 접근할 수 없게 됩니다.

하지만 시스템이 공격받고 있는 상황이 아닌 경우 LocalPolicy의 `nsih` 필드와 펌웨어 측정을 변경하는 합법적 소프트웨어 업데이트를 수용하여 새로운 macOS 측정값을 가리키도록 해야 합니다. 펌웨어 측정 통합을 시도하지만 신뢰할 수 있는 확인된 정보가 없는 다른 시스템에서는 사용자가 보안을 비활성화하고 펌웨어를 업데이트한 다음, 보안을 다시 활성화해야 새로운 측정 기준을 캡처할 수 있습니다. 이로 인해 소프트웨어 업데이트 중 공격자가 펌웨어를 변조할 수 있는 위험이 크게 증가합니다. Image4 매니페스트가 필요한 모든 측정값을 포함한다는 사실은 이 시스템에 도움을 줍니다. 일반적인 시동 과정 중 측정값이 일치하는 경우, SMRK로 SMDK를 암호화 해제하는 하드웨어는 제시된 향후 SMRK로 SMDK를 암호화할 수도 있습니다. 하드웨어는 소프트웨어 업데이트 후 예상되는 측정값을 지정함으로써 현재 운영 체제에서 접근 가능한 SMDK를 암호화하여 향후 운영 체제에서 접근할 수 있게 합니다. 마찬가지로 고객이 LocalPolicy에서 자신의 보안 설정을 합법적으로 변경하는 경우, 다음 재시동 시 LLB가 계산하는 LocalPolicy에 대한 측정값을 기반으로 하여 SMDK를 향후 SMRK로 암호화해야 합니다.

Apple 파일 시스템의 역할

APFS(Apple 파일 시스템)는 암호화를 중점에 두고 설계된 Apple 소유의 파일 시스템입니다. APFS는 iPhone, iPad, Mac, Apple TV 및 Apple Watch와 같은 Apple의 모든 플랫폼에 적용되어 있습니다. APFS는 플래시/SSD 저장 장치에 최적화되었으며, 강력한 암호화, 쓰기 시 복사(Copy-on-Write) 메타데이터, 공간 공유, 파일 및 디렉토리 복제, 스냅샷, 빠른 디렉토리 크기 조정, 원자적 안전 저장 프리미티브(Atomic safe-save primitives), 향상된 파일 시스템 기반, I/O 통합 기능을 사용하는 고유한 쓰기 시 복사(Copy-on-Write) 설계 등의 특징으로 최대의 성능을 이끌어내면서도 데이터 신뢰성을 확보합니다.

저장 공간 공유

APFS는 저장 공간을 필요에 따라 할당합니다. 단일 APFS 컨테이너에 다수의 볼륨이 포함된 경우, 컨테이너의 남은 공간을 필요에 따라 공유하거나 개별 볼륨에 할당할 수 있습니다. 개별 볼륨은 전체 컨테이너의 일부만 사용하므로, 사용할 수 있는 공간은 컨테이너의 전체 크기에서 컨테이너의 모든 볼륨이 사용하고 있는 공간을 뺀 크기와 같습니다.

다중 볼륨

macOS 10.15 이상에서 Mac을 시동하는 데 사용되는 APFS 컨테이너는 최소 다섯 개의 볼륨을 포함해야 하며, 처음 세 개의 볼륨은 사용자가 볼 수 없도록 가려져 있습니다.

- **사전 시동 볼륨:** 이 볼륨은 암호화되지 않았으며 컨테이너의 각 시스템 볼륨을 시동하는 데 필요한 데이터가 포함됩니다.
- **VM 볼륨:** 이 볼륨은 암호화되지 않았으며 macOS가 암호화된 스왑 파일을 저장하는 데 사용됩니다.
- **복구 볼륨:** 이 볼륨은 암호화되지 않았으며 복구용 OS를 시동하기 위해 시스템 볼륨을 잠금 해제하지 않은 상태로 사용 가능해야 합니다.
- **시스템 볼륨:** 다음을 포함합니다.
  - Mac을 시동하는 데 필요한 모든 파일
  - macOS에 기본으로 설치된 모든 앱(기존에 /응용 프로그램 폴더에 있던 앱은 이제 /시스템/응용 프로그램에 있음)

  참고: 기본적으로 Apple 시스템 프로세스를 포함한 어떤 프로세스도 시스템 볼륨에 쓰기 작업을 수행할 수 없습니다.
- **데이터 볼륨:** 다음과 같이 변경될 수 있는 데이터가 포함됩니다.
  - 사진, 음악, 비디오, 문서를 포함한 사용자의 폴더에 있는 데이터
  - AppleScript와 Automator 응용 프로그램을 포함한 사용자가 설치한 앱
  - 사용자, 조직, 타사 앱이 설치한 사용자 지정 프레임워크 및 데몬
  - 사용자가 소유하고 쓸 수 있는 위치(/응용 프로그램, /라이브러리, /사용자, /Volumes, /usr/local, /private, /var, /tmp)

모든 추가 시스템 볼륨에 데이터 볼륨이 생성됩니다. 사전 시동, VM, 복구 볼륨은 모두 공유되며 복제되지 않습니다.

macOS 11 이상에서 시스템 볼륨이 스냅샷으로 캡처됩니다. 운영 체제는 변경 가능한 시스템 볼륨의 단순 읽기 전용 마운트가 아닌 시스템 볼륨의 스냅 샷에서 시동됩니다.

iOS 및 iPadOS 기기의 저장 공간은 최소 두 개의 APFS 볼륨으로 나뉘어 있습니다.

- 시스템 볼륨
- 데이터 볼륨

키체인 데이터 보호

대부분의 앱은 키 및 로그인 토큰 같은 작지만 민감한 데이터와 암호를 안전하게 처리해야 합니다. 키체인은 이러한 항목을 안전하게 저장하는 방법을 제공합니다. 다양한 Apple 운영 체제는 서로 다른 메커니즘을 사용하여 여러 키체인 보호 클래스와 관련된 보증을 시행합니다. macOS(Apple Silicon이 탑재된 Mac 포함)에서 이러한 보증을 시행하는 데 데이터 보호가 직접 사용되지 않습니다.

개요

키체인 항목은 서로 다른 두 개의 AES-256-GCM 키인 테이블 키(메타데이터) 및 행별 키(비밀 키)를 사용하여 암호화됩니다. 키체인 메타데이터(kSecValue를 제외한 모든 속성)는 검색 속도를 높이기 위해 메타데이터 키로 암호화되고 비밀 값(kSecValueData)은 비밀 키로 암호화됩니다. 메타데이터 키는 Secure Enclave로 보호되지만 빠른 키체인 쿼리를 위해 응용 프로그램 프로세서에 캐시됩니다. 비밀 키는 Secure Enclave 내에서 항상 왕복으로 움직여야 합니다.

키체인은 파일 시스템에 저장되어 있는 SQLite 데이터베이스로 구현되어 있습니다. 데이터베이스는 단 하나이며, `securityd` 데몬이 각 프로세스 또는 앱의 키체인 항목 접근 권한을 결정합니다. 결과적으로 키체인 접근 API가 데몬으로 요청되고 데몬은 앱의 'Keychain-access-groups', 'application-identifier', 'application-group' 권한을 쿼리하는 방식입니다. 단일 프로세스로 접근을 제한하는 대신에 접근 그룹을 통해 앱 간에 키체인 항목이 공유될 수 있습니다.

키체인 항목은 같은 개발자가 개발한 앱 사이에서만 공유될 수 있습니다. 키체인 항목을 공유하기 위해 타사 앱은 해당 응용 프로그램 그룹의 Apple Developer Program을 통해 할당받은 접두사가 지정된 접근 그룹을 사용합니다. 접두사 요구 사항 및 응용 프로그램 그룹 특정성은 코드 서명, 권한 설정 프로파일 및 Apple Developer Program을 통해 강제로 적용됩니다.

키체인 데이터는 파일 데이터 보호에 사용했던 것과 비슷한 클래스 구조를 사용해 보호됩니다. 이러한 클래스는 파일 데이터 보호 클래스와 동일하게 동작하지만 고유한 키와 기능을 사용합니다.

사용 가능 시기	파일 데이터 보호	키체인 데이터 보호
잠금 해제한 경우	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
잠겨 있는 경우	NSFileProtectionComplete UnlessOpen	✕
처음 잠금 해제한 경우	NSFileProtectionComplete UntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
항상	NSFileProtectionNone	kSecAttrAccessibleAlways
암호 활성화됨	✕	kSecAttrAccessibleWhen PasscodeSetThisDeviceOnly

백그라운드 새로 고침 서비스를 활용하는 앱은 백그라운드 업데이트 중에 접근해야 하는 키체인 항목에 대해 **kSecAttrAccessibleAfterFirstUnlock** 클래스를 사용할 수 있습니다.

kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly 클래스는 **kSecAttrAccessibleWhenUnlocked** 클래스와 똑같이 동작하지만 기기의 암호가 구성된 경우에만 사용 가능합니다. 이 클래스는 System Keybag에만 존재하기 때문에 다음과 같은 제한 사항이 있습니다.

- iCloud 키체인과 동기화되지 않음
- 백업되지 않음
- Escrow keybag에 포함되지 않음

암호가 제거되거나 재설정된 경우 이 클래스 키를 삭제하여 이 항목을 사용할 수 없는 것으로 간주합니다.

다른 키체인 클래스는 '이 기기에서만'의 대응 항목을 가지고 있습니다. 대응 항목은 백업 중에 기기에서 복사되는 경우 UID로 항상 보호되며, 백업이 다른 기기에 복원되는 경우에는 사용할 수 없습니다. Apple은 보호되는 정보의 종류와 iOS 및 iPadOS에서 필요로 하는 경우에 따라 달라지는 키체인 클래스를 선택함으로써 보안성과 사용성의 균형을 맞추었습니다.

키체인 데이터 클래스 보호

아래에 나열된 클래스 보호는 키체인 항목을 대상으로 시행됩니다.

항목	접근 가능 시기
Wi-Fi 암호	처음 잠금 해제한 경우
Mail 계정	처음 잠금 해제한 경우
Microsoft Exchange ActiveSync 계정	처음 잠금 해제한 경우
VPN 암호	처음 잠금 해제한 경우
LDAP, CalDAV, CardDAV	처음 잠금 해제한 경우
소셜 네트워크 계정 토큰	처음 잠금 해제한 경우
Handoff 알림 암호화 키	처음 잠금 해제한 경우
iCloud 토큰	처음 잠금 해제한 경우
iMessage 키	처음 잠금 해제한 경우
홈 공유 암호	잠금 해제한 경우
Safari 암호	잠금 해제한 경우
Safari 책갈피	잠금 해제한 경우
Finder/iTunes 백업	잠금 해제한 경우, 이동할 수 없음
VPN 인증서	처음 잠금 해제한 경우, 이동할 수 없음
Bluetooth® 키	항상, 이동할 수 없음
APNS(Apple 푸시 알림 서비스) 토큰	항상, 이동할 수 없음
iCloud 인증서 및 개인 키	항상, 이동할 수 없음
SIM PIN	항상, 이동할 수 없음
나의 찾기 토큰	항상
음성 메시지	항상

macOS에서는 구성 프로파일을 통해 설치된 모든 키체인 항목을 **항상** 사용할 수 있습니다. iOS 및 iPadOS에서는 구성 프로파일을 통해 설치된 키체인 항목이 유형, 참조 방식 및 설치 날짜에 따라 다른 접근성을 가지고 있습니다. 기본적으로, 구성 프로파일을 통해 설치된 키체인 항목은 **처음 잠금을 해제한 후에 사용할 수 있고, 이동할 수 없습니다**. 그러나 다음 경우에는 구성 프로파일을 통해 설치된 키체인 항목을 **항상** 사용할 수 있습니다.

- iOS 15 또는 iPadOS 15 이상으로 업그레이드하기 전에 설치되었을 경우
- 신원이 아닌 인증서일 경우
- `com.apple.mdm` 페이로드의 `IdentityCertificateUUID`에 의해 참조된 신원일 경우

키체인 접근 제어

키체인은 접근 제어 목록(ACL)을 통해 접근성과 인증 요구 사항에 대한 정책을 설정할 수 있습니다. Face ID 및 Touch ID 또는 기기 암호 입력을 통해 인증하는 경우에만 키체인 항목에 접근할 수 있도록 명시하여 사용자의 직접 입력이 필요한 조건을 확립할 수 있습니다. 또한, 항목이 추가된 이후에 Face ID 및 Touch ID 등록이 변경되지 않도록 명시하여 항목 접근을 제한할 수도 있습니다. 이러한 제한 사항 덕분에 해커가 지문을 추가해도 키체인 항목에 접근할 수 없습니다. ACL은 Secure Enclave 내에서 평가되어 명시된 제약 조건이 충족되는 경우에만 커널에 공개됩니다.

macOS의 키체인 아키텍처

또한 macOS에서는 키체인에 접근 권한을 제공하여 사용자 이름과 암호, 디지털 ID, 암호화 키, 보안 메모를 편리하고 안전하게 저장할 수 있습니다. 키체인에는 /응용 프로그램/유틸리티/에 위치한 키체인 접근 앱을 열어서 접근할 수 있습니다. 키체인을 사용하면 출처별로 자격 증명을 입력하거나 기억할 필요가 없습니다. Mac의 사용자별로 최초 기본 키체인이 생성되지만 사용자는 특정한 용도로 사용할 키체인을 별도로 생성할 수 있습니다.

macOS는 사용자 키체인 외에도 다양한 시스템 수준의 키체인을 활용해 네트워크 자격 증명과 PKI(공개 키 인프라) ID 등 사용자별로 특정하지 않은 인증 자산을 유지합니다. 이러한 키체인 중 하나인 시스템 루트는 변경이 불가능하며 인터넷 PKI 루트 인증 기관(CA) 인증서를 저장해 온라인 뱅킹과 전자상거래 등의 일반적인 작업을 보조합니다. 사용자는 내부에서 권한이 설정된 CA 인증서를 관리되는 Mac 컴퓨터에 이와 유사하게 배포해 내부 사이트와 서비스를 검증하는 데 도움을 얻을 수 있습니다.

FileVault

macOS에서 FileVault를 사용한 볼륨 암호화

Mac 컴퓨터는 FileVault라는 내장 암호화 기능으로 모든 데이터를 안전하게 보호합니다. FileVault는 AES-XTS 데이터 암호화 알고리즘을 사용해 전체 내부 볼륨과 제거 가능한 저장 장치의 볼륨을 보호합니다.

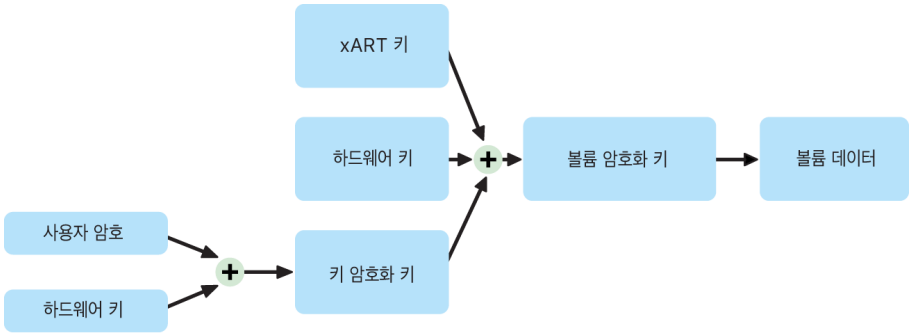
사실상 Apple Silicon이 탑재된 Mac의 FileVault는 볼륨 키와 함께 데이터 보호 클래스 C를 사용하여 구현됩니다. Apple Silicon이 탑재된 Mac과 Apple T2 보안 칩이 탑재된 Mac에는 암호화된 내장 저장 장치와 Secure Enclave가 직접 연결되어 Secure Enclave의 하드웨어 보안 기능과 AES 엔진의 하드웨어 보안 기능을 활용합니다. 사용자가 Mac에서 FileVault를 켜면 시동 시에 자격 증명을 요구합니다.

참고: (1) **T2 칩 탑재 이전 모델**이거나, (2) **Mac 출고 시 포함되지 않은** 내부 저장 공간이 있거나, (3)외장 저장 장치가 연결된 Mac 컴퓨터의 경우: FileVault가 켜진 후에 모든 기존 파일 및 추가로 작성된 데이터는 암호화됩니다. FileVault를 켜기 전에 추가되었다가 삭제된 데이터는 암호화되지 않으며 포렌식 데이터 복구 도구로 복구할 수 있습니다.

FileVault가 켜진 내부 저장 공간

유효한 로그인 자격 증명이나 암호화된 복구 키가 없을 경우 물리적 저장 장치를 제거하고 다른 컴퓨터에 연결하더라도 내부 APFS 볼륨은 암호화된 상태로 유지되며 무단 접근으로부터 보호됩니다. macOS 10.15의 경우에는 시스템 볼륨 및 데이터 볼륨이 포함됩니다. macOS 11부터는 SSV(서명된 시스템 볼륨) 기능을 통해 시스템 볼륨이 보호되지만 데이터 볼륨은 암호화로 보호됩니다. Apple Silicon이 탑재된 Mac 및 T2 칩이 탑재된 Mac에서 내부 볼륨 암호화는 키 계층을 구성하고 관리하는 방식으로 구현되고, 칩에 내장된 하드웨어 암호화 기술을 기반으로 구축됩니다. 이러한 키 계층은 다음과 같은 네 가지 목표를 동시에 달성하도록 설계되었습니다.

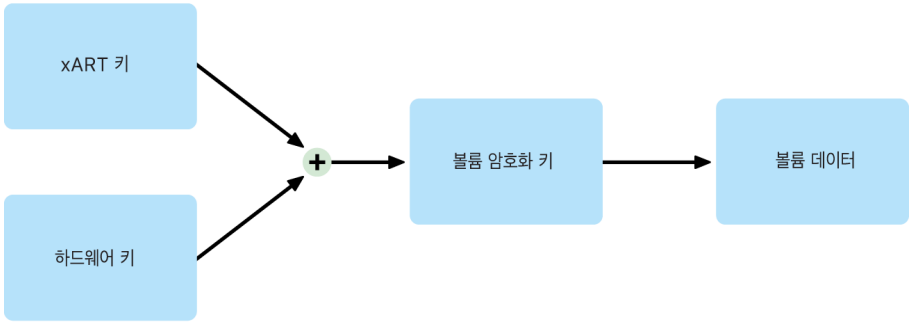
- 암호화 해제에 사용자의 암호를 요구
- Mac에서 제거된 저장 미디어에 직접 가해지는 무작위 대입 공격으로부터 시스템 보호
- 필요한 암호화 자료를 삭제하여 신속하고 안전하게 콘텐츠를 제거할 수 있는 방안 제공
- 사용자가 전체 볼륨을 다시 암호화하지 않고 암호를 변경(따라서 파일 보호에 사용되는 암호화 키도 함께 변경)할 수 있도록 허용



Apple Silicon이 탑재된 Mac 및 T2 칩이 탑재된 Mac에서는 모든 FileVault 키 처리가 Secure Enclave에서 수행되며, 암호화 키는 Intel CPU에 절대로 직접 노출되지 않습니다. 기본적으로 모든 APFS 볼륨은 볼륨 암호화 키와 함께 생성됩니다. 볼륨과 메타데이터 콘텐츠는 이 볼륨 암호화 키로 암호화되며, 이 볼륨 키는 키 암호화 키(KEK)로 래핑됩니다. FileVault가 켜진 상태에서 KEK는 사용자 암호와 하드웨어 UID의 조합으로 보호됩니다.

FileVault가 꺼진 내부 저장 공간

Apple Silicon이 탑재된 Mac 또는 T2 칩이 탑재된 Mac에서는 FileVault가 켜져 있지 않더라도 최초 설정 지원 과정에서 볼륨은 암호화된 상태이지만, 볼륨 암호화 키는 Secure Enclave의 하드웨어 UID로만 보호됩니다.



FileVault를 나중에 켤 경우, 데이터는 이미 암호화된 상태였으므로 활성화가 즉시 처리되며, 재전송 방지 처리 과정으로 하드웨어 UID만을 기반으로 하는 기존의 키가 볼륨 암호화 해제에 사용되지 못하게 막습니다. 이후 볼륨은 앞서 설명한 바와 같이 사용자 암호와 하드웨어 UID의 조합으로 보호됩니다.

FileVault 볼륨 삭제

볼륨을 삭제하면 Secure Enclave를 통해 볼륨 암호화 키가 안전하게 삭제됩니다. 이를 통해 나중에 Secure Enclave를 사용하더라도 이 키를 사용해서는 접근할 수 없게 됩니다. 또한 모든 볼륨 암호화 키는 미디어 키로 래핑됩니다. 미디어 키는 데이터에 기밀성을 더해주지는 않지만, 대신 데이터를 신속하고 안전하게 지울 수 있도록 설계되었습니다(미디어 키가 없으면 암호 해제가 불가능).

Apple Silicon이 탑재된 Mac 및 T2 칩이 탑재된 및 Mac에서 미디어 키는 Secure Enclave가 지원하는 기술(예: 원격 MDM 명령)을 통해 지울 수 있습니다. 미디어 키를 이렇게 삭제하면 볼륨이 암호화 형식으로 접근할 수 없게 렌더링됩니다.

제거 가능한 저장 장치

제거 가능한 저장 장치를 암호화할 때에는 Secure Enclave의 보안 기능이 사용되지 않으며, T2 칩이 탑재되지 않은 Intel 기반 Mac과 같은 방식으로 암호화가 수행됩니다.

macOS에서 FileVault 관리

macOS에서는 조직이 SecureToken 또는 Bootstrap Token을 사용하여 FileVault를 관리할 수 있습니다.

Secure Token 사용

macOS 10.13 이상 버전의 APFS(Apple 파일 시스템)는 FileVault 암호화 키를 생성하는 방법을 변경합니다. CoreStorage 볼륨에 있는 이전 버전의 macOS에서 FileVault 암호화 프로세스에 사용되던 키는 사용자나 기관이 Mac에서 FileVault를 켠 경우에 생성되었습니다. APFS 볼륨에 있는 macOS에서 이 키는 사용자를 만들거나 첫 사용자의 암호를 설정하거나 어떤 사용자가 Mac에 처음으로 로그인할 때 생성됩니다. 이 암호화 키의 구현, 생성 시기, 저장 방법은 모두 **Secure Token**이라는 기능의 일부입니다. 더 자세히 말하면, Secure Token은 사용자 암호로 보호되는 KEK(키 암호화 키)가 래핑된 것입니다.

APFS에 FileVault를 배포할 때 사용자는 다음과 같은 작업을 계속할 수 있습니다.

- MDM(모바일 기기 관리) 솔루션에 저장해 에스크로가 가능한 PRK(개인 복구 키) 등 기존 도구와 프로세스 사용
- 사용자가 Mac에서 로그인하거나 로그아웃할 때까지 FileVault 활성화 연기
- IRK(기관 복구 키) 생성 및 사용

macOS 11에서 Mac의 첫 사용자의 초기 암호를 설정하면 해당 사용자에게 Secure Token이 부여됩니다. 일부 작업흐름의 경우 최상의 방법은 아니지만 이전과 같이 첫 번째 Secure Token을 부여하면 해당 사용자 계정으로 로그인해야 할 수 있습니다. 이러한 상황이 발생하지 않도록 하려면 사용자의 암호를 설정하기 전에 다음과 같이 프로그램을 통해 생성한 사용자의 `AuthenticationAuthority` 속성에 `;DisabledTags;SecureToken`을 추가하십시오.

```
sudo dscl . append /Users/<user name> AuthenticationAuthority
";DisabledTags;SecureToken"
```

Bootstrap Token 사용

macOS 10.15에 도입된 새로운 **Bootstrap Token** 기능은 모바일 계정과 기기 등록으로 만들어진 선택적인 관리자 계정('관리형 관리자') 양쪽 모두에 Secure Token을 부여하는 기능을 지원합니다. macOS 11에서 Bootstrap Token은 로컬 사용자 계정을 포함하여 Mac 컴퓨터에 로그인하는 모든 사용자에게 Secure Token을 부여할 수 있습니다. macOS 10.15 이상에서 Bootstrap Token 기능을 사용하려면 다음과 같은 요건을 충족해야 합니다.

- Mac을 감독하도록 Apple School Manager 또는 Apple Business Manager를 사용해 MDM에 Mac을 등록
- MDM 공급업체 지원

macOS 10.15.4 이상에서 MDM 솔루션이 기능을 지원하는 경우 Secure Token이 활성화된 사용자가 처음 로그인할 때 Bootstrap Token이 생성되고 MDM으로 에스크로됩니다. 필요한 경우 `profiles` 명령어 라인 도구를 사용하여 Bootstrap Token을 생성하고 MDM에 에스크로할 수도 있습니다.

macOS 11에서는 Bootstrap Token을 사용하여 사용자 계정에 Secure Token을 부여하는 이상의 작업을 수행할 수도 있습니다. Apple Silicon이 탑재된 Mac에서는 MDM을 통해 관리되는 상태의 경우에 Bootstrap Token을 사용하여 커널 확장 프로그램 및 소프트웨어 업데이트의 설치를 승인할 수 있습니다.

기관 및 개인 복구 키 비교

CoreStorage 및 APFS 볼륨 양쪽에서 FileVault는 기관 복구 키(이전에 **FileVault Master identity**로 알려진 IRK) 사용을 통한 볼륨 잠금 해제를 지원합니다. IRK는 볼륨의 잠금을 해제하거나 FileVault 를 완전히 끄기 위한 명령어 라인 작업에 유용하지만, 특히 macOS의 최신 버전에서 조직에 대한 활용성은 제한되어 있습니다. Apple Silicon이 탑재된 Mac의 경우, IRK는 다음 두 가지 이유에서 아무런 기능성도 제공하지 않습니다. 먼저, IRK는 복구용 OS에 접근하는 데 사용할 수 없으며, 둘째, 더 이상 대상 디스크 모드가 지원되지 않기 때문에 다른 Mac에 연결하여 볼륨의 잠금을 해제할 수 없습니다. 이러한 이유 등으로 인해, **Mac 컴퓨터의 FileVault를 기관이 관리하는 데 있어 IRK의 사용은 더 이상 권장되지 않습니다**. 대신 개인 복구 키(PRK)를 사용해야 합니다.

Apple이 사용자의 개인 데이터를 보호하는 방법

사용자 데이터에 대한 앱 접근 방지

Apple 기기는 데이터를 안전하게 암호화하는 동시에, Data Vault 등 여러 기술을 사용하여 권한이 없는 앱에서 사용자의 개인정보에 접근하는 것을 방지합니다. iOS 및 iPadOS의 설정과 macOS의 시스템 설정(macOS 13 이상) 또는 시스템 환경설정(macOS 12 또는 이전 버전)에서 사용자는 특정 정보에 대한 접근 권한이 있는 앱을 확인할 수 있으며 접근을 승인하거나 취소할 수도 있습니다. 다음의 경우에 접근이 강제됩니다.

- **iOS, iPadOS 및 macOS:** 캘린더, 카메라, 연락처, 마이크, 사진, 미리 알림 및 음성 인식
- **iOS 및 iPadOS:** Bluetooth, 홈, 미디어, 미디어 앱 및 Apple Music, 동작 및 피트니스
- **iOS 및 watchOS:** 건강
- **macOS:** 입력 모니터링(예: 키보드 스트로크), 알림 메시지, 화면 녹화(예: 스크린샷 및 비디오) 및 시스템 설정(macOS 13 이상) 또는 시스템 환경설정(macOS 12 또는 이전 버전)

iOS 13.4 이상 및 iPadOS 13.4 이상에서 모든 타사 앱은 Data Vault에서 자동으로 데이터를 보호합니다. Data Vault는 샌드박스되어 있지 않은 프로세스에서도 데이터에 무단으로 접근하는 것을 방지할 수 있습니다. iOS 15 이상의 추가 클래스는 로컬 네트워크, 근처 상호 작용, 리서치 센서 및 사용 데이터, 집중 모드를 포함합니다.

사용자가 iCloud에 로그인하면 iOS 및 iPadOS의 앱은 기본적으로 iCloud Drive에 접근할 수 있습니다. 사용자는 설정의 iCloud에서 각 앱 접근 권한을 제어할 수 있습니다. 또한 iOS 및 iPadOS에서는 앱 간의 데이터 이동과 MDM(모바일 기기 관리) 솔루션에서 설치한 계정 및 사용자가 설치한 계정 간에 데이터 이동을 방지하는 제한 설정을 제공합니다.

사용자의 건강 데이터에 대한 접근 방지

HealthKit는 iPhone 및 Apple Watch의 건강 및 피트니스 데이터용 중앙 저장소를 제공합니다. HealthKit는 또한 호환되는 BLE(Bluetooth Low Energy) 심박수 측정기 및 iOS 기기에 내장된 동작 인식 보조 프로세서와 같은 건강 및 피트니스 기기와 직접 작동합니다. HealthKit와 건강 앱 및 운동 앱, 의료 기관, 건강 및 운동 기기 간의 모든 상호 작용에는 사용자의 허락이 필요합니다. 이 데이터는 데이터 보호 클래스인 Protected Unless Open에 저장됩니다. 기기가 잠긴 지 10분이 지나면 건강 데이터에 접근할 수 없으며 해당 데이터에 접근하려면 암호를 입력하거나 Face ID 및 Touch ID를 사용하여 기기를 잠금 해제해야 합니다.

건강 및 피트니스 데이터 수집 및 저장

또한 HealthKit는 앱의 접근 권한, HealthKit에 연결된 기기의 이름, 새로운 데이터가 사용 가능할 경우 앱 실행에 사용되는 스케줄 정보 등의 관리 데이터를 수집하고 저장합니다. 이 데이터는 데이터 보호 클래스인 Protected Until First User Authentication에 저장됩니다. 임시 저널 파일은 기기가 잠겨지는 경우에 생성되는 건강 기록(예를 들어 사용자가 운동 중일 때)을 저장합니다. 이 파일은 데이터 보호 클래스인 Protected Unless Open에 저장됩니다. 기기가 잠금 해제되면 기본 건강 데이터베이스에 임시 저널 파일을 가져오고 병합이 완료되면 파일은 삭제됩니다.

건강 데이터는 iCloud에 저장할 수 있습니다. 건강 데이터의 종단간 암호화는 iOS 12 이상 및 이중 인증이 필요합니다. iOS 12 이상 및 이중 인증을 사용하지 않는 경우에도 사용자의 데이터는 저장 및 전송 시 여전히 암호화되지만 종단간으로 암호화되지는 않습니다. 이중 인증을 켜고 iOS 12 이상으로 업데이트하면 사용자의 건강 데이터가 종단간 암호화로 마이그레이션됩니다.

사용자가 Finder(macOS 10.15 이상) 또는 iTunes(macOS 10.14 또는 이전 버전)를 사용하여 기기를 백업하는 경우, 해당 백업이 암호화되는 경우에만 건강 데이터가 저장됩니다.

임상 건강 기록

사용자는 건강 앱 내에서 지원되는 건강 시스템에 로그인하여 자신의 임상 건강 기록 사본을 받을 수 있습니다. 사용자를 건강 시스템에 연결할 때 해당 사용자는 OAuth 2 클라이언트 자격 증명을 사용하여 인증합니다. 연결한 후 TLS 1.3으로 보호되는 연결을 통해 임상 건강 기록 데이터가 의료 기관에서 직접 다운로드됩니다. 다운로드한 후 임상 건강 기록이 다른 건강 데이터와 함께 안전하게 저장됩니다.

건강 데이터 신뢰성

데이터베이스에 저장된 데이터는 메타데이터를 가지고 있어 각 데이터 기록의 출처를 추적할 수 있습니다. 이 메타데이터에는 앱 식별자가 포함되어 있어 기록을 저장한 앱을 식별할 수 있습니다. 추가적으로 선택적인 메타데이터 항목은 디지털 서명된 기록의 사본을 포함할 수 있습니다. 이로 인해 신뢰하는 기기에서 생성된 기록은 데이터 신뢰성을 유지할 수 있습니다. 디지털 서명에 사용된 포맷은 RFC 5652에 명시된 CMS(암호화 메시지 구문)입니다.

타사 앱에서의 건강 데이터 접근

HealthKit API에 대한 접근은 권한을 통해 제어되며 앱은 데이터의 사용 방식에 대한 제한 사항을 따라야 합니다. 예를 들어 앱은 건강 데이터를 광고에 사용할 수 없습니다. 앱은 또한 건강 데이터 사용에 대해 상세히 설명한 개인정보 처리방침을 사용자에게 필수적으로 제공해야 합니다.

사용자는 개인정보 보호 설정에서 건강 데이터에 접근하는 앱을 제어할 수 있습니다. 연락처 앱, 사진 앱 및 다른 iOS 데이터 소스처럼 앱이 건강 데이터에 대한 접근을 요청하는 경우 사용자에게 접근 승인을 요청합니다. 하지만 건강 데이터의 경우 앱은 건강 데이터의 각 유형에 대해서와 마찬가지로 읽기 및 쓰기 데이터에 대한 접근을 따로 부여받습니다. 사용자는 설정 > 건강 > 데이터 접근 및 기기에서 건강 데이터 접근 권한을 보거나, 회수할 수 있습니다.

데이터 쓰기 권한이 부여된 경우 앱은 앱이 쓴 데이터를 읽을 수도 있습니다. 데이터 읽기 권한이 부여된 경우 앱은 모든 소스가 쓴 데이터를 읽을 수 있습니다. 하지만 앱은 다른 앱에 부여된 권한을 확인할 수 없습니다. 또한 앱은 건강 데이터에 읽기 접근 권한이 있는지를 확인할 수 없습니다. 앱이 읽기 접근 권한을 가지지 않은 경우 모든 쿼리에 데이터 없음을 반환합니다. 데이터 없음은 데이터베이스가 비어 있을 때 반환하는 결과와 같습니다. 이렇게 함으로써 앱이 사용자가 추적하는 데이터 유형을 학습하여 사용자의 건강 상태를 추측하는 것을 방지합니다.

사용자 의료 정보

건강 앱은 사용자에게 의료 정보 양식을 제공해 긴급 상황에서 중요하게 사용될 수 있는 정보를 작성하는 옵션을 제공합니다. 이 정보는 수동으로 입력되고 업데이트되며 건강 데이터베이스의 정보와는 동기화되지 않습니다.

의료 정보는 잠금 화면에서 긴급상황 버튼을 탭하여 볼 수 있습니다. 이 정보는 데이터 보호 클래스인 No Protection을 사용해 기기에 저장되므로, 기기 암호를 입력하지 않고도 접근이 가능합니다. 의료 정보는 선택적 기능으로 사용자가 안전과 개인정보 보호 중 선택하여 활성화할 수 있습니다. 이 데이터는 iOS 13 또는 이전 버전에서 iCloud 백업에 백업됩니다. iOS 14에서 의료 정보는 CloudKit를 사용하는 기기 간에 동기화되며 나머지 건강 데이터와 동일한 암호화 특성을 갖습니다.

건강 공유

iOS 15에서 건강 앱은 사용자가 다른 사용자와 건강 데이터를 공유하는 옵션을 제공합니다. 건강 데이터는 종단간 iCloud 암호화를 사용하는 두 사용자 간에 공유되고 Apple은 건강 공유를 통해 전송된 데이터에 접근할 수 없습니다. 이 기능을 사용하려면 통신하는 두 사용자는 모두 iOS 15 이상을 사용하고 이중 인증을 활성화해야 합니다.

사용자들은 건강 앱에서 '제공자와 공유' 기능을 사용하여 의료 서비스 제공자에게 건강 데이터를 공유할 수도 있습니다. 이 기능을 사용하여 공유한 데이터는 종단간 암호화를 사용하는 사용자가 선택한 의료 기관만 사용 가능하며, Apple은 '제공자와 공유' 기능을 통해 공유된 건강 데이터의 암호화를 해제하거나, 보거나, 접근하기 위한 암호화 키를 유지하거나 그에 대한 접근 권한을 갖지 않습니다. 이 서비스의 설계가 사용자의 건강 데이터를 보호하는 방법에 대한 자세한 내용은 Apple 의료 기관용 신청 설명서의 보안 및 개인정보 보호 섹션에서 확인할 수 있습니다.

디지털 서명 및 암호화

접근 제어 목록

키체인 데이터는 ACL(접근 제어 목록)로 분할 및 보호됩니다. 따라서 타사 앱으로 저장된 자격 증명은 사용자가 명확하게 승인하지 않는 한 다른 ID를 사용하는 다른 앱에서 접근할 수 없습니다. 이 보호 기능은 조직 내에서 Apple 기기의 다양한 앱과 서비스에 대한 인증 자격 증명을 얻는 메커니즘을 제공합니다.

Mail

Mail 앱 사용자는 전자 서명 및 암호화된 메시지를 전송할 수 있습니다. Mail 앱은 호환되는 스마트 카드에 첨부된 PIV(개인 식별 인증) 토큰의 디지털 서명과 암호화 인증서에서 적절한 RFC 5322 대소문자 구분 이메일 주소 주체나 주체 대체 이름을 자동으로 발견합니다. 구성된 이메일 계정이 첨부된 PIV 토큰의 디지털 서명이나 암호화 인증서에 있는 이메일 주소와 일치할 경우, Mail 앱은 새로운 메시지 윈도우 도구 막대에 서명 버튼을 자동으로 표시합니다. Mail 앱에 수신자의 이메일 암호화 인증서가 있거나, Microsoft Exchange GAL(Global Address List)을 발견할 수 있는 경우 새로운 메시지 도구 막대에 잠금 해제된 아이콘이 나타납니다. 잠긴 상태의 잠금 아이콘은 메시지가 수신자의 공개 키로 암호화되어 전송됨을 나타냅니다.

메시지별 S/MIME

iOS, iPadOS, macOS는 메시지별 S/MIME를 지원합니다. 즉, S/MIME 사용자는 기본적으로 모든 메시지를 서명 및 암호화할지, 아니면 메시지를 개별적으로 서명 및 암호화할지 선택할 수 있습니다.

S/MIME에 사용되는 ID는 구성 프로파일, MDM(모바일 기기 관리) 솔루션, SCEP(단순 인증서 등록 프로토콜), Microsoft Active Directory 인증 기관 등을 사용하는 Apple 기기로 전달될 수 있습니다.

스마트 카드

macOS 10.12 이상 버전은 PIV 카드를 기본으로 지원합니다. 이러한 카드는 상업 기관과 정부 기관 등에서 이중 인증, 디지털 서명, 암호화 등에 널리 사용됩니다.

스마트 카드는 공개 키와 개인 키 한 쌍과 관련 인증서로 이루어진 디지털 ID를 하나 이상 가지고 있습니다. PIN(개인 식별 번호)으로 스마트 카드의 잠금을 해제하면 인증, 암호화, 서명 작업에 사용되는 개인 키에 접근할 수 있습니다. 인증서는 사용할 수 있는 키는 어느 것인지, 인증서와 연결된 속성은 무엇인지, 인증 기관(CA) 인증서를 통해 검증(서명)될 수 있는지 등을 결정합니다.

스마트 카드는 이중 인증에 사용될 수 있습니다. 카드의 잠금을 해제하는 데 필요한 두 가지 요소는 '사용자가 소지하는 것'(카드) 및 '사용자가 아는 것'(PIN)입니다. macOS 10.12 이상에서는 Safari에서 웹 사이트 접속에 스마트 카드 로그인 윈도우 인증과 클라이언트 인증서 인증을 기본으로 지원합니다. Kerberos 지원 서비스에 대한 단일 로그인에 활용되는 키 쌍을 사용한 Kerberos 인증(PKINIT)도 지원됩니다. 스마트 카드와 macOS에 대해 자세히 알아보려면 **Apple 플랫폼 배포**의 스마트 카드 통합 개요를 참조하십시오.

암호화된 디스크 이미지

macOS에서 암호화된 디스크 이미지는 사용자의 민감한 문서나 파일 등을 보관하거나 전송하는 보안 컨테이너의 역할을 수행합니다. 암호화된 디스크 이미지는 /응용 프로그램/유틸리티/에 위치한 디스크 유틸리티로 만듭니다. 디스크 이미지는 128비트 또는 256비트 AES 암호화를 사용해 암호화할 수 있습니다. 마운트된 디스크 이미지는 Mac에 연결된 로컬 볼륨과 동일하게 취급되므로, 사용자는 그 안에 저장된 파일과 폴더를 복사하고 이동하거나 열 수 있습니다. FileVault와 마찬가지로 디스크 이미지에 있는 콘텐츠는 실시간으로 암호화되고 암호화 해제됩니다. 암호화된 디스크 이미지를 제거 가능한 미디어에 저장하거나, 이메일 메시지 첨부 파일로 전송하거나, 원격 서버에 저장하는 등의 방식으로 활용해 문서, 파일, 폴더 등을 안전하게 주고받을 수 있습니다. 암호화된 디스크 이미지에 대한 더 자세한 내용은 디스크 유틸리티 사용 설명서를 참조하십시오.

앱 보안

앱 보안 개요

오늘날에는 앱이 보안 아키텍처에서 가장 중요한 요소 중 하나입니다. 앱이 사용자에게 놀라운 생산성을 제공하더라도 제대로 관리되지 않는다면 시스템 보안, 안정성 및 사용자 데이터에 부정적인 영향을 줄 가능성이 있습니다.

이런 이유로 Apple에서는 앱에 알려진 악성 코드가 없고 변조되지 않았음을 확인할 수 있도록 계층형 보호 기능을 제공합니다. 추가 보호 기능은 앱에서 사용자 데이터에 접근하는 것을 신중하게 조정합니다. 이러한 보안 제어는 앱을 위한 안정적이고 안전한 플랫폼을 제공하여 수천 명의 개발자가 시스템 무결성을 해치지 않으면서 수십만 개의 앱을 iOS, iPadOS 및 macOS에 제공할 수 있도록 합니다. 그리고 사용자는 바이러스, 악성 코드 또는 무단 공격에 대한 걱정 없이 이러한 앱을 Apple 기기에서 사용할 수 있습니다.

iPhone 및 iPad의 모든 앱은 App Store에서 다운로드할 수 있고 샌드박스되어 가장 정밀한 제어를 제공합니다.

Mac에서 대부분의 앱은 App Store에서 가져오지만 Mac 사용자가 인터넷에서 앱을 다운로드하여 사용하기도 합니다. 안전한 인터넷 다운로드를 위해 macOS는 제어 단계를 추가합니다. 첫째, macOS 10.15 이상에서의 모든 Mac 앱은 기본적으로 Apple의 공증을 받아야 실행할 수 있습니다. 이 요구 사항은 앱이 App Store를 통해 제공되지 않더라도 해당 앱에 알려진 악성 코드가 없음을 보장할 수 있도록 합니다. 둘째, macOS에는 악성 코드를 차단하고 필요한 경우 악성 코드를 제거할 수도 있는 최신 안티바이러스 보호 기능이 포함되어 있습니다.

플랫폼 전반에 걸친 추가 제어 기능인 샌드박스는 앱의 무단 접근으로부터 사용자 데이터를 보호합니다. 그리고 macOS에서 중요한 영역의 데이터는 자체적으로 보호되기 때문에 접근을 시도하는 앱이 샌드박스되어 있는지와 상관없이 데스크탑, 문서, 다운로드 폴더 및 기타 영역에 있는 파일에 대한 모든 앱의 접근을 사용자가 계속 제어할 수 있도록 합니다.

고유 기능	유사 기능(타사)
플러그인 비승인 목록, Safari 확장 프로그램 비승인 목록	바이러스/악성 코드 정의
파일 격리	바이러스/악성 코드 정의
XProtect/Yara 서명	바이러스/악성 코드 정의, 엔드포인트 보호
Gatekeeper	엔드포인트 보호–신뢰하는 소프트웨어만 실행되도록 앱의 코드 서명을 요구함
eficheck (Apple T2 보안 칩이 탑재되지 않은 Mac의 경우 필수)	엔드포인트 보호–루트킷 감지
응용 프로그램 방화벽	엔드포인트 보호–방화벽
패킷 필터(pf)	방화벽 솔루션
시스템 무결성 보호	macOS에 내장됨
강제적 접근 제어	macOS에 내장됨
KEXT 제외 목록	macOS에 내장됨
의무 앱 코드 서명	macOS에 내장됨
앱 공증	macOS에 내장됨

iOS 및 iPadOS의 앱 보안

iOS 및 iPadOS의 앱 보안 개요

다른 모바일 플랫폼과는 달리 iOS 및 iPadOS는 사용자가 서명되지 않은 잠재적인 악성 앱을 웹 사이트를 통해 설치하거나 신뢰하지 않는 앱을 실행하도록 허용하지 않습니다. 그 대신 (EU 이외의 경우) 모든 앱을 App Store에서 다운로드해야 합니다. App Store의 모든 앱은 확인된 개발자가 제공하며 이러한 앱은 모두 자동화된 심사 및 사람의 심사를 거쳐야 합니다. 런타임 시, 페이지가 로드되는 동안 모든 실행 가능한 메모리 페이지의 코드 서명을 확인하여 앱이 설치되거나 마지막으로 업데이트된 이후에 앱이 변경되지 않았는지를 확인합니다.

앱의 출처가 승인된 출처인 것이 확인되면 iOS 및 iPadOS는 해당 앱이 다른 앱 또는 시스템 전체를 해치는 것을 방지하기 위해 고안된 보안책을 시행합니다.

App Store 보안에 관하여

App Store는 사용자가 안전하게 앱을 검색하고 다운로드할 수 있는 신뢰할 수 있는 공간입니다. App Store에서 앱은 Apple 지침을 준수하는 것에 동의한 확인된 개발자가 제공하며, 이러한 앱은 수정 방지에 대한 암호화 보증을 통해 사용자에게 안전하게 배포됩니다. 모든 앱 및 각각의 앱 업데이트는 심사를 통해 개인정보 보호, 보안 및 안전 요구 사항을 충족하는지 평가를 받습니다. 이 프로세스는 악성 코드, 사이버 범죄자, 사기꾼이 App Store에 침투하지 못하도록 막아 사용자를 보호하도록 설계되었으며, 지속적으로 향상되고 있습니다. 또한 어린이용으로 설계된 앱은 어린이를 안전하게 지키도록 마련된 엄격한 데이터 수집 및 보안 지침을 따라야 하며, iOS 및 iPadOS의 유해 콘텐츠 차단 기능과 긴밀하게 통합되어야 합니다.

App Store 보안 보호 사항에는 다음이 포함됩니다.

- **알려진 악성 코드에 대한 자동화된 스캔:** 악성 코드가 App Store에 침투하여 사용자에게 도달하거나 공격하는 것을 방지합니다.
- **전문가 팀 사람들이 수행하는 심사:** 마케팅 텍스트 및 스크린샷을 포함한 앱 설명의 정확성을 심사합니다. 이를 통해 악성 코드를 인기 있는 앱으로 위장하거나, 실제로는 제공되지 않는 흥미로운 기능을 제공한다고 주장하는 가장 흔한 악성 코드 배포 사기 방식에 철저히 대비할 수 있습니다.
- **수동 확인:** 앱이 불필요하게 민감한 데이터에 대한 접근을 요청하는지 확인하고, 어린이를 대상으로 한 앱이 엄격한 데이터 수집 및 안전 규칙을 따르는지 추가로 평가합니다.
- **사용자 중심의 신뢰할 수 있는 리뷰:** 문제를 표면화하며, 다수의 사용자를 현혹하려는 공격자의 성공 가능성을 크게 낮춥니다. 악성 앱이 심사 프로세스에서 자신의 동작을 완벽히 숨기더라도 해당 앱의 사용자가 문제를 발견하고 리포트하여 다른 사람과 Apple에게 알리기 때문에 탐지가 가능합니다. App Store는 이러한 신호의 유용성을 향상하도록 사기성 리뷰에 적극적으로 대응합니다.
- **수정 및 제거를 위한 프로세스:** 문제가 발생한 경우의 방안입니다. 어떤 앱이 App Store에 등록됐지만 나중에 지침을 어긴 것으로 판별된 경우, Apple은 개발자와 협력하여 문제를 빠르게 해결합니다. 사기 및 악성 활동이 연관된 위험한 상황의 경우, 해당 앱은 App Store에서 즉시 제거되며, 해당 앱을 다운로드한 사용자는 앱의 악성 동작에 대해 알림을 받을 수 있습니다.

iOS 및 iPadOS의 앱 보안은 모든 계층이 조합되어 이루어집니다. 강력한 앱 심사로 악성 앱의 설치를 방지하고, 강력한 플랫폼 보호로 악성 앱이 미칠 수 있는 손상을 제한합니다. iOS 및 iPadOS의 보안 설계는 소비자용 기기를 위한 최고 수준의 강력한 보호 기능을 사용자에게 제공하지만, 사용자를 사기로 인한 선택들로부터 보호하도록 설계되지는 않았습니다. 앱 심사에서는 사용자를 공격하거나 민감한 데이터에 대한 접근을 허용하도록 속이려는 앱으로부터 사용자를 보호하도록 설계된 App Store 정책을 적용하고 있습니다. 그리고 기기상의 보호 기능을 우회하려는 매우 심각한 악성 앱의 경우, 앱 심사는 이러한 앱이 아예 처음부터 사용자의 기기에 들어오기 어렵도록 하고 있습니다.

App Store 보안책만으로 완벽할 수는 없지만, 이는 플랫폼 보안을 위한 심층 방어(defense-in-depth) 전략의 일환으로서 iOS 및 iPadOS 사용자를 겨냥한 광범위한 공격을 무용하게 만들고, 경제적 이득을 노리는 공격자가 이익을 취하지 못하게 만드는 데 기여합니다. Apple은 앱에 악성 코드가 없고 앱이 정확하게 소개되도록 App Store 등록 전에 모든 앱을 심사하고, 앱에 유해한 문제가 있을 경우 앱이 배포되지 않도록 신속하게 제거하고 향후 변종이 퍼지는 것을 제한함으로써 App Store 생태계의 보안을 유지하고 고객이 App Store를 안심하고 사용할 수 있도록 지원합니다.

iOS 및 iPadOS의 앱 코드 서명 프로세스

iOS 및 iPadOS의 경우 Apple은 의무 코드 서명 및 엄격한 개발자 로그인 등을 통한 앱 보안을 제공합니다.

의무 코드 서명

iOS 또는 iPadOS 커널이 시작되면 해당 커널은 어떤 사용자 프로세스 및 앱을 실행할지를 제어합니다. iOS 및 iPadOS는 모든 앱이 알려지고 승인된 출처를 가지며 변조되지 않았음을 확인하기 위해 모든 실행 코드가 Apple이 발급한 인증서를 사용해 서명되도록 요구합니다. Mail 및 Safari와 같이 기기에 설치되어 제공되는 앱은 Apple이 서명했습니다. 타사 앱 또한 Apple이 발급한 인증서를 사용하여 확인되고 서명되어야 합니다. 의무 코드 서명은 신뢰 체인의 개념을 운영 체제에서부터 앱으로 확장하고 타사 앱이 서명되지 않은 코드 리소스를 로드하거나 자체 수정 코드를 사용하는 것을 방지합니다.

개발자가 앱에 서명하는 방법

개발자는 인증서 확인에 서명할 수 있습니다(Apple Developer Program을 통해). 또한 프레임워크를 앱에 내장하고 Apple에서 발급한 인증서로 해당 코드를 검증할 수 있습니다(팀 식별자 문자열을 통해).

- **인증서 확인:** 앱을 개발하거나 iPhone 또는 iPad 기기에 앱을 설치하려는 개발자는 Apple에 등록하고 Apple Developer Program에 가입해야 합니다. Apple은 각 개발자의 실제 신원이 개인인지 기업인지 확인한 후에 인증서를 발급합니다. 개발자는 이 인증서를 사용하여 App Store에 배포할 앱을 서명하고 배포할 수 있습니다. 그 결과로 App Store의 모든 앱은 신원 확인이 가능한 개인 또는 조직에서 제출하기 때문에 악성 앱 생성이 억제됩니다. 또한 Apple에서 앱을 검토하여 설명대로 정상적으로 작동하는지 명백한 오류 또는 중요한 다른 문제가 있는지 확인합니다. 이미 논의한 기술 이외에도 이러한 큐레이션 프로세스를 통해 사용자는 구매하는 앱의 품질을 신뢰할 수 있습니다.
- **코드 서명 확인:** iOS 및 iPadOS는 개발자들이 앱 내에 프레임워크를 내장할 수 있도록 허용해 앱 자체에서 사용되거나 앱에 내장된 확장 프로그램에서 사용할 수 있도록 합니다. 시스템 및 다른 앱에서 타사 코드를 주소 공간 내에 로드하는 것을 방지하기 위해 시스템은 시작 시점에 프로세스가 링크하는 모든 동적 라이브러리의 코드 서명 확인을 수행합니다. 이 확인 절차는 Apple이 발급한 인증서에서 추출한 팀 식별자(Team ID)를 통해 수행됩니다. 팀 식별자는 예를 들어 1A2B3C4D5F와 같은 10자로된 알파벳 숫자 문자열입니다. 프로그램은 시스템과 함께 탑재된 플랫폼 라이브러리 또는 동일한 팀 식별자가 주 실행 파일로서 코드 서명에 있는 모든 라이브러리에 링크하게 됩니다. 시스템의 한 부분으로 탑재되는 실행 파일은 팀 식별자가 없기 때문에 시스템 자체와 함께 탑재되는 라이브러리에만 링크하게 됩니다.

기업 내부 전용 앱 확인하기

자격을 갖춘 기업체는 조직 내부에서 사용할 목적으로 기업 내부 전용 앱을 작성하고 직원에게 배포할 수 있습니다. 기업 및 조직은 ADEP(Apple Developer Enterprise Program)에 신청할 수 있습니다. 자격 요건에 대한 더 많은 정보를 보려면 Apple Developer Enterprise Program 웹 사이트를 참조하십시오. 조직이 ADEP의 구성원이 되면 인증한 기기에서 기업 내부 전용 앱 사용을 허용하는 권한 설정 프로파일을 신청할 수 있습니다.

사용자가 이러한 앱을 사용하려면 권한 설정 프로파일을 설치해야 합니다. 이를 통해 조직이 의도한 사용자만 iPhone 및 iPad에 해당 앱을 설치하도록 할 수 있습니다. MDM(모바일 기기 관리)을 통해 설치된 앱은 조직 및 기기 간의 관계가 이미 구축되었기 때문에 절대적으로 신뢰할 수 있습니다. MDM을 통해 설치된 앱이 아닌 경우 사용자는 설정에서 앱의 권한 설정 프로파일을 승인해야 합니다. 조직에서는 알 수 없는 개발자의 앱을 사용자가 승인할 수 없게 제한할 수도 있습니다. 기업 내부 전용 앱이 처음 실행되는 경우 기기는 Apple로부터 앱을 실행할 수 있다는 확인을 받아야 합니다.

iOS 및 iPadOS의 런타임 프로세스 보안

iOS 및 iPadOS는 '샌드박스', 선언된 권한 및 ASLR(Address Space Layout Randomization)을 사용하여 런타임 보안을 보장합니다.

샌드박스

모든 타사 앱은 '샌드박스'되어 있어 다른 앱이 저장한 파일에 접근하거나 기기에 변경 사항을 만들 수 없습니다. 샌드박스는 앱이 다른 앱에서 저장한 정보를 수집하거나 변경하는 것을 방지하도록 설계되었습니다. 각 앱은 파일에 대한 고유 홈 디렉토리를 가지며 앱이 설치될 때에 임의로 할당됩니다. 타사 앱이 다른 디렉토리의 정보에 접근해야 하는 경우 명백하게 iOS 및 iPadOS에서 제공하는 서비스를 통해서만 접근할 수 있습니다.

또한 시스템 파일 및 리소스는 사용자가 설치한 앱으로부터 보호됩니다. 타사 앱과 마찬가지로, iOS 및 iPadOS에 있는 대부분의 시스템 파일 및 리소스는 권한이 없는 'mobile' 사용자로 실행됩니다. 전체 운영 체제 파티션은 읽기 전용으로 마운트되어 있습니다. 원격 로그인 서비스와 같은 불필요한 툴은 시스템 소프트웨어에 없기 때문에 API에서는 앱이 다른 앱 또는 iOS 및 iPadOS 자체를 수정하기 위해 권한을 확대하는 것을 승인하지 않습니다.

권한 사용

타사 앱에서 사용자 정보와 iCloud 및 확장성과 같은 기능에 접근할 경우 선언된 권한을 사용해 제어됩니다. 권한은 쌍으로 된 키 값으로 앱에 로그인하여 UNIX 사용자 ID와 같은 런타임 요소를 능가하는 승인을 허용합니다. 권한은 디지털로 서명되어 있기 때문에 변경이 불가능합니다. 권한은 또한 시스템 앱과 데몬에서 광범위하게 사용되어 특정 권한이 필요한 작업을 수행합니다. 그렇지 않은 경우 루트로 실행하기 위한 프로세스를 요청합니다. 이를 통해 손상된 시스템 앱 또는 데몬이 권한을 확대할 가능성을 크게 줄입니다.

추가적으로 앱은 시스템에서 제공한 API를 통해서만 백그라운드 프로세스를 실행할 수 있습니다. 이렇게 하면 앱 성능을 저하시키거나 배터리 사용 시간을 현저하게 줄이지 않으면서 계속 작동할 수 있게 됩니다.

ASLR(Address Space Layout Randomization)

ASLR(Address Space Layout Randomization)은 메모리 변형 버그 공격을 막습니다. 내장된 앱은 ASLR을 사용하여 실행 시에 모든 메모리 영역을 무작위로 할당합니다. ASLR은 실행 시 동작뿐 아니라, 실행 코드, 시스템 라이브러리 및 관련 프로그래밍 구성의 메모리 주소를 임의로 할당하여 수많은 공격의 가능성을 더욱 줄입니다. 예를 들어 RTL(Return-To-Libc) 공격은 스택 및 시스템 라이브러리의 메모리 주소를 조종해 기기를 속여 악성 코드를 실행하도록 할 수 있습니다. 이러한 요소들을 임의로 배치하면 특히 다수의 기기에 대한 공격은 더욱 힘들어지게 됩니다. Xcode 및 iOS나 iPadOS 개발 환경에서 자동으로 ASLR 지원을 켠 상태로 타사 프로그램을 컴파일합니다.

실행 안 함 기능

iOS 및 iPadOS에서는 메모리 페이지를 실행 불가능으로 표시하는 ARM의 실행 안 함(XN) 기능을 사용해 더욱 강력한 보호 기능을 제공합니다. 실행 및 쓰기가 모두 가능하게 표시된 메모리 페이지는 엄격히 제어된 조건의 앱에서만 사용할 수 있습니다. 커널이 Apple 전용 동적 코드 서명 권한의 존재 여부를 확인합니다. 게다가 하나의 `mmap` 호출만이 실행 및 쓰기가 가능한 페이지를 요청할 수 있어, 이 경우에도 무작위의 주소가 주어집니다. Safari는 이 기능을 JavaScript just-in-time(JIT) 컴파일러에 사용합니다.

iOS, iPadOS 및 macOS의 확장 프로그램 지원

iOS, iPadOS 및 macOS에서는 확장 프로그램을 제공하여 앱이 다른 앱으로 기능을 제공할 수 있습니다. 확장 프로그램은 특정 목적을 위해 서명된 실행 가능한 바이너리로서 앱 내에 패키지되어 있습니다. 설치하는 동안 시스템은 자동으로 확장 프로그램을 인식하고 일치하는 시스템을 사용하는 다른 앱에서 확장 프로그램을 사용하도록 허용합니다.

확장 포인트

확장 프로그램을 지원하는 시스템 영역을 **확장 포인트**라고 부릅니다. 각각의 확장 포인트는 API를 제공하며 해당 영역의 정책을 시행합니다. 시스템에서는 확장 포인트 지정 매칭 규칙에 따라 확장 프로그램의 사용 가능 여부를 판단합니다. 시스템은 필요한 경우 자동으로 확장 프로그램 프로세스를 실행하며 확장 프로그램의 수명을 관리합니다. 권한을 사용해 특정 시스템 앱이 확장 프로그램을 사용하지 못하게 제한할 수 있습니다. 예를 들어 오늘 보기 위젯이 알림 센터에만 나타나고 공유 확장 프로그램이 공유 패널에서만 사용 가능하도록 합니다. 확장 포인트의 예시로는 오늘 위젯, 공유, 동작, 사진 편집, 파일 제공자 및 사용자 설정 키보드가 있습니다.

확장 프로그램 통신 방식

확장 프로그램은 자신의 주소 공간에서 실행됩니다. 확장 프로그램과 이를 활성화한 앱 간의 통신은 시스템 프레임워크를 통한 프로세스 간 통신을 사용합니다. 확장 프로그램과 앱은 서로 간의 파일 또는 메모리 공간에 대한 접근 권한이 없습니다. 확장 프로그램은 다른 확장 프로그램, 확장 프로그램을 포함하는 앱 및 확장 프로그램을 사용하는 앱으로부터 분리되도록 디자인되어 있습니다. 다른 타사 앱처럼 샌드박스되어 확장 프로그램을 포함하는 앱의 컨테이너와 분리된 컨테이너를 가지고 있습니다. 하지만 확장 프로그램을 포함하는 앱과 개인정보 보호 제어에 대한 권한을 같이 공유합니다. 그렇기 때문에 사용자가 앱에서 연락처 앱의 접근을 허용하면 앱에 내장된 확장 프로그램에도 이 권한이 확장되지만, 해당 앱이 활성화한 확장 프로그램에는 권한이 허용되지 않습니다.

사용자 설정 키보드 사용 방법

사용자 설정 키보드는 사용자가 시스템 전체에 활성화시키는 특별한 유형의 확장 프로그램입니다. 키보드 확장 프로그램이 활성화되면 키보드 확장 프로그램이 암호 입력 및 보안 텍스트 보기를 제외한 모든 텍스트 필드에 사용됩니다. 사용자 데이터 전송을 제한하기 위해 사용자 설정 키보드는 기본적으로 매우 제한된 샌드박스에서 실행되어 네트워크, 프로세스를 대신해 네트워크 작업을 실행하는 서비스, 입력한 데이터를 추출할 수 있는 확장 프로그램을 허용하는 API에 대한 접근을 차단합니다. 사용자 설정 키보드 개발자는 확장 프로그램이 오픈 액세스 권한을 가지도록 요청할 수 있으며, 사용자가 동의하는 경우 시스템이 확장 프로그램을 기본 샌드박스에서 실행할 수 있습니다.

MDM 및 확장 프로그램

MDM(모바일 기기 관리) 솔루션에 등록된 기기, 문서 및 키보드 확장 프로그램은 Managed Open In 규칙을 따릅니다. 예를 들어 MDM 솔루션은 사용자가 관리형 앱에서 관리되지 않는 문서 제공자에게 문서를 보내는 것을 막을 수 있습니다. 또는 사용자가 관리되지 않은 키보드를 앱에서 사용하는 것을 막을 수 있습니다. 추가적으로 앱 개발자는 타사 키보드 확장 프로그램이 자신의 앱에서 사용되는 것을 막을 수 있습니다.

iOS 및 iPadOS의 앱 보호와 앱 그룹

iOS 및 iPadOS의 경우 조직은 IOS SDK를 사용하거나 Apple Developer 포털에서 앱 그룹에 참여하여 앱을 보호할 수 있습니다.

앱 내 데이터 보호 적용

iOS 및 iPadOS용 iOS 소프트웨어 개발 키트(SDK)는 API 전체 모음을 제공하므로 타사 및 내부 개발자가 데이터 보호를 손쉽게 적용하여 가장 높은 수준으로 앱을 보호할 수 있도록 합니다. 데이터 보호는 파일 및 데이터베이스 API(NSFileManager, CoreData, NSData 및 SQLite 등)에 사용할 수 있습니다.

Mail 앱 데이터베이스(첨부 파일 포함), 관리되는 책, Safari 책갈피, 앱 실행 이미지 및 위치 데이터 또한 키를 통해 암호화된 상태로 보관됩니다. 또한 이 키는 기기에서 사용자가 설정한 암호로 보호됩니다. 캘린더(첨부 파일 제외), 연락처, 미리 알림, 메모, 메시지 및 사진 앱은 `Data Protection` 권한인 **Protected Until First User Authentication** 클래스를 구현합니다.

특정 데이터 보호 클래스에 할당되지 않은 사용자가 설치한 앱은 기본으로 Protected Until First User Authentication 클래스에 할당됩니다.

앱 그룹 참여

앱 그룹의 일부로 구성된 경우 특정한 개발자 계정이 소유한 앱 및 확장 프로그램은 콘텐츠를 공유할 수 있습니다. 개발자가 Apple Developer 포털에 적절한 그룹을 생성하고 원하는 앱과 확장 프로그램을 포함할 수 있습니다. 앱 그룹으로 구성된 경우에 앱은 다음에 접근할 수 있습니다.

- 저장 공간을 위한 볼륨 상의 공유된 컨테이너(그룹에 속한 앱이 최소 한 개라도 설치되어 있는 경우 기기에 계속 남음)
- 공유된 환경설정
- 공유된 키체인 항목

Apple Developer 포털은 각각의 앱 그룹 ID(GID)가 전체 앱 생태계에서 고유함을 보장합니다.

macOS의 앱 보안

macOS의 앱 보안 개요

macOS의 앱 보안은 여러 개의 계층으로 구성되어 있으며, 첫 번째는 App Store에서 서명되고 신뢰하는 앱만 실행하는 옵션입니다. 또한 macOS 계층형 보호 기능은 인터넷에서 다운로드한 앱에 알려진 악성 코드가 없는지 확인합니다. macOS는 악성 코드를 감지하고 제거하는 기술을 보유하며, 이와 함께 신뢰할 수 없는 앱의 사용자 데이터 접근을 방지하도록 고안된 보호 기능을 제공합니다. Notarization 및 XProtect 업데이트와 같은 Apple 서비스는 악성 코드 설치를 방지하기 위해 설계되었습니다. 필요한 경우, 이러한 서비스는 처음에 감지되지 않았을 수 있는 악성 코드를 찾아 빠르고 효율적으로 제거합니다. 따라서 macOS 사용자는 신뢰할 수 없거나 서명되지 않은 코드를 실행하는 것을 포함하여, 본인에게 적합한 보안 모델 내에서 자유롭게 사용할 수 있습니다.

macOS의 앱 코드 서명 프로세스

모든 App Store 앱은 Apple에서 서명합니다. 서명은 앱이 변조되거나 변경되지 않았음을 확인하도록 설계된 절차입니다. Apple 기기에 제공되는 모든 앱에도 Apple이 서명합니다.

macOS 10.15 버전의 경우 App Store 외부에서 배포된 모든 앱은 반드시 Apple이 발급한 개발자 ID 인증서(개인 키와 통합됨)를 사용하여 서명되어야 하며, 기본 Gatekeeper 설정으로 실행하려면 Apple의 공증을 받아야 합니다. 사내에서 개발한 앱도 Apple이 발급한 개발자 ID로 서명하여 사용자가 해당 앱의 무결성을 확인할 수 있어야 합니다.

macOS에서 코드 서명 및 공증 작업은 다양한 목표를 위해 독립적으로 수행되며, 여러 행위자에 의해 수행될 수 있습니다. 개발자는 Apple이 발급한 개발자 ID 인증서를 사용하여 코드 서명을 수행합니다. 이 서명을 확인하면 사용자는 개발자의 소프트웨어가 제작 및 서명된 이후로 변조되지 않았음을 확인할 수 있습니다. 소프트웨어 배포 체인 안의 누구나 공증이 가능하며, 공증은 Apple이 악성 코드를 확인하기 위해 코드 사본을 제공받았으며 알려진 악성 코드가 발견되지 않았음을 증명합니다. 공증의 결과는 티켓이며, 티켓은 Apple 서버에 저장되고 원하는 경우 누구나 개발자의 서명을 무효화하지 않고 앱과 함께 보관할 수 있습니다.

시스템으로 보호되는 권한을 활성화하려면 MAC(강제적 접근 제어)에 코드 서명이 필요합니다. 예를 들어 방화벽을 통해 접근해야 하는 앱은 올바른 MAC 권한으로 코드 서명되어야 합니다.

macOS의 Gatekeeper 및 런타임 보호

macOS는 Gatekeeper 기술 및 런타임 보호를 제공하여 신뢰하는 소프트웨어만이 사용자의 Mac에서 실행되도록 보장합니다.

Gatekeeper

macOS에는 사용자의 Mac에서 신뢰하는 소프트웨어만 실행되도록 설계된 **Gatekeeper**라는 보안 기술이 포함되어 있습니다. 사용자가 App Store 외부에서 앱, 플러그인 또는 설치 프로그램 패키지를 다운로드하여 열면, Gatekeeper는 해당 소프트웨어가 확인된 개발자가 제작한 것인지, Apple 공증을 통해 알려진 악성 콘텐츠가 없음이 증명된 것인지, 변조되지 않았는지를 확인합니다. 또한 다운로드한 소프트웨어를 처음 열 때 Gatekeeper는 단순 데이터 파일로 눈속임하는 실행 코드를 사용자가 실행하도록 하는 것은 아닌지 확인하기 위해 사용자 승인을 요청합니다. Gatekeeper는 다운로드한 소프트웨어로 작성한 파일의 출처도 추적합니다.

기본적으로 Gatekeeper는 다운로드한 모든 소프트웨어가 App Store 또는 등록된 개발자에 의해 서명되고 Apple의 공증을 받았음을 보장합니다. App Store 심사 프로세스 및 공증 과정은 앱에 알려진 악성 코드가 없는지 확인하도록 설계되었습니다. 따라서 기본적으로 **Mac으로 소프트웨어를 가져온 경로와 상관없이 macOS의 모든 소프트웨어는 처음 열 때 알려진 악성 콘텐츠가 있는지 검사합니다.**

사용자 및 조직은 App Store에서 설치한 소프트웨어만 허용하는 옵션을 설정할 수 있습니다. 아니면 MDM(모바일 기기 관리) 솔루션에서 제한하지 않는 경우, Gatekeeper 정책을 무시하고 모든 소프트웨어를 열도록 할 수 있습니다. 조직은 MDM을 사용하여 대체 ID로 서명된 소프트웨어를 허용하는 등 Gatekeeper 설정을 구성할 수 있습니다. 필요에 따라 Gatekeeper를 완전히 비활성화할 수도 있습니다.

Gatekeeper는 또한 정상적인 앱에 악성 플러그인을 배포할 수 없도록 보호합니다. 앱을 사용하면 사용자가 알 수 없는 상태에서 악성 플러그인 로드가 실행되는 경우가 있습니다. 필요한 경우 Gatekeeper에서 앱을 임의의 읽기 전용 위치에서 실행합니다. Gatekeeper는 앱과 함께 배포된 플러그인이 자동으로 로드되는 것을 방지하기 위해 설계되었습니다.

런타임 보호

시스템 파일, 리소스 및 커널은 사용자의 앱 공간으로부터 보호됩니다. App Store의 모든 앱은 샌드박스되어 다른 앱이 저장한 데이터에 대한 접근을 제한합니다. App Store의 앱이 다른 앱의 데이터에 접근해야 하는 경우, macOS에서 제공하는 API 및 서비스를 사용해야만 접근할 수 있습니다.

macOS에서의 악성 코드로부터 보호

Apple은 악성 코드를 빠르게 발견하고 차단하기 위해 위협 인텔리전스 프로세스를 운영합니다.

3중 방어 체계

악성 코드 방어 체계는 다음 세 계층으로 구성되어 있습니다.

1. **악성 코드의 설치 또는 실행 방지:** App Store 또는 Notarization과 결합한 Gatekeeper

2. **고객 시스템에서 악성 코드가 실행되지 않도록 차단:** Gatekeeper, Notarization 및 XProtect

3. **이미 실행된 악성 코드에 대한 치료:** XProtect

첫 번째 방어 계층은 악성 코드의 배포를 막고 한 번도 실행되지 않도록 설계되었습니다. 이는 App Store 및 Notarization과 결합한 Gatekeeper가 지향하는 목표입니다.

다음 방어 계층은 악성 코드가 Mac에 나타나면 빠르게 식별하고 차단하여 확산을 막고 이미 악성 코드가 자리 잡은 Mac 시스템을 치료하는 것입니다. XProtect는 Gatekeeper 및 Notarization과 함께 이러한 방어 체계를 추가합니다.

마지막으로 XProtect 는 실행에 성공한 악성 코드를 치료하는 역할을 합니다.

아래에 설명된 이러한 보호 기능을 결합하여 바이러스 및 악성 코드에 대해 가장 적합한 보호를 지원합니다. 특히 Apple Silicon이 탑재된 Mac에는 실행 가능한 악성 코드로 인한 잠재적 손상을 제한하기 위한 추가 보호 기능이 있습니다. macOS가 악성 코드로부터 사용자 데이터를 보호하는 방법은 사용자 데이터에 대한 앱 접근 방지를 참조하고, macOS에서 악성코드가 시스템에서 수행할 수 있는 작업을 제한하는 방법은 운영 체제 무결성을 참조하십시오.

Notarization

Notarization은 Apple이 제공하는 악성 코드 스캔 서비스입니다. App Store 외부에서 macOS용 앱을 배포하려는 개발자는 배포 프로세스의 일부로서 앱을 스캔하여 제출합니다. Apple은 이 소프트웨어에서 알려진 악성 코드를 스캔하고 악성 코드가 발견되지 않는 경우 Notarization 티켓을 발행합니다. 일반적으로 개발자는 Gatekeeper가 오프라인에서도 앱을 확인하고 실행할 수 있도록 이 티켓을 앱에 고정합니다.

또한 Apple은 이전에 공증을 받았더라도 악성으로 알려진 앱에 대해 해지 티켓을 발행할 수 있습니다. macOS는 새로운 해지 티켓을 정기적으로 확인하여 Gatekeeper가 최신 정보를 보유하고 이러한 파일의 실행을 차단할 수 있도록 합니다. 이 프로세스는 새로운 XProtect 서명을 푸시하는 백그라운드 업데이트보다 백그라운드에서 업데이트가 훨씬 더 자주 발생하기 때문에 악성 앱을 매우 빠르게 차단할 수 있습니다. 또한 이 보호 기능은 이전에 공증을 받은 앱과 그렇지 않은 앱에 모두 적용할 수 있습니다.

XProtect

macOS는 악성 코드의 서명 기반 감지 및 제거를 위한 내장 안티바이러스 기술인 **XProtect**를 포함하고 있습니다. 해당 시스템에서는 서명 기반 악성 코드 감지를 수행하는 도구인 YARA 서명을 사용하며, Apple은 이를 주기적으로 업데이트합니다. Apple은 새로운 악성 코드 감염 및 변종을 모니터링하고, 시스템 업데이트와는 별개로 서명을 자동으로 업데이트하여 Mac을 악성 코드 감염에서 보호합니다. XProtect는 알려진 악성 코드의 실행을 자동으로 감지하고 차단합니다. macOS 10.15 이상에서 XProtect는 다음과 같은 경우 알려진 악성 콘텐츠를 검사합니다.

- 앱이 처음 실행된 경우
- 앱이 파일 시스템에서 변경된 경우
- XProtect 서명이 업데이트된 경우

XProtect가 알려진 악성 코드를 감지하면 소프트웨어가 차단되고 사용자에게 이를 알리며, 해당 소프트웨어를 휴지통으로 이동하는 옵션을 표시합니다.

참고: 공증은 알려진 파일(또는 파일 해시)에 대해 효과적이며 이전에 실행된 앱에서 사용할 수 있습니다. XProtect의 서명 기반 규칙은 특정 파일 해시보다 더 일반적이어서 Apple이 보지 못한 변종을 찾을 수 있습니다. XProtect는 변경된 앱이나 처음 실행하는 앱만 스캔합니다.

XProtect에는 악성 코드가 Mac에 침투하는 경우 감염을 치료하는 기술도 있습니다. 예를 들어, 이 기능은 보안 업데이트 및 시스템 데이터 파일의 자동 업데이트의 일부로서 Apple에서 자동으로 제공되는 업데이트를 기반으로 감염을 치료하는 엔진을 포함합니다. 이 시스템은 업데이트된 정보를 받으면 악성 코드를 제거하고 주기적으로 계속 감염되었는지 확인합니다. 그러나 XProtect는 Mac을 자동으로 재시동하지 않습니다. 또한, XProtect에는 행위 분석을 기반으로 알 수 없는 악성 코드를 감지하는 고급 엔진이 포함됩니다. 이 엔진이 감지한 악성 코드에 대한 정보(어떤 소프트웨어가 다운로드했는지에 대한 정보 포함)는 XProtect 서명과 macOS 보안을 개선하는 데 사용됩니다.

자동 XProtect 보안 업데이트

Apple은 최신 위협 인텔리전스를 기반으로 XProtect 업데이트를 자동으로 배포합니다. macOS는 기본적으로 업데이트를 매일 확인합니다. CloudKit 동기화를 통해 배포되는 공증 업데이트는 훨씬 더 자주 발생합니다.

Apple이 새로 발견된 악성 코드에 대처하는 방법

새로운 악성 코드가 발견되면 다음과 같은 여러 단계를 수행할 수 있습니다.

- 연관된 모든 개발자 ID 인증서는 제거됩니다.
- 모든 파일(앱 및 관련 파일)에 대해 공증 해지 티켓이 발급됩니다.
- XProtect 서명이 개발되고 공개됩니다.

  이러한 서명은 또한 이전에 공증을 받은 소프트웨어에 소급적으로 적용되며, 새로 악성 코드가 감지될 경우, 하나 이상의 이전의 조치가 이루어질 수 있습니다.

궁극적으로 악성 코드 감지는 Mac 사용자에게 가능한 최고의 보호 기능을 전파하기 위해 다음에 이어지는 몇 초, 몇 시간 및 며칠 단위로 일련의 단계를 시작합니다.

macOS에서 앱의 파일 접근 제어

Apple은 사용자의 데이터를 사용하는 앱을 사용자가 완전히 투명하게 알고, 이에 동의하고, 제어할 수 있어야 한다고 생각합니다. macOS 10.15에서 이 모델은 시스템에 의해 시행되며 모든 앱이 문서, 다운로드, 데스크탑, iCloud Drive 및 네트워크 볼륨의 파일에 접근하기 전에 사용자 동의를 얻어야 함을 보장합니다. macOS 10.13 이상에서 전체 저장 장치에 접근해야 하는 앱은 시스템 설정(macOS 13 이상) 또는 시스템 환경설정(macOS 12 또는 이전 버전)에서 명시적으로 추가되어야 합니다. 또한 접근성 및 자동화 기능은 다른 보호 기능을 피해가지 않도록 하기 위해 사용자 권한이 필요합니다. 접근 정책에 따라 사용자는 다음과 같이 설정을 변경하도록 요청받거나 변경해야 합니다.

- macOS 13 이상: 시스템 설정 > 개인정보 보호 및 보안 > 개인정보 보호
- macOS 12 또는 이전 버전: 시스템 환경설정 > 보안 및 개인 정보 보호 > 개인 정보 보호

항목	앱에서 사용자에게 메시지를 표시함	사용자가 시스템 개인정보 보호 설정을 변경해야 함
접근성	✗	✓
전체 내부 저장 공간 접근	✗	✓
파일 및 폴더 **참고:** 데스크탑, 문서, 다운로드, 네트워크 볼륨 및 제거 가능한 볼륨 포함	✓	✗
자동화(Apple 이벤트)	✓	✗

Mac에서 FileVault를 활성화한 사용자는 특수 시작 모드에 대한 접근 권한을 받기 위해 시동 프로세스를 계속하기 전에 먼저 유효한 자격 증명을 제공하도록 요청을 받습니다. 유효한 로그인 자격 증명이나 복구 키가 없으면 물리적 저장 장치를 제거하고 다른 컴퓨터에 연결하더라도 전체 볼륨은 암호화된 상태로 유지되며 무단 접근으로부터 보호됩니다.

기업용 설정에서 데이터를 보호하려면, IT 부서에서 MDM(모바일 기기 관리)을 사용하여 FileVault 구성 정책을 정의하고 적용해야 합니다. 조직에서는 기관 복구 키 또는 개인 복구 키(MDM에 저장해 에스크로 가능)를 사용하거나, 둘을 조합해 사용하는 등 몇 가지 방법을 사용해 암호화 볼륨을 관리할 수 있습니다. MDM에서 키 순환도 정책으로 설정할 수 있습니다.

메모 앱의 보안 기능

메모 앱에는 보안 메모 기능이 있습니다. 사용자는 iPhone, iPad, Mac 및 iCloud 웹 사이트에서 보안 메모 기능으로 특정 메모의 콘텐츠를 보호할 수 있습니다. 사용자는 다른 사람과 안전하게 메모를 공유할 수도 있습니다.

보안 메모

보안 메모는 사용자가 입력한 암호(암호문구)를 사용하여 종단간 암호화되며, iOS, iPadOS, macOS 기기 및 iCloud 웹 사이트에서 보안 메모를 보려면 이 암호가 필요합니다. 각 iCloud 계정('나의' 기기 계정 포함)은 별도의 암호문구를 가질 수 있습니다.

사용자가 메모를 보호하면 PBKDF2 및 SHA256을 통하여 사용자의 암호문구에서 16바이트 키가 파생됩니다. 메모 및 모든 첨부파일은 AES-GCM(Galois/Counter Mode의 AES)을 사용하여 암호화됩니다. Core Data 및 CloudKit에 새로운 기록을 생성하여 암호화된 메모, 첨부 파일, 태그 및 초기화 벡터를 저장합니다. 새로운 기록이 생성되고 기존의 암호화되지 않은 데이터는 삭제됩니다. 암호화를 지원하는 첨부 파일은 이미지, 스케치, 표, 지도 및 웹 사이트가 있습니다. 다른 유형의 첨부 파일을 포함하는 메모는 암호화할 수 없으며 지원되지 않는 첨부 파일은 보안 메모에 추가될 수 없습니다.

보안 메모를 보려면 사용자가 암호문구를 입력하거나 Face ID 또는 Touch ID를 사용하여 인증해야 합니다. 사용자가 보안 메모를 보거나 생성하기 위해 사용자 인증에 성공하면, 메모 앱에서 보안 세션을 엽니다. 보안 세션이 열려 있는 동안 사용자는 추가 인증 없이 다른 메모를 보거나 보호할 수 있습니다. 하지만 보안 세션은 제공된 암호문구로 보호되는 메모에만 적용됩니다. 사용자가 다른 암호문구로 보호되는 메모를 보려면 다시 인증을 받아야 합니다. 다음과 같은 경우 보안 세션이 닫힙니다.

- 사용자가 메모 앱에서 지금 잠금 버튼을 탭한 경우
- 메모 앱이 백그라운드로 전환된 지 3분(macOS는 8분) 이상 지난 경우
- iOS 또는 iPadOS 기기가 잠긴 경우

보안 메모의 암호문구를 변경하려면 사용자는 현재의 암호문구를 입력해야 합니다. Face ID 및 Touch ID는 암호문구를 변경하는 데 사용할 수 없기 때문입니다. 새로운 암호문구를 선택하고 나면, 메모 앱은 이전 암호문구로 암호화되어 동일한 계정에 있는 모든 기존 메모의 키를 다시 래핑합니다.

사용자가 세 번 연속하여 암호문구를 잘못 입력하면, 메모 앱은 사용자가 설정 시 제공한 암호 힌트를 보여줍니다(제공한 경우). 사용자가 암호문구를 계속하여 기억하지 못하는 경우, 메모 설정에서 암호문구를 변경할 수 있습니다. 암호문구 재설정 기능으로 사용자는 보안 메모를 새로 생성할 때 새로운 암호문구를 사용할 수는 있지만 이전 암호문구로 보호한 메모는 볼 수 없습니다. 이전 암호문구로 보호한 메모는 사용자가 이전 암호문구를 기억하는 경우에만 볼 수 있습니다. 암호문구를 재설정하려면 사용자의 iCloud 계정 암호문구가 필요합니다.

공유 메모

암호문구로 종단간 암호화되지 않은 메모는 다른 사람과 공유할 수 있습니다. 공유 메모는 사용자가 메모에 넣은 모든 텍스트 또는 첨부 파일에 대해 CloudKit로 암호화한 데이터 유형을 계속 사용합니다. 자료는 CKRecord에서 암호화된 키로 항상 암호화됩니다. 생성일 및 수정일 등의 메타데이터는 암호화되지 않습니다. 공유 참여자가 서로의 데이터를 암호화하고 암호화를 해제하는 프로세스는 CloudKit에서 관리합니다.

단축어 앱의 보안 기능

단축어 앱에서 단축어는 iCloud를 사용하여 Apple 기기에 동기화됩니다(선택 사항). iCloud를 통해 다른 사용자와 단축어를 공유할 수도 있습니다. 단축어는 암호화된 포맷으로 기기 내에 저장됩니다.

사용자 설정 단축어는 스크립트나 프로그램처럼 다용도로 사용할 수 있습니다. 인터넷에서 단축어를 다운로드할 때, Apple에서 단축어가 검증되지 않았다는 경고가 사용자에게 표시되고 사용자에게 단축어를 검사할 기회가 주어집니다. 악성 단축어로부터 보호하기 위해 업데이트된 악성 코드 정의가 다운로드되어 런타임에서 악성 단축어를 식별합니다.

또한 공유 시트에서 사용자 설정 단축어를 호출한 경우 Safari의 웹 사이트에서 사용자가 지정한 JavaScript를 실행할 수도 있습니다. 악의적인 JavaScript(예: 소셜 미디어 웹 사이트에서 사용자의 데이터를 수집하는 스크립트 실행)로부터 보호하기 위해 앞서 언급한 악성 코드 정의를 기반으로 JavaScript 유효성을 검사합니다. 사용자가 도메인에서 JavaScript를 처음으로 실행한 경우 해당 도메인의 현재 웹 페이지에서 JavaScript를 포함하는 단축어 실행을 허용하라는 요청이 나타납니다.

서비스 보안

서비스 보안 개요

Apple은 사용자가 자신의 기기에서 활용성과 생산성을 높일 수 있도록 하는 강력한 서비스를 구축했습니다. 이러한 서비스는 클라우드 저장소 및 동기화, 암호 저장, 인증, 결제, 메시지, 통신 등을 위한 강력한 기능을 제공하며, 사용자의 개인정보 및 데이터의 보안을 안전하게 보호합니다.

이번 챕터에서는 iCloud, Apple로 로그인, Apple Pay, iMessage, Apple Messages for Business, FaceTime, 나의 찾기 및 연속성에서 사용하는 보안 기술을 다룹니다.

참고: 일부 Apple 서비스 및 콘텐츠는 일부 국가 또는 지역에서만 사용할 수 있습니다.

Apple ID 및 관리형 Apple ID

Apple ID 보안 개요

Apple ID는 Apple 서비스에 로그인할 때 사용하는 계정입니다. 사용자가 Apple ID를 안전하게 보호하여 해당 계정에 무단 접근을 방지하는 것이 중요합니다. 이를 위해 Apple ID는 다음을 충족하는 강력한 암호를 필요로 합니다.

- 최소 8자 길이
- 영문자 및 숫자를 모두 포함
- 3개 이상의 연속된 동일한 문자를 포함할 수 없음
- 일반적으로 사용되는 암호 제외

사용자는 이 기준을 넘어서 문자와 구두점을 더 추가해 암호를 강화할 수 있습니다.

또한 Apple은 해당 계정에 중요한 변경 사항이 적용되는 경우 이메일, 푸시 알림 또는 둘 다를 통해 사용자에게 알립니다. 예를 들어, 암호나 청구 정보가 변경되거나 Apple ID가 새로운 기기에 로그인하는 데 사용된 경우가 있습니다. 모르는 내용이 있는 경우 사용자는 Apple ID 암호를 즉시 변경하도록 안내를 받게 됩니다.

추가로 Apple은 사용자의 계정을 보호하기 위해 고안된 다양한 정책과 절차를 채택합니다. 여기에는 로그인 재시도 횟수 제한과 암호 재설정 횟수 제한, 해킹 발생 시 이를 확인하기 위한 적극적인 사기 방지 모니터링 및 사용자 보안에 영향을 미치는 새로운 정보에 맞추어 정책을 조정하기 위한 Apple의 주기적인 정책 검토가 포함됩니다.

참고: 관리형 Apple ID 암호 정책은 Apple School Manager 또는 Apple Business Manager에서 관리자가 설정합니다.

이중 인증

사용자의 계정을 더욱 안전하게 보호하기 위해서 Apple에서는 Apple ID를 한 번 더 보호하는 **이중 인증**을 기본으로 사용합니다. 이중 인증은 다른 사람이 암호를 알더라도 계정 소유자만 계정에 접근할 수 있도록 개발되었습니다. 이중 인증을 사용하면 사용자의 iPhone, iPad 또는 Mac과 같은 신뢰하는 기기나, 이러한 신뢰하는 기기 또는 전화번호로 인증을 완료한 기타 기기에서만 사용자의 계정에 접근할 수 있습니다. 새로운 기기에서 처음으로 로그인하려는 경우 두 가지 정보가 필요한데, 하나는 Apple ID 암호이고, 다른 하나는 사용자의 신뢰하는 기기에 표시되거나 신뢰할 수 있는 전화번호로 발송되는 6자리 확인 코드입니다. 확인 코드를 입력하면 사용자는 새로운 기기를 신뢰하며 새로운 기기가 로그인하기에 안전하다고 확인하게 됩니다. 암호만으로는 사용자의 계정에 접근하지 못하므로 이중 인증은 사용자의 Apple ID와 사용자가 Apple에 저장한 모든 개인정보에 대한 보안을 향상합니다. 이중 인증은 또한 iOS, iPadOS, macOS, tvOS, watchOS 및 Apple 웹 사이트에서 사용하는 인증 시스템에 직접 통합되어 있습니다.

사용자가 웹 브라우저로 Apple 웹 사이트에 로그인하면 사용자의 iCloud 계정과 연결된 모든 신뢰하는 기기에 웹 세션 승인을 요청하는 2차 인증 요청이 전송됩니다. 사용자가 신뢰하는 기기의 브라우저에서 Apple 웹 사이트에 로그인하는 경우 사용 중인 근처 기기에 확인 코드가 로컬로 표시됩니다. 사용자가 해당 기기에 코드를 입력하면 웹 세션이 승인됩니다.

암호 재설정 및 계정 복구

Apple ID 계정 암호를 잊어버린 경우, 사용자는 신뢰하는 기기에서 암호를 재설정할 수 있습니다. 신뢰하는 기기를 사용할 수 없지만 암호는 알고 있는 경우, 사용자는 신뢰하는 전화번호를 사용하여 SMS 확인을 통해 인증할 수 있습니다. 또한, Apple ID를 즉시 복구하려면 SMS와 함께 이전에 사용한 암호를 통해 재설정하면 됩니다. 이와 같은 옵션을 사용할 수 없는 경우 계정 복구 프로세스를 진행해야 합니다. 자세한 내용은 Apple 지원 문서 Apple ID 암호를 재설정할 수 없을 때 계정 복구를 사용하는 방법을 참조하십시오.

관리형 Apple ID 보안

관리형 Apple ID는 Apple ID와 매우 유사하지만 기업 또는 교육 기관에서 소유하고 제어합니다. 관리형 Apple ID를 소유한 조직에서는 암호를 재설정하거나 FaceTime 및 iMessage와 같은 통신을 끄거나 임직원, 교사 및 학생에 대한 역할별 권한을 설정할 수 있습니다.

관리형 Apple ID의 경우, App Store, App, HomeKit 및 나의 찾기 등의 일부 서비스를 사용할 수 없습니다.

관리형 Apple ID의 접근 관리

조직은 Apple Business Manager, Apple School Manager 및 Apple Business Essential에서 사용 가능한 접근 관리를 사용해 관리형 Apple ID를 사용할 수 있는 기기 및 사용할 수 있는 서비스를 정의할 수 있습니다.

접근 관리를 사용하면 사용자가 관리형 Apple ID로 모든 기기에 로그인할 수 있는지, 관리형 기기에만 로그인할 수 있는지, 관리형 및 감독 중인 기기에만 로그인할 수 있는지 정의할 수 있습니다. 또한 관리자는 사용자들이 웹에서 iCloud에 로그인할 수 있도록 허용할지 여부를 구성할 수 있습니다. 이를 통해 조직은 조직 데이터에 대한 접근 권한을 부여할지 여부를 결정하는 요소로 기기의 관리 상태를 사용할 수 있습니다.

관리자는 사용자가 사용할 수 있는 iCloud 서비스를 정의할 수도 있습니다. 이는 Apple Developer 프로그램 및 AppleSeed for IT 베타 프로그램의 접근을 정의하고 privacy.apple.com에서 Apple 개인정보 보호 포털에 접근할 수 있는지 여부를 결정합니다.

또한 관리형 Apple ID는 Keynote, Numbers, Pages, 미리 알림 및 메모를 사용하는 문서와 FaceTime 및 iMessage를 사용하는 통신과의 공동 작업을 지원합니다. 이와 같은 서비스의 경우, 조직은 사용자가 모든 사람과 공동 작업할 수 있는지 또는 동일한 Apple School Manager, Apple Business Manager 또는 Apple Business Essential 조직 내에서 생성된 계정으로만 공동 작업할 수 있는지 정의할 수 있습니다.

접근 관리 규칙이 변경되면 사용자가 관리형 Apple ID로 로그인한 기기에 반영됩니다. 기기 관리 상태의 요구 사항이 변경되는 경우, 기기 상태가 새로운 요구 사항을 충족하지 못하면 기기에서 관리형 Apple ID가 자동으로 로그아웃됩니다.

관리형 Apple ID 검사하기

Apple School Manager에서 생성된 관리형 Apple ID는 **검사**를 지원하여 조직에서 법적 규정과 개인정보 보호 규정을 준수하도록 합니다. 관리자, 사이트 관리자, 직원 관리자 또는 강사 역할의 사용자는 특정 관리형 Apple ID 계정을 검사할 수 있습니다.

검사자는 조직 체계에 따라 자신의 아래에 속한 계정만 모니터링할 수 있습니다. 교사는 학생을 모니터링할 수 있고, 중간 관리자는 교사와 학생을 검사할 수 있고, 관리자는 중간 관리자, 교사, 학생을 검사할 수 있는 방식입니다.

Apple School Manager를 사용해 자격 증명 검사가 요청될 경우, 검사가 요청된 관리형 Apple ID에만 접근할 수 있는 특별한 계정이 발급됩니다. 검사자는 사용자가 iCloud 또는 CloudKit가 활성화된 앱에 저장한 콘텐츠를 읽거나 수정할 수 있습니다. 모든 검사 접근 요청은 Apple School Manager에 기록됩니다. 기록에는 검사자의 신원 정보, 검사자가 접근을 요청한 관리형 Apple ID, 요청 시간 및 검사의 시행 여부가 나타납니다.

iCloud

iCloud 보안 개요

iCloud는 사용자의 연락처, 캘린더, 사진, 문서 등을 저장하고 사용자의 모든 기기에서 자동으로 해당 정보를 최신으로 유지합니다. 또한 타사 업체가 iCloud를 사용하여 문서뿐만 아니라 앱 데이터의 키 값을 개발자가 정의한 대로 저장하고 동기화할 수도 있습니다. 사용자는 Apple ID로 로그인하여 iCloud를 설정하고, 사용하고자 하는 서비스를 선택할 수 있습니다. iCloud Drive 및 iCloud 백업과 같은 특정 iCloud 기능은 IT 관리자가 MDM(모바일 기기 관리) 구성 프로파일을 사용하여 비활성화할 수 있습니다.

iCloud는 사용자 데이터를 보호하기 위해 강력한 보안 방식을 사용하고 엄격한 정책을 시행합니다. 대부분의 iCloud 데이터는 iCloud 서버에 업로드되기 전에, 기기에서 생성된 iCloud 키를 사용하여 사용자의 기기에서 먼저 암호화됩니다. 종단간 암호화되지 않은 데이터의 경우, 사용자의 기기에서 이러한 iCloud 키를 Apple 데이터 센터의 iCloud HSM(하드웨어 보안 모듈)으로 안전하게 업로드합니다. 이를 통해 Apple은 사용자가 데이터를 복구하도록 돕고, 새로운 기기 로그인, 백업 복원, 웹에서의 iCloud 데이터 접근 등 사용자의 필요에 따라 사용자를 대신해 데이터를 암호화 해제할 수 있습니다. 사용자의 기기와 iCloud 서버 간의 데이터 이동은 TLS를 통해 전송 중에 별도로 암호화되며, iCloud 서버는 보관을 위한 추가 암호화 계층을 사용하여 사용자 데이터를 저장합니다.

Apple에서 암호화 키를 사용할 수 있는 경우 이는 Apple 데이터 센터에서 보호됩니다. 타사 데이터 센터에 저장된 데이터를 처리하는 경우, 이러한 암호화 키는 필요한 처리를 수행하는 동안에 한해 보안된 서버에서 실행되는 Apple 소프트웨어로만 접근 가능합니다. 추가적인 개인정보 보호 및 보안을 위해서 많은 Apple 서비스는 종단간 암호화를 사용합니다. 즉, 오직 해당 사용자만이 Apple ID로 로그인한 신뢰하는 기기에서만 사용자의 iCloud 데이터에 접근할 수 있습니다.

Apple은 사용자가 iCloud에 저장하는 데이터를 암호화하고 보호할 수 있는 두 가지 옵션을 제공합니다.

- **표준 데이터 보호(기본 설정):** 사용자의 iCloud 데이터가 암호화되고, 암호화 키가 Apple 데이터 센터에서 보호되고, Apple이 데이터 및 계정 복구를 지원할 수 있습니다. 특정 iCloud 데이터(건강 데이터 및 iCloud 키체인의 암호를 포함한 14개의 데이터 카테고리)만 종단간 암호화됩니다.
- **iCloud용 고급 데이터 보호:** Apple의 가장 높은 수준의 클라우드 데이터 보안을 제공하는 선택적 설정입니다. 사용자가 고급 데이터 보호를 켜는 경우, 신뢰할 수 있는 기기에서 iCloud 데이터 대부분의 암호화 키에 단독으로 접근할 수 있으므로 종단간 암호화를 통해 보호됩니다. 사용자가 고급 데이터 보호를 켜면 종단간 암호화를 사용하는 데이터 카테고리 수가 23개로 늘어나며 iCloud 백업, 사진, 메모 등이 여기에 포함됩니다.

종단간 암호화로 보호되는 iCloud 데이터의 구체적인 카테고리는 Apple 지원 문서 iCloud 데이터 보안 개요에 나열되어 있습니다.

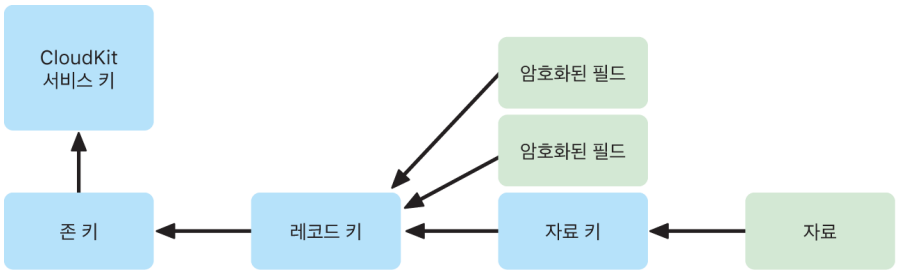
iCloud 암호화

앱과 시스템 소프트웨어가 사용자를 대신해 iCloud에 데이터를 저장하고 여러 기기 및 웹에서 최신 상태를 유지하도록 해주는 CloudKit 프레임워크 및 API를 시작으로 iCloud의 데이터 암호화와 데이터 저장 공간 모델 간 밀접한 연관성이 생겼습니다.

CloudKit 암호화

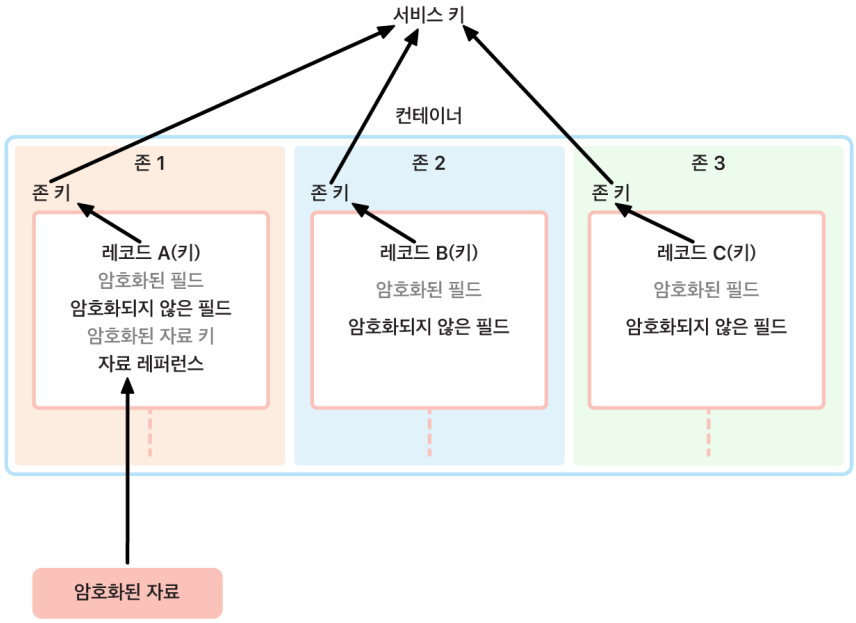
CloudKit는 앱 개발자가 iCloud에 키 값 데이터, 구조적 데이터 및 자료(이미지 또는 비디오와 같이 데이터베이스와 별개로 저장되는 대규모 데이터)를 저장하도록 허용하는 프레임워크입니다. CloudKit는 컨테이너에 그룹화된 공개 및 개인 데이터베이스를 모두 지원합니다. 공개 데이터베이스는 전역적으로 공유되고, 대개 일반적인 자료에 사용되며, 암호화되지 않습니다. 개인 데이터베이스는 각 사용자의 iCloud 데이터를 저장합니다.

CloudKit는 데이터의 구조와 일치하는 키의 계층 구조를 사용합니다. 각 컨테이너의 개인 데이터베이스는 **CloudKit 서비스 키**라고 하는 비대칭 키에 기반한 키 계층으로 보호됩니다. 이러한 키는 각 iCloud 사용자에 대해 고유하며 사용자의 신뢰하는 기기에서 생성됩니다. 데이터가 CloudKit에 기록되면, 모든 레코드 키가 사용자의 신뢰하는 기기에서 생성되고 데이터를 업로드하기 전에 적합한 키 계층으로 래핑됩니다.



Apple 지원 문서 iCloud 데이터 보안 개요에 나열된 많은 Apple 서비스는 iCloud 키체인 동기화와 같은 방식으로 보호되는 CloudKit 서비스 키로 종단간 암호화를 사용합니다. 이러한 CloudKit 컨테이너의 서비스 키는 사용자의 신뢰하는 기기에서만 사용 가능하며 Apple 또는 타사에서 접근할 수 없습니다. 해당 키는 사용자가 iCloud 키체인을 사용해 암호, 패스키 및 기타 사용자 데이터를 동기화하지 않기로 선택한 경우에도 사용자의 기기 간에 동기화됩니다. 기기를 분실한 경우 사용자는 iCloud 키체인 복구 보안, 계정 복구 연락처 또는 계정 복구 키를 사용하여 iCloud 키체인 데이터를 복구할 수 있습니다.

암호화 키 관리



CloudKit에 있는 암호화된 데이터의 보안은 그에 상응하는 보안 키의 보안에 달려 있습니다. CloudKit 서비스 키는 종단간 암호화(end-to-end encrypted) 및 인증 후 사용 가능(available-after-authentication)의 두 가지 카테고리로 나눌 수 있습니다.

- **종단간 암호화 서비스 키:** 종단간 암호화되는 iCloud 서비스의 경우, 관련 CloudKit 서비스 개인 키는 절대 Apple 서버에 제공되지 않습니다. 개인 키를 포함한 서비스 키 쌍은 사용자의 신뢰하는 기기에서 로컬로 생성되며 iCloud 키체인 보안을 사용하여 사용자의 다른 기기로 전송됩니다. iCloud 키체인 복구 및 동기화 흐름이 Apple 서버에 의해 조정되긴 하지만, 사용자의 키체인 데이터에 대한 Apple 서버의 접근은 암호화 방식으로 차단되어 있습니다. iCloud 키체인에 대한 접근 권한과 그에 대한 모든 복구 메커니즘을 상실하는 최악의 상황이 발생하면 CloudKit에 있는 종단간 암호화된 데이터는 유실됩니다. Apple은 이러한 데이터 복구를 도울 수 없습니다.
- **인증 후 사용 가능 서비스 키:** 사진 및 iCloud Drive와 같은 다른 서비스의 경우, 서비스 키는 Apple 데이터 센터의 iCloud HSM(하드웨어 보안 모듈)에 저장되고, 일부 Apple 서비스가 이에 접근할 수 있습니다. 사용자가 새로운 기기에서 iCloud에 로그인하고 자신의 Apple ID를 인증하면, 추가적인 사용자 상호 작용이나 입력 없이 Apple 서버에서 이러한 키에 접근할 수 있습니다. 예를 들어, 사용자가 iCloud.com에 로그인하고 나면 사용자는 온라인에서 자신의 사진을 즉시 볼 수 있습니다. 이러한 서비스 키는 **인증 후 사용 가능** 키입니다.

iCloud용 고급 데이터 보호

iCloud용 고급 데이터 보호는 Apple의 가장 높은 수준의 클라우드 데이터 보안을 제공하는 선택적 설정입니다. 사용자가 고급 데이터 보호를 켜는 경우, 사용자의 신뢰하는 기기는 대부분의 iCloud 데이터 암호화 키에 대한 접근 권한을 단독으로 유지하게 되고 이를 통해 **종단간 암호화**로 보호됩니다. 고급 데이터 보호를 켜면 종단간 암호화를 사용하여 보호되는 데이터 카테고리의 수가 14개에서 23개로 늘어나며 iCloud 백업, 사진, 메모 등이 여기에 포함됩니다.

참고: 이 기능은 일부 국가 또는 지역에서만 사용할 수 있습니다.

개념적으로 고급 데이터 보호는 간단합니다. 기기에서 생성되고 이후 Apple 데이터 센터의 **인증 후 사용 가능(available-after-authentication)** iCloud HSM(하드웨어 보안 모듈)에 업로드된 모든 CloudKit 서비스 키는 해당 HSM에서 삭제되고 그 대신 계정의 iCloud 키체인 보호 도메인에서 전적으로 유지됩니다. 이러한 키는 기존의 **종단간 암호화(end-to-end encrypted)** 서비스 키처럼 처리되므로, 더 이상 Apple이 이러한 키를 읽거나 해당 키에 접근할 수 없습니다.

또한 고급 데이터 보호는 타사 개발자가 암호화된 것으로 표시한 CloudKit 필드와 모든 CloudKit 자료를 자동으로 보호합니다.

고급 데이터 보호 활성화하기

사용자가 고급 데이터 보호를 켜면 사용자의 신뢰하는 기기에서 두 가지 동작이 수행됩니다. 첫째, 해당 기기는 고급 데이터 보호를 켜려는 사용자의 의도를 종단간 암호화(end-to-end-encryption)에 참여하는 다른 기기에 전달합니다. 이를 위해 해당 기기는 기기-로컬 키로 서명된 새로운 값을 iCloud 키체인 기기 메타데이터에 작성합니다. Apple 서버는 이 증명이 사용자의 다른 기기와 동기화되는 동안 이를 제거하거나 수정할 수 없습니다.

둘째, 해당 기기는 Apple 데이터 센터에서 **인증 후 사용 가능(available-after-authentication)** 서비스 키 제거를 시작합니다. 이러한 키는 iCloud HSM에 의해 보호되므로 이 삭제는 즉각적이고, 영구적이고, 되돌릴 수 없습니다. 해당 키가 삭제되고 나면 Apple은 사용자의 서비스 키로 보호되는 **모든** 데이터에 더 이상 접근할 수 없습니다. 이 시점에 해당 기기는 비동기 키 순환 작업을 시작하여, 키가 이전에 Apple 서버에 제공되었던 각 서비스에 대해 새로운 서비스 키를 생성합니다. 네트워크 중단 또는 다른 오류로 인해 키 순환이 실패할 경우, 해당 기기는 키 순환이 성공할 때까지 재시도합니다.

서비스 키 순환이 성공하고 나면 서비스에 기록된 새로운 데이터는 이전의 서비스 키로 암호화 해제할 수 없습니다. 이 데이터는 사용자의 신뢰하는 기기로만 제어되고 Apple에 제공된 적이 없는 새로운 키로 보호됩니다.

고급 데이터 보호 및 iCloud.com 웹 접근

사용자가 처음 고급 데이터 보호를 켜면 iCloud.com의 데이터에 대한 웹 접근이 자동으로 꺼집니다. 이는 iCloud 웹 서버가 사용자의 데이터를 암호화 해제하고 표시하는 데 필요한 키에 더 이상 접근할 수 없기 때문입니다. 사용자는 웹 접근을 다시 켜고, 신뢰하는 기기의 참여를 사용하여 암호화된 iCloud 데이터를 웹에서 접근하도록 선택할 수 있습니다.

웹 접근을 켠 후 사용자는 iCloud.com을 방문할 때마다 신뢰하는 기기 중 하나에서 웹 로그인을 인증해야 합니다. 이 인증은 기기가 웹에 접근할 수 있는 자격을 '부여'합니다. 향후 1시간 동안 이 기기는 개별 서비스 키를 업로드하라는 특정 Apple 서버의 요청을 승인합니다. 하지만 이러한 요청은 iCloud.com에서 일반적으로 접근 가능한 서비스 허용 목록에 대해서만 승인됩니다. 다시 말해, 사용자가 웹 로그인을 인증하더라도 서버 요청은 사용자의 기기가 iCloud.com에서 보도록 의도되지 않은 데이터(건강 데이터 또는 iCloud 키체인의 암호 등)에 대한 서비스 키를 업로드하도록 요구할 수 없습니다. Apple 서버는 사용자가 웹에서 접근하도록 요청하는 특정 데이터를 암호화 해제하는 데 필요한 서비스 키만 요청합니다. 서비스 키가 업로드될 때마다 서비스 키는 사용자가 인증한 웹 세션에 연결된 임시 키를 사용하여 암호화되며, 데이터가 일시적으로 Apple 서버에 제공되는 iCloud 서비스를 보여주는 알림이 사용자의 기기에 표시됩니다.

사용자의 선택 유지하기

고급 데이터 보호 및 iCloud.com 웹 접근 설정은 사용자만 변경할 수 있습니다. 이러한 값은 사용자의 iCloud 키체인 기기 메타데이터에 저장되며 사용자의 신뢰하는 기기 중 하나에서만 변경할 수 있습니다. Apple 서버는 사용자를 대신해 이러한 설정을 수정하거나 이전 구성으로 되돌릴 수 없습니다.

공유 및 공동 작업의 보안 영향

대부분의 경우, 서로 공동 작업을 하기 위해 사용자가 공유 메모, 공유 미리 알림, iCloud Drive의 공유 폴더 또는 iCloud 공유 사진 보관함 등을 사용하여 콘텐츠를 공유하고 모든 사용자가 고급 데이터 보호를 켠 경우, Apple 서버는 공유를 설정하기 위해서만 사용되고 공유 데이터의 암호화 키에 대한 접근 권한은 갖지 않습니다. 콘텐츠는 종단간 암호화되고 참가자의 신뢰하는 기기에서만 접근 가능합니다. 각 공유 작업의 제목 및 대표 축소판은 수신하는 사용자에게 미리보기를 표시하기 위해 표준 데이터 보호를 사용하여 Apple이 저장할 수 있습니다.

공동 작업을 활성화할 때 '해당 링크를 가진 누구나' 옵션을 선택하면 Apple 서버가 URL을 여는 누구나에게 접근 권한을 제공할 수 있어야 하므로 해당 콘텐츠는 표준 데이터 보호를 사용하여 Apple 서버에 제공됩니다.

iWork 공동 작업 및 사진의 공유 앨범 기능은 고급 데이터 보호를 지원하지 않습니다. 사용자가 iWork 문서에서 공동 작업하거나 iCloud Drive의 공유 폴더에서 iWork 문서를 여는 경우, 해당 문서의 암호화 키는 Apple 데이터 센터의 iWork 서버에 안전하게 업로드됩니다. 이는 iWork의 실시간 공동 작업을 수행하려면 참가자 간의 문서 변경 사항을 조율하기 위한 서버 측 조정이 필요하기 때문입니다. 공유 앨범 기능은 웹에서 앨범을 공개적으로 공유하도록 허용하기 때문에 공유 앨범에 추가되는 사진은 표준 데이터 보호를 사용하여 저장됩니다.

고급 데이터 보호 비활성화하기

사용자는 언제든지 고급 데이터 보호를 끌 수 있습니다. 끄도록 결정한 경우 다음과 같은 작업이 수행됩니다.

1. 사용자의 기기가 먼저 새로운 선택을 iCloud 키체인 참여 메타데이터에 기록합니다. 그러면 이 설정은 모든 기기에 안전하게 동기화됩니다.

2. 사용자의 기기가 모든 **인증 후 사용 가능(available-after-authentication)** 서비스의 서비스 키를 Apple 데이터 센터의 iCloud HSM에 안전하게 업로드합니다. iCloud 키체인 및 건강 데이터와 같이 표준 데이터 보호를 사용하여 종단간 암호화되는 서비스의 키는 여기에 절대 포함되지 않습니다.

기기는 고급 데이터 보호를 켜기 전에 생성된 원래 서비스 키와 사용자가 해당 기능을 켠 후에 생성된 새로운 서비스 키 모두를 업로드합니다. 이를 통해 인증 후 이러한 서비스의 모든 데이터에 접근할 수 있으며 해당 계정을 표준 데이터 보호로 되돌릴 수 있습니다. 표준 데이터 보호를 사용하면 사용자가 계정에 대한 접근 권한을 상실할 경우 사용자가 대부분의 데이터를 복구하도록 Apple이 다시 도울 수 있습니다.

고급 데이터 보호가 지원되지 않는 iCloud 데이터

전역 이메일, 연락처 및 캘린더 시스템과의 상호 운영을 위해 iCloud Mail, 연락처 및 캘린더는 종단간 암호화되지 않습니다.

iCloud는 고급 데이터 보호가 켜져 있어도 사용자 특정 CloudKit 서비스 키 보호를 사용하지 않고 일부 데이터를 저장합니다. 보호를 받으려면 컨테이너의 스키마에서 CloudKit 기록 필드에 '암호화(encrypted)'를 명시하여야 합니다. 또한 암호화된 필드를 읽고 쓰려면 전용 API를 사용해야 합니다. 파일 또는 개체가 수정된 날짜 및 시간은 사용자의 정보를 정렬할 때 사용되고, 파일 및 사진 데이터의 체크섬은 Apple이 사용자의 iCloud 및 기기의 저장 공간을 중복 제거하고 최적화하도록 돕는 데 사용됩니다. 이 모두는 파일 및 사진 자체에 대한 접근 권한을 사용하지 않습니다. 특정 데이터 카테고리에 암호화가 어떻게 사용되는지에 대한 자세한 정보는 Apple 지원 문서 iCloud 데이터 보안 개요에서 확인할 수 있습니다.

데이터 중복 제거에 체크섬을 사용하는 **수렴형 암호화(convergent encryption)**라고 하는 잘 알려진 기술을 적용하는 등의 결정은 iCloud 서비스가 시작되었을 때 원래 설계의 일부였습니다. 이 메타데이터는 항상 암호화되지만 암호화 키는 표준 데이터 보호를 사용하여 Apple이 저장합니다. 모든 사용자에 대한 보안 보호를 계속 강화하기 위해 Apple은 고급 데이터 보호가 켜져 있을 때 이와 같은 메타데이터를 포함한 더 많은 데이터가 종단간 암호화되도록 계속 노력하고 있습니다.

고급 데이터 보호 요구 사항

iCloud용 고급 데이터 보호를 켜기 위한 요구 사항에는 다음이 포함됩니다.

- 사용자의 계정이 종단간 암호화를 지원해야 합니다. 종단간 암호화를 사용하려면 Apple ID에 대한 이중 인증이 필요하고 암호가 신뢰하는 기기에 설정되어 있어야 합니다. 자세한 내용은 Apple 지원 문서 Apple ID의 이중 인증을 참조하십시오.
- 사용자가 Apple ID로 로그인한 기기가 iOS 16.2, iPadOS 16.2, macOS 13.1, tvOS 16.2, watchOS 9.2 이상 및 Windows용 iCloud 최신 버전으로 업데이트되어야 합니다. 이 요구 사항은 이전 버전의 iOS, iPadOS, macOS, tvOS 또는 watchOS가 계정 상태를 복구하려는 잘못된 시도로 **인증 후 사용 가능(available-after-authentication)** HSM에 새로 생성된 서비스 키를 다시 업로드하여 이를 잘못 처리하는 것을 방지합니다.
- 사용자는 계정에 대한 접근 권한을 상실할 경우 iCloud 데이터를 복구하는 데 사용할 수 있는 1개 이상의 대체 복구 방법(1개 이상의 복구 연락처 또는 복구 키)을 설정해야 합니다.

복구 연락처의 정보가 오래되거나 사용자가 이를 잊는 등 복구 방법이 실패하면 Apple은 사용자의 종단간 암호화된 iCloud 데이터를 복구하는 것을 도울 수 없습니다.

iCloud용 고급 데이터 보호는 Apple ID에 대해서만 켤 수 있습니다. 관리형 Apple ID 및 자녀 계정(나라 또는 지역별로 다름)은 지원되지 않습니다.

iCloud 백업의 보안

iCloud는 기기 설정, 앱 데이터, 카메라 롤의 사진 및 비디오, 메시지 앱의 대화를 포함한 정보를 매일 Wi-Fi를 통해 백업합니다. iCloud 백업은 기기가 잠겨 있고, 전원에 연결되어 있으며, Wi-Fi로 인터넷에 연결되어 있을 때에만 수행됩니다. iOS 및 iPadOS에서 사용되는 저장 공간 암호화를 고려하여 설계된 iCloud 백업은 증분 자동 백업 및 복원을 수행하는 동안 데이터를 안전하게 유지합니다. 기본적으로 iCloud 백업 서비스 키는 Apple 데이터 센터의 iCloud HSM(하드웨어 보안 모듈)에 안전하게 백업되며, 인증 후 사용 가능(available-after-authentication) 데이터 카테고리의 일부입니다. iCloud용 고급 데이터 보호를 켠 사용자의 경우, iCloud 백업 서비스 키는 종단간 암호화로 보호되며, 신뢰하는 기기를 사용하는 사용자에게만 제공됩니다.

기기가 잠겨 있을 때 접근할 수 없는 데이터 보호 클래스에 파일이 생성되면, 해당 파일의 파일별 키가 iCloud 백업 keybag의 클래스 키를 사용하고 원래의 암호화된 상태로 파일을 iCloud에 백업하여 암호화합니다. CloudKit 암호화에 설명된 것과 같이 모든 파일은 전송 중 암호화되며, 저장 시 계정 기반 키를 사용하여 암호화됩니다.

iCloud 백업 keybag은 기기가 잠겨 있을 때 액세스할 수 없는 데이터 보호 클래스에 대한 비대칭(Curve25519) 키를 포함합니다. 백업 세트는 사용자의 iCloud 계정에 저장되며 사용자 파일의 사본과 iCloud 백업 keybag으로 구성됩니다. iCloud 백업 keybag은 임의 키로 보호되며, 이 임의 키 또한 백업 세트와 함께 저장됩니다. 사용자의 iCloud 암호는 암호화에 사용되지 않으므로 iCloud 암호를 변경해도 기존 백업이 무효화되지 않습니다.

복원 시에는 사용자의 iCloud 계정에서 백업된 파일, iCloud 백업 keybag 및 keybag용 키를 가져옵니다. iCloud 백업 keybag은 keybag용 키를 사용하여 암호화 해제됩니다. 그런 다음 keybag의 파일별 키를 사용하여 백업 세트에 있는 파일을 암호화 해제하며, 이 파일은 파일 시스템에 새로운 파일로 작성되어 데이터 보호 클래스에 따라 다시 암호화됩니다.

다음 콘텐츠는 iCloud 백업을 사용하여 백업됩니다.

- 구매한 음악, 영화, TV 프로그램, 앱 및 책의 기록. 사용자의 iCloud 백업은 사용자의 기기에 있는 구입한 콘텐츠에 대한 정보를 포함합니다. 구입한 콘텐츠 자체는 포함하지 않습니다. 사용자가 iCloud 백업을 사용하여 복원하면 iTunes Store, App Store, Apple TV 앱 또는 Apple Books에서 구입한 콘텐츠가 자동으로 다운로드됩니다. 일부 유형의 콘텐츠는 일부 국가 또는 지역에서 자동으로 다운로드되지 않으며, 환불되었거나 해당 매장에서 더 이상 사용할 수 없게 된 경우 이전에 구입한 항목을 사용할 수 없습니다. 전체 구입 내역은 사용자의 Apple ID에 연결되어 있습니다.
- 사용자의 기기에 저장된 사진 및 비디오. 사용자가 iOS 8.1, iPadOS 13.1 또는 OS X 10.10.3 이상에서 iCloud 사진을 활성화하면, 사진과 비디오는 iCloud에 이미 저장된 상태이므로 사용자의 iCloud 백업에 포함되지 않습니다.

- 연락처, 캘린더 이벤트, 미리 알림 및 메모
- 기기 설정값
- 앱 데이터
- 홈 화면 및 앱 구성
- HomeKit 구성
- 의료 정보 데이터
- 음성 메모 암호(필요한 경우, 백업 중에 사용한 물리적인 SIM 카드 필요)
- 메시지, Apple Messages for Business, 문자 메시지(SMS) 및 MMS 메시지(필요한 경우, 백업 중에 사용한 물리적인 SIM 카드 필요)

또한 iCloud 백업은 해당 기기의 Secure Enclave UID 루트 암호화 키에서 파생된 키로 암호화되어 있는 로컬 기기 키체인을 백업하는 데 사용됩니다. 이 키는 해당 기기에 고유하며 Apple은 이 키에 대해 알지 못합니다. 이를 통해 데이터베이스를 생성한 기기에만 데이터베이스를 복원할 수 있으며, 이는 Apple을 포함한 다른 어느 누구도 해당 데이터베이스를 읽을 수 없음을 의미합니다. 자세한 내용은 Secure Enclave를 참조하십시오.

iCloud에 메시지 보관

'iCloud에 메시지 보관'은 모든 기기에서 사용자의 전체 메시지 기록이 업데이트되고 사용 가능하도록 유지합니다.

표준 데이터 보호를 사용하면 'iCloud에 메시지 보관'은 iCloud 백업이 꺼져 있을 때 종단간 암호화됩니다. iCloud 백업이 켜져 있는 경우, 해당 백업은 사용자가 iCloud 키체인에 대한 접근 권한 및 신뢰하는 기기를 상실하더라도 메시지를 복구하도록 Apple이 도울 수 있게 'iCloud에 메시지 보관' 암호화 키의 사본을 포함합니다. 사용자가 iCloud 백업을 끄면 앞으로 사용할 'iCloud에 메시지 보관'을 보호하도록 새로운 키가 기기에 생성됩니다. 새로운 키는 iCloud 키체인에만 저장되고, 신뢰하는 기기에서만 접근할 수 있으며, 컨테이너에 작성된 새로운 데이터는 이전의 컨테이너 키로는 암호화 해제할 수 없습니다.

고급 데이터 보호를 사용하면 'iCloud에 메시지 보관'은 항상 종단간 암호화됩니다. iCloud 백업이 켜져 있는 경우, 'iCloud에 메시지 보관' 암호화 키를 포함한 내부의 모든 항목이 종단간 암호화됩니다. 사용자가 고급 데이터 보호를 켜면 'iCloud에 메시지 보관' 컨테이너 키는 물론 iCloud 백업 서비스 키 또한 함께 롤링됩니다. 자세한 내용은 Apple 지원 문서 iCloud 데이터 보안 개요를 참조하십시오.

iCloud 비공개 릴레이 보안

iCloud 비공개 릴레이는 Safari로 웹 브라우징을 할 때 사용자를 보호할 뿐만 아니라 모든 DNS 이름 확인 요청도 보호합니다. 이는 Apple을 포함한 어떤 단일 주체도 사용자의 IP 주소와 브라우징 활동을 연관시킬 수 없도록 합니다. 이 작업은 Apple이 관리하는 수신 프록시와 콘텐츠 제공자가 관리하는 송신 프록시 등 다양한 프록시를 사용하여 수행됩니다. iCloud 비공개 릴레이를 사용하려면 사용자는 iOS 15, iPadOS 15 또는 macOS 12.0.1 이상을 실행 중이어야 하며 Apple ID로 iCloud+ 계정에 로그인한 상태여야 합니다. 이 경우 설정 > iCloud 또는 시스템 설정 > iCloud에서 iCloud 비공개 릴레이를 켤 수 있습니다.

자세한 내용은 iCloud 비공개 릴레이 개요를 참조하십시오.

계정 복구 연락처 보안

사용자는 고급 데이터 보호를 켰는지 여부에 상관없이 모든 종단간 암호화된 데이터를 포함하여 iCloud 계정 및 데이터를 복구하는 데 도움을 받을 수 있도록 신뢰하는 사람 최대 5명을 계정 복구 연락처로 추가할 수 있습니다. Apple과 복구 연락처 모두 사용자의 종단간 암호화된 iCloud 데이터를 복구하기 위해 필요한 정보를 각자 가지고 있지 않습니다.

복구 연락처는 개인정보 보호를 염두에 두고 설계되었습니다. 사용자가 선택한 복구 연락처에 대해 Apple은 알지 못합니다. Apple 서버는 사용자가 연락처에 도움을 요청하고 해당 연락처가 실제로 복구를 지원하기 시작한 후 복구 시도의 나중 과정에서만 복구 연락처에 대한 정보를 알 수 있습니다. 해당 정보는 복구가 완료된 후 유지되지 않습니다.

복구 연락처 보안 프로세스

사용자가 계정 복구 연락처를 설정할 경우, 해당 연락처와 관련된 키가 생성됩니다. 이 키는 종단간 암호화된 CloudKit 데이터를 포함하는 사용자의 iCloud 데이터에 대한 접근을 방지합니다. 다음으로, 무작위 256비트 AES 키가 생성되고 복구 연락처 키를 암호화하여 복구 연락처 패킷을 생성하는 데 사용됩니다. 암호화된 패킷은 안전하게 저장하기 위해 복구 연락처로 전송되며, 무작위 AES 키는 Apple에 저장됩니다. AES 키 및 패킷은 기본 키에 대한 어떤 정보도 자체적으로 제공하지 않습니다. 복구 시 사용자의 기기는 복구 연락처에게서는 복구 연락처 패킷을, Apple에게서는 AES 키를 성공적으로 얻은 다음, 둘을 조합하여 원본 키를 복구하고 사용자의 iCloud 데이터에 접근할 수 있습니다.

계정 복구 연락처를 설정하기 위해 사용자의 기기는 Apple 서버와 통신하여 Apple이 보유하게 될 키 정보의 할당분(위에서 언급된 AES 키)을 업로드합니다. 이후 해당 기기는 복구 연락처에 대해 종단간 암호화된 CloudKit 컨테이너를 설정하여 복구 연락처에 필요한 부분(AES 키를 사용하여 암호화된 복구 연락처 패킷)을 공유합니다. Apple에 의해 생성된 인증 비밀은 복구 연락처를 통해서도 공유됩니다. 이는 계정을 복구하는 데 사용되고, 계정의 암호를 재설정하는 데 도움이 됩니다. 복구 연락처를 초대 및 승인하는 통신은 상호 인증된 IDS 채널을 통해 이루어집니다. 복구 연락처는 수신된 정보를 자신의 iCloud 키체인에 자동으로 저장합니다. Apple은 CloudKit 컨테이너의 콘텐츠나, 이 정보를 저장하는 iCloud 키체인에 접근할 수 없습니다. 공유가 실행될 때 Apple 서버는 복구 연락처를 익명의 ID로만 볼 수 있습니다.

나중에 사용자가 계정 및 iCloud 데이터를 복구해야 할 때 복구 연락처에 도움을 요청할 수 있습니다. 이때 복구 연락처의 기기에서 복구 코드가 생성되고, 복구 연락처는 사용자를 직접 만나거나 사용자에게 전화를 거는 등 대역 외 방식으로 복구 코드를 사용자에게 제공합니다. 그런 다음 사용자가 자신의 기기에 복구 코드를 입력하여 SPAKE2+ 프로토콜을 사용하는 보안 연결을 기기 간에 설정합니다. Apple은 이러한 콘텐츠에 접근할 수 없습니다. 이 상호 작용은 Apple 서버에 의해 조정되지만 Apple은 복구 과정을 시작할 수 없습니다.

보안 연결이 설정되고 필요한 모든 보안 확인이 완료된 다음, 복구 연락처의 기기는 자신이 할당받은 키 정보와 이전에 설정된 인증 비밀을 복구를 요청하는 사용자에게 반환합니다. 사용자가 이 인증 비밀을 Apple 서버에 제시하면 Apple이 보관하는 키 정보에 접근할 수 있습니다. 인증 비밀을 제공하면 계정 접근 복원을 위한 계정 암호 재설정도 승인됩니다.

마지막으로, 사용자의 기기는 Apple과 계정 복구 연락처로부터 수신한 키 정보를 다시 결합한 다음 iCloud 데이터를 암호화 해제 및 복구하는 데 사용합니다.

복구 연락처가 사용자의 허가 없이 복구를 시작하지 않도록 방지하기 위해 사용자 계정의 사용 여부를 확인하는 등의 안전 장치가 마련되어 있습니다. 계정이 사용 중일 경우, 복구 연락처를 사용하여 복구하기 위해서는 최근 기기 암호 또는 iCloud 보안 코드 정보를 요구합니다.

유산 관리자 보안

사용자가 사망한 이후 지정된 수취인이 데이터에 접근할 수 있기를 바라는 경우, 사용자는 유산 관리자를 계정에서 설정할 수 있습니다. 유산 관리자는 복구 연락처와 유사하게 설정되지만, 수취인이 사용하는 키 정보는 고인의 iCloud 키체인의 암호화를 해제하는 데 필요한 정보를 포함하지는 않습니다. 사용된 키 구조는 계정 복구 연락처와 동일하지만, 이 경우에는 Apple이 암호화된 패킷을 저장하고 수취인은 AES 키를 보관합니다. 이렇게 하면 수취인이 받는 부분이 줄어들기 때문에 필요한 경우에 더 쉽게 프린트할 수 있으며, 기본 키에 대한 정보를 개별적으로 제공하지 않는 동일한 속성을 여전히 제공합니다.

수취인이 수신하는 키 정보는 사용자를 대상으로 하는 문서에서 액세스 키로 언급됩니다. 액세스 키는 지원되는 기기에서 자동으로 저장되지만, 프린트하거나 오프라인으로 저장하여 사용할 수도 있습니다. 자세한 내용은 Apple 지원 문서 Apple ID의 유산 관리자를 추가하는 방법을 참조하십시오.

사용자가 사망한 이후 유산 관리자는 Apple 청구 웹 사이트에 로그인하여 접근을 시작할 수 있습니다. 이를 위해서는 사망진단서가 필요하며, 이전 섹션에서 언급된 인증 비밀을 사용하여 부분적으로 승인이 진행됩니다. 모든 보안 확인이 완료된 다음, Apple은 새 계정을 위한 사용자 이름 및 암호를 발행하고 유산 관리자에게 필요한 키 정보를 제공합니다.

이 정보는 필요할 때 액세스 키를 더 쉽게 입력하기 위해 관련된 QR 코드와 함께 알파벳 숫자 코드로 제공됩니다. 입력한 다음에는 고인의 iCloud 데이터에 대한 접근이 복원됩니다. 기기에서 이 과정을 수행하거나 온라인에서 접근을 설정할 수 있습니다. 자세한 내용은 Apple 지원 문서 유산 관리자로서 Apple 계정에 대한 접근 권한 요청하기를 참조하십시오.

암호 관리

암호 보안 개요

iOS, iPadOS 및 macOS는 사용자가 암호를 사용하는 타사 앱 및 웹 사이트에서 보다 간편하게 인증할 수 있도록 지원합니다. 암호를 관리하는 가장 좋은 방법은 암호를 사용하지 않아도 되는 것입니다. ‘Apple로 로그인’ 기능으로 사용자는 추가 계정 또는 암호를 생성하고 관리하지 않아도 Apple ID 이중 인증으로 로그인을 보호하면서 타사 앱 및 웹 사이트에 로그인할 수 있습니다. ‘Apple로 로그인 기능’을 지원하지 않는 사이트의 경우 ‘자동으로 강력한 암호 생성’ 기능으로 사용자 기기는 사이트 및 앱에 대한 고유하고 강력한 암호를 자동으로 생성하고, 동기화하고, 입력할 수 있습니다. iOS 및 iPadOS에서 암호는 사용자가 설정 > 암호에서 제어 및 관리할 수 있는 특별한 암호 자동 완성 키체인에 저장됩니다.

macOS의 Safari 암호 환경설정에서 저장된 암호를 관리할 수 있습니다. 이 동기화 시스템은 사용자가 수동으로 생성한 암호를 동기화하는 데에도 사용될 수 있습니다.

‘Apple로 로그인’ 보안

‘Apple로 로그인’은 기타 단일 로그인 시스템에 대한 대안으로 개인정보를 보호합니다. 사용자에게 편리하고 효율적인 탭 로그인 방식을 제공하고, 투명성과 개인정보에 대한 통제권을 부여합니다.

‘Apple로 로그인’을 사용하면 사용자는 계정을 설정하고 이미 가지고 있는 Apple ID를 사용하여 앱 및 웹 사이트에 로그인할 수 있으며, 자신의 개인정보를 더 많이 제어할 수 있습니다. 앱은 계정을 설정할 때만 사용자 이름과 이메일 주소를 요청할 수 있으며 사용자는 항상 다음을 선택할 수 있습니다. 개인 이메일 주소를 앱과 공유하거나 개인 이메일을 비공개로 유지하고 새로운 Apple 개인 이메일 릴레이 서비스를 대신 사용할 수 있습니다. 이 이메일 릴레이 서비스는 사용자의 개인 주소로 전달되는 고유한 익명 이메일 주소를 공유하므로 사용자는 보안 수준을 유지하고 개인정보를 제어하는 동시에 개발자로부터 유용한 정보를 받을 수 있습니다.

‘Apple로 로그인’ 기능은 보안을 위해 구축되었습니다. ‘Apple로 로그인’을 사용하는 모든 사용자의 Apple ID는 이중 인증이 활성화되어 있어야 합니다. 이중 인증은 사용자의 Apple ID뿐만 아니라 앱에 설정한 계정도 보호할 수 있습니다. 나아가 Apple은 개인정보를 보호하는 사기 방지 신호를 개발하고 ‘Apple로 로그인’ 기능에 통합했습니다. 이 신호는 개발자에게 직접 유치한 신규 사용자가 봇이나 스크립트로 작성된 계정이 아닌 실제 사람이라는 확신을 심어줍니다.

자동으로 강력한 암호 사용

iCloud 키체인이 활성화된 경우, 사용자가 Safari에서 웹 사이트에 가입하거나 암호를 변경할 때 iOS, iPadOS 및 macOS가 강력하고 고유한 암호를 무작위로 생성합니다. iOS 및 iPadOS의 경우 앱에서도 자동으로 강력한 암호 생성 기능을 사용할 수 있습니다. 사용자는 강력한 암호를 사용하지 않으려면 선택 해제해야 합니다. 생성된 암호는 키체인에 저장되며 iCloud 키체인이 활성화된 경우 기기 간에 최신 상태를 유지합니다.

기본적으로 iOS 및 iPadOS에서 생성된 암호는 20자입니다. 하나의 숫자, 하나의 대문자, 두 개의 하이픈 및 16개의 소문자로 구성되어 있습니다. 생성된 암호는 강력하며 71비트의 엔트로피를 포함합니다.

암호는 암호 생성이 가능한 암호 필드인지 확인하는 휴리스틱(Heuristics)을 기반으로 생성됩니다. 휴리스틱이 암호 생성이 가능한 문맥별 암호를 인식하지 못한 경우, 앱 개발자는 텍스트 필드에 `UITextContentType.newPassword`를 설정할 수 있으며 웹 개발자는 <input> 요소에 `autocomplete= “new-password”`를 설정할 수 있습니다.

생성된 암호와 관련 서비스의 호환 여부를 보장하기 위해 앱 및 웹 사이트에서 규칙을 제공합니다. 개발자는 input 요소에서 `UITextInputPasswordRules` 또는 `passwordrules` 속성을 사용하여 이러한 규칙을 제공합니다. 그런 다음 기기는 이러한 규칙을 충족할 수 있는 가장 강력한 암호를 생성합니다.

암호 자동 완성 보안

암호 자동 완성은 키체인에 저장된 자격 증명을 자동으로 채웁니다. iCloud 키체인 암호 관리자 및 암호 자동 완성은 다음 기능을 제공합니다.

- 앱 및 웹 사이트에서 자격 증명 채우기
- 강력한 암호 생성
- 암호를 앱 및 Safari 웹 사이트 모두에 저장
- 사용자의 연락처와 안전하게 암호 공유
- 자격 증명을 요구하는 근처의 Apple TV에 암호 제공

iOS 및 iPadOS에서만 앱 내에서 암호를 생성 및 저장하고 Apple TV에 암호를 제공할 수 있습니다.

앱 내 암호 자동 완성

Safari의 암호 자동 완성과 유사하게, iOS 및 iPadOS에서 저장된 사용자 이름 및 암호를 앱 내 인증서 관련 필드에 입력할 수 있습니다. iOS 및 iPadOS의 경우 사용자가 소프트웨어 키보드의 QuickType 막대에서 키를 탭해야 합니다. macOS의 경우 Mac Catalyst로 제작한 앱의 경우 인증서 관련 필드 아래에 '암호' 드롭다운 메뉴가 표시됩니다.

동일한 apple-app-site-association 파일로 구동되는 동일한 앱-웹 사이트 연동 메커니즘을 사용하여 앱과 웹 사이트가 강력하게 연동된 경우, 암호 자동 완성 키체인에 저장된 영역이 있으면 iOS 및 iPadOS QuickType 막대와 macOS 드롭다운 메뉴는 앱에 대한 자격 증명을 즉시 제안합니다. 이를 통해 사용자는 Safari에 저장된 자격 증명을 보안 속성이 동일하지만 API를 채택하지 않은 앱에 공개할지 선택할 수 있습니다.

암호 자동 완성은 사용자가 앱에 인증서를 공개하는 것에 동의하기 전까지는 어떠한 인증서 정보도 유출하지 않습니다. 인증서 목록은 앱 프로세스에서 도출하거나 가져옵니다.

앱과 웹 사이트가 신뢰 관계이며 사용자가 앱 내에서 자격 증명을 제출한 경우 iOS 및 iPadOS에서 사용자에게 나중에 사용할 수 있도록 해당 자격 증명을 암호 자동 완성 키체인에 저장하라는 메시지를 표시합니다.

저장된 암호에 접근할 수 있는 앱 권한

iOS, iPadOS 및 macOS 앱은 암호 자동 완성 키체인이 `ASAuthorizationPasswordProvider` 및 `SecAddSharedWebCredential`을 사용하여 사용자 로그인을 돕도록 요청할 수 있습니다. 암호 공급자 및 그 요청은 'Apple로 로그인' 기능과 함께 사용할 수 있으므로, 사용자 계정이 암호 기반인지 'Apple로 로그인'을 통해 생성되었는지와 상관없이 사용자가 앱에 로그인할 수 있도록 동일한 API가 호출됩니다.

앱은 앱 개발자 및 웹 사이트 관리자 모두가 허가하고 사용자가 동의한 경우에만 저장된 암호에 접근할 수 있습니다. 앱 개발자는 앱 내에 권한을 포함시켜 Safari에 저장된 암호에 접근할 의도를 표명합니다. 해당 권한은 관련 웹 사이트의 전체 주소 도메인 이름을 나열하며 이 웹 사이트는 Apple이 인증한 앱의 고유 앱 식별자를 파일로 만들어 서버에 저장해 두어야 합니다.

com.apple.developer.associated-domains 권한을 가진 앱이 설치된 경우 iOS 및 iPadOS는 목록에 있는 각각의 웹 사이트에 TLS 요청을 보내 다음 파일 중 하나를 요청합니다.

- apple-app-site-association
- .well-known/apple-app-site-association

설치되는 앱의 앱 식별자가 목록 파일에 있다면 iOS 및 iPadOS는 웹 사이트와 앱이 신뢰 관계를 가진 것으로 표시합니다. 신뢰 관계를 통해서만 위의 두 가지 API가 사용자에게 요청을 보내고 사용자는 반드시 동의를 선택해야 앱에 암호를 공개, 업데이트 또는 삭제할 수 있습니다.

암호 보안 권장 사항

iOS, iPadOS 및 macOS의 암호 자동 완성의 암호 목록은 저장된 암호 중 다른 웹 사이트에서 **재사용**된 암호, **보안에 취약**한 암호 및 **데이터 유출**로 침해된 암호를 표시합니다.

개요

두 개 이상의 서비스에 동일한 암호를 사용하면 해당 계정이 크리덴셜 스터핑(Credential Stuffing) 공격에 취약해질 수 있습니다. 서비스의 보안을 뚫고 암호가 유출되면 공격자는 다른 서비스에 동일한 자격 증명을 사용하여 또 다른 계정을 공격할 수 있습니다.

- 서로 다른 도메인에서 두 개 이상의 저장된 암호에 대해 동일한 암호가 사용된 경우 **재사용된** 암호로 표시됩니다.
- 공격자가 쉽게 추측할 수 있는 암호는 보안에 **취약한** 암호입니다. iOS, iPadOS 및 macOS는 사전에 있는 단어 사용, 일반적인 대체 문자(예: 'password' 대신 'p4ssw0rd' 사용), 키보드에서 찾은 패턴(예: QWERTY 키보드에서 'q12we34r'), 연속되는 글자 반복(예: '123123') 등의 기억하기 쉬운 암호를 생성하는 일반적인 패턴을 감지합니다. 이러한 패턴은 서비스의 암호 생성 최소 요구 사항을 충족하는 암호를 생성하기 위해 주로 사용되지만, 암호 획득을 무작위로 시도하려는 공격자가 일반적으로 사용하는 방법이기도 합니다.

  많은 서비스가 4자리 또는 6자리 PIN 코드를 따로 요구하기 때문에 이러한 짧은 암호는 다른 규칙으로 평가됩니다. PIN 코드가 연속된 숫자(예: '1234' 또는 '8765')이거나 반복되는 패턴(예: '123123' 또는 '123321')처럼 가장 일반적인 PIN 코드 중 하나인 경우, 보안 강도가 약한 것으로 간주됩니다.
- 암호 모니터링 기능에서 암호가 데이터 유출에 포함되었다고 보는 경우 **유출된** 암호로 표시됩니다. 자세한 내용은 암호 모니터링를 참조하십시오.

취약하고 재사용되었으며 유출된 암호는 암호 목록(macOS)에 표시되거나 전용 보안 권장 사항 인터페이스(iOS 및 iPadOS)에 표시됩니다. 사용자가 보안에 취약한 암호나 데이터 유출로 침해된 기존 저장 암호로 Safari의 웹 사이트에 로그인하는 경우 자동으로 강력한 암호를 사용하도록 암호 업그레이드를 적극 권장하는 알림이 표시됩니다.

iOS 및 iPadOS에서 계정 인증 보안 업그레이드하기

인증 서비스 프레임워크에서 계정 인증 변경 확장 프로그램을 구현한 앱은 암호 기반 계정이 'Apple로 로그인'을 사용하도록 전환하거나 자동으로 강력한 암호를 사용하도록 한 번의 탭을 통한 간편한 업그레이드를 제공할 수 있습니다. 이 확장 포인트는 iOS 및 iPadOS에서 사용할 수 있습니다.

앱이 확장 포인트를 구현하고 기기에 설치된 경우, 설정의 iCloud 키체인 암호 관리자에서 앱과 연결된 자격 증명에 대한 보안 권장 사항을 볼 때 확장 업그레이드 옵션이 표시됩니다. 사용자가 위험한 상태의 자격 증명을 사용하여 앱에 로그인 할 때도 업그레이드가 제공됩니다. 앱에는 로그인 후 사용자에게 업그레이드 옵션을 표시하지 않도록 시스템을 설정하는 기능이 있습니다. 새로운 AuthenticationServices API를 사용하면 앱의 계정 설정 또는 계정 관리 화면에서 앱이 자체적으로 확장 프로그램을 호출하고 업그레이드를 수행할 수도 있습니다.

앱은 강력한 암호 업그레이드, 'Apple로 로그인' 업그레이드 중 하나 이상을 지원하도록 선택할 수 있습니다. 강력한 암호 업그레이드의 경우, 시스템은 사용자를 위해 자동으로 강력한 암호를 생성합니다. 필요한 경우 앱은 사용자 설정 암호 규칙을 제공하여 새로운 암호를 생성할 때 해당 규칙을 따르도록 할 수 있습니다. 사용자가 계정에 대해 암호를 사용하는 방식에서 'Apple로 로그인'을 사용하도록 변경하면, 시스템은 계정을 연결할 확장 프로그램에 새로운 Apple로 로그인 자격 증명을 제공합니다. 사용자의 Apple ID 이메일은 자격 증명의 일부로 제공되지 않습니다. 'Apple로 로그인' 업그레이드에 성공한 후, 이전에 사용한 암호 자격 증명이 사용자의 키체인에 저장되어 있는 경우 시스템에서 해당 자격 증명을 키체인에서 삭제합니다.

계정 인증 변경 확장 프로그램은 업그레이드를 진행하기 전에 추가 사용자 인증을 수행할 수 있습니다. 암호 관리자 내에서 시작되었거나 앱에 로그인한 후 시작된 업그레이드의 경우, 확장 프로그램은 업그레이드할 계정의 사용자 이름과 암호를 제공합니다. 앱 내 업그레이드의 경우, 사용자 이름만 제공됩니다. 확장 프로그램에서 추가 사용자 인증을 요구하는 경우, 업그레이드를 진행하기 전에 사용자 설정 사용자 인터페이스를 표시하도록 요청할 수 있습니다. 이러한 사용자 인터페이스를 표시하도록 하는 의도는 사용자가 2차 인증 요소를 입력하여 업그레이드를 승인하도록 하기 위한 것입니다.

암호 모니터링

암호 모니터링은 사용자의 암호 자동 완성 키체인에 저장된 암호와 여러 온라인 조직에서 발생한 유출에 노출된 것으로 알려진 암호로 구성된 지속적으로 업데이트되는 선별 목록과 비교하여 매칭하는 기능입니다. 이 기능이 켜져 있으면 모니터링 프로토콜이 사용자의 암호 자동 완성 키체인 암호를 선별된 목록과 비교하여 지속적으로 매칭합니다.

모니터링 작동 방식

사용자의 기기는 계속해서 각 암호 또는 암호 관리자의 사용 패턴과 무관한 간격을 쿼리하면서 사용자의 암호에 라운드 로빈 점검을 수행합니다. 이를 통해 확인 상태와 유출된 암호가 선별된 목록이 최신으로 유지됩니다. 사용자가 가진 고유 암호 개수와 관련된 정보의 유출을 방지하기 위해 요청은 일괄 처리되며 동시에 수행됩니다. 고정된 수의 암호는 각 검사에서 동시에 확인되며 사용자가 가진 개수가 이 수보다 적은 경우 임의의 암호가 생성되고 쿼리에 추가되어 차이를 보완합니다.

암호를 매칭하는 방법

암호 매칭은 두 개의 프로세스로 이루어집니다. 가장 흔하게 유출되는 암호는 사용자 기기의 로컬 목록에 포함되어 있습니다. 이 목록에 사용자의 암호가 포함되면 외부 상호 작용 없이 즉시 사용자에게 알립니다. 이렇게 하면 암호 위반으로 인해 위험에 가장 많이 노출된 사용자 암호에 대한 정보가 유출되지 않습니다.

가장 빈도가 높은 목록에 해당 암호가 포함되어 있지 않으면 유출 빈도가 낮은 암호와 매칭됩니다.

사용자 암호와 선별된 목록 비교하기

로컬 목록에 없는 암호가 매칭되는 암호인지 확인하려면 Apple 서버와의 상호 작용이 필요합니다. 합법적 사용자 암호가 Apple로 전송되지 않도록 하기 위해 사용자의 암호를 대량의 유출된 암호 목록과 비교하는 일종의 암호화 **비공개 교집합**이 배포됩니다. 이렇게 하면 암호가 침해될 위험이 낮기 때문에 Apple에 정보가 거의 공유되지 않습니다. 사용자 암호의 경우 이 정보는 사용자 암호의 15비트 프리픽스 암호화 해시로 제한됩니다. 가장 흔하게 유출되는 암호 로컬 목록을 통해 이 상호 작용 프로세스에서 가장 자주 유출되는 암호를 제거하면 웹 서비스 버킷에서 암호의 상대적 빈도에 대한 델타 값이 감소하며, 이러한 조회 항목에서는 사용자 암호 추측이 불가능합니다.

기본 프로토콜은 이 문서 작성 시점에 약 15억개의 암호를 포함한 선별된 암호 목록을 2^{15}개의 서로 다른 버킷으로 분할합니다. 암호가 속한 버킷은 암호의 SHA256 해시 값의 처음 15비트에 기반합니다. 또한 유출된 각 암호(pw)는 NIST P256 곡선의 타원 곡선 포인트와 연결됩니다. $P_{pw} = \alpha \cdot H_{SWU}(pw)$에서 α는 Apple만 알고 있는 비밀 임의 키이고 H_{SWU}는 Shallue-van de Woestijne-Ulas 방법을 기반으로 암호를 곡선 포인트에 매핑하는 임의 오라클 함수입니다. 이러한 변환은 암호 값을 계산적으로 숨기고 암호 모니터링을 통해 새롭게 유출된 암호가 드러나지 않도록 설계되었습니다.

비공개 교집합을 계산하기 위해 사용자의 기기는 SHA256(upw)의 15비트 프리픽스 λ를 사용하여 사용자의 암호가 속한 버킷을 결정합니다. 여기서 upw는 사용자 암호 중 하나입니다. 기기는 자체 임의 상수 β를 생성하고 λ와 일치하는 버킷에 대한 요청과 함께 포인트 $P_c = \beta \cdot H_{SWU}(upw)$를 서버로 보냅니다. 여기서 β는 사용자의 암호에 관한 정보를 숨기고 해당 암호로부터 Apple에 노출되는 정보를 λ로 제한합니다. 마지막으로 서버는 사용자 기기에서 전송한 포인트를 가져와서 $\alpha P_c = \alpha\beta \cdot H_{SWU}(upw)$를 계산한 다음, 적절한 버킷 포인트 $B\lambda = \{$프리픽스 λ로 시작하는 $P_{pw} \mid SHA256(pw)\}$과 함께 기기에 반환합니다.

반환된 정보를 통해 기기는 $B'_\lambda = \{\beta \cdot P_{pw} \mid P_{pw} \in B_\lambda\}$를 계산할 수 있으며, $\alpha P_c \in B'_\lambda$의 경우에 사용자 암호가 유출되었는지 확인합니다.

다른 사용자 또는 Apple 기기에 암호 전송

Apple은 AirDrop을 사용하여 다른 사용자나 Apple 기기 또는 Apple TV에서 암호를 안전하게 전송합니다.

AirDrop을 사용하여 다른 기기에 자격 증명 저장하기

iCloud가 활성화되면 사용자는 AirDrop을 사용해서 저장된 자격 증명을 다른 기기에 전송할 수 있습니다. 자격 증명에는 사용자 이름 및 암호와 이름 및 암호가 저장된 웹 사이트를 포함합니다. AirDrop으로 자격 증명을 전송하는 기능은 사용자의 설정과 상관없이 항상 '연락처만' 모드로 동작합니다. 사용자가 동의한 후 수신 기기에서 자격 증명이 사용자의 암호 자동 완성 키체인에 저장됩니다.

Apple TV의 앱에서 자격 증명 채우기

Apple TV 앱에서 암호 자동 완성을 사용하여 자격 증명을 채울 수 있습니다. tvOS에서 커서가 사용자 이름 또는 암호 텍스트 필드에 있을 때 Apple TV는 BLE(Bluetooth Low Energy)를 통해 암호 자동 완성 요청 알림을 시작합니다.

근처에 있는 iPhone 또는 iPad는 해당 사용자에게 Apple TV와 자격 증명 공유에 초대하는 메시지를 표시합니다. 암호화 방식을 설정하는 방법은 다음과 같습니다.

- 기기와 Apple TV가 동일한 iCloud 계정을 사용하는 경우 기기 간에 자동으로 암호화됩니다.
- Apple TV에서 사용하는 계정이 아닌 다른 iCloud 계정으로 기기에 로그인한 경우, PIN 코드를 사용하여 암호화된 연결을 설정하라는 메시지가 사용자에게 표시됩니다. 이 메시지를 수신하려면 iPhone은 반드시 잠금 해제되어 있어야 하며 Apple TV와 연결된 Siri Remote와 가까이에 있어야 합니다.

BLE 링크 암호화를 사용하여 암호화된 연결이 구축된 후 자격 증명이 Apple TV에 전송되며 앱의 관련 텍스트 필드에 자동으로 채워집니다.

자격 증명 제공업체 확장 프로그램

iOS, iPadOS 및 macOS에서 사용자는 사용 중인 타사 앱을 암호 설정(iOS 및 iPadOS)의 암호 자동 완성 또는 시스템 설정(macOS 13 이상)이나 시스템 환경설정(macOS 12 또는 이전 버전)의 확장 프로그램 설정에 대한 자격 증명 제공업체로 지정할 수 있습니다. 이 메커니즘은 앱 확장 프로그램에 내장되어 있습니다. 자격 증명 제공업체 확장 프로그램은 자격 증명을 선택할 수 있는 보기를 **반드시 제공해야 합니다**. 확장 프로그램은 자격 증명이 QuickType 막대(iOS 및 iPadOS) 또는 자동 완성 제안(macOS)에서 바로 제공되도록 저장된 자격 증명에 대한 메타데이터를 **선택적으로 제공할 수 있습니다**. 메타데이터에는 자격 증명의 웹 사이트와 연결된 사용자 이름이 포함되지만 암호는 포함되지 않습니다. 사용자가 앱 또는 Safari의 웹 사이트에서 자격 증명을 채울 때 iOS, iPadOS 및 macOS는 확장 프로그램과 통신하여 암호를 수신합니다. 자격 증명 메타데이터는 자격 증명 제공업체 앱의 컨테이너 내부에 저장되며 앱이 삭제되면 자동으로 제거됩니다.

iCloud 키체인

iCloud 키체인 보안 개요

iCloud 키체인을 사용하면 사용자가 Apple에 정보를 노출하지 않고 iPhone 및 iPad 기기와 Mac 컴퓨터 간에 암호 및 패스키를 안전하게 동기화할 수 있습니다. 강력한 개인정보 보호와 보안을 포함하여 iCloud 키체인의 디자인과 아키텍처는 사용 편의성과 사용자의 모든 기기에 접근할 수 없는 경우에도 키체인 콘텐츠를 복구할 수 있는 능력을 목표로 합니다. iCloud 키체인은 키체인 동기화와 키체인 복구라는 두 가지 서비스로 구성됩니다.

iCloud 키체인과 키체인 복구는 사용자의 암호 및 패스 키가 다음 조건에서도 계속 보호되도록 설계되었습니다.

- 사용자의 iCloud 계정이 침해된 경우.
- iCloud가 외부 공격 또는 직원에 의해 침해된 경우.
- 타사가 사용자 계정에 접근하는 경우.

iCloud 키체인의 암호 관리자 통합

iOS, iPadOS 및 macOS는 Safari에서 계정 암호로 사용할 수 있는 암호화된 강력한 임의의 문자열을 자동으로 생성합니다. iOS 및 iPadOS 또한 앱에서 사용할 강력한 암호를 생성할 수 있습니다. 생성된 암호는 키체인에 저장되며 다른 기기에 동기화됩니다. 키체인 항목은 Apple 서버를 통해 기기에서 기기로 전송되지만 Apple 및 다른 기기가 해당 내용을 읽을 수 없도록 종단간 암호화됩니다.

키체인 동기화 보안

사용자가 이중 인증 계정에서 iCloud 키체인을 처음으로 켜면, 기기는 자체 동기화 ID를 구축하고 생성합니다. 동기화 ID는 P-384를 사용하여 비대칭 타원형 키로 구성되며, 기기의 키체인에 저장됩니다. 각 기기는 사용자의 다른 기기의 동기화 ID 목록을 자체적으로 유지하며, 신원 키 중 하나를 사용하여 목록에 서명합니다. 이 목록은 CloudKit에 저장되어 사용자의 기기가 모든 사용자 기기에서 키체인 데이터를 안전하게 동기화하는 방법에 대한 합의에 도달할 수 있도록 합니다.

이전 iCloud 기기와의 호환성을 위해 비슷한 동기화 신뢰 서클이 생성되고, 다른 동기화 ID도 형성됩니다. 동기화 ID의 공개 키가 서클에 들어가면 서클은 두 번 서명됩니다. 먼저 동기화 ID의 개인 키로 서명된 다음 사용자의 iCloud 계정 암호에서 파생된 비대칭 타원형 키(P-256 사용)로 다시 서명됩니다. 또한 서클에 매개 변수(무작위 솔트 및 반복)가 저장되어 사용자의 iCloud 암호를 기반으로 하는 키를 생성하는 데 사용됩니다.

동기화 서클의 iCloud 저장 공간

이중 인증 계정의 경우, 각 기기의 신뢰하는 기기 목록이 CloudKit에 저장됩니다. 사용자의 iCloud 암호를 알지 못하면 목록을 읽을 수 없고 소유 기기의 개인 키가 없으면 수정할 수 없습니다.

마찬가지로, 서명된 동기화 서클은 사용자의 iCloud 키 값 저장 공간 영역에 저장됩니다. 사용자의 iCloud 암호를 알지 못하면 읽을 수 없고 해당 구성원의 동기화 ID의 개인 키가 없으면 유효하게 수정할 수 없습니다.

사용자의 다른 기기를 동기화 서클에 추가하는 방법

새 기기는 iCloud에 로그인하면서 iCloud 키체인 동기화 서클에 둘 중 한 방법으로 합류합니다. 기존의 iCloud 키체인 기기와 페어링하고 후원을 받거나 iCloud 키체인 복구를 사용합니다.

페어링 흐름 동안 신청 기기는 동기화 서클 및 동기화 목록(이중 인증 계정을 위해)을 위해 새로운 동기화 ID를 생성하고 후원자에게 제시합니다. 후원자는 동기화 서클에 신규 구성원의 공개 키를 추가하고 사용자의 iCloud 암호에서 파생된 키 및 동기화 ID로 다시 서명합니다. 새로운 동기화 서클은 iCloud에 저장되며, 여기에서 서클의 새로운 구성원이 비슷한 방식으로 서명을 합니다. 이중 인증 계정에서 후원자 기기는 연결된 기기에 ID 키로 서명된 **증빙서**도 제공하며 신청 기기를 신뢰할 수 있다는 사실을 보여줍니다. 그 다음 신뢰하는 동기화 ID의 개별 목록에 신청 기기를 포함하도록 업데이트합니다.

이제 서명 서클에 두 명의 구성원이 존재하게 되며 각 구성원은 상대의 공개 키를 가집니다. 그리고 상황에 따라 적절하게 CloudKit 또는 iCloud 키 값 저장 공간을 통해 개별 키체인 항목을 교환할 수 있습니다. 서클 구성원이 둘 다 같은 항목에 대한 업데이트가 있는 경우 둘 중 하나가 선택되어 결과적으로 일관성을 가집니다. 동기화된 각 항목은 암호화되고 사용자의 신뢰 서클 내 기기로만 암호화를 해제할 수 있으며, 다른 어떤 기기나 Apple을 통해서도 암호화를 해제할 수 없습니다.

새 기기가 동기화 서클에 합류하면 이 '합류 과정'이 반복됩니다. 예를 들어서 세 번째 기기가 합류하면 기존의 기기 둘 중 하나와 페어링이 가능합니다. 새로운 구성원이 추가되면 각 구성원은 새로운 구성원과 동기화합니다. 이를 통해 모든 구성원이 동일한 키체인 항목을 가질 수 있게 됩니다.

동기화되는 특정 항목

iMessage 키와 같은 일부 키체인 항목은 특정 기기에만 해당되기 때문에 기기에 남아야 합니다. 예기치 않은 데이터 전송을 방지하려면, 동기화되는 모든 항목은 `kSecAttrSynchronizable` 속성으로 확실하게 표시되어야 합니다.

Apple은 Wi-Fi 암호, HomeKit 암호화 키 및 종단간 iCloud 암호화를 지원하는 기타 키체인 항목뿐 아니라 Safari 사용자 데이터(사용자 이름, 암호 및 신용 카드 번호 포함)에 대해 이 속성을 설정합니다.

또한, 기본적으로 타사 앱에서 추가된 키체인 항목은 동기화하지 않습니다. 개발자는 키체인에 항목을 추가할 때 `kSecAttrSynchronizable` 속성을 설정해야 합니다.

iCloud 키체인 복구 보안

iCloud 키체인은 사용자의 키체인 데이터를 Apple에 에스크로할 수 있습니다. 이때 Apple에서는 암호 및 키체인에 포함된 다른 데이터를 읽지 못합니다. 기기를 하나만 가지고 있더라도 키체인 복구는 데이터 유실에 대한 안전망을 제공합니다. Safari를 사용해 웹 계정용으로 무작위로 강력한 암호 또는 패스키를 생성하는 경우 해당 암호는 키체인에만 기록되기 때문에 유실 방지가 특히 중요합니다.

키체인 복구의 기본은 보조 인증과 보안 에스크로 서비스로서 Apple이 키체인 복구를 위해 특별히 개발한 기술입니다. 사용자의 키체인은 강력한 암호를 사용하여 암호화되고 에스크로 서비스는 일련의 엄격한 조건이 충족될 때에만 키체인의 사본을 제공합니다.

보조 인증 사용

강력한 암호를 설정하는 몇 가지 방법은 다음과 같습니다.

- 이중 인증이 사용자의 계정에 활성화되어 있는 경우 기기 암호는 에스크로된 키체인을 복구하는 데 사용됩니다.
- 이중 인증이 설정되어 있지 않으면 사용자는 6자리 암호로 iCloud 보안 코드를 생성하도록 요청받습니다. 사용자는 이중 인증 대신 자신만의 긴 코드를 지정하거나 기기에서 암호화된 무작위 코드를 생성하여 자체적으로 기록하고 유지하도록 할 수도 있습니다.

키체인 에스크로 프로세스

암호가 설정되면 키체인이 Apple로 에스크로됩니다. iOS, iPadOS 또는 macOS 기기는 먼저 사용자의 키체인 사본을 내보내서 비대칭 keybag으로 키를 래핑하도록 암호화하여 사용자의 iCloud 키 값 저장 공간 영역에 배치합니다. Keybag은 사용자의 iCloud 보안 코드와 에스크로 레코드를 저장하는 HSM(하드웨어 보안 모듈) 클러스터의 공개 키로 래핑됩니다. 이는 사용자의 **iCloud 에스크로 레코드**가 됩니다. 이중 인증 계정의 경우 키체인은 CloudKit에도 저장되며 iCloud 에스크로 레코드의 콘텐츠로만 복구할 수 있는 중간 키로 래핑되어 동일한 수준의 보호를 제공합니다.

에스크로 레코드의 콘텐츠는 복구 기기도 iCloud 키체인에 재합류할 수 있게 허용하며 모든 기존 기기에 복구 기기가 성공적으로 에스크로 프로세스를 수행했으며 계정 소유자에게 승인받았음을 증명합니다.

참고: 사용자는 보안 코드를 설정하는 것 외에도 iCloud 계정의 전화번호를 등록해야 합니다. 이는 키 체인 복구 도중 2차 인증 단계를 제공합니다. 사용자는 SMS 메시지를 받게 되고 복구 진행을 위해 메시지에 회신해야 합니다.

iCloud 키체인용 에스크로 보안

iCloud는 인증된 사용자와 기기만 복구를 수행할 수 있도록 키체인 에스크로에 대한 보안 인프라를 제공합니다. 순서적으로 iCloud 뒤에 위치한 HSM(하드웨어 보안 모듈) 클러스터는 에스크로 레코드를 보호합니다. 앞서 설명한 대로 각각의 클러스터는 관리 하에 에스크로 레코드를 암호화하는 데 사용되는 키를 가지고 있습니다.

키체인을 복구하려면 사용자는 iCloud 계정과 암호로 인증하고 등록된 전화번호로 전송된 SMS에 응답해야 합니다. 완료되면 사용자는 iCloud 보안 코드를 입력해야 합니다. HSM 클러스터는 SRP(Secure Remote Password) 프로토콜을 사용하여 사용자가 iCloud 보안 코드를 아는지 확인합니다. 코드 자체는 Apple에 전송되지 않습니다. 아래 설명처럼 클러스터의 구성원은 사용자가 레코드 가져오기에 허용된 최대 시도 횟수를 초과하지 않았는지 개별적으로 확인합니다. 구성원 과반수가 동의하는 경우 클러스터는 에스크로 레코드의 래핑을 해제하여 사용자의 기기로 전송합니다.

그런 다음, 기기는 에스크로된 데이터를 사용하여 사용자의 키체인을 암호화하는 데 사용한 임의 키의 래핑을 해제합니다. 이 키를 사용하면 CloudKit 및 iCloud 키 값 저장 공간에서 검색된 키체인이 암호화 해제되어 기기에 복원됩니다. 에스크로 서비스는 에스크로 레코드 인증 및 검색 시도를 10번까지만 허용합니다. 여러 번 실패한 후에는 레코드가 잠기므로 추가 시도를 승인받으려면 사용자는 Apple 지원에 문의해야 합니다. 10번 실패하는 경우 HSM 클러스터가 에스크로 레코드를 파기하여 키체인이 영원히 유실됩니다. 이를 통해 키체인 데이터를 희생하지만 무작위 대입 공격으로 레코드를 가져오려는 시도를 방지합니다.

이러한 정책은 HSM 펌웨어에 구현되어 있습니다. 펌웨어의 변경을 허용하는 관리 접근 카드는 파기되었습니다. 펌웨어를 변경하거나 개인 키에 접근하기 위한 시도가 있는 경우 HSM 클러스터는 개인 키를 삭제합니다. 이렇게 되면 클러스터로 보호된 각 키체인의 소유자는 해당 에스크로 레코드가 유실되었음을 알리는 메시지를 받게 됩니다. 그리고 나서 다시 등록하도록 선택할 수 있습니다.

Apple Pay

Apple Pay 보안 개요

사용자는 Apple Pay를 지원하는 iPhone, iPad, Mac 및 Apple Watch 기기로 매장, 앱, Safari의 웹에서 개인정보를 공개하지 않고도 간편하고 안전하게 결제할 수 있습니다. 사용자는 Apple Pay가 활성화된 교통 카드, 학생 ID 카드 및 접근 카드를 Apple 지갑에 추가할 수도 있습니다. 하드웨어 및 소프트웨어에 통합된 보안성을 제공하며 사용이 쉽습니다.

Apple Pay는 또한 사용자 개인정보를 보호할 수 있도록 디자인되었습니다. Apple Pay는 사용자와 관련이 있을 수 있는 거래 내역 정보를 수집하지 않습니다. 결제 거래는 사용자, 판매처 및 카드 발급처 간에 이루어집니다.

Apple Pay 구성요소 보안

Apple Pay는 몇 가지 하드웨어 및 소프트웨어 기능을 사용하여 안전하고 신뢰할 수 있는 결제 방식을 제공합니다.

Secure Element

Secure Element는 업계 표준의 Java Card 플랫폼을 사용하는 인증된 칩으로서 전자 결제에 대한 금융 업계의 요구 사항을 준수합니다. Secure Element IC 및 Java 카드 플랫폼은 EMVCo 보안 평가 프로세스에 따라 인증됩니다. 보안 평가가 성공적으로 완료되면 EMVCo는 고유 IC 및 플랫폼 인증서를 발급합니다.

Secure Element IC는 CC 표준에 따라 인증을 받아 왔습니다.

NFC 컨트롤러

NFC 컨트롤러는 근거리 무선 통신 프로토콜을 처리하며 응용 프로그램 프로세서와 Secure Element 간의 통신 및 Secure Element와 POS 단말기 간의 통신을 전달합니다.

Apple 지갑

Apple 지갑은 신용 카드, 체크 카드 및 매장 카드를 추가하고 관리하며 Apple Pay를 사용하여 결제를 진행할 수 있습니다. 사용자는 Apple 지갑에서 사용자의 카드를 볼 수 있으며 카드 발급처에서 제공하는 경우 발급처의 개인정보 처리방침, 최근 거래 내역 등의 자세한 정보를 볼 수 있습니다. 사용자는 다음에서 Apple Pay에 카드를 추가할 수 있습니다.

- iOS 및 iPadOS의 설정 지원 및 설정 앱
- Apple Watch를 위한 Watch 앱
- Touch ID를 지원하는 Mac 컴퓨터의 시스템 설정(macOS 13 이상) 또는 시스템 환경설정(macOS 12 이하)의 지갑 및 Apple Pay

또한, 사용자는 Apple 지갑을 통해 교통 카드, 적립 카드, 탑승권, 티켓, 기프트 카드, 학생 ID 카드 및 접근 카드 등을 추가하고 관리할 수 있습니다.

Secure Enclave

iPhone, iPad, Apple Watch, Touch ID가 탑재된 Mac 컴퓨터 및 Touch ID가 탑재된 Magic Keyboard를 사용하는 Apple Silicon이 탑재된 Mac 컴퓨터에서 Secure Enclave은 인증 프로세스를 관리하고 결제 거래 진행을 허용합니다.

Apple Watch에서는 기기가 잠금 해제되어야 하며 사용자가 측면 버튼을 이중 클릭해야 합니다. 이중 클릭이 인식되면 응용 프로그램 프로세서를 통하지 않고 Secure Element 또는 Secure Enclave(사용 가능한 경우)로 바로 전달됩니다.

Apple Pay 서버

Apple Pay 서버는 Apple 지갑에 저장된 신용 카드, 체크 카드, 교통 카드, 학생 ID 카드 및 접근 카드의 설정 및 권한 설정을 관리합니다. 또한 서버는 Secure Element에 저장된 기기 계정 번호도 관리합니다. Apple Pay 서버는 기기 및 결제 네트워크 또는 카드 발급처 서버 모두와 통신합니다. Apple Pay 서버는 또한 앱 내 또는 웹상 결제의 결제 승인서를 다시 암호화합니다.

Apple Pay가 사용자의 구매 내역을 보호하는 방법

Secure Element

Secure Element는 Apple Pay를 관리하기 위해 특별히 디자인된 애플릿을 호스트합니다. 또한 결제 네트워크 또는 카드 발급처가 인증한 애플릿을 포함합니다. 결제 네트워크 또는 카드 발급처는 키를 사용하여 신용 카드, 체크 카드 또는 선불 카드 데이터를 암호화하고 애플릿으로 전송합니다. 이 키는 결제 네트워크나 카드 발급처 그리고 애플릿의 보안 도메인에서만 알고 있습니다. 이 카드 데이터는 애플릿 안에 저장되며 Secure Element의 보안 기능을 사용하여 보호됩니다. 거래 중에는 단말기가 전용 하드웨어 버스의 NFC 컨트롤러를 통해 Secure Element와 직접 통신합니다.

NFC 컨트롤러

Secure Element의 게이트웨이인 NFC 컨트롤러는 모든 비접촉식 결제 거래가 기기와 가까운 거리에 있는 POS 단말기를 통해 진행되도록 합니다. NFC 컨트롤러는 범위 내의 단말기가 보내는 결제 요청만을 비접촉식 거래로 인식합니다.

신용 카드, 체크 카드 또는 선불 카드(매장 카드 포함) 소지자가 Face ID, Touch ID 또는 암호를 사용하여 결제를 승인하거나 잠금 해제된 Apple Watch에서 측면 버튼을 이중 클릭하여 결제를 승인하면 Secure Element의 결제 애플릿이 준비한 비접촉식 응답이 컨트롤러에 의해 NFC 필드로 단독 전달됩니다. 그 결과 비접촉식 결제 거래의 결제 승인 세부 사항은 로컬 NFC 필드에 포함되어 응용 프로그램 프로세서에 절대 노출되지 않습니다. 그에 반해서 앱 내 결제 및 웹상 결제의 결제 승인 세부 사항은 Apple Pay 서버의 Secure Element가 암호화를 먼저 진행하고 나서 응용 프로그램 프로세서에 전달됩니다.

신용 카드, 체크 카드 및 선불 카드

카드 권한 설정 보안 개요

사용자가 Apple 지갑에 신용 카드, 체크 카드 또는 선불 카드를 추가하는 경우(매장 카드 포함) Apple은 카드 발급처나 카드 발급처의 공인 서비스 제공업체(주로 결제 네트워크)에 카드 정보를 사용자 계정 및 기기와 같은 기타 정보와 함께 안전하게 전송합니다. 카드 발급처(또는 서비스 제공업체)는 이 정보를 사용하여 Apple 지갑에 카드를 추가할 수 있는지를 판단합니다. Apple Pay에서는 카드 권한 설정 프로세스의 하나로서 다음 세 번의 서버측 요청을 사용해 카드 발급처 또는 결제 네트워크와 통신을 주고받습니다.

- 필수 입력 필드
- 카드 확인
- 링크 및 권한 설정

카드 발급처 또는 결제 네트워크는 이러한 요청을 사용해 카드 발급처가 Apple 지갑에 카드를 추가하거나 카드를 확인 및 승인할 수 있게 만듭니다. 이러한 클라이언트-서버 세션은 TLS 1.2를 사용하여 데이터를 전송합니다.

전체 카드 번호는 기기 또는 Apple Pay 서버에 저장되지 않습니다. 대신에 고유 기기 계정 번호가 생성되어 암호화되며 Secure Element에 저장됩니다. 이 고유 기기 계정 번호는 Apple이 접근할 수 없는 방식으로 암호화되어 있습니다. 기기 계정 번호는 기기마다 고유하고 대부분의 신용 카드 또는 체크 카드 번호와는 달라 카드 발급처 또는 결제 네트워크에서는 마그네틱 카드, 전화 통화 또는 웹 사이트에서의 사용을 금지할 수 있습니다. Secure Element의 기기 계정 번호는 절대 Apple Pay 서버에 보관되거나 iCloud에 백업되지 않으며, iOS, iPadOS, watchOS 기기 및 Touch ID를 지원하는 Mac 컴퓨터, Touch ID가 탑재된 Magic Keyboard를 사용하는 Apple Silicon이 탑재된 Mac 컴퓨터에서 격리됩니다.

Apple Watch에서 사용하는 카드는 iPhone의 Apple Watch 앱을 통해 또는 카드 발급처의 iPhone 앱 내에서 Apple Pay 권한이 설정됩니다. Apple Watch에 카드를 추가하려면 시계가 Bluetooth 통신 범위 내에 있어야 합니다. Apple Watch에서 사용하기 위해 특별히 등록된 카드는 고유 기기 계정 번호를 가지게 됩니다. 기기 계정 번호는 Apple Watch의 Secure Element 내에 저장됩니다.

신용 카드, 체크 카드 또는 선불 카드(매장 카드 포함)가 추가되면 동일한 iCloud 계정으로 로그인된 기기에서 설정 지원을 사용할 때 카드 목록에 해당 카드가 나타납니다. 이 카드는 한 기기에서만 활성화되어 있어도 이 목록에 계속 유지됩니다. 카드가 사용자의 모든 기기에서 제거된 지 7일이 지나면 이 목록에서 제거됩니다. 이 기능은 각각의 iCloud 계정에서 이중 인증이 활성화되어 있어야 합니다.

Apple Pay에 신용 카드 또는 체크 카드 추가하기

Apple 기기에서 Apple Pay에 신용 카드를 수동으로 추가할 수 있습니다.

신용 카드 또는 체크 카드를 수동으로 추가하기

카드를 수동으로 추가하기 위해 이름, 카드 번호, 만료일 및 CVV를 사용하여 권한 설정 프로세스를 진행할 수 있습니다. 설정, Apple 지갑 또는 Apple Watch 앱에서 사용자가 기기에 있는 카메라로 캡처해 정보를 입력할 수 있습니다. 카메라가 카드 정보를 캡처하면 Apple은 이름, 카드 번호 및 만료일 정보를 채웁니다. 카드 사진은 절대 기기 또는 사진 보관함에 저장되지 않습니다. 모든 필드가 작성되면 카드 확인 프로세스를 통해 CVV를 제외한 필드를 확인합니다. 그런 다음 정보는 암호화되어 Apple Pay 서버로 전송됩니다.

카드 확인 프로세스에서 사용 약관 ID를 반환하면 Apple은 카드 발급처의 사용 약관을 다운로드하여 사용자에게 표시합니다. 사용자가 발급처의 사용 약관에 동의하면 Apple은 링크 및 권한 설정 프로세스에 CVV 정보와 함께 동의한 약관의 ID를 전송합니다. 추가적으로 링크 및 권한 설정 프로세스의 일환으로 Apple은 기기의 정보를 카드 발급처 또는 네트워크에 공유합니다. 공유되는 정보에는 (a) iTunes 및 App Store 계정 활동(예: iTunes에서 오래된 거래 내역 존재 여부), (b) 사용자의 기기(예: 기기의 전화번호, 이름 및 모델 그리고 Apple Pay 설정을 위해 연결되어 있는 Apple 기기 정보), (c) 카드를 추가했을 때 사용자의 대략적인 위치(위치 서비스를 활성화한 경우)가 포함되어 있습니다. 카드 발급처는 이 정보를 사용하여 Apple Pay에 카드를 추가할 수 있는지를 판단합니다.

링크 및 권한 설정 프로세스가 완료되면 다음 두 가지 작업이 진행됩니다.

- 기기가 신용 카드 및 체크 카드를 표시하는 Apple 지갑 패스 파일 다운로드를 시작합니다.
- 기기가 카드를 Secure Element로 바인딩합니다.

패스 파일에는 카드 사진을 다운로드할 수 있는 URL, 연락처 정보, 관련 카드 발급처의 앱 및 지원 기능과 같은 카드에 대한 메타데이터가 포함됩니다. 또한 Secure Element 개인 맞춤화 완료 여부, 카드가 발급처에 의해 정지되었는지의 여부 또는 해당 카드로 Apple Pay를 통해 결제하기 전에 추가 확인이 필요한지 여부 등의 정보를 포함하는 패스 상태도 포함합니다.

iTunes Store 계정에 저장된 신용 카드 또는 체크 카드 추가하기

iTunes에 저장된 신용 카드 또는 체크 카드를 사용하려면 사용자는 Apple ID 암호를 다시 입력하도록 요청받을 수 있습니다. 그리고 카드 번호를 iTunes에서 가져오게 되며 카드 확인 프로세스가 시작됩니다. 카드가 Apple Pay에서 사용하기에 적합하다면 기기는 카드 발급처의 사용 약관을 다운로드하고 사용자에게 표시한 다음, 약관 ID와 카드 보안 코드를 링크 및 권한 설정 프로세스로 전송합니다. iTunes 계정에 저장된 카드는 추가 확인이 이루어질 수 있습니다.

카드 발급처의 앱을 사용해 신용 카드 또는 체크 카드 추가하기

앱에서 Apple Pay 사용이 가능한 경우 앱과 카드 발급처의 서버에 대해 키가 설정됩니다. 이 키는 카드 발급처에 전송되는 카드 정보를 암호화하는 데 사용됩니다. 이는 Apple 기기에서 해당 정보를 읽지 못하도록 방지하기 위한 설계입니다. 이러한 권한 설정 작업 흐름은 이전에 설명한 수동으로 카드를 추가하는 경우와 비슷하지만 일회용 암호가 CVV 대신에 사용된다는 점이 다릅니다.

카드 발급처의 웹 사이트에서 신용 카드 또는 체크 카드 추가하기

일부 카드 발급처는 Apple 지갑을 위해 웹 사이트에서 직접 카드 권한 설정 절차를 시작할 수 있는 기능을 제공합니다. 이 경우 사용자는 권한을 설정하려는 카드를 카드 발급처의 웹 사이트에서 선택하면서 작업을 시작합니다. 그 다음 사용자는 독립적인 Apple 로그인 환경(Apple의 도메인 내부에 포함)으로 안내되고 Apple ID로 로그인하라는 요청을 받습니다. 성공적으로 로그인 한 다음 사용자는 카드의 권한을 설정할 기기를 한 개 이상 선택하고 권한 설정 결과를 각 대상 기기에서 확인해야 합니다.

추가 확인하기

카드 발급처는 신용 카드 또는 체크 카드가 추가 확인이 필요한지 여부를 결정할 수 있습니다. 카드 발급처가 제공하는 방법에 따라 사용자는 추가 확인 방법을 선택할 수 있습니다. 예를 들어 문자 메시지, 이메일, 고객 서비스 전화, 또는 승인된 타사 앱을 통한 확인 방법이 있습니다. 문자 메시지나 이메일의 경우 사용자는 카드 발급처가 이미 가지고 있는 연락처 정보에서 선택할 수 있습니다. Apple 지갑, 설정 또는 Apple Watch 앱에 입력해야 하는 코드가 전송됩니다. 고객 서비스 전화 또는 앱을 사용한 확인 방법은 카드 발급처에서 직접 프로세스를 진행합니다.

Apple Pay와 결제 승인

Secure Enclave가 있는 기기에서는 Secure Enclave에서 인증된 경우에만 결제를 허용합니다. 이는 Touch ID를 지원하는 iPhone, iPad 또는 Mac(또는 Touch ID를 지원하는 Magic Keyboard와 페어링됨)에서 사용자가 생체 인증 또는 기기 암호를 사용하여 인증했는지 확인하는 작업이 포함됩니다. 가능한 경우 생체 인증이 기본 방식이지만 언제든지 암호를 사용할 수 있으며, 지문 인식 시도가 세 번 실패하거나 얼굴 인식 시도가 두 번 실패하면(iPhone 및 iPad의 경우) 자동으로 요청됩니다. 다섯 번 실패한 경우에는 암호를 요구합니다. 또한, 생체 인증을 구성하지 않았거나 Apple Pay에 대해 켜지 않은 경우에도 암호를 요구합니다. Apple Watch에서는 암호를 입력해 기기를 잠금 해제한 다음 측면 버튼을 이중 클릭하여 결제를 허용해야 합니다.

공유 페어링 키 사용

Secure Enclave 및 Secure Element는 AES 기반의 암호화 및 인증을 사용하고 암호화 재전송 방지 값을 사용하여 재전송 공격으로부터 보호하는 직렬 인터페이스를 통해 통신합니다. 양측이 직접 연결되어 있지는 않지만 제조 중에 권한이 설정된 공유 페어링 키를 사용하여 안전하게 통신합니다. 해당 과정 중에, Secure Enclave는 UID키 및 Secure Element의 고유 식별자에서 페어링 키를 생성합니다. 그런 다음 제조 과정에서 하드웨어 보안 모듈(HSM)로 페어링 키를 안전하게 전송합니다. 그 후 HSM은 페어링 키를 Secure Element에 삽입합니다.

보안 거래 허용

사용자가 Secure Enclave에 직접 통신하는 물리적 제스처를 포함하여 거래를 승인하는 경우 Secure Enclave는 인증 유형에 대해 서명된 데이터와 거래 유형에 대한 세부 사항(비접촉식 또는 앱 내 결제)을 권한 무작위(AR: Authorization Random) 값과 연관된 Secure Element로 전송합니다. 사용자가 처음으로 신용 카드 권한을 설정할 때 Secure Enclave에서 AR 값을 생성하며, 그 값은 Apple Pay가 활성화되어 있는 동안 유지됩니다. 이는 Secure Enclave의 암호화 및 안티 롤백 메커니즘으로 보호됩니다. 또한, 페어링 키를 활용하여 Secure Element로 안전하게 전송됩니다. 새로운 AR 값을 받게 되는 경우, Secure Element는 이전에 추가한 카드를 제거됨으로 표시합니다.

동적 보안용 결제 암호문 사용

결제 애플릿에서 생성된 결제 거래는 결제 암호문과 기기 계정 번호를 포함합니다. 일회용 코드인 이 암호문은 거래 카운터와 키를 사용해 계산됩니다. 거래 카운터는 새로운 거래마다 증가하는 값입니다. 키는 개인 맞춤화 중에 결제 애플릿에서 권한이 설정되어 결제 네트워크, 카드 발급처 또는 둘 다에서 알고 있는 값입니다. 결제 방법에 따라 다음을 포함하여 다른 데이터도 계산하는 데 사용될 수 있습니다.

- NFC 거래용 터미널 예측 불가 번호
- 앱 내 거래용 Apple Pay 서버 재전송 방지 값
- 카드 소지자 확인 방법(CVM) 정보 등 사용자 인증 결과

이러한 보안 코드는 결제 네트워크 및 카드 발급처에 제공되어 거래를 확인하는 데 도움을 줍니다. 보안 코드의 길이는 거래 유형에 따라 다를 수 있습니다.

Apple Pay를 사용하여 카드로 결제하기

Apple Pay를 사용하여 매장, 앱 및 웹 사이트에서 구입한 항목을 결제할 수 있습니다.

매장에서 카드로 결제하기

iPhone 또는 Apple Watch가 켜져 있고 NFC 필드를 인식하는 경우 요청된 카드(해당 카드에 자동 선택이 켜져 있는 경우) 또는 설정 앱에서 관리되는 기본 카드가 사용자에게 제시됩니다. 사용자는 또한 Apple 지갑으로 이동해 카드를 선택할 수 있고 기기가 잠겨 있는 경우 다음 방법으로 선택할 수 있습니다.

- Face ID가 있는 기기에서 측면 버튼 이중 클릭
- Touch ID가 있는 기기에서 홈 버튼 이중 클릭
- 잠금 화면에서 Apple Pay를 허용하는 손쉬운 사용 기능 사용하기

그런 다음, 정보를 전달하기 전에 사용자는 Face ID, Touch ID 또는 암호를 사용하여 인증해야 합니다. Apple Watch가 잠금 해제된 경우 측면 버튼을 이중 클릭하면 결제용 기본 카드가 활성화됩니다. 사용자가 승인하지 않으면 결제 정보가 전송되지 않습니다.

사용자가 승인한 후 기기 계정 번호 및 특정 거래 동적 보안 코드를 사용하여 결제가 진행됩니다. Apple 또는 사용자의 기기는 신용 카드 및 체크 카드의 전체 번호를 거래처에 보내지 않습니다. Apple은 거래가 이루어진 대략적인 시간 및 장소와 같은 거래 정보를 익명으로 받을 수 있으며 이를 통해 Apple Pay 및 다른 Apple 제품과 서비스를 향상합니다.

앱에서 카드로 결제하기

iOS, iPadOS, macOS 및 watchOS 앱에서 결제할 때도 Apple Pay를 사용할 수 있습니다. 사용자가 앱 내에서 Apple Pay를 사용해 결제하면 Apple은 개발자 또는 거래처에게 보낼 암호화된 거래 정보를 받습니다. 해당 정보를 개발사 또는 거래처에 보내기 전에 개발사 특정 키로 그 정보를 다시 암호화합니다. Apple Pay는 추정 결제 금액과 같은 거래 정보를 익명으로 유지합니다. 이러한 정보를 통해서는 사용자의 신원을 확인할 수 없으며 사용자의 구매 항목에 대한 정보는 절대 포함되지 않습니다.

앱이 Apple Pay 결제 거래를 개시하면 거래처보다 먼저 Apple Pay 서버가 기기로부터 암호화된 거래 정보를 받습니다. 그리고 Apple Pay는 해당 거래 정보를 거래처 특정 키로 다시 암호화하고 거래처에 거래 정보를 릴레이합니다.

앱에서 결제를 요청하는 경우 API를 호출하여 기기가 Apple Pay를 지원하는지, 그리고 거래처에서 승인하는 결제 네트워크에서 사용할 수 있는 신용 카드 또는 체크 카드를 사용자가 가지고 있는지를 판단합니다. 그리고 앱에서 청구 주소, 배송 주소 및 연락처 등의 거래를 진행하고 완료하기 위한 모든 정보를 요청합니다. 그런 다음 앱은 iOS, iPadOS, macOS 또는 watchOS에 Apple Pay 시트를 요청하여 사용해야 하는 카드 등 필요한 정보를 요청합니다.

이 단계에서 앱은 시/도, 우편번호 정보를 받아 최종 배송비를 계산합니다. 하지만 사용자가 Face ID, Touch ID 또는 기기 암호로 결제를 승인하기 전에는 요청한 모든 정보가 제공되지 않습니다. 결제가 승인된 후 Apple Pay 시트에 표시된 정보는 거래처에 전송됩니다.

앱 클립에서 카드로 결제하기

앱 클립은 사용자가 전체 앱을 다운로드하지 않고도 자전거 대여나 주차 요금 결제와 같은 작업을 빠르게 수행할 수 있도록 하는 앱의 일부분입니다. 앱 클립이 결제를 지원하는 경우, 사용자는 'Apple로 로그인'을 사용한 다음 Apple Pay로 결제할 수 있습니다. 앱 클립 내에서 결제하는 경우, 모든 보안 및 개인정보 보호 조치는 사용자가 앱 내에서 결제할 때와 동일합니다.

앱 결제를 사용자가 인증하고 거래처가 확인하는 방법

사용자 및 거래처는 Apple 서버, Secure Element, 기기 및 앱의 API에 정보를 전달하여 안전한 앱 결제를 보장합니다. 첫째, 사용자가 앱 결제를 인증하면 앱은 Apple Pay 서버를 호출하여 암호화 재전송 방지 값을 얻습니다. 서버는 이 값 및 다른 거래 데이터를 Secure Element로 전송하여 결제 승인서를 계산하며, 결제 승인서는 Apple 키를 통해 암호화됩니다. 그런 다음, Secure Element는 결제 자격 증명을 Apple Pay 서버로 반환하여 암호를 해독하고, 해당 재전송 방지 값을 Apple Pay 서버가 원래 보낸 재전송 방지 값에 대해 확인하고, 거래처 ID의 연결된 거래처 키로 다시 암호화할 수 있도록 합니다. 그 후 Apple 서버는 해당 결제를 기기로 반환하고, 처리를 위해 거래처 시스템으로 전달하는 API와 함께 앱 API로 다시 전달합니다. 거래처는 결제 자격 증명의 암호화를 해제하여 거래의 정확한 수취인인지 확인합니다.

API는 지원하는 거래처 ID를 명시하는 권한을 요구합니다. 앱은 또한 서명을 위해 Secure Element에 보낼 주문 번호 또는 고객 신원과 같은 추가 데이터(주문 번호 또는 고객 ID 등)를 포함시켜 거래가 다른 고객에게 넘어가지 않도록 합니다. 이 작업은 PKPaymentRequest에 applicationData를 명시할 수 있는 앱 개발자가 수행합니다. 이 데이터의 해시는 암호화된 결제 데이터에 포함되어 있습니다. 그래서 거래처는 자신의 applicationData 해시가 결제 데이터의 정보와 일치하는지를 확인해야 합니다.

웹 사이트에서 카드로 결제하기

Apple Pay는 iPhone, iPad, Apple Watch 및 Touch ID를 지원하는 Mac 컴퓨터의 웹 사이트에서 결제하는 데 사용할 수 있습니다. Mac에서 Apply Pay 결제를 시작하고 동일한 iCloud 계정을 사용하여 Apple Pay가 활성화된 iPhone이나 Apple Watch에서 결제를 완료할 수도 있습니다.

웹에서 Apple Pay를 사용하려면 웹 사이트가 Apple에 등록되어야 합니다. 도메인이 등록되면 Apple이 TLS 클라이언트 인증서를 발급한 후에만도메인 이름 검증이 수행됩니다. Apple Pay를 지원하는 웹 사이트는 HTTPS를 통해 콘텐츠를 제공해야 합니다. 웹 사이트는 결제 거래가 있을 때마다 Apple이 발행한 TLS 클라이언트 인증서를 사용하여 Apple 서버로 안전하고 고유한 거래처 세션을 얻어야 합니다. 거래처 세션 데이터는 Apple에서 서명합니다. 거래처 세션 서명이 확인되면 웹 사이트에서 사용자가 Apple Pay가 활성화된 기기를 사용하는지와 신용 카드, 체크 카드 또는 선불 카드가 기기에 활성화되어 있는지를 쿼리할 수 있습니다. 다른 세부 사항은 공유되지 않습니다. 사용자가 이러한 정보를 공유하는 것을 원하지 않는다면 iPhone, iPad 및 Mac 기기의 Safari 개인정보 보호 설정에서 Apple Pay 쿼리를 비활성화할 수 있습니다.

거래처 세션이 확인되면 사용자가 앱 내에서 결제할 때와 동일한 개인정보 보호 및 보안 방안이 사용됩니다.

사용자가 Mac에서 iPhone이나 Apple Watch로 결제 관련 정보를 전송하려는 경우, Apple Pay Handoff는 암호화된 종단간 Apple IDS(Identity Service) 프로토콜을 사용하여 결제 관련 정보를 사용자의 Mac에서 인증을 시도하는 기기로 전송합니다. Mac의 IDS 클라이언트는 사용자의 기기 키를 사용하여 암호화를 수행하기 때문에, 다른 기기에서는 이 정보의 암호화를 해제할 수 없으며 해당 키는 Apple에 공유되지 않습니다. Apple Pay Handoff 기기를 발견하는 절차는 일부 메타데이터와 함께 사용자 신용 카드의 유형과 고유 식별자 확인을 포함합니다. 사용자 카드의 기기 계정 번호는 공유되지 않으며 사용자의 iPhone 또는 Apple Watch에 계속 안전하게 보관됩니다. Apple은 또한 사용자가 최근에 사용한 연락처, 배송 및 청구 주소를 iCloud 키체인을 통해 안전하게 전송합니다.

사용자가 Face ID, Touch ID 또는 암호를 사용하거나 Apple Watch의 측면 버튼을 이중 클릭하여 결제를 승인하면 웹 사이트 거래처별 인증서에 맞추어 암호화된 결제 토큰이 사용자의 iPhone이나 Apple Watch에서 Mac으로 안전하게 전송된 다음 거래처 웹 사이트로 전달됩니다.

기기는 가까운 거리에 있어야 결제를 요청하고 완료할 수 있습니다. BLE(Bluetooth Low Energy) 알림을 통해 거리를 확인합니다.

자동 결제 및 거래처 토큰

iOS 16 이상에서 Apple Pay를 제공하는 앱 및 웹 사이트는 사용자의 모든 기기에서 안전한 결제를 일관적으로 허용하는 Apple Pay 거래처 토큰을 사용할 수 있습니다. 또한 iOS 16의 업데이트된 Apple Pay 결제 시트는 사전 승인된 결제 환경을 최적화합니다. Apple Pay API의 새로운 결제 유형을 사용하는 앱 및 웹 사이트 개발자들은 구독, 정기 결제, 할부 결제 및 카드 잔액 자동 충전의 결제 시트 환경을 미세 조정할 수 있습니다.

거래처 토큰은 기기별로 제한되기 않기 때문에 사용자가 기기에서 결제 카드를 제거해도 정기 결제를 계속할 수 있습니다.

여러 거래처와 결제하기

iOS 16 이상에서 단일 Apple Pay 결제 시트 내에서 여러 거래처의 결제 금액을 지정할 수 있는 기능이 Apple Pay에 추가되었습니다. 이 기능을 사용하면 고객들이 항공, 렌터카, 호텔이 포함된 여행 패키지 등의 번들을 구매한 다음 개별 거래처에게 결제 금액을 유연하게 보낼 수 있습니다.

Apple Pay의 비접촉식 패스

Apple은 Apple VAS(부가 가치 서비스) 프로토콜을 사용하여 지원되는 패스에서 호환되는 NFC 단말기로 데이터를 전송합니다. VAS 프로토콜은 비접촉식 단말기 또는 iPhone 앱에 구현할 수 있으며 NFC를 사용하여 지원되는 Apple 기기와 통신합니다. VAS 프로토콜은 짧은 거리에서 동작하며 비접촉식 패스를 개별적으로 제시하는데 사용되거나 Apple Pay 거래의 일부로 사용될 수 있습니다.

NFC 단말기 가까이 기기를 가져가면 해당 단말기는 패스 요청을 전송하여 패스 정보를 수신합니다. 만약 사용자가 패스 공급자의 식별자가 있는 카드를 가지고 있는 경우 Face ID, Touch ID 또는 암호를 사용하여 인증할 것을 요청받습니다. 패스 정보, 타임스탬프 및 일회용 무작위 ECDH P-256 키가 패스 공급자의 공개 키와 함께 사용되어 단말기로 전송되는 패스 데이터의 암호화 키를 파생합니다.

iOS 12.0.1에서 iOS 13까지는 거래처의 NFC 단말기에 패스를 가져가기 전에 사용자가 수동으로 패스를 선택할 수 있습니다. iOS 13.1 이상에서는 패스 공급자가 수동으로 패스를 선택하여 사용자 인증을 요구하거나 인증 없이 사용할 수 있습니다.

Apple Pay로 카드 사용 불가능 상태

Secure Element에 추가된 신용 카드, 체크 카드 및 선불 카드는 카드를 추가한 때와 동일한 페어링 키와 AR(Authorization Random) 값을 사용하여 Secure Element가 승인된 경우에만 사용할 수 있습니다. 새로운 AR 값을 받게 되는 경우, Secure Element는 이전에 추가한 카드를 제거됨으로 표시합니다. 이렇게 하면 다음과 같은 시나리오에서 운영 체제가 Secure Enclave의 AR 복사본을 유효하지 않은 것으로 표시하여 Secure Enclave에 카드 사용이 불가능하다고 전달합니다.

방식	기기
암호가 비활성화됨	iPhone, iPad, Apple Watch
암호가 비활성화됨	Mac
사용자가 iCloud에서 로그아웃	iPhone, iPad, Mac, Apple Watch
사용자가 모든 콘텐츠 및 설정 지우기를 선택	iPhone, iPad, Mac, Apple Watch
기기가 복구 모드에서 복원됨	iPhone, iPad, Mac, Apple Watch
페어링 해제	Apple Watch

카드 정지, 제거 및 삭제하기

사용자는 나의 찾기를 사용해 기기를 분실 모드로 설정하여 iPhone, iPad 및 Apple Watch에서 Apple Pay 사용을 정지시킬 수 있습니다. 사용자는 또한 나의 찾기를 사용하거나 iCloud.com을 방문하거나 Apple 지갑을 사용해 기기에서 직접 Apple Pay의 카드를 제거 및 삭제할 수 있습니다. 카드는 Apple Watch에서 직접 제거하거나 iCloud 설정 또는 iPhone의 Apple Watch 앱에서 제거할 수 있습니다. 기기가 셀룰러 또는 Wi-Fi 네트워크에 연결되어 있지 않은 오프라인 상태에서도 카드 발급처 또는 관련 결제 네트워크에서는 기기에 저장된 카드를 사용하여 결제하는 기능을 Apple Pay에서 정지시키거나 제거할 수 있습니다. 사용자는 또한 카드 발급처에 연락하여 Apple Pay의 카드를 정지하거나 지울 수 있습니다.

사용자가 기기 전체를 지우는 경우(모든 콘텐츠 및 설정 지우기 또는 나의 찾기를 사용하거나 기기를 복원) iPhone, iPad, Mac 및 Apple Watch는 Secure Element로 명령을 보내 모든 카드를 제거된 것으로 표시합니다. 삭제됨으로 표시하면 카드는 즉시 사용 불가능 상태로 변경되고, Apple Pay 서버에 연결되면 Secure Element에서 카드가 완전히 삭제됩니다. Secure Enclave는 별도로 AR을 유효하지 않음으로 표시하여 이미 등록한 카드에 대한 결제 승인을 불가능하게 만듭니다. 기기가 온라인 상태가 되면 기기는 Apple Pay 서버로 접근을 시도하여 Secure Element에 있는 모든 카드가 삭제된 것을 확인합니다.

Apple Card 보안

지원되는 iPhone 및 Mac 모델에서 사용자는 안전하게 Apple Card를 신청할 수 있습니다.

Apple Card 신청

iOS 12.4 이상, macOS 10.14.6 이상, watchOS 5.3 이상에서 Apple Pay와 함께 Apple Card를 사용하여 매장에서, 앱 내에서, 그리고 웹상에서 결제할 수 있습니다.

Apple Card를 신청하려면 사용자는 Apple Pay가 호환되는 iPhone 또는 iPad에서 iCloud 계정으로 로그인해야 하며, iCloud 계정에 이중 인증을 설정해 두어야 합니다. 또는 Apple ID로 로그인한 후에 apply.applecard.apple에서 신청할 수 있습니다. 신청이 승인되면, 적용되는 모든 기기에서 사용자의 Apple ID로 로그인하여 Apple 지갑이나 설정 > 지갑 및 Apple Pay에서 Apple Card를 사용할 수 있습니다.

사용자가 Apple Card를 신청할 때 Apple ID 공급자 파트너사가 사용자 신원 정보를 안전한 방식으로 확인한 다음, 신원 및 신용 평가를 위한 목적으로 Goldman Sachs Bank USA에 공유합니다.

신청 시 제공된 주민등록번호나 신분증 이미지는 각각의 키로 암호화되어 Apple ID 공급자 파트너사 및 Goldman Sachs Bank USA에 안전하게 전송됩니다. Apple은 이 데이터의 암호화를 해제할 수 없습니다.

신청 시 제공된 소득 정보 및 청구 금액 결제에 사용되는 은행 계좌 정보는 키로 암호화되어 Goldman Sachs Bank USA에 안전하게 전송됩니다. 은행 계좌 정보는 키체인에 저장됩니다. Apple은 이 데이터의 암호화를 해제할 수 없습니다.

Apple 지갑에 Apple Card를 추가할 때 사용자가 신용 카드 또는 체크 카드를 등록할 때의 정보와 동일한 정보가 Apple 파트너사인 Goldman Sachs Bank USA와 Apple Payments Inc.에 공유될 수 있습니다. 이 정보는 문제 해결, 사기 방지 및 규제 목적으로만 사용됩니다.

iOS 14.6 이상, iPadOS 14.6 이상 및 watchOS 7.5 이상에서 Apple Card를 소지한 iCloud 가족의 가족 대표는 13세 이상의 iCloud 가족 구성원과 카드를 공유할 수 있습니다. 초대를 확인하기 위해서는 사용자 인증이 필요합니다. Apple 지갑은 Secure Enclave 내부의 키를 사용해서 소유자와 초대받은 사용자를 바인딩하는 서명을 계산합니다. 그 서명은 Apple 서버에서 검증됩니다.

원하는 경우, 가족 대표는 구성원에 거래 제한을 설정할 수 있습니다. 구성원의 카드는 언제든 Apple 지갑을 사용하여 지출을 일시 정지하기 위해 잠길 수도 있습니다. 공동 소유자 또는 18세 이상의 구성원이 초대를 받아들이고 신청하면 Apple 지갑의 Apple Card 신청 섹션에 명시된 동일한 신청 프로세스를 진행합니다.

Apple Card 사용

Apple 지갑 앱에서 Apple Card의 실물 카드를 주문할 수 있습니다. 사용자가 실물 카드를 받은 후 실물 카드의 두 겹 봉투에 있는 NFC 태그를 사용하여 카드를 활성화할 수 있습니다. 해당 태그는 카드마다 고유하며 다른 사용자의 카드를 활성화하는 데 사용할 수 없습니다. Apple 지갑 설정에서 카드를 수동으로 활성화하는 방법도 있습니다. 또한 사용자는 Apple 지갑에서 언제든지 실물 카드를 잠그거나 잠금 해제할 수 있습니다.

Apple Card 결제 및 Apple 지갑 패스 세부 사항

Apple Card 계좌로 납부해야 하는 금액을 웹 브라우저 또는 Apple Cash 및 은행 계좌가 설정된 iOS의 Apple 지갑에서 납부할 수 있습니다. 청구 금액을 Apple Cash 및 은행 계좌로 특정 날짜에 한번에 결제하거나 반복 결제하도록 설정할 수 있습니다. 사용자가 결제할 때, Apple Cash와 유사한 암호화 재전송 방지 값을 받기 위해 Apple Pay 서버로 요청이 이루어집니다. 결제 설정 세부 사항과 함께 재전송 방지 값은 Secure Element로 전송되어 결제 서명을 계산합니다. 그 다음, 서명은 Apple Pay 서버로 반환됩니다. Apple Pay 서버의 서명과 재전송 방지 값을 통해 결제의 인증, 무결성 및 정확성이 확인되며, 이를 처리하기 위해 Goldman Sachs Bank USA로 전달됩니다.

Apple Card 번호는 Apple 지갑이 인증서를 제시하여 가져옵니다. Apple Pay 서버는 인증서가 유효한지 확인해서 Secure Enclave에서 키가 생성되었는지 확인합니다. 그 다음 이 키를 사용해서 Apple Card 번호를 암호화하고 Apple 지갑에게 반환해서 Apple Card 번호를 요청한 iPhone만 암호화 해제를 할 수 있게 합니다. 암호화 해제 이후 Apple Card 번호는 iCloud 키체인에 저장됩니다.

Apple 지갑을 사용하여 Apple Card 번호의 세부 사항을 패스에 표시하려면 Face ID, Touch ID 또는 암호를 통한 사용자 인증이 필요합니다. 사용자는 카드 정보 섹션에서 이를 변경할 수 있으며 이전 정보는 비활성화됩니다.

사기 보호(고급)

iOS 15 이상 및 iPadOS 15 이상에서 Apple Card 사용자는 Apple 지갑의 사기 방지(고급)를 활성화할 수 있습니다. 활성화되면 카드 보안 코드는 며칠에 한 번씩 새로고침됩니다.

Apple Cash 보안

iOS 11.2 이상, iPadOS 13.1 이상 및 watchOS 4.2 이상을 사용하는 경우 iPhone, iPad, Apple Watch에서 Apple Cash를 통해 다른 사용자와 돈을 보내거나 받고, 송금을 요청할 수 있습니다. 사용자가 돈을 받으면 Apple Cash 계좌에 해당 금액이 추가되며, Apply Pay를 지원하는 모든 기기에서 사용자의 Apple ID로 로그인하여 Apple 지갑이나 설정 > 지갑 및 Apple Pay에서 금액을 확인할 수 있습니다.

iOS 14, iPadOS 14 및 watchOS 7에서는 Apple Cash로 신원이 확인된 iCloud 가족의 가족 대표가 18세 미만 가족 구성원의 Apple Cash를 활성화할 수 있습니다. 가족 대표는 해당 사용자의 송금 기능을 가족 구성원 또는 연락처에 저장된 상대로만 제한하도록 선택할 수 있습니다. 18세 미만의 가족 구성원이 Apple ID 계정 복구를 진행할 경우, 가족 대표는 해당 사용자의 Apple Cash 카드를 다시 수동으로 활성화해야 합니다. 18세 미만의 가족 구성원이 iCloud 가족에서 나간 경우, Apple Cash 잔액은 가족 대표의 계좌로 자동 이체됩니다.

Apple Cash를 설정하면 신용 카드 및 체크 카드를 등록했을 때와 동일한 정보가 Apple 제휴 은행인 Green Dot Bank와 공유되고, 다른 Apple 부서에서는 알 수 없도록 따로 정보를 보관하고 처리함으로써 사용자의 개인정보를 보호하기 위해 설립된 Apple의 자회사 Apple Payments Inc.와 공유될 수 있습니다. 이 정보는 문제 해결, 사기 방지 및 규제 목적으로만 사용됩니다.

iMessage에서 Apple Cash 사용하기

개인 간 거래 및 Apple Cash를 사용하려면 사용자는 Apple Cash 호환 기기에서 iCloud 계정으로 로그인해야 하며, iCloud 계정에 이중 인증을 설정해 두어야 합니다. 메시지 앱을 사용하거나 Siri에게 요청하여 사용자 간에 송금을 요청하고 이체할 수 있습니다. 사용자가 송금을 시도할 때 iMessage는 Apple Pay 시트를 표시합니다. 항상 Apple Cash 잔액이 가장 먼저 사용됩니다. 필요한 경우 추가 금액은 사용자의 Apple 지갑에 등록된 두 번째 신용 카드 또는 체크 카드에서 가져옵니다.

매장, 앱, 웹에서 Apple Cash 사용하기

Apple 지갑의 Apple Cash 카드는 Apple Pay를 통해 매장, 앱 및 웹에서 결제 시 사용할 수 있습니다. 또한 Apple Cash 계좌에 있는 금액을 은행 계좌로 이체할 수 있습니다. 다른 사용자로부터 송금을 받을 수 있을 뿐만 아니라, Apple 지갑의 체크 카드 또는 선불 카드에서 Apple Cash 계좌로 입금할 수 있습니다.

거래가 완료되면 Apple Payments Inc.는 문제 해결, 사기 방지 및 규제 등을 위해 사용자의 거래 데이터를 보관 및 사용할 수 있습니다. 다른 Apple 부서는 사용자가 누구에게 송금을 했는지, 누구로부터 송금을 받았는지 또는 Apple Cash 카드로 어디서 구입을 진행했는지 등의 정보에 대해 알 수 없습니다.

사용자가 Apple Pay로 송금하거나, Apple Cash 계좌에 입금하거나, 은행 계좌로 이체할 때 Apple Pay 서버에 요청을 보내 암호화 재전송 방지 값을 받습니다. 이는 앱 내에서 Apple Pay에 반환한 값과 비슷한 값입니다. 재전송 방지 값은 다른 거래 데이터와 함께 Secure Element로 전송되어 결제 서명을 계산합니다. 서명은 Apple Pay 서버로 반환됩니다. Apple Pay 서버는 재전송 방지 값 및 결제 서명을 통해 거래의 인증, 무결성 및 정확성을 확인합니다. 그런 다음 송금이 실행되고 거래가 완료되었다는 알림이 나타납니다.

거래가 다음과 관련된 경우:

- Apple Cash에 금액을 추가하기 위한 체크 카드
- Apple Cash 잔액이 부족한 경우에 추가 금액 보충

암호화된 결제 승인서도 생성되어 앱 및 웹 사이트 내에서 Apple Pay가 작동하는 것과 유사한 방식으로 Apple Pay 서버에 전송됩니다.

Apple Cash 계정의 잔액이 특정 금액을 초과하거나 비정상적 활동이 감지되면 사용자에게 신원을 확인하라는 메시지가 표시됩니다. 주민등록번호 또는 질문에 답변하기(예: 예전에 살았던 곳의 도로 주소 확인)와 같이 사용자의 신원을 확인하기 위해 제공된 정보는 Apple 파트너사에 안전하게 전송되고 파트너사의 키를 통해 암호화됩니다. Apple은 이 데이터의 암호화를 해제할 수 없습니다. 사용자가 Apple ID 계정 복구를 수행하는 경우 다시 신원을 확인하도록 요청을 받게 되며, 신원을 확인한 후에야 Apple Cash 잔액에 대한 접근 권한을 되찾을 수 있습니다.

Tap to Pay on iPhone 보안

iOS 15.4 이상에서 사용 가능한 Tap to Pay on iPhone은 거래처가 iPhone 및 파트너사가 활성화한 iOS앱을 사용하여 Apple Pay 및 기타 비접촉식 결제를 승인할 수 있게 허용합니다. 이 서비스를 사용하면 지원되는 iPhone 기기 사용자는 비접촉식 결제 및 Apple Pay NFC가 활성화된 패스를 안전하게 승인할 수 있습니다. Tap to Pay on iPhone이 있으면 거래처는 비접촉식 결제를 승인하기 위해서 별도의 하드웨어가 필요하지 않습니다.

Tap to Pay on iPhone은 결제자의 개인정보를 보호할 수 있도록 설계되었습니다. 이 서비스는 결제자와 관련이 있을 수 있는 거래 내역 정보를 수집하지 않습니다. 신용/체크 카드 번호(PAN)와 같은 결제 카드 정보는 Secure Element에 의해 보호되며 거래처의 기기에 표시되지 않습니다. 결제 카드 정보는 거래처의 결제 서비스 제공자, 결제자 및 카드 발급처 간에만 공유됩니다. 또한, Tap to Pay 서비스는 결제자의 이름, 주소 또는 전화번호를 수집하지 않습니다.

Tap to Pay on iPhone은 공인받은 보안 연구소에서 외부 평가를 받고 사용 가능한 지역의 모든 결제 네트워크에서 사용할 수 있도록 승인되었습니다.

비접촉식 결제 요소 보안

- **Secure Element:** Secure Element는 비접촉식 결제 카드 데이터를 읽고 보호하는 결제 커널을 호스트합니다.
- **NFC 컨트롤러:** NFC 컨트롤러는 근거리 무선 통신 프로토콜을 처리하며 응용 프로그램 프로세서와 Secure Element 간의 통신 및 Secure Element와 비접촉식 결제 카드 간의 통신을 전달합니다.
- **Tap to Pay on iPhone 서버:** Tap to Pay on iPhone 서버는 기기의 결제 커널 설치 및 권한 설정을 관리합니다. 서버는 Tap to Pay on iPhone 기기의 보안도 결제 카드 산업 보안 표준 위원회(PCI SSC)의 Contactless Payments on COTS(CPoC) 표준과 호환되고 PCI DSS를 준수하는 방식으로 결제를 모니터링합니다.

Tap to Pay가 신용 카드, 체크 카드 및 선불 카드를 읽는 방법

Tap to Pay가 보안 권한을 설정하는 방법

충분히 권한이 있는 앱을 사용해서 처음으로 Tap to Pay on iPhone을 사용하면 Tap to Pay on iPhone 서버는 기기가 기기 모델 및 iOS 버전과 같은 자격 기준을 만족하는지 및 암호를 설정했는지 확인합니다. 인증이 완료된 후 결제 승인 애플릿은 Tap to Pay on iPhone 서버에서 다운로드되고 관련된 결제 커널 구성과 함께 Secure Element에 설치됩니다. 이 작업은 Tap to Pay on iPhone 서버와 Secure Element 간에 안전하게 수행됩니다. Secure Element는 설치 전에 데이터의 무결성 및 신뢰성을 확인합니다.

Tap to Pay가 카드를 안전하게 읽는 방법

Tap to Pay on iPhone 앱이 ProximityReader 프레임워크에서 카드 읽기를 요청하는 경우, iOS에서 제어하는 시트가 나타나고 사용자에게 결제 카드를 탭하라는 메시지를 표시합니다. 탭 화면이 활성화되어 있을 때 민감한 카드 데이터를 노출할 수 있는 센서를 읽을 수 있는 앱은 없습니다. iOS는 결제 카드 리더기를 초기화한 다음 Secure Element의 결제 커널에 카드 읽기 시작을 요청합니다.

이 시점에서 Secure Element는 읽기 모드의 NFC 컨트롤러를 제어합니다. 이 모드에서는 NFC 컨트롤러를 통해서 결제 카드와 Secure Element 간에만 카드 데이터 교환이 허용됩니다. 이 모드에서는 결제 카드 읽기만 가능합니다.

Secure Element에서 결제 승인 애플릿은 결제 카드 읽기를 완료한 뒤 카드 데이터를 암호화하고 서명합니다. 결제 카드 데이터는 결제 서비스 제공자에게 도달하기 전까지는 암호화되고 인증된 상태를 유지합니다. 앱에 의해 카드 읽기를 요청받은 결제 서비스 제공자만이 결제 카드 데이터의 암호화를 해제할 수 있습니다. 결제 서비스 제공자는 결제 카드 데이터 암호화 해제 키를 Tap to Pay on iPhone 서버로부터 요청해야 합니다. Tap to Pay on iPhone 서버는 데이터의 무결성 및 신뢰성을 확인하고 결제 카드 데이터 암호화 해제 키를 요청한 지 60초 이내에 카드 읽기가 수행되었는지 확인한 다음, 암호화 해제 키를 결제 서비스 제공자에게 보냅니다.

이 모델은 거래처를 위한 거래 내역을 처리하는 PSP를 제외한 누군가가 결제 카드 데이터를 암호화 해제할 수 없도록 돕습니다.

PIN 입력을 사용하여 거래 인증하기

iOS 16.0 이상에서 지원되는 PIN 입력은 결제자가 거래처의 기기에서 PIN을 입력하여 거래를 인증하게 해줍니다. PIN 입력 화면은 결제 카드로 교환된 정보에 기반하여, 탭한 이후 즉시 트리거될 수 있습니다. 결제 서비스 제공자는 일회성 거래에만 유효한 서명된 토큰을 제공하여 PIN 화면을 트리거할 수도 있습니다.

PIN 입력 메커니즘은 공인받은 보안 연구소에서 외부 평가를 받고 사용 가능한 지역의 모든 결제 네트워크에서 사용할 수 있도록 승인되었습니다. PIN 입력 화면은 스크린샷 및 화면 미러링으로부터 보호되며, PIN 입력 화면이 활성화되어 있는 동안 어떤 앱도 PIN 값의 일부를 제공할 수 있는 모든 센서를 읽을 수 없습니다.

입력한 PIN 숫자는 Secure Element에 의해 안전하게 캡처됩니다. Secure Element는 이러한 PIN 숫자를 사용하여 결제 업계 표준을 준수하는 암호화된 PIN 블록을 생성합니다. Apple은 추가 처리를 위해, PCI PIN을 준수하는 백엔드에서 PSP로 암호화된 PIN 블록을 안전하게 제공합니다.

PIN 값은

- 거래처가 자신의 기기에서 사용할 수 없습니다.
- 언제라도 Apple에 의해 암호화가 해제되지 않습니다.
- Apple에 의해 저장되지 않습니다.

Apple 지갑 사용하기

Apple 지갑을 사용한 접근

사용자는 지원되는 iPhone 및 Apple Watch 기기의 Apple 지갑 앱에 여러 유형의 키를 저장할 수 있습니다. 해당 키에 익스프레스 모드가 지원되고 켜져 있을 경우, 사용자가 문 앞에 도착하면 올바른 키가 자동으로 제시되어 근거리 무선 통신(NFC)를 사용하여 탭만 하면 안으로 들어갈 수도 있습니다.

사용자 편의성

익스프레스 모드

키가 Apple 지갑에 추가되면 익스프레스 모드가 기본적으로 켜집니다. 익스프레스 모드에서 키는 Face ID, Touch ID 또는 암호 인증을 제공하거나 Apple Watch의 측면 버튼을 이중 클릭할 필요 없이 지원되는 단말기와 상호 작용합니다. 이 기능을 비활성화하려면 사용자는 키를 대표하는 Apple 지갑의 카드 앞에 있는 더 보기 버튼을 탭해서 익스프레스 모드를 끌 수 있습니다. 익스프레스 모드를 다시 켜려면 사용자는 Face ID, Touch ID 또는 암호를 사용해야 합니다.

키 공유

iOS 16 이상에서 특정 키 유형은 공유할 수 있습니다.

사용자는 키 소유자의 iPhone에서 초대받은 키 수신자의 iPhone으로 보안 및 개인정보 보호가 강제 적용된 상태에서 집 또는 차 키 등의 키 접근 권한을 공유할 수 있습니다. 키는 Apple 지갑에서 키의 공유 아이콘을 탭하여 공유할 수 있으며 공유 시트에 나타나는 방법을 사용해 공유할 수도 있습니다. 또한 키 소유자는 각 공유 키의 접근 수준 및 유효 기간을 선택할 수 있습니다. 키 소유자는 공유한 모든 키를 확인할 수 있으며 최초 키 소유자가 다른 사용자에게 키를 다시 공유한 경우를 포함해 모든 공유 키의 접근 권한을 취소할 수 있습니다.

키 공유 초대는 메일상자 내의 전용 서버에 의해 익명으로 저장되고 보안이 유지되며 AES 128 또는 256 암호화 키로 보호됩니다. 암호화 키는 의도된 키 수신인을 제외한 서버 또는 다른 사람과 절대 공유되지 않으며 키 수신인만 초대를 암호화 해제할 수 있습니다. 메일상자를 생성하면 키 소유자의 iPhone은 서버에 의해 해당 메일상자에만 바인딩되는 기기 클레임을 제공합니다. 키 수신자의 iPhone은 이 메일상자에 처음 접근할 때 키 수신자 기기 클레임을 제시합니다. 유효한 기기 클레임을 제시하는 키 소유자 및 키 수신자 iPhone 기기만 해당 메일상자에 접근할 수 있습니다. 각 iPhone 기기 클레임에는 RFC4122에 따른 고유한 UUID 값이 있습니다.

추가 보안 조치로 키 소유자는 키 수신자의 iPhone에서 요구하는 무작위로 생성된 6자리 활성화 코드를 켤 수 있습니다. 코드 재시도 횟수는 키 소유자 또는 파트너 서버에 의해 강제 적용 및 검증됩니다. 이 활성 코드는 키 소유자가 키 수신자에게 전달해야 하며, 키 수신자는 키 소유자 또는 파트너 서버에서 검증을 요구할 때 해당 코드를 제시해야 합니다.

키 수신자가 초대를 수락하면 해당 초대는 즉시 수신한 iPhone에 의해 서버에서 삭제됩니다. 키 공유 초대를 포함한 메일상자에도 제한된 수명이 있으며, 이는 메일상자 생성 시 설정되고 서버에서 강제 적용합니다. 만료된 초대는 서버에서 자동으로 삭제됩니다.

기존 제조업체에 따라 키를 Apple 외 기기와도 공유할 수 있지만 해당 기기의 키 공유 보안 방법은 Apple과 다를 수 있습니다.

개인정보 보호 및 보안

Apple 지갑의 액세스 키는 iPhone 및 Apple Watch에 내장된 개인정보 보호 및 보안을 충분히 활용합니다. Apple 지갑의 키를 언제 어디서 사용하는지는 Apple과 공유되지 않고 Apple 서버에도 저장되지 않으며 자격 증명은 지원되는 기기의 Secure Element 안에 안전하게 저장됩니다. Secure Element는 특별히 설계된 애플릿을 호스트해서 액세스 키를 추출하거나 유출할 수 없게 보장하면서 안전하게 관리합니다.

켤 때 이중 인증이 필요하지 않은 학생 ID를 제외한 키의 권한을 설정하기 전에 사용자는 호환되는 iPhone으로 iCloud 계정에 로그인되어 있고 iCloud 계정을 위한 이중 인증이 켜져 있어야 합니다.

사용자가 권한 설정을 시작하면 링크 및 권한 설정과 같이 신용 및 체크 카드 권한 설정을 할 때와 비슷한 단계가 발생합니다. 거래 중에는 리더기가 구축된 보안 채널을 사용해서 NFC 컨트롤러를 통해 Secure Element와 통신합니다.

iPhone 및 Apple Watch를 포함해서 키로 권한 설정을 할 수 있는 기기의 수는 각 파트너사가 정의 및 제어하며 파트너사에 따라 다를 수 있습니다. 이 접근은 특정 요구사항을 위해서 각 파트너사가 기기 유형별로 권한이 설정된 키의 최대 수를 제어할 수 있게 허용합니다. 이 목적을 위해서 Apple은 파트너사에 기기 유형 및 익명의 기기 식별자를 제공합니다. 개인정보 보호 및 보안상의 이유로 식별자는 파트너사마다 다릅니다.

또한 파트너사는 파트너사별로 고유한 익명의 사용자 식별자를 받으며, 이를 사용하면 초기에 권한을 설정할 때 키를 사용자 iCloud 계정에 안전하게 바인딩할 수 있습니다. 이 방법은 파트너사와 생성한 사용자 계정이 침해당해(예: 탈취 공격을 당한 경우) 다른 사용자가 키를 설정하지 못하도록 보호합니다.

키는 다음에 의해 비활성화되거나 제거될 수 있습니다.

- 나의 찾기를 사용하여 원격으로 기기 지우기
- 나의 찾기에서 분실 모드 활성화
- MDM(모바일 기기 관리) 원격 지우기 명령 수신
- Apple ID 계정 페이지에서 모든 카드 제거
- iCloud.com에서 모든 카드 제거
- Apple 지갑에서 모든 카드 제거
- 발급처의 앱에서 해당 카드 제거

iOS 15.4 이상에서 이용자가 Face ID를 지원하는 iPhone의 측면 버튼을 이중 클릭하거나 Touch ID 를 지원하는 iPhone에서 홈 버튼을 이중 클릭하면 패스 및 액세스 키 세부 사항은 기기에 인증되기 전에는 표시되지 않습니다. 호텔 예약 세부 사항과 같은 패스별 정보가 Apple 지갑에 표시되기 전에 Face ID, Touch ID 또는 암호 인증이 요구됩니다.

액세스 키 유형

Apple 지갑에서 접근할 수 있는 다양한 유형에는 호텔, 기업 배지, 학생 ID, 집 키 및 차 키가 있습니다.

호텔

Apple 지갑의 호텔 객실 키는 기존 플라스틱 호텔 키 카드 외에도 개인정보 보호 및 보안 혜택을 투숙객에게 추가로 제공하면서 체크인부터 체크아웃까지 손쉬운 비접촉식 경험을 제공합니다. 지원되는 지점의 호텔 투숙객은 호환 가능한 iPhone 및 Apple Watch Series 4 및 이후 모델에서 Apple 지갑의 객실 키로 탭하여 잠금 해제할 수 있습니다.

Apple 지갑의 기능은 고객의 번거로움을 최소한으로 줄이도록 특별히 설계되었습니다.

- 숙박 전 Apple 지갑에 패스를 추가하기 위해 호텔 앱에서 미리 권한 설정
- Apple 지갑에서 체크인 및 객실 배정을 시작하기 위한 체크인 패스 타일
- 현재 숙박을 연장 및 변경하기 위한 사후 키 업데이트 권한 설정
- Apple 지갑의 단일 패스를 위한 다중 객실 키 지원
- Apple 지갑의 만료된 키 자동 아카이빙

Disney MagicMobile 패스

사용자는 iPhone 또는 Apple Watch의 Apple 지갑에 Disney MagicMobile 패스를 추가해 지원되는 Disney 테마파크에 입장할 수 있습니다. MagicMobile 패스는 파크 입장 할 때 뿐만 아니라 파크의 다른 적용 가능한 리더기에서 사용할 수 있습니다.

Disney MagicMobile 패스를 추가하려면 iCloud 계정에 이중 인증을 활성화하고, 유효한 My Disney Experience 계정과 연결된 지원되는 테마파크의 표를 구매하거나 예약해둔 상태여야 합니다. iPhone의 My Disney Experience 앱에서 사용자는 Apple 지갑에 추가할 패스를 2개 이상 선택할 수 있습니다. 사용자에게 페어링된 Apple Watch가 있는 경우, 선택한 패스는 사용자의 iPhone 및 페어링된 Apple Watch에 자동으로 설정됩니다. 익스프레스 모드는 iPhone 및 Apple Watch 기기 모두에 추가된 패스에서 자동으로 켜집니다. 사용하기 편리하도록 익스프레스 모드를 켜면 현재 기기에 추가된 모든 MagicMobile 패스에서도 켜집니다.

여러 패스를 단일 기기에 추가해 모든 모임 구성원들의 패스를 관리할 수 있습니다. 사용자들은 My Disney Experience 앱을 사용해 다른 사용자들과 패스를 공유할 수도 있습니다. 이렇게 하면 수신자가 기기의 Apple 지갑 앱에 공유 패스를 추가할 수 있습니다.

기업 배지

지원되는 파트너사의 직원 배지를 iPhone 및 Apple Watch의 Apple 지갑에 추가해서 전 세계의 직원들이 업무 공간에 비접촉식 접근을 할 수 있게 허용합니다. 배지를 추가하려면 직원은 고용주가 제공한 앱에 로그인할 때 사용하는 계정에 다중 인증을 활성화해야 합니다.

직원 배지는 Apple의 접근 기능을 이용하여 사용자가 다음을 할 수 있게 합니다.

- 파트너사의 앱 설치를 요구하지 않는 푸시 권한 설정을 통해 직원 배지를 페어링된 Apple Watch에 자동으로 추가
- 익스프레스 모드를 사용하여 사무실 편의 시설에 원활하게 접근
- iPhone 배터리가 방전된 후에도 업무 공간에 접근

학생 ID 카드

iOS 12 이상 버전을 사용하는 경우 지원되는 캠퍼스의 학생, 교수 및 직원은 자신의 ID 카드를 지원되는 iPhone 및 Apple Watch 모델의 Apple 지갑에 추가하여 해당 카드를 사용할 수 있는 모든 곳에 출입하거나 결제할 수 있습니다.

사용자는 학생 ID 카드 발급처 또는 지원 학교에서 제공하는 앱을 통해 자신의 Apple 지갑 앱에 추가할 수 있습니다. 이러한 동작에서 발생하는 기술적인 프로세스는 카드 발급처의 앱을 사용해 신용 카드 또는 체크 카드 추가하기에 설명된 내용과 동일합니다. 또한, 발급처의 앱은 사용자의 학생 ID에 대한 접근을 보호하는 이중 인증을 계정에 지원해야 합니다. 사용자의 iPhone 및 페어링된 Apple Watch에서 동시에 카드를 설정할 수 있습니다.

다가구 주택

세입자 및 지원 파트너사 시설 직원은 Apple 지갑의 홈 키를 이용해서 건물, 호 및 공용 공간에 접근할 수 있습니다. 홈 키는 파트너사가 제공한 앱에서 권한 설정할 수 있습니다. 매끄러운 구성 설정을 지원하는 파트너사의 경우, 부동산 관리자는 세입자에게 선호하는 메시지 경로(예: 이메일 또는 SMS)를 사용하여 권한 설정을 시작하기 위한 링크를 보내서 세입자가 링크만 클릭하면 키를 교환하게 할 수 있습니다. 앱 클립도 안전하고 원활한 경험을 제공하며 파트너사의 앱을 설치하지 않아도 키의 권한을 설정할 수 있게 합니다. 자세한 내용은 Apple 지원 문서 iPhone에서 앱 클립 사용하기를 참조하십시오.

다가구 주택 키도 익스프레스 모드에서 사용하고 친구 및 가족 구성원과 안전하게 공유할 수 있습니다. 자세한 내용은 키 공유를 참조하십시오.

홈 키

Apple 지갑의 홈 키는 지원되는 NFC가 활성화된 도어락에 iPhone 또는 Apple Watch를 간편하게 탭해서 사용할 수 있습니다. 사용자가 홈 키를 설정하고 사용하는 방법에 대한 자세한 내용은 Apple 지원 문서 iPhone에서 홈 키로 문 열기를 참조하십시오.

사용자가 홈 키를 설정하면 모든 가족 구성원도 자동으로 홈 키를 받습니다. 홈 키를 추가로 공유하거나 공유 홈의 구성원을 삭제하려면 홈의 소유자는 홈 앱을 사용해서 초대 및 구성원을 관리할 수 있습니다. 사용자가 홈 키가 있는 홈에 초대받기를 선택하면 사용자 기기의 Apple 지갑에 홈 키 권한 설정을 시작합니다. 사용자가 홈을 떠나기로 선택하거나 홈 소유자가 접근을 철회하는 경우에도 Apple 지갑에서 홈 키를 제거합니다.

차 키

차 키를 Apple 지갑에 디지털로 저장하는 기능은 지원되는 iPhone 기기 및 페어링된 Apple Watch 기기에서 기본적으로 사용할 수 있습니다. 차 키는 Apple 지갑에서 패스(자동차 제조업체를 대신하여 Apple에서 생성)로 나타나며 Apple Pay 카드를 사용하는 모든 과정(iCloud 분실 모드, 원격 지우기, 로컬 패스 삭제, 모든 콘텐츠 및 설정 지우기)을 지원합니다. 표준 Apple Pay 카드의 경우, 소유자의 iPhone, Apple Watch 및 차량 Human Machine Interface(HMI)에서 공유 차 키를 삭제할 수 있습니다.

차 키를 사용하면, 예를 들어 차량을 잠금 해제하거나 잠그고, 트렁크를 여닫고, 알람을 켜거나 끄고, 엔진을 시동하거나 차량을 운전 모드로 설정할 수 있습니다. '표준 트랜잭션'은 공동 인증을 제공하며 엔진 시동 기능을 사용하려면 필요한 트랜잭션입니다. 잠금 해제 및 잠금 트랜잭션은 성능을 이유로 필요한 경우 '빠른 트랜잭션'을 사용할 수도 있습니다.

지원되는 소유 차량과 iPhone을 연결(또는 페어링)하면 키가 생성됩니다. 모든 키는 타원형 곡선(NIST P-256) 온보드 키 생성(ECC-OBKG)을 기반으로 Secure Element 내에서 생성되며 개인 키는 Secure Element를 벗어나지 않습니다. 기기와 차량 간의 통신은 NFC 또는 Bluetooth® LE와 초광대역(UWB)의 조합 중 하나를 사용합니다. 키 관리는 상호 인증된 TLS를 통해 Apple에서 자동차 제조업체 서버로 연결하는 API를 사용합니다. 키가 iPhone과 페어링되면 해당 iPhone과 페어링된 모든 Apple Watch도 키를 받을 수 있습니다. 키가 차량 또는 기기에서 삭제된 경우 복원할 수 없습니다. 분실되거나 도난당한 기기에 있는 키는 사용을 중단하거나 재개할 수 있지만 새 기기에 다시 배포하려면 새롭게 페어링 또는 공유해야 합니다.

차 키도 익스프레스 모드에서 사용하고 친구 및 가족 구성원과 안전하게 공유할 수 있습니다. 자세한 내용은 키 공유를 참조하십시오. 디지털 차 키의 보안 및 개인정보 보호에 대한 자세한 내용은 iOS의 차 키 보안의 내용을 참조하십시오.

스쿠터 키

iOS 17 이상 및 지원되는 파트너사가 있는 특정 국가 또는 지역에서 사용자는 다음과 같은 목적으로 지원되는 iPhone 및 페어링된 Apple Watch에서 파트너 앱에 권한 설정된 스쿠터 키를 Apple 지갑 앱으로 직접 가져올 수 있습니다.

- 탭하여 스쿠터 잠금 또는 잠금 해제
- 탭하여 스쿠터 트렁크 잠금 또는 잠금 해제(사용 가능한 경우)

Secure Element의 전용 애플릿을 사용하면 스쿠터 키와 연결된 암호화 자격 증명을 안전하게 처리하고 스쿠터를 안전하게 이용할 수 있습니다.

사용자들은 패스 뒷면에서 차대번호(VIN)의 마지막 네 자리와 면허증 또는 번호판 등 스쿠터에 대한 추가 정보를 확인할 수 있습니다. 이러한 정보는 비공개 정보로 간주될 수 있으며 생체 인증 또는 기기 암호를 사용할 때만 해당 정보에 접근할 수 있습니다.

스쿠터 키도 익스프레스 모드에서 사용하고 친구 및 가족 구성원과 안전하게 공유할 수 있습니다. 자세한 내용은 키 공유를 참조하십시오.

iOS의 차 키 보안

개발자는 지원되는 iPhone과 페어링된 Apple Watch로 실물 키 없이도 안전하게 차량에 접근하도록 지원할 수 있습니다.

소유자 페어링

소유자는 해당 차량의 소유를 증명(자동차 제조업체에 따라 방식이 다름)해야 하며 자동차 제조업체에서 받은 이메일 링크를 통해 자동차 제조업체 앱에서 페어링 절차를 시작하거나 차량 메뉴에서 페어링 절차를 시작할 수 있습니다. 모든 경우에 소유자는 NIST P-256 곡선이 적용된 SPAKE2+ 프로토콜을 통해 보안 페어링 채널을 생성하는 데 사용되는 기밀의 일회성 페어링 암호를 iPhone에 제시해야 합니다. 앱 또는 이메일 링크를 사용하면 자동으로 iPhone에 암호가 전송되지만 차량에서 페어링을 시작하는 경우에는 수동으로 암호를 입력해야 합니다.

키 공유

소유자의 페어링된 iPhone은 iMessage 및 Apple Identity Service(IDS)를 통해 기기별 초대장을 전송하여 자격을 가진 가족 구성원과 친구의 iPhone 기기(및 해당 사람의 페어링된 Apple Watch 기기)에 키를 공유할 수 있습니다. 모든 공유 명령은 종단간 암호화된 IDS 기능을 사용하여 교환됩니다. 소유자의 페어링된 iPhone은 초대 전달을 방지하기 위해서 공유 진행 도중 IDS 채널이 변경되지 않도록 합니다.

초대를 수락하면 가족 구성원 또는 친구의 iPhone이 디지털 키를 생성하고, 해당 키가 정품 Apple 기기에서 생성된 것임을 확인하기 위해 키 생성 인증서 체인을 소유자의 페어링된 iPhone으로 다시 전송합니다. 소유자의 페어링된 iPhone은 다른 가족 구성원 또는 친구 iPhone의 ECC 공개 키에 서명하고, 해당 서명을 가족 구성원 또는 친구의 iPhone으로 다시 전송합니다. 소유자 기기에서의 서명 작업에는 사용자 인증(Face ID, Touch ID 또는 암호 입력) 및 Face ID 및 Touch ID의 이용에서 설명한 대로 안전하게 처리된 사용자 의도가 필요합니다. 초대를 전송하는 데는 인증이 필요하며 해당 인증은 Secure Element에 저장되어 친구의 기기에서 서명 요청을 보내는 경우 사용됩니다. 키 권한은 차량 OEM 서버에서 온라인으로 제공되거나 차량에 처음 공유 키를 사용하는 도중에 차량에 제공됩니다.

키 삭제

키는 키홀더 기기, 소유자의 기기, 차량에서 삭제할 수 있습니다. 키홀더 iPhone에서 키를 삭제하는 경우 키홀더 기기에서 해당 키를 사용하는 중이더라도 바로 삭제가 이루어집니다. 그러므로 삭제 전에 엄중한 경고 메시지가 표시됩니다. 차량에서 키 삭제는 언제나 가능하거나 차량이 온라인일 때만 가능합니다.

키홀더 기기 또는 차량에서 키를 삭제하는 경우 모든 삭제 절차가 자동차 제조업체 측의 KIS(키 인벤토리 서버)로 보고됩니다. KTS는 보험 목적으로 차량에 대해 발급된 키가 등록되어 있는 서버입니다.

소유자는 소유자 패스 뒷면에서 삭제를 요청할 수 있습니다. 삭제 요청은 먼저 자동차 제조업체에 전송되어 업체가 차량에서 키를 제거하도록 합니다. 차량에서 키를 제거할 수 있는 요건은 자동차 제조업체에서 정의합니다. 차량에서 키가 제거된 경우에만 자동차 제조업체는 원격 삭제 요청을 키홀더 기기로 전송합니다.

기기에서 키가 제거된 경우 디지털 차 키를 관리하는 애플릿에서 암호화 형식으로 서명된 제거 증명을 생성하며 해당 증명은 자동차 제조업체에서 삭제 증명 자료로 사용하며 KIS에서 키를 제거할 때도 사용합니다.

NFC 표준 트랜잭션

NFC 키를 사용하는 차량의 경우, 표준 트랜잭션은 리더기와 iPhone에 임시 키 쌍을 생성하여 리더기와 iPhone 간의 보안 채널을 엽니다. 키 합의 방식을 사용하여 공유 비밀이 리더기와 iPhone에 파생될 수 있으며 해당 공유 비밀은 키 유도 함수인 Diffie-Hellman과 페어링 절차에서 생성된 장기 키 서명을 통해 공유 대칭 키를 생성하는 데 사용할 수 있습니다.

차량 측에서 생성된 임시 공개 키는 리더기의 장기간 개인 키로 서명되며 iPhone에서 해당 리더기를 인증합니다. iPhone 관점에서 보자면 이 프로토콜은 통신을 가로채려는 공격자로부터 개인정보를 보호하기 위해 설계되었습니다.

마지막으로 iPhone에서는 구축된 보안 채널을 통해 공개 키 식별자와 리더기의 데이터를 암호화하고 리더기의 데이터에서 파생된 확인 요청 및 일부 추가 앱 특정 데이터에 대한 서명도 암호화합니다. 리더기에서 iPhone 서명을 확인하는 이 절차를 통해 리더기에서 기기를 인증할 수 있게 됩니다.

빠른 트랜잭션

iPhone은 이전에 표준 트랜잭션에서 공유된 비밀을 기반으로 암호문을 생성합니다. 이 암호문을 통해 성능에 민감한 경우에 차량이 기기를 빠르게 인증할 수 있습니다. 또한, 표준 트랜잭션에서 이전에 공유된 비밀 및 새로운 임시 키 쌍으로부터 세션 키를 유도하여 차량과 기기 간의 보안 채널을 구축합니다. 차량에서 보안 채널을 구축할 수 있는 경우 해당 차량이 iPhone에 인증됩니다.

BLE/UWB 표준 트랜잭션

UWB를 사용하는 차량의 경우, Bluetooth LE 세션이 차량과 iPhone 간에 구축됩니다. NFC 트랜잭션과 비슷하게 공유된 비밀 사항은 양측에서 파생되며 안전한 세션의 설립을 위해 사용됩니다. 이 세션은 URSK(UWB 레인징 비밀 키)를 파생하고 동의하기 위해 사용됩니다. URSK는 사용자 기기 및 차량의 UWB 라디오에 제공되어 사용자 기기를 차량 근처 또는 내부의 특정 위치에 정확하게 위치시킬 수 있습니다. 그 다음 차량은 기기 위치를 사용해서 차량 잠금 해제 허용 또는 시동 걸기에 대한 결정을 내립니다. URSK는 사전 정의된 TTL을 가집니다. TTL 만료 시 레인징 방해를 방지하기 위해서 URSK는 보안 레인징이 활성화되지 않았지만 BLE가 연결되어 있는 도안 기기 SE 및 차량 HSM/SE에서 미리 파생될 수 있습니다. 이러면 시간이 촉박한 상황에서 새 URSK를 파생하기 위한 표준 트랜잭션의 필요성이 사라집니다. 미리 파생된 URSK는 매우 빠르게 차 및 기기의 UWB 라디오에 전송되어 UWB 레인징 방해를 방지할 수 있습니다.

개인정보 보호

자동차 제조업체의 키 인벤토리 서버(KIS)에서는 기기 ID, SEID 또는 Apple ID를 저장하지 않습니다. 키 추적 서버에서는 변경 가능한 식별자인 인스턴스 CA 식별자만을 저장합니다. 인스턴스 CA 식별자는 기기의 개인 데이터나 서버와도 연결되어 있지 않기 때문에 사용자가 기기를 완전히 삭제하는 경우 해당 식별자도 삭제됩니다(모든 콘텐츠 및 설정 지우기 사용).

Apple 지갑에 교통 카드 및 전자머니 카드 추가하기

여러 국가에서 지원되는 iPhone 및 Apple Watch 모델의 Apple 지갑에 지원되는 교통 카드 및 전자머니 카드를 추가할 수 있습니다. 운영 업체에 따라 실물 카드에서 디지털 Apple 지갑으로 금액, 정기권 또는 둘 다를 전송하거나, Apple 지갑 또는 카드 발급처의 앱에서 새로운 교통 카드 또는 전자머니 카드의 권한을 설정할 수 있습니다. 교통 카드가 Apple 지갑에 추가되면 사용자는 교통 카드 리더기 근처에서 자신의 iPhone 또는 Apple Watch를 들고 있기만 해도 대중교통을 이용할 수 있습니다. 일부 교통 카드를 사용하여 결제할 수도 있습니다.

교통 카드 및 전자머니 카드의 작동 원리

등록된 교통 카드 및 전자머니 카드는 사용자의 iCloud 계정에 연결됩니다. 사용자가 Apple 지갑에 두 장 이상의 카드를 등록하는 경우, Apple 또는 카드 발급처에서 사용자의 개인정보 및 카드 간 계정 정보를 연결할 수 있습니다. 교통 카드, 전자머니 카드 및 거래는 일련의 계층형 암호화 키로 보호됩니다.

실물 카드에서 Apple 지갑으로 잔액을 전송하는 과정에서 사용자는 카드의 고유 정보를 입력해야 합니다. 사용자는 카드 소유자임을 증명하기 위해 개인정보를 입력해야 할 수도 있습니다. iPhone에서 Apple Watch로 승차권을 전송할 때 두 기기 모두 온라인 상태여야 합니다.

Apple 지갑, 교통 카드 또는 전자머니 카드 발급처의 앱을 통해 신용 카드, 체크 카드 또는 선불 카드로 잔액을 충전할 수 있습니다. Apple Pay 사용 시 잔액 재충전 보안 사항에 대해 알아보려면 앱에서 카드로 결제하기를 참조하십시오. 카드 발급처의 앱에서 카드를 발급받는 방법에 대해 알아보려면 카드 발급처의 앱을 사용해 신용 카드 또는 체크 카드 추가하기를 참조하십시오.

실물 카드에서 권한 설정을 지원하는 경우, 교통 카드 및 전자머니 발급처는 실물 카드를 인증하고 사용자가 입력한 데이터를 확인하기 위한 암호화 키를 가집니다. 데이터 확인이 끝나면 시스템은 Secure Element에 대한 기기 계정 번호를 생성할 수 있으며 Apple 지갑에 잔액이 전송되고 새로 추가된 패스를 활성화할 수 있습니다. 일부 카드에서는 실물 카드의 권한 설정을 마치면 실물 카드가 비활성화됩니다.

각 권한 설정의 마무리 단계에서 카드 잔액이 기기에 저장되어 있으면, 암호화되어 Secure Element의 지정된 애플릿에 저장됩니다. 발급처는 잔액 거래를 위해 카드 데이터에 암호화 작업을 수행하는 키를 가집니다.

기본적으로 교통 카드 사용자는 익스프레스 교통 카드 경험을 통해 요금 충전 또는 탑승 시 Face ID, Touch ID 및 암호 요청 없이 빠르게 사용할 수 있습니다. 익스프레스 모드가 활성화되어 있는 근처 비접촉식 카드 리더기의 경우 최근 방문한 역, 거래 내역, 추가 티켓 등의 정보에 접근할 수 있습니다. 지갑 및 Apple Pay 설정에서 익스프레스 교통 카드를 비활성화하여 Face ID, Touch ID 또는 암호 인증을 요청을 켤 수 있습니다. 전자머니 카드는 익스프레스 모드를 지원하지 않습니다.

다른 Apple Pay 카드와 마찬가지로 사용자는 다음과 같은 방법으로 전자머니 카드를 정지하거나 제거할 수 있습니다.

- 나의 찾기를 사용하여 원격으로 기기 지우기
- 나의 찾기에서 분실 모드 활성화
- MDM(모바일 기기 관리) 원격 지우기 명령 입력
- Apple ID 계정 페이지에서 모든 카드 제거
- iCloud.com에서 모든 카드 제거
- Apple 지갑에서 모든 카드 제거
- 발급처의 앱에서 해당 카드 제거

Apple Pay 서버는 카드 발급처에 해당 카드 사용 중단 또는 비활성화를 고지합니다. 사용자가 온라인 상태의 기기에서 교통 카드 또는 전자머니 카드를 제거하면 동일한 Apple ID로 로그인한 기기에 해당 카드를 추가하여 잔액을 복구할 수 있습니다. 기기가 오프라인 상태이거나, 전원이 꺼져 있거나, 사용할 수 없는 상태인 경우 복구할 수 없습니다.

가족 구성원의 Apple Watch에 교통 카드 및 전자머니 카드 추가하기

iOS 15 이상 및 watchOS 8 이상에서 iCloud 가족의 가족 대표는 iPhone의 Watch 앱을 사용해서 가족 구성원의 Apple Watch 기기에 교통 카드 및 전자머니 카드를 추가할 수 있습니다. 이 카드 중 하나의 권한을 가족 구성원의 Apple Watch에 설정하는 경우 Apple Watch는 가까이 있어야 하고 Wi-Fi 또는 Bluetooth를 사용해서 가족 대표의 iPhone에 연결되어 있어야 합니다. 이를 위해서 가족 구성원의 Apple ID는 이중 인증이 활성화되어 있어야 합니다.

가족 구성원은 Apple Watch에서 iMessage를 사용하여 교통 카드 또는 전자머니 카드에 금액을 충전하기 위한 요청을 보낼 수 있습니다. iMessage 보안 개요에 기술된 대로 메세지 콘텐츠는 종단간 암호화로 보호됩니다. Wi-Fi 또는 셀룰러 연결을 사용하여 원격으로 가족 구성원의 Apple Watch의 카드에 금액을 추가할 수 있습니다. 이를 위해 서로 근접하게 있을 필요는 없습니다.

참고: 이 기능은 일부 국가 또는 지역에서만 사용할 수 있습니다.

신용 및 체크 카드

일부 도시에서는 교통 카드 리더기가 스마트(EMV) 카드로 대중 교통 요금을 지불하는 것이 지원됩니다. 사용자가 해당 리더기에 EMV 신용 카드 또는 체크 카드를 접촉시킬 때 '매장에서 신용 카드 및 체크 카드로 결제'하는 것과 마찬가지로 사용자 인증이 필요합니다.

iOS 12.3 이상에서 Apple 지갑의 일부 EMV 신용/체크 카드는 익스프레스 교통 카드를 위해 활성화될 수 있습니다. 익스프레스 교통 카드를 통해 사용자는 Face ID, Touch ID 및 암호를 입력하지 않고 지원되는 대중교통 운영 업체에 교통 요금을 지불할 수 있습니다. 사용자가 EMV 신용 카드 또는 체크 카드의 권한을 설정할 때 Apple 지갑에 권한 설정된 첫 번째 카드가 익스프레스 교통 카드용으로 사용됩니다. 사용자는 Apple 지갑에서 카드 앞면의 더 보기 버튼을 탭하고 '익스프레스 교통 카드 설정'을 '없음'으로 설정하여 익스프레스 교통 카드를 비활성화할 수 있습니다. 또한 사용자는 Apple 지갑을 사용하여 다른 신용 카드 또는 체크 카드를 익스프레스 교통 카드로 선택할 수 있습니다. 익스프레스 모드를 다시 활성화하거나 익스프레스 교통 카드로 다른 카드를 선택하려면 Face ID, Touch ID 또는 암호가 필요합니다.

익스프레스 승차에 Apple Card 및 Apple Cash를 사용할 수 있습니다.

Apple 지갑의 ID

Apple 지갑의 ID

iOS 15.4 이상을 실행하는 iPhone 8 및 이후 모델과 watchOS 8.4 이상을 실행하는 Apple Watch Series 4 및 이후 모델에서 사용자는 주 발급 신분증 또는 운전면허증을 Apple 지갑에 추가하고 iPhone 또는 Apple Watch를 탭하여 지원되는 장소에서 원활하고 안전하게 제시할 수 있습니다.

참고: 이 기능은 지원되는 미국 주에서만 사용 가능합니다.

Apple 지갑의 ID는 사용자의 기기에 내장된 하드웨어 및 소프트웨어의 보안 기능을 사용해서 신분을 보호하고 개인정보를 안전하게 지킬 수 있도록 돕습니다.

Apple 지갑에 운전면허증 또는 주 발급 신분증 추가하기

iPhone에서 사용자는 Apple 지갑 화면 상단의 추가(+) 버튼을 탭하기만 해도 면허증 또는 ID 추가를 시작할 수 있습니다. 사용자가 설치 당시에 페어링한 Apple Watch를 갖고 있다면 Apple Watch의 Apple 지갑에 운전면허증 또는 ID도 추가하라는 메시지가 표시됩니다.

우선 사용자들은 iPhone을 사용해서 실물 운전면허증 또는 주 발급 신분증의 앞면과 뒷면을 스캔하도록 요청받습니다. iPhone은 이미지의 품질 및 유형을 평가해서 주 행정 기관에서 제공된 이미지를 허용할 수 있는지 확인합니다. 이런 ID 카드 이미지는 기기의 주 행정 기관의 키로 암호화된 다음, 주 행정 기관으로 전송됩니다.

그 다음 사용자는 얼굴 및 머리로 일련의 동작을 수행하도록 요청을 받게 됩니다. 사용자의 기기 및 Apple이 이 동작을 검토해 사진, 비디오 또는 가면을 사용해서 다른 사람의 ID를 Apple 지갑에 추가하는 위험을 줄입니다. 동작의 분석 결과는 주 행정 기관으로 전송되지만 동작의 영상은 전송되지 않습니다.

Apple 지갑에 ID 카드를 추가하는 사람이 ID 카드의 소유자와 동일 인물임을 확인하기 위해 사용자는 셀피를 찍으라는 요청을 받습니다. 사용자의 사진이 주 행정 기관에 제출되기 전에 Apple 서버와 사용자의 기기는 사진을 일련의 얼굴과 머리 움직임을 수행한 사람의 사진과 유사한지 비교하고 제출된 사진이 ID에 있는 것과 유사한 실제 사람의 사진인지 확인하도록 돕습니다. 비교가 이루어지고 나면 사진은 기기상에서 암호화된 다음 주 행정 기관으로 전송되어, 사용자의 ID에 대해 기관에서 자체적으로 보유하고 있는 이미지와 해당 사진을 대조합니다.

마지막으로 사용자는 Face ID 또는 Touch ID 인증 수행을 요청받습니다. 사용자의 기기는 단일 Face ID 또는 Touch ID 생체 인식 기능을 주 ID에 연결하여 해당 ID를 이 iPhone에 추가한 사람만 표시할 수 있도록 합니다. 등록된 기타 생체 정보는 ID 표시를 승인하는 데 사용할 수 없습니다. 이는 기기상에서만 발생하며 주 행정 기관으로 전송되지 않습니다.

주 행정 기관은 디지털 ID 설정에 필요한 정보만 받습니다. 이는 사용자 ID의 앞면과 뒷면 이미지, PDF417 바코드에서 읽은 데이터 및 ID 확인 프로세스의 일부로써 사용자가 찍은 셀피를 포함합니다. 발급 주도 사용자의 장치 사용 패턴, 설정 데이터 및 개인 Apple ID에 대한 정보에 기반하며 사기를 방지하는 데 사용되는 한 자릿수 값을 받습니다. 다음으로 Apple ID에 추가되는 ID의 승인 또는 거부는 궁극적으로 발급 주의 결정에 달렸습니다.

주 행정 기관이 Apple 지갑에 주 발급 신분증 또는 운전면허증의 추가를 허용하면, iPhone의 Secure Element에 사용자 ID를 해당 특정 기기에 고정시키는 키 페어가 생성됩니다. Apple Watch에 추가하는 경우 Apple Watch에 의해 키 페어가 Secure Element에 생성됩니다.

ID가 iPhone에 등록된 다음, Apple 지갑의 사용자 ID에 반영된 정보는 Secure Enclave가 보호하는 암호화된 형식으로 저장됩니다.

신분증 리더기로 Apple 지갑의 운전면허증 또는 주 발급 신분증 사용하기

Apple 지갑의 ID를 사용하려면 사용자는 iPhone이 신분증 리더기에 정보를 제공하기 전에 Apple 지갑에 있는 ID와 관련된 Face ID 또는 Touch ID 장치로 인증을 해야 합니다.

Apple Watch의 Apple 지갑에서 ID를 사용하려면 사용자는 Apple Watch를 착용할 때마다 관련된 Face ID 외모 또는 Touch ID 지문을 매번 사용하여 iPhone을 잠금 해제해야 합니다. 그러면, 다시 Apple Watch를 착용 해제하기 전까지 인증할 필요 없이 Apple 지갑에서 ID를 사용할 수 있습니다. 이 기능은 watchOS의 시스템 보안에서 자세히 설명된 기본적인 자동 잠금 해제 기능을 활용합니다.

사용자가 iPhone 또는 Apple Watch를 신분증 리더기 옆에 가져다 대거나 앱 내에서 ID를 공유하면 어떤 특정 정보가 요청되고 누가 요청하며 저장할 의도가 있는지 표시하는 메시지 창을 볼 수 있습니다. 관련된 Face ID 또는 Touch ID로 인증한 다음 요청된 신원 정보는 기기로부터 공개됩니다.

중요사항: 사용자는 ID를 제시하기 위해서 기기를 잠금 해제하거나 보여주거나 넘겨 줄 필요가 없습니다.

사용자가 Face ID 또는 Touch ID 대신에 음성 명령, 스위치 제어 또는 Assistive Touch와 같은 손쉬운 사용 기능을 활성화했다면 암호를 사용해서 정보에 접근하고 제시할 수 있습니다.

신분증 리더기로의 신원 데이터의 전송은 보안 위험을 발견, 예방 및 경감할 수 있는 다중 보안 메커니즘을 제공하는 ISO/IEC 18013-5 표준을 따릅니다. 이는 신원 데이터 무결성 및 위조 방지, 장치 바인딩, 사전 동의 및 라디오 링크를 통한 사용자 데이터 기밀로 구성됩니다.

iOS 앱으로 Apple 지갑의 운전면허증 또는 주 발급 신분증 사용하기

사용자는 Apple 지갑에서 iOS 앱으로 운전면허증 또는 주 발급 신분증 정보를 공유할 수도 있습니다. 사용자가 자신의 ID를 앱과 공유하면 Apple 지갑은 앱 개발자에게 등록된 암호화 인증서를 가져와 유효성을 검사합니다.

이 인증서는 사용자가 공유하는 데 동의한 정보를 암호화하는 데 사용됩니다. 이 정보는 HPKE를 사용하여 지갑에 의해 암호화되며 Apple에서 절대 사용할 수 없습니다. 지갑 앱은 주기적으로 Apple 서버에 쿼리하여 해당 ID가 아직 유효한지 확인합니다. 최근에 확인을 수행하지 않은 경우, 사용자가 자신의 ID를 앱과 공유할 때 확인이 발생할 수 있습니다.

Apple 지갑 ID의 보안

다음 기능을 통해 Apple 지갑의 ID를 사용할 때 보안을 강화할 수 있습니다.

신원 데이터 무결성 및 위조 방지

Apple 지갑의 ID는 발급처가 제공하는 서명을 사용하여 모든 ISO/IEC 18013-5 준수 리더기가 Apple 지갑의 사용자 ID를 인증할 수 있게 허용합니다. 또한 지갑 앱에 있는 ID의 모든 데이터 요소는 각자 위조로부터 보호받습니다. 이를 통해서 신분증 리더기는 Apple 지갑의 ID에 있는 데이터 요소의 특정한 하위 집합을 요청하고 Apple 지갑의 ID가 동일한 하위 집합으로 응답할 수 있도록 허용하며 요청된 데이터만 공유하고 사용자의 개인정보 보호를 최대화합니다.

기기 바인딩

Apple 지갑 인증의 ID는 기기 서명을 사용하여 ID 복제 및 신분 표시의 재전송을 방지합니다. Apple 지갑은 iPhone 기기의 Secure Element에 ID 인증을 위한 개인 키를 저장하므로, ID는 주 행정 기관이 ID를 생성해 준 동일한 기기에 바인딩됩니다.

사전 동의

Apple 지갑의 ID는 인증을 사용해 ISO/IEC 18013-5 표준에서 정의된 프로토콜을 사용하는 리더기를 식별할 수 있습니다. 프레젠테이션 중에 리더기가 Apple Wallet에서 신뢰하는 자체 인증서를 가지고 있는 경우, 아이콘이 표시되어 사용자가 의도한 대상과 상호 작용하고 있음을 확인할 수 있게 합니다.

라디오 링크를 통한 사용자 데이터 기밀성

세션 암호화는 Apple 지갑의 ID와 신분증 리더기 간에 교환되는 모든 PII(개인 식별 정보)가 암호화되는지 확인합니다. 암호화는 응용 프로그램 레이어에 의해 수행됩니다. 따라서 세션 암호화의 보안은 전송 레이어가 제공한 보안(예: NFC, Bluetooth 및 Wi-Fi)에 의존하지 않습니다.

사용자의 정보를 안전하게 지키는 Apple 지갑의 ID

Apple 지갑의 ID 는 ISO/IEC 18013-5에 명시된 '기기 검색' 프로세스를 따릅니다. 기기 검색은 제시 중에 서버 호출을 할 필요를 없애므로 사용자가 Apple과 발급처에 의해 추적당하지 않도록 보호합니다.

ID 검증자 보안

iOS 17 이상에서 미국 업체 및 조직은 iPhone을 사용해 ISO 18013-5 준수 모바일 ID를 직접 원활하고 안전하게 읽을 수 있습니다. 외부 하드웨어는 필요 없습니다. ID 검증자는 확인 사용 사례에 따라 다음과 같은 두 가지 방법으로 사용할 수 있습니다.

- **ID 검증자 디스플레이 전용:** 시각적 확인만 필요한 사용 사례의 경우, iOS 사용자 인터페이스를 사용해 이름, 나이, ID 사진, **N**세 이상 데이터를 표시할 수 있습니다. 이 서비스는 ID 제시자와 관련이 있을 수 있는 **개인 식별 정보**(PII)의 수집을 허용하지 않습니다.
- **ID 검증자 데이터 전송:** 이를 통해 앱은 법적 인증 요건을 충족하기 위해 생년월일 및 주소 등의 추가 데이터 요소를 요청할 수 있습니다. ID 검증자 데이터 전송 API에 대한 접근은 권한을 통해 관리되며 앱은 데이터의 사용 방식을 존중하며 제한 사항을 따라야 합니다. 예를 들어, 앱은 신원 데이터를 요청하기 위한 법적 요건을 입증해야 합니다. 또한 앱은 요청된 신원 데이터의 처리, 보관 또는 기타 사용에 대해 자세히 설명하는 개인정보 처리방침을 유지해야 합니다.

모바일 ID 읽기

ID 검증자는 ISO/IEC 18013-5 표준에서 정의된 프로토콜을 따릅니다. ID 검증자 API 요청을 사용하는 앱이 모바일 ID 읽기를 요청하면 iOS에서 제어하는 시트가 나타나고 모바일 ID 소유자에게 기기를 신분증 리더기 근처에 가져다 대라는 메시지를 표시합니다. 최초 NFC 연결(ISO/IEC 18013-5 표준에 의해 정의된 대로 NFC 대신 QR 코드를 사용하여 Bluetooth 핸드오버 프로세스를 시작할 수 있음)은 두 기기 간에 안전한 Bluetooth® Low Energy(BLE) 연결을 설정합니다. 이때 모바일 ID 소유자는 요청 중인 정보를 기기에서 검토할 수 있습니다. 모바일 ID 소유자가 동의하면 요청된 신분증 데이터가 리더기로 전송됩니다. ID 검증자 데이터 전송 API를 사용하는 앱은 처리를 위해 응답 데이터를 받으며, ID 검증자 디스플레이 전용 API를 사용하는 앱은 iOS에서 직접 표시되는 데이터를 볼 수 있습니다.

ISO/IEC 18013-5 표준은 보안 위험을 발견, 예방 및 경감하기 위해 여러 보안 메커니즘을 제공합니다. 그 중 ID 검증자는 발급처 서명 및 기기 서명 확인을 모두 수행합니다. 또한, ID 검증자는 ISO/IEC 18013-5 표준에서 정의된 프로토콜을 사용해 리더기 인증을 지원합니다. 앱은 아이콘 및 이름을 표시하여 ID 소유자가 리더기의 인증서를 사용해 의도한 대상과 상호 작용하고 있다는 확신을 제공할 수 있습니다.

발급처 및 기기 확인

위조 방지를 위해 ID 검증자는 신뢰하는 모바일 신분증 발급처를 통해 Mobile Security Object의 서명을 확인합니다. ID 검증자 데이터 전송은 앱이 iOS 대신 자체적으로 서명 확인을 진행할 수 있는 API를 제공하기도 합니다. 모바일 ID가 한 기기에서 다른 기기로 복제되지 않았다는 확신을 기업 또는 조직에 주기 위해 ID 검증자는 세션 데이터를 통해 서명을 확인합니다.

리더기 인증

제시 당시 ID 검증자 리더기 요청은 Apple 루트 인증 기관(CA)과 연결 고리가 있는 리더기 인증서와 관련된 비공개 키로 서명되며, 여기에는 기업이 데이터를 저장할 의도가 있는지 여부를 소유자에게 알려주는 관련 x509 사용자 설정 확장 프로그램을 포함합니다. 응용 프로그램이 ID 소유자에게 이름 및 아이콘을 표시하려는 경우, 앱 관리자는 Apple Business Register를 통해 등록하고 정확한 브랜드 정보를 제공해야 합니다. 제출한 정보가 확인되면 거래 시 리더기 인증서가 ID 소유자에게 Apple Register의 엔티티에 대한 정보를 리더기 인증서를 통해 제공합니다.

iMessage

iMessage 보안 개요

Apple의 iMessage는 iPhone 및 iPad 기기, Apple Watch 및 Mac 컴퓨터를 위한 메시지 전송 서비스입니다. iMessage는 문자, 사진, 연락처, 위치, 링크 등의 첨부 항목과 올린 엄지 아이콘 등 메시지에 바로 제공된 첨부 항목을 지원합니다. 등록된 모든 기기에 메시지가 나타나므로 사용자는 어떤 기기에서도 대화를 이어갈 수 있습니다. iMessage는 APNS(Apple 푸시 알림 서비스)를 폭넓게 사용합니다. Apple은 메시지 또는 첨부 파일 내용을 기록하지 않으며 해당 콘텐츠는 종단간 암호화 기술로 안전하게 보호되어 보낸 사람과 받는 사람을 제외한 누구도 해당 콘텐츠에 접근할 수 없습니다. Apple은 해당 데이터의 암호화를 해제할 수 없습니다.

사용자가 기기에서 iMessage를 켜면 기기는 서비스에 사용할 수 있는 암호화 및 서명 키 쌍을 생성합니다. NIST P-256 커브에 암호화를 위한 암호화 RSA 1280비트 키와 암호화 EC 256비트 키가 있습니다. 서명의 경우, ECDSA(Elliptic Curve Digital Signature Algorithm) 256비트 서명 키가 사용됩니다. 개인 키는 기기의 키체인에 저장되며 처음 잠금을 해제한 후에만 사용할 수 있습니다. 공개 키는 Apple IDS(Identity Service)로 전송됩니다. Apple IDS(Identity Service)에 전송된 공개 키는 해당 기기의 APNS 주소, 사용자의 전화번호 또는 이메일 주소와 연결됩니다.

사용자가 iMessage를 사용하도록 추가 기기를 활성화하면 암호화 및 서명 공개 키, APNS 주소 및 관련 전화번호가 디렉토리 서비스에 추가됩니다. 또한 사용자는 더 많은 이메일 주소를 추가할 수 있으며 이메일 주소는 확인 링크를 통해 확인됩니다. 전화번호는 이동통신사 네트워크와 SIM을 통해 확인됩니다. 일부 네트워크의 경우 SMS 사용이 요구되며, SMS 요금이 부과되는 경우에는 확인 대화상자가 사용자에게 표시됩니다. iMessage 외에도 FaceTime 및 iCloud와 같은 몇몇 시스템 서비스의 경우 전화번호 확인이 필요할 수 있습니다. 사용자의 등록된 기기는 모두 새로운 기기, 전화번호 또는 이메일 주소가 추가될 때 알림 메시지를 표시합니다.

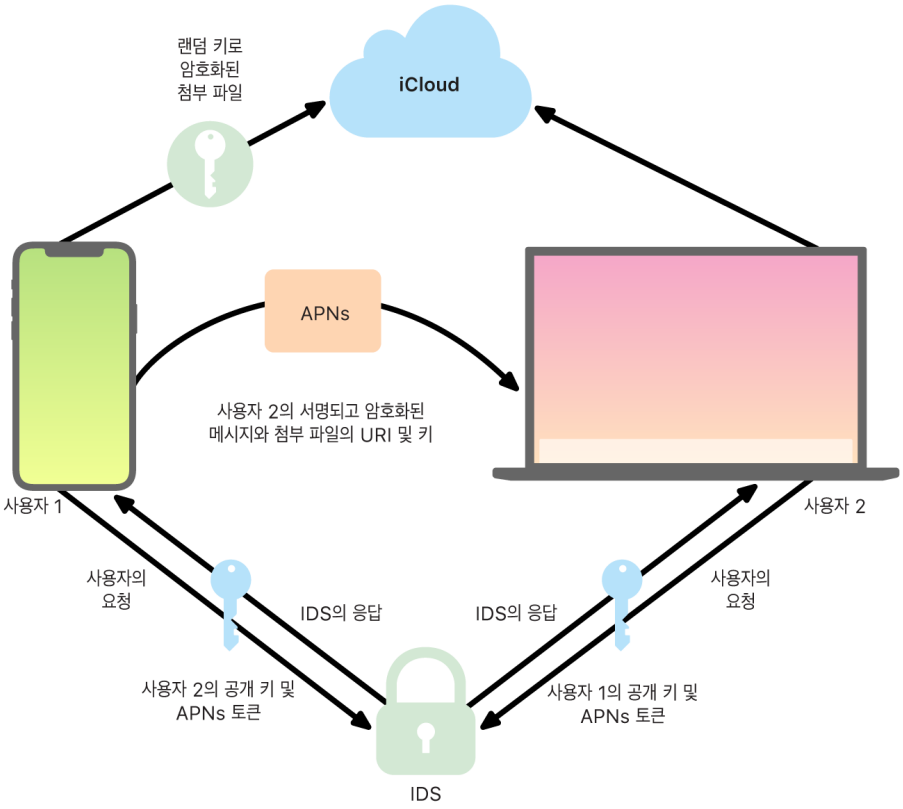
iMessage가 메시지를 안전하게 주고받는 방법

사용자는 이메일 주소 또는 이름을 입력하여 새로운 iMessage 대화를 시작할 수 있습니다. 전화번호 또는 이메일 주소를 입력하면 기기가 Apple IDS(Identity Service)에 연결하여 해당 번호 또는 주소와 관련한 모든 기기에 대한 공개 키와 APNS 주소를 가져옵니다. 사용자가 이름을 입력하면 기기는 우선 사용자의 연락처 앱을 사용하여 해당 이름과 관련한 전화번호와 이메일 주소를 수집한 다음 IDS에서 공개 키와 APNS 주소를 가져옵니다.

사용자가 보내는 메시지는 수신자의 각 기기에서 개별적으로 암호화됩니다. 수신하는 기기의 공개 암호화 키 및 서명 키는 IDS에서 가져옵니다. 또한, 전송하는 기기는 각각의 수신하는 기기에 대해 무작위로 88비트 값을 생성하고 HMAC-SHA256 키로 사용하여 전송자와 수신자의 공개 키와 평문에서 파생된 40비트 값을 구성합니다. 88비트 값과 40비트 값을 조합하여 128비트 키가 만들어지고 이 키는 CTR(Counter) 모드에서 AES에 사용되어 메시지를 암호화합니다. 40비트 값은 수신하는 쪽에서 암호화 해제된 평문의 무결성을 확인하기 위해 사용합니다. 메시지별 AES 키는 RSA-OAEP를 사용하여 수신하는 기기의 공개 키로 암호화됩니다. 그리고 암호화된 메시지 텍스트와 암호화된 메시지 키의 조합은 SHA-1로 해시되며, 해당 해시는 전송하는 기기의 개인 서명 키를 사용하여 ECDSA(Elliptic Curve Digital Signature Algorithm)로 서명됩니다. iOS 13 이상, iPadOS 13.1 이상에서 기기는 RSA 암호화 대신 ECIES(Elliptic Curve Integrated Encryption Scheme) 암호화를 사용할 수 있습니다.

결과로 나온 메시지는 수신하는 기기당 하나이며 암호화된 메시지 텍스트, 암호화된 메시지 키와 보낸 사람의 디지털 서명으로 구성됩니다. 그런 다음 전송을 위해 APNS로 발송됩니다. 타임스탬프나 APNS 라우팅 정보와 같은 메타데이터는 암호화되지 않습니다. APNS와의 통신은 전방향 안전 TLS 채널을 사용하여 암호화됩니다.

APNS는 iOS 또는 iPadOS 버전에 따라 최대 4KB 또는 16KB의 크기의 메시지만 릴레이할 수 있습니다. 메시지 텍스트가 너무 길거나 사진과 같은 첨부 파일이 포함되어 있는 경우 첨부 파일은 CTR 모드의 AES와 무작위로 생성된 256비트 키로 암호화되어 iCloud에 업로드됩니다. 첨부 파일의 AES 키, 해당 URI(Uniform Resource Identifier) 및 암호화된 형태의 SHA-1 해시는 아래의 다이어그램에 나타난 대로 일반 iMessage 암호화를 통해 기밀성과 무결성을 보호하면서 수신자에게 iMessage 콘텐츠로 전송됩니다.



그룹 대화에서는 각 수신자와 수신하는 기기가 이 과정을 반복합니다.

수신하는 쪽의 각 기기는 APNS에서 메시지 사본을 받고 필요한 경우 iCloud에서 첨부 파일을 검색합니다. 가능한 경우, 보낸 사람의 전화번호 또는 이메일 주소가 수신자의 연락처와 일치하면 이름이 표시됩니다.

모든 푸시 알림과 마찬가지로 메시지는 전송되는 경우 APNS에서 삭제됩니다. 그러나 다른 APNS 알림과 달리 iMessage 메시지는 오프라인 기기에 전송을 위해 대기합니다. 메시지는 Apple 서버에 최대 30일 동안 저장됩니다.

iMessage 이름 및 사진 공유 보안

iMessage 이름 및 사진 공유는 iMessage를 사용하여 이름과 사진을 공유할 수 있는 기능입니다. 사용자는 내 카드 정보를 선택하거나 이름을 사용자화하고 선택한 이미지를 포함할 수 있습니다. iMessage 이름 및 사진 공유는 이름과 사진을 배포하는 데 2단계 시스템을 사용합니다.

데이터는 필드로 세분화되고 개별적으로 암호화되고 인증되며, 아래 프로세스로 함께 인증됩니다. 다음은 세 가지 필드입니다.

- 이름
- 사진
- 사진 파일 이름

데이터 생성의 첫 번째 단계 중 하나는 기기에 128비트 키 레코드를 임의로 생성하는 것입니다. 그런 다음 이 레코드 키는 HKDF-HMAC-SHA256으로 파생되어 Key 1:Key 2:Key 3 = HKDF(레코드 키, '별명')의 세 가지 하위 키를 생성합니다. 각 필드에서 임의의 96비트 IV(초기화 백터)가 생성되며 데이터는 AES-CTR 및 Key 1을 사용하여 암호화됩니다. 그런 다음 MAC(메시지 인증 코드)은 Key 2를 사용하고 필드 이름, 필드 IV 및 필드 암호문을 포함하는 HMAC-SHA256으로 계산됩니다. 마지막으로 개별 필드 MAC 값 세트가 연결되고 해당 MAC은 Key 3을 사용하여 HMAC-SHA256으로 계산됩니다. 256비트 MAC은 암호화 데이터와 나란히 보관됩니다. 이 MAC의 첫 번째 128비트는 RecordID로 사용됩니다.

그런 다음 이 암호화 레코드는 CloudKit 공개 데이터 베이스의 RecordID에 보관됩니다. 이 레코드 키는 절대 변경되지 않으며 사용자가 이름 및 사진을 변경할 때 매번 새로운 암호화 레코드가 생성됩니다. 사용자 1이 자신의 이름과 사진을 사용자 2에게 공유하려는 경우 iMessage 페이로드 내부의 RecordID와 함께 암호화된 레코드 키를 전송합니다.

사용자 2의 기기가 이 iMessage 페이로드를 받으면 기기는 별명 및 사진 RecordID와 키가 페이로드에 포함되어 있음을 인식합니다. 그런 다음 사용자 2의 기기는 공개 CloudKit 데이터베이스로 이동되어 RecordID의 암호화된 이름 및 사진을 검색하고 iMessage를 사용하여 전송합니다.

메시지를 검색한 후 사용자 2의 기기는 페이로드 암호화를 해제하고 RecordID 자체로 서명을 확인합니다. 이 단계를 통과하면 사용자 2에게 이름과 사진이 표시되고, 사용자 2는 이를 연락처에 추가하거나 메시지용으로 사용할 수 있습니다.

보안된 Apple Messages for Business

Apple Messages for Business는 메시지 앱을 사용하여 사용자가 업체와 소통을 할 수 있게 허용하는 메시지 서비스입니다. 사용자는 Apple Messages for Business로 언제든지 대화를 제어할 수 있습니다. 또한, 대화를 삭제하고 앞으로 업체에서 메시지를 보내지 못하도록 차단할 수도 있습니다. 개인정보 보호를 이유로 사용자의 전화번호, 이메일 주소 또는 iCloud 계정 정보는 업체에 표시되지 않습니다. 대신 Apple IDS(Identity Service)에 의해 **Opaque ID**라는 사용자 설정 고유 식별자가 생성되어 업체에 공유됩니다. Opaque ID는 사용자의 Apple ID와 업체의 비즈니스 ID 사이의 관계에 있어 고유한 성질을 가집니다. 사용자는 Apple Messages for Business를 통해 연락하는 업체마다 다른 Opaque ID를 가집니다. 사용자는 개인 식별 정보를 업체와 공유할지 여부와 그 시기를 결정하고 Apple Messages for Business 서비스는 대화 기록을 결코 저장하지 않습니다.

Apple Messages for Business는 Apple Business Manager에서 생성된 관리형 Apple ID를 지원하며 Apple School Manager에서 iMessage 및 FaceTime에 관리형 Apple ID를 사용할 수 있는지를 결정합니다.

업체에 전송된 메시지는 사용자의 기기와 Apple의 메시지 서버 간에 암호화되며 iMessage와 동일한 보안 및 Apple 메시지 서버를 사용합니다. Apple 메시지 서버는 이러한 메시지를 RAM에서 암호화 해제하고 TLS 1.2를 사용하여 암호화된 링크를 통해 업체에 릴레이합니다. Apple의 Apple Messages for Business 서비스를 통해 메시지가 전송되는 동안 메시지는 절대 암호화되지 않은 형태로 저장되지 않습니다. 업체의 답장 역시 TLS 1.2를 통해 Apple 메시지 서버에 전송되며, 각 수신 기기에 대해 고유한 공개 키를 사용하여 암호화됩니다.

사용자 기기가 온라인 상태인 경우 메시지는 즉시 전달되며 Apple 메시지 서버에 캐시되지 않습니다. 사용자의 기기가 온라인 상태가 아닌 경우 암호화된 메시지는 최대 30일 동안 캐시되어 기기가 다시 온라인 상태가 되면 메시지를 받을 수 있습니다. 기기가 다시 온라인 상태가 되면 그 즉시 메시지가 전달되고 캐시에서 삭제됩니다. 30일이 지나면 전달되지 않은 캐시된 메시지가 만료되어 영구적으로 삭제됩니다.

FaceTime 보안

FaceTime은 Apple의 영상 및 음성 통화 서비스입니다. iMessage와 마찬가지로 FaceTime 통화는 APNS(Apple 푸시 알림 서비스)를 사용하여 사용자의 등록된 기기에 초기 연결을 구축합니다. FaceTime 통화의 음성/영상 콘텐츠는 종단간 암호화 기술로 안전하게 보호되어 보낸 사람과 받는 사람을 제외한 누구도 해당 콘텐츠에 접근할 수 없습니다. Apple은 해당 데이터의 암호화를 해제할 수 없습니다.

초기 FaceTime 연결은 사용자의 등록 기기 간에 데이터 패킷을 릴레이하는 Apple 서버 인프라를 통해 구축되었습니다. 릴레이되는 연결을 통한 APNS(Apple 푸시 알림 서비스) 알림 및 STUN(Session Traversal Utilities for NAT) 메시지를 사용하여 기기는 신원 인증서를 확인하고 각 세션에 대한 공유 비밀을 구축합니다. 공유 비밀은 SRTP(Secure Real Time Protocol)를 사용해 스트리밍되는 미디어 채널의 세션 키를 가져오는 데 사용됩니다. SRTP 패킷은 Counter Mode의 AES256를 사용하여 암호화되며 HMAC-SHA1을 사용하여 인증됩니다. 초기 연결 및 보안 설정 후 FaceTime은 STUN 및 ICE(Internet Connectivity Establishment)를 사용하여 기기간에 피어 투 피어 연결을 구축합니다(가능한 경우).

그룹 FaceTime을 통해 FaceTime에서 지원하는 동시 참가자 수가 최대 33명으로 늘었습니다. 기존 일대일 FaceTime과 마찬가지로 통화는 초대된 참가자의 기기 간에 종단간 암호화됩니다. 일대일 FaceTime의 많은 인프라와 디자인이 그룹 FaceTime에서 재사용되지만 이런 그룹 통화는 Apple IDS(Identity Service)에서 제공하는 인증을 기반으로 설계된 새로운 키 구축 메커니즘이 특징입니다. 이 프로토콜은 전방향 안전성을 제공하기 때문에 사용자 기기가 침해된 경우에도 이전 통화 내용이 유출되지 않습니다. 세션 키는 AES-SIV를 통해 래핑되며 임시 P-256 ECDH 키가 포함된 Elliptic Curve Integrated Encryption Scheme(ECIES) 구성을 사용하여 참가자에게 배포됩니다.

새로운 전화번호 또는 이메일 주소가 진행 중인 그룹 FaceTime 통화에 추가되면, 이미 활성화되어 있는 기기는 새로운 미디어 키를 구축하며 이전에 사용된 키를 새로 초대된 기기와 공유하지 않습니다.

나의 찾기

나의 찾기 보안

Apple 기기의 나의 찾기 앱은 고급 공개 키 암호화 기술을 기반으로 구축되었습니다.

개요

나의 찾기 앱은 iOS, iPadOS 및 macOS에서 나의 iPhone 찾기 및 나의 친구 찾기를 하나의 단일 앱에 통합한 앱입니다. 나의 찾기는 오프라인 상태인 Mac을 포함한 분실 기기를 찾는데 도움이 됩니다. 온라인 상태인 기기는 iCloud를 통해 위치를 사용자에게 보고할 수 있습니다. 오프라인 상태인 기기의 나의 찾기 기능은 분실 기기가 근처에서 사용 중인 다른 Apple 기기가 감지할 수 있는 단거리 Bluetooth 신호를 보냄으로써 작동합니다. 근처에 있는 기기는 감지된 분실 기기의 위치를 iCloud로 중계하여 사용자가 나의 찾기 앱에서 기기를 찾을 수 있도록 합니다. 이 과정에서 관련된 모든 사용자의 개인정보와 보안은 안전하게 유지됩니다. 나의 찾기는 오프라인이며 잠자기 상태인 Mac에서도 작동합니다.

Bluetooth와 전 세계에서 사용 중인 수억 대의 iOS, iPadOS 및 macOS 기기를 통해 사용자는 Wi-Fi 또는 셀룰러 네트워크에 연결할 수 없는 경우에도 잃어버린 기기를 찾을 수 있습니다. 나의 찾기 설정에서 '오프라인 찾기'가 활성화된 모든 iOS, iPadOS 또는 macOS 기기는 '탐색 기기' 역할을 합니다. 이는 기기가 Bluetooth를 사용하여 오프라인 상태의 다른 분실 기기가 있는지 감지하고, 네트워크 연결을 사용하여 대략적인 위치를 해당 기기의 소유자에게 다시 알릴 수 있음을 의미합니다. 기기에 오프라인 찾기 기능이 활성화되어 있으면 다른 사용자도 같은 방식으로 기기를 찾을 수 있습니다. 이 전체 상호 작용은 종단간 암호화되고 익명으로 처리되며 배터리 및 데이터를 효율적으로 사용하도록 설계되었습니다. 배터리 수명 및 셀룰러 데이터 요금제 사용에 미치는 영향이 최소화되며 사용자 개인정보가 더 안전하게 보호됩니다.

참고: 나의 찾기는 일부 국가 또는 지역에서만 사용할 수 있습니다.

종단간 암호화

나의 찾기는 고급 공개 키 암호화 기술을 기반으로 구축되었습니다. 나의 찾기 설정에서 오프라인 찾기가 활성화되면 EC(Elliptic Curve) P-224 개인 암호화 키 쌍 {d,P}가 기기에서 바로 생성됩니다. **d**는 개인 키이고 **P**는 공개 키입니다. 또한 256비트 비밀 SK_0 및 카운터 $_i$는 0으로 초기화됩니다. 이 개인 키 쌍과 비밀은 Apple로 전송되지 않으며 iCloud 키체인을 사용하여 종단간 암호화 방식으로 사용자의 다른 기기 간에만 동기화됩니다. 비밀과 카운터는 다음과 같은 재귀 구조로 현재 대칭 키 SK_i를 도출하는 데 사용됩니다. $SK_i = KDF(SK_{i-1}, \text{“update”})$.

키 SK_i를 기반으로 두 개의 큰 정수 u_i 및 v_i는 $(u_i,v_i) = KDF(SK_i, \text{“diversify”})$로 계산됩니다. **d**로 표시된 P-224 개인 키와 **P**로 표시된 상응하는 공개 키는 모두 임시 키 쌍을 계산하기 위해 두 정수를 포함하는 아핀 관계를 사용하여 파생됩니다. 파생된 개인 키는 d_i로, $d_i = u_i * d + v_i$(P-224 곡선 순서를 모듈로 연산)이며 상응하는 공개 부분은 P_i이고, $P_i = u_i*P + v_i*G$임을 확인합니다.

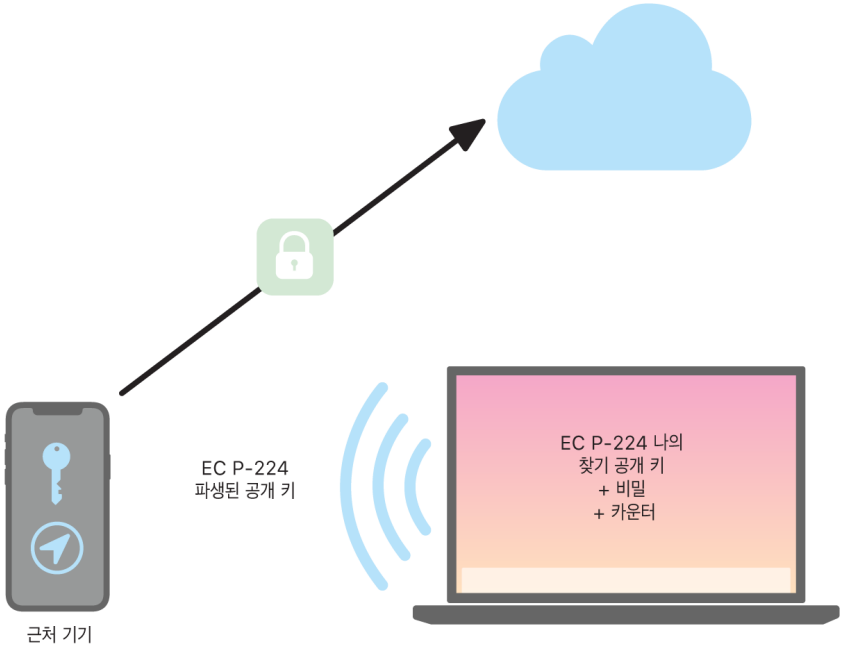
기기를 분실했는데 Wi-Fi 또는 셀룰러에 연결할 수 없는 경우(예: 공원 벤치에 두고 온 MacBook Pro), 파생된 공개 키 P_i를 Bluetooth 페이로드로 제한된 기간 동안 주기적으로 브로드캐스트합니다. P-224를 사용하면 공개 키 표현이 단일 Bluetooth 페이로드에 적합할 수 있습니다. 그런 다음 주변의 기기는 자신의 위치를 공개 키로 암호화하여 오프라인 상태의 기기를 찾는 데 도움을 줄 수 있습니다. 공개 키는 카운터의 증가 값과 위 과정을 사용하여 약 15분마다 새로운 키로 대치되기 때문에 영구 식별자가 사용자를 추적할 수 없습니다. 파생 메커니즘은 동일한 기기에 여러 공개 키 P_i가 연결되는 것을 방지합니다.

사용자 및 기기를 익명으로 유지하기

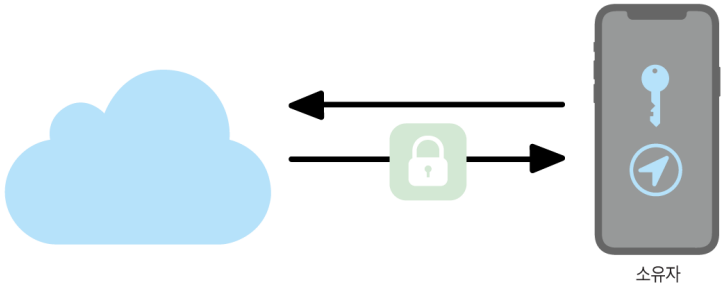
위치 정보 및 기타 데이터가 완전히 암호화되도록 하는 것 외에도 사용자의 신원은 서로에게, 그리고 Apple에게 비공개로 유지됩니다. 탐색 기기가 Apple에 전송한 트래픽은 콘텐츠 또는 헤더에 인증 정보가 없습니다. 결과적으로 Apple은 누구의 기기를 찾았는지, 누가 기기를 찾았는지 알 수 없습니다. 또한 Apple은 탐색 기기의 신원을 나타내는 정보를 기록하지 않으며, 탐색 기기와 소유자를 연관시킬 수 있는 정보를 보유하지 않습니다. 기기 소유자는 누가 기기를 찾았는지 표시하지 않고 나의 찾기 앱에서 암호를 해제하고 표시하는 암호화된 위치 정보만 수신합니다.

나의 찾기 기능을 사용하여 분실한 Apple 기기 찾기

Bluetooth 범위 내의 오프라인 찾기가 활성화된 모든 Apple 기기는 나의 찾기가 허용된 다른 Apple 기기에서 이 신호를 감지하고 현재 브로드캐스트 키 P_i를 읽을 수 있습니다. 브로드캐스트에서의 ECIES 구성 및 공개 키 P_i를 사용하여 탐색 기기는 현재 위치 정보를 암호화하여 Apple에 릴레이합니다. 암호화된 위치는 Bluetooth 페이로드에서 얻은 P-224 공개 키 P_i의 SHA256 해시로 계산되는 서버 인덱스와 연결됩니다. Apple은 암호 해제 키를 가지고 있지 않으므로 Apple은 탐색기가 암호화한 위치를 읽을 수 없습니다. 분실 기기의 소유자는 인덱스를 다시 구성하고 암호화된 위치를 암호화 해제할 수 있습니다.



분실 기기를 찾으려는 경우, 위치 검색 기간 동안 예상되는 카운터 값의 범위가 추정됩니다. 검색 기간의 카운터 값 범위에서 원본 개인 P-224 키 **d**와 비밀 값 Sk_i에 대해 알고 있으면, 소유자는 전체 검색 기간에 대한 값 세트 $\{d_i, SHA256(P_i)\}$를 다시 구성할 수 있습니다. 분실 기기를 찾는 데 사용된 소유자 기기는 인덱스 값 $SHA256(P_i)$을 사용하여 서버에 쿼리를 수행하고 서버에서 암호화된 위치를 다운로드할 수 있습니다. 그런 다음 나의 찾기 앱은 일치하는 개인 키 d_i를 사용하여 암호화된 위치를 로컬에서 암호화 해제하고 분실 기기의 대략적인 위치를 앱에 표시합니다. 소유자의 앱에서 여러 탐색 기기의 위치 리포트를 통합하여 보다 정확한 위치를 생성합니다.



오프라인 상태의 기기 찾기

사용자가 기기에서 나의 iPhone 찾기를 활성화한 경우, iOS 13 이상, iPadOS 13.1 이상 및 macOS 10.15 이상으로 기기를 업그레이드하면 오프라인 찾기가 기본적으로 활성화됩니다. 이렇게 하면 모든 사용자가 기기를 분실했을 때 가장 높은 확률로 기기를 찾을 수 있을 수 있습니다. 하지만 사용자가 참여를 원하지 않으면 언제든지 기기의 나의 찾기 설정에서 오프라인 찾기를 비활성화할 수 있습니다. 오프라인 찾기가 비활성화되면 해당 기기는 더 이상 탐색기 역할을 수행하지 않으며 다른 탐색 기기에서 감지할 수 없습니다. 하지만 기기가 Wi-Fi 또는 셀룰러 네트워크에 연결할 수 있는 상태이면 사용자는 기기를 찾을 수 있습니다.

오프라인 상태의 분실 기기를 찾으면 사용자는 기기를 찾았다는 알림 및 이메일 메시지를 받게 됩니다. 분실 기기의 위치를 보려면 나의 찾기 앱을 열고 기기 탭을 선택합니다. 나의 찾기는 기기를 찾기 전처럼 기기를 빈 지도에 표시하는 대신 대략적인 주소와 이전에 기기가 감지된 시간에 대한 정보가 있는 지도 위치를 표시합니다. 더 많은 위치 리포트를 받으면 현재 위치와 타임스탬프가 모두 자동으로 업데이트됩니다. 사용자는 오프라인 상태의 기기에서 사운드를 재생하거나 기기를 원격으로 지울 수는 없지만, 위치 정보를 사용하여 이동 경로를 다시 추적하거나 기기 복구에 도움이 되는 다른 조치를 취할 수 있습니다.

연속성

연속성 보안 개요

연속성은 iCloud, Bluetooth 및 Wi-Fi 같은 기술을 활용하여 사용자가 한 기기에서 다른 기기로 하던 작업을 계속하고, 전화를 걸거나 받고, 문자 메시지를 주고받으며, 셀룰러 인터넷 연결을 공유할 수 있도록 해줍니다.

Handoff 보안

Apple은 한 기기에서 다른 기기로, 내장 앱과 웹 사이트 간에 Handoff를 안전하게 처리하며, 대용량 데이터 Handoff도 처리합니다.

Handoff가 안전하게 작동하는 방법

Handoff를 사용하면 사용자의 iOS, iPadOS 및 macOS 기기가 서로 가까이에 있을 때 자동으로 한 기기에서 수행 중인 작업을 다른 기기로 전달할 수 있습니다. Handoff를 사용하면 사용자가 기기를 전환하고 즉시 작업을 이어갈 수 있습니다.

사용자가 Handoff를 지원하는 두 번째 기기에서 iCloud에 로그인하면 두 기기가 APNS를 사용하여 BLE(Bluetooth Low Energy) 4.2 대역 외 페어링을 구축합니다. 개별 메시지는 iMessage에서의 메시지와 비슷한 방법으로 암호화됩니다. 기기가 페어링된 후 각 기기는 기기의 키체인에 저장되는 대칭 256비트 AES 키를 생성합니다. 이 키는 BLE 알림을 암호화하고 인증할 수 있습니다. 알림은 재전송 방지책과 함께 GCM 모드의 AES256을 사용하여 기기의 현재 동작을 iCloud와 페어링된 다른 기기에 전달합니다.

기기가 새로운 키에서 처음 알림을 받는 경우, 발신하는 기기에 BLE 연결을 구축하고 알림 암호화 키 교환을 수행합니다. 이 연결은 iMessage 암호화 방법과 비슷한 방법으로 개별 메시지 암호화 방식과 표준 BLE 4.2 암호화 방식을 사용하여 보호됩니다. 일부 경우에 이 메시지는 BLE 대신 APNS를 사용하여 전송됩니다. 동작 페이로드는 iMessage와 동일한 방법으로 보호되고 전송됩니다.

네이티브 앱과 웹 사이트 간의 Handoff

Handoff를 사용하면 iOS, iPadOS 또는 macOS 네이티브 앱에서 앱 개발자가 합법적으로 제어하는 도메인의 웹 페이지에서 사용자 활동을 재개할 수 있습니다. 또한 Handoff를 통해 네이티브 앱 사용자 동작을 웹 브라우저에서 재개할 수도 있습니다.

네이티브 앱이 개발자가 제어하지 않는 웹 사이트를 재개하지 못하도록 하려면 앱이 재개하려는 웹 도메인에 대한 합법적인 제어를 입증해야 합니다. 웹 사이트 도메인을 통한 제어는 공유 웹 자격 증명을 위한 메커니즘을 통해 구축됩니다. 자세한 내용은 저장된 암호에 접근할 수 있는 앱 권한을 참조하십시오. 시스템은 사용자 동작 Handoff를 승인하도록 앱을 허용하기 전에 앱의 도메인 이름 제어가 유효한지 확인해야 합니다.

웹 페이지 Handoff의 소스는 Handoff API를 채택한 어떤 브라우저든 가능합니다. 사용자가 웹 페이지를 볼 때 시스템은 암호화된 Handoff 알림 바이트에서 웹 페이지의 도메인 이름을 알립니다. 사용자의 다른 기기만 알림 바이트의 암호화를 해제할 수 있습니다.

수신하는 기기에서 해당 시스템은 설치된 네이티브 앱이 알려진 도메인 이름에 대해 Handoff를 승인함을 감지하고 해당 네이티브 앱 아이콘을 Handoff 옵션으로 표시합니다. Handoff 실행 시, 네이티브 앱은 전체 URL과 웹 페이지 제목을 받습니다. 하지만 브라우저에서 네이티브 앱으로 다른 정보는 전달되지 않습니다.

반대로 네이티브 앱은 Handoff를 수신하는 기기에 동일한 네이티브 앱이 설치되어 있지 않으면 폴백 URL을 지정할 수도 있습니다. 이 경우, 기본 브라우저가 Handoff API를 사용한다면 시스템은 사용자의 기본 브라우저를 Handoff 앱 옵션으로 표시합니다. Handoff가 요청되면 브라우저가 실행되고 소스 앱이 제공한 폴백 URL을 받게 됩니다. 폴백 URL을 네이티브 앱 개발자가 제어하는 도메인 이름으로 제한해야 한다는 요구 사항은 없습니다.

대용량 데이터 Handoff

Handoff의 기본 기능을 사용하는 것 외에도 일부 앱은 Apple이 만든 피어 투 피어 Wi-Fi 기술을 통해(AirDrop과 흡사) 대용량의 데이터 전송을 지원하는 API도 사용할 수 있습니다. 예를 들어, Mail 앱은 이러한 API를 사용하여 대용량 첨부 파일을 포함한 임시 저장 메일의 Handoff를 지원합니다.

앱이 이런 API를 사용하면 두 기기 간의 교환이 Handoff에서와 마찬가지로 시작됩니다. 그러나 수신하는 기기는 BLE(Bluetooth Low Energy)를 사용하여 초기 페이로드를 받은 후에 Wi-Fi를 통해 새로운 연결을 시작합니다. 이 연결은 TLS로 암호화되며 iCloud 키체인으로 공유된 ID를 통해서 신뢰가 파생됩니다. 그리고 인증서에서 신원을 사용자의 신원과 대조하여 확인합니다. 마지막으로 추가 페이로드 데이터가 전송이 완료될 때까지 이 암호화된 연결을 통해 전송됩니다.

공통 클립보드

공통 클립보드는 Handoff를 활용하여 사용자의 클립보드 콘텐츠를 안전하게 모든 기기에 전송할 수 있어 한 기기에서 복사한 콘텐츠를 다른 기기에서 붙여넣을 수 있는 기능입니다. 콘텐츠는 다른 Handoff 데이터와 동일한 방법으로 보호되며 앱 개발자가 공유를 거부하도록 선택하지 않은 이상 공통 클립보드와 자동으로 공유되도록 기본 설정됩니다.

또한 사용자가 클립보드 데이터를 앱에 붙여넣지 않더라도 앱은 클립보드 데이터에 대한 접근 권한을 가집니다. 공통 클립보드를 사용하면 데이터 접근 권한이 iCloud 로그인을 통해 연결된 사용자의 다른 기기의 앱까지 확대됩니다.

iPhone 셀룰러 통화 릴레이 보안

Mac, iPad 또는 HomePod이 사용자의 iPhone과 동일한 Wi-Fi 네트워크에 있으면 사용자의 iPhone 셀룰러 연결을 사용하여 전화를 걸고 받을 수 있습니다. 구성하려면 기기에서 동일한 Apple ID 계정을 사용하여 iCloud와 FaceTime 모두에 로그인해야 합니다.

수신 통화가 도착하면 설정된 기기 모두에서 APNS(Apple 푸시 알림 서비스)를 통해 알림을 받게 됩니다. 각 알림은 iMessage와 동일한 종단간 암호화를 사용합니다. 동일한 네트워크에 있는 기기들은 수신 통화 알림 사용자 인터페이스를 나타냅니다. 사용자가 전화를 받는 즉시 두 기기 간의 안전한 피어 투 피어 연결을 통해 오디오가 사용자의 iPhone에서 다른 기기로 완벽하게 전송됩니다.

한 기기에서 전화를 받는 경우 가까이에 있는 iCloud로 연결된 기기의 벨소리가 BLE(Bluetooth Low Energy)를 사용한 알림을 받아 바로 꺼집니다. 알림 바이트는 Handoff 알림과 같은 방식을 통하여 암호화됩니다.

발신 통화도 또한 APNS를 통해 iPhone에 릴레이됩니다. 비슷한 방식으로 오디오는 기기 간에 안전한 피어 투 피어 링크를 통해 전송됩니다. 사용자가 FaceTime 설정에서 iPhone 셀룰러 통화를 끔으로써 기기에서 전화 통화 릴레이를 비활성화할 수 있습니다.

iPhone 문자 메시지 전달 보안

문자 메시지 전달 기능을 통해 iPhone에서 받은 SMS 문자 메시지를 사용자의 등록된 iPad 또는 Mac에 자동으로 전송할 수 있습니다. 각 기기는 동일한 Apple ID 계정을 사용하여 iMessage 서비스에 로그인해야 합니다. 사용자의 신뢰 서클 내 기기에 문자 메시지 전달 기능이 켜져 있고 이중 인증이 활성화되어 있는 경우 자동으로 등록됩니다. 또는 iPhone에서 무작위 6자리 숫자 코드가 생성됩니다. 이 코드를 사용하여 각 기기를 등록할 수 있습니다.

기기가 연결된 후 iMessage 보안 개요에서 설명한 방법을 통해 iPhone에서 수신한 SMS 문자 메시지를 암호화하여 각 기기로 전달합니다. 동일한 방법을 통해 iPhone으로 답장을 전송한 다음, iPhone은 이동통신사의 SMS 전송 방식을 사용하여 그 답장을 문자 메시지로 전송합니다. 문자 메시지 전달은 메시지 설정에서 켜거나 끌 수 있습니다.

Instant Hotspot 보안

Instant Hotspot은 다른 Apple 기기를 개인용 iPhone 및 iPad 핫스팟에 연결합니다. Instant Hotspot을 지원하는 iPhone 및 iPad 기기는 BLE(Bluetooth Low Energy)를 사용해 동일한 개인 iCloud 계정 또는 가족 공유를 사용하는 계정으로 로그인한 기기를 찾아 통신합니다(iOS 13 및 iPadOS 필요). OS X 10.10 이상이 설치된 호환되는 Mac 컴퓨터는 동일한 기술을 통해 Instant Hotspot iPhone 및 iPad 기기를 찾아 통신합니다.

사용자가 기기에서 처음으로 Wi-Fi 설정 패널에 들어가는 경우 기기는 BLE 알림을 내보냅니다. 알림은 동일한 iCloud 계정에 로그인된 모든 기기가 인증한 식별자를 포함합니다. 해당 식별자는 DSID(Destination Signaling Identifier)에서 생성됩니다. DSID는 iCloud 계정에 연결되어 있으며 주기적으로 교체됩니다. 동일한 iCloud 계정에 로그인된 다른 기기가 가까이에 있고 개인용 핫스팟을 지원하면 Instant Hotspot을 사용할 수 있음을 나타내는 신호와 응답을 감지합니다.

가족 공유에 포함되어 있지 않은 사용자가 개인용 핫스팟을 사용할 iPhone 또는 iPad를 선택하면 해당 기기가 개인용 핫스팟을 켜도록 요청을 보냅니다. 해당 요청은 BLE 암호화를 사용하여 암호화된 링크를 통해 전송됩니다. 이는 iMessage 암호화와 비슷한 방법입니다. 그런 다음 기기는 개인용 핫스팟 연결 정보와 같은 메시지별 암호화를 사용하여 동일한 BLE 링크를 통해 반응합니다.

가족 공유 구성원인 사용자의 경우, HomeKit 기기에서 정보 동기화를 위해 사용하는 것과 유사한 메커니즘을 사용하여 개인용 핫스팟 연결 정보가 안전하게 공유됩니다. 특히 사용자 간에 핫스팟 정보를 공유하는 연결은 각 기기 전용 Ed25519 공개 키로 인증된 ECDH(Curve25519) 임시 키로 보호됩니다. 사용된 공개 키는 가족 공유가 설정되었을 때 IDS를 사용하여 이전에 가족 공유 구성원 간에 동기화되었던 키입니다.

네트워크 보안

네트워크 보안 개요

Apple 기기에 저장된 데이터를 보호하기 위해 Apple이 사용하는 기본 제공 안전 장치 이외에도, 많은 방책이 마련되어 있어 조직은 기기에서 또는 기기로부터 전송되는 정보를 안전하게 보호할 수 있습니다. 이러한 모든 안전 장치 및 방책은 네트워크 보안에 포함됩니다.

사용자는 세계 어느 곳에서든 기업 네트워크에 접근할 수 있어야 하므로 모바일 사용자가 인증을 받고 사용자의 데이터가 전송 중에 보호되도록 하는 것이 중요합니다. 이러한 보안 목적을 달성하기 위해 iOS, iPadOS, macOS는 Wi-Fi 및 셀룰러 데이터 네트워크 연결의 최신 표준과 입증된 기술을 통합합니다. 이러한 이유로 Apple의 운영 체제는 권한을 부여받고 인증받은 암호화된 통신에 대해 표준 네트워크 프로토콜을 사용하며 개발자에게 접근 권한을 제공합니다.

TLS 보안

iOS, iPadOS 및 macOS는 전송 계층 보안(TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3)과 DTLS(Datagram Transport Layer Security)를 지원합니다. TLS 프로토콜은 AES128 및 AES256을 모두 지원하며 전방향 안정성을 제공하는 암호 모음을 선호합니다. Safari, 캘린더 및 Mail과 같은 인터넷 앱은 자동으로 이 프로토콜을 사용하여 기기와 네트워크 서비스 간의 암호화된 통신 채널을 활성화합니다. CFNetwork와 같은 상위 수준 API는 개발자가 TLS를 앱에 쉽게 적용할 수 있으며 Network.framework와 같은 하위 수준 API는 세부 제어 권한을 제공합니다. CFNetwork는 SSL 3을 허가하지 않으며 Safari와 같은 WebKit를 사용하는 앱은 SSL 3 연결이 금지되어 있습니다.

iOS 11 이상 및 macOS 10.13 이상에서 SHA-1 인증서는 사용자가 신뢰하지 않은 경우 더 이상 TLS 연결을 허용하지 않습니다. 2048비트 미만의 RSA 키를 지닌 인증서도 허용하지 않습니다. RC4 대칭 암호 모음은 iOS 10과 macOS 10.12에서 제거되었습니다. 기본적으로 SecureTransport API로 구현된 TLS 클라이언트 또는 서버는 RC4 암호 모음이 활성화되어 있지 않고 RC4 암호 모음만 사용할 수 있는 경우에는 연결할 수 없습니다. 보안 강화를 위해 RC4를 요구하는 서비스 또는 앱은 안전한 암호 모음을 사용하도록 업그레이드되어야 합니다. iOS 12.1에서, 2018년 10월 15일 이후에 시스템에서 신뢰하는 루트 인증서를 통해 발급받은 인증서에 TLS 연결을 허용하려면 해당 인증서가 '신뢰하는 인증서 투명성' 로그에 기록되어 있어야 합니다. iOS 12.2에서는 Network.framework 및 NSURLSession API에 대해 TLS 1.3이 기본적으로 활성화되어 있습니다. SecureTransport API를 사용하는 TLS 클라이언트는 TLS 1.3을 사용할 수 없습니다.

앱 전송 보안

앱 전송 보안은 기본적인 연결 요구 사항을 제공하여 NSURLConnection, CFURL 또는 NSURLSession API를 사용하는 경우 앱이 보안 연결을 위한 모범 사례를 따르도록 합니다. 기본적으로 앱 전송 보안은 특히 다음과 같이 전방향 안정성을 제공하는 암호 모음만을 포함하도록 암호 선택을 제한합니다.

- 갈루아/카운터 모드(GCM)의 ECDHE_ECDSA_AES 및 ECDHE_RSA_AES
- CBC(암호 블록 체인) 모드

앱에서는 도메인별로 전방향 안정성 요구 사항을 비활성화할 수 있습니다. 비활성화된 경우에는 사용 가능한 암호 세트에 RSA_AES가 추가됩니다.

서버는 반드시 TLS 1.2 및 전방향 안전성을 지원해야 하며, 인증서는 반드시 유효해야 하고, SHA256 또는 더 강력한 최소 2048비트 RSA 키나 256비트 타원곡선 키로 서명되어야 합니다.

앱에서 앱 전송 보안을 덮어쓰지 않는 이상 이러한 요구 사항에 부합하지 않는 네트워크 연결은 실패하게 됩니다. 유효하지 않은 인증서를 사용하는 경우 무조건 실패하게 되고 연결을 잃게 됩니다. 앱 전송 보안은 iOS 9 이상 및 macOS 10.11 이상 버전용으로 컴파일된 앱에 자동으로 적용됩니다.

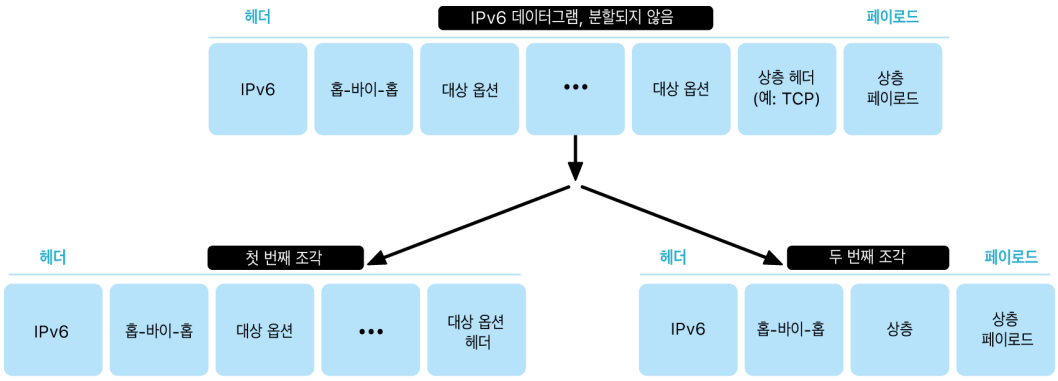
인증 유효성 검사

TLS 인증서의 신뢰 상태 평가는 RFC 5280에 명시된 것과 같이 기존 업계 표준에 따라 수행되며, RFC 6962(인증서 투명성)와 같은 새로운 표준을 통합합니다. iOS 11 이상 및 macOS 10.13 이상에서 Apple 기기는 파기 및 제한된 인증서의 현재 목록으로 주기적으로 업데이트됩니다. 이 목록은 Apple이 신뢰하는 각 내장 루트 인증 기관 및 그 하위 CA 발급 기관이 발급하는 CRL(인증서 해지 목록)에서 취합되었습니다. 또한 이 목록에는 Apple의 재량에 의해 다른 제약이 포함될 수 있습니다. 이 정보는 네트워크 API 기능을 사용하여 보안 연결을 할 때마다 참조됩니다. CA에서 해지한 인증서가 너무 많아 개별적으로 나열할 수 없는 경우, 신뢰도 평가를 위해 OCSP(온라인 인증 상태 응답)가 대신 필요하며 이를 사용할 수 없는 경우, 신뢰도 평가에 실패하게 됩니다.

IPv6 보안

모든 Apple 운영 체제는 IPv6를 지원하며 사용자의 개인정보와 네트워킹 스택 안정성을 보호하기 위해 몇 가지 메커니즘이 구현됩니다. SLAAC(Stateless Address Autoconfiguration)를 사용하면 모든 인터페이스의 IPv6 주소는 네트워크를 통한 기기 추적을 방지하는 동시에 네트워크 변경이 발생하지 않을 때 주소 안정성을 보장하여 우수한 사용자 경험을 제공하는 방식으로 생성됩니다. RFC 3972부터 주소 생성 알고리즘은 암호화로 생성된 주소를 기반으로 합니다. 이것은 인터페이스별 변경자에 의해 확장되어 동일한 네트워크상의 다른 인터페이스도 결국에는 다른 주소를 갖도록 합니다. 그뿐만 아니라 기본 설정 수명이 24시간인 임시 주소가 생성되며 이는 기본적으로 모든 새로운 연결에 사용됩니다. iOS 14, iPadOS 14 및 watchOS 7에 도입된 개인 Wi-Fi 주소 기능에 따라 기기가 연결하는 모든 Wi-Fi 네트워크에 고유한 링크 로컬 주소가 생성됩니다. RFC 7217부터 네트워크의 SSID는 Network_ID 매개 변수와 유사하게 주소 생성을 위한 추가적 요소로 포함됩니다. 이러한 처리 방법은 iOS 14, iPadOS 14 및 watchOS 7에서 사용됩니다.

IPv6 확장 헤더 및 단편화에 기반한 공격을 방지하기 위해 Apple 기기는 RFC 6980, RFC 7112 및 RFC 8021에 명시된 보안 조치를 구현합니다. 여러 방법 중에서도 이는 특히 상층 헤더가 두 번째 조각(아래에 표시됨)에서만 나타나고 이로 인해 상태 정보를 기억하지 않는 패킷 필터와 같은 보안 제어 모호성을 유발할 수 있는 경우의 공격을 방지합니다.



그 밖에도 Apple 운영 체제의 IPv6 스택 신뢰도를 보장하기 위해 Apple 기기는 인터페이스당 프리픽스의 개수 제한과 같이 IPv6 관련 데이터 구조에 다양한 제한을 시행합니다.

VPN(Virtual Private Network) 보안

VPN(Virtual Private Network)과 같은 보안 네트워크 서비스는 일반적으로 최소한의 설정과 구성으로 iPhone, iPad 및 Mac 기기에서 작동합니다.

지원되는 프로토콜

이러한 기기는 다음과 같은 프로토콜 및 인증 방식을 지원하는 VPN 서버와 동작합니다.

- 공유 비밀에서 인증한 IKEv2/IPsec, RSA 인증서, ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서, EAP-MSCHAPv2 또는 EAP-TLS
- App Store의 적절한 클라이언트 앱을 사용한 SSL-VPN
- MS-CHAPV2 암호로 사용자가 인증하거나 공유 비밀로 컴퓨터가 인증하는 L2TP/IPsec(iOS, iPadOS 및 macOS) 및 RSA SecurID 또는 CRYPTOCard(macOS만 해당)
- 암호, RSA SecurID 또는 CRYPTOCard로 사용자가 인증하거나 공유 비밀 및 인증서로 컴퓨터가 인증하는 Cisco IPsec(macOS만 해당)

지원되는 VPN 배포

iOS, iPadOS 및 macOS는 다음을 지원합니다.

- **VPN On Demand:** 인증서 기반 인증을 사용하는 네트워크용으로 VPN 구성 프로파일을 사용해 VPN 연결이 요구되는 도메인을 IT 정책에서 명시할 수 있습니다.
- **Per App VPN:** 더욱 세분화된 기반에서 VPN 연결을 용이하게 하는 용도로 MDM(모바일 기기 관리) 솔루션은 Safari에서 각 관리되는 앱 또는 특정 도메인에 대한 연결을 지정할 수 있습니다. 이렇게 하면 사용자의 개인 데이터를 제외한 안전한 데이터가 기업 네트워크로 전송되고 기업 네트워크에서 발송될 수 있습니다.

iOS 및 iPadOS는 다음을 지원합니다.

- **Always On VPN:** MDM 솔루션을 통해 관리하고 Mac용 Apple Configurator, Apple School Manager, Apple Business Manager 또는 Apple Business Essential을 통해 감독하는 기기 전용입니다. Always On VPN을 통해 사용자는 셀룰러 또는 Wi-Fi 네트워크에 연결할 경우 보안을 활성화하기 위해 VPN을 켤 필요가 없어집니다. 조직은 모든 IP 트래픽을 조직으로 터널링하여 기기 트래픽을 완전히 제어할 수 있습니다. 후속 암호화를 위한 매개 변수 및 키의 기본 교환인 IKEv2는 데이터 암호화를 통해 트래픽 전송을 보호합니다. 조직에서는 조직의 기기에서 받거나 보내는 트래픽을 모니터링 및 필터링하고 조직 네트워크 내의 데이터를 보호하며 기기의 인터넷 연결을 제한할 수 있습니다.

Wi-Fi 보안

무선 네트워크에 대한 보안 연결

모든 Apple 플랫폼은 업계 표준 Wi-Fi 인증 및 암호화 프로토콜을 지원하여 다음과 같은 보안 무선 네트워크에 연결할 때 인증된 접근 및 기밀성을 제공합니다.

- 개인용 WPA2
- 기업용 WPA2
- 전환형 WPA2/WPA3
- 개인용 WPA3
- 기업용 WPA3
- 기업용 WPA3 192비트 보안

WPA2 및 WPA3는 각 연결을 인증하며 128비트 AES 암호화를 제공하여 무선 전송 데이터에 대한 기밀성을 보장합니다. 이는 Wi-Fi 네트워크 연결을 통해 통신할 때, 데이터가 보호될 수 있는 가장 높은 수준의 보안 품질을 사용자에게 제공합니다.

WPA3 지원

WPA3는 다음 Apple 기기에서 지원됩니다.

- iPhone 7 및 이후 모델
- iPad 5세대 및 이후 모델
- Apple TV 4K 및 이후 모델
- Apple Watch Series 3 및 이후 모델
- Mac 컴퓨터(2013년 후반 및 이후 모델, 802.11ac 이상 탑재)

최신 기기는 호환되는 무선 액세스 포인트(AP)에 연결 시 256비트 AES 암호화 지원을 포함하여 기업용 WPA3 192비트 보안 인증을 지원합니다. 이 암호화는 무선으로 전송되는 트래픽에 대해 더욱 강력한 기밀 보호를 제공합니다. 기업용 WPA3 192비트 보안은 모든 iPhone 11 및 이후 모델, iPad 7세대 이상의 모든 iPad 모델 및 Apple Silicon이 탑재된 모든 Mac 컴퓨터에서 지원됩니다.

PMF 지원

Apple 플랫폼은 무선 전송 데이터를 보호하는 것 외에도, 802.11w에 정의된 PMF(Protected Management Frame) 서비스를 통해 WPA2 및 WPA3 수준의 보호를 유니캐스트 및 멀티캐스트 관리 프레임까지 확장합니다. PMF는 다음 Apple 기기에서 지원됩니다.

- iPhone 6 및 이후 모델
- iPad Air 2 및 이후 모델
- Apple TV HD 및 이후 모델
- Apple Watch Series 3 및 이후 모델
- Mac 컴퓨터(2013년 후반 및 이후 모델, 802.11ac 이상 탑재)

802.1X를 지원하여 Apple 기기는 다양하고 폭넓은 RADIUS 인증 환경과 통합됩니다. EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0 및 PEAPv1을 포함한 802.1X 무선 인증 방식을 지원합니다.

플랫폼 보호

Apple 운영 체제는 네트워크 프로세서 펌웨어의 취약성으로부터 기기를 보호합니다. 즉, Wi-Fi가 있는 네트워크 컨트롤러는 응용 프로그램 프로세서 메모리에 대한 접근이 제한됩니다.

- 네트워크 프로세서에 접속하는 데 USB 또는 SDIO(Secure Digital Input Output)를 사용하는 경우, 네트워크 프로세서는 응용 프로그램 프로세서에 DMA(직접 메모리 접근) 트랜잭션을 시작할 수 없습니다.
- PCIe를 사용하는 경우, 각 네트워크 프로세서는 분리된 PCIe 버스에 위치해 있습니다. 각 PCIe 버스에 있는 IOMMU(입력/출력 메모리 관리 유닛)는 네트워크 프로세서의 DMA가 네트워크 패킷과 제어 구조가 들어 있는 메모리 및 리소스에만 접근하도록 것을 제한합니다.

삭제될 프로토콜

Apple 제품은 다음과 같은 삭제 예정의 Wi-Fi 인증 및 암호화 프로토콜을 지원합니다.

- WEP Open(40비트 및 104비트 키)
- WEP Shared(40비트 및 104비트 키)
- Dynamic WEP
- TKIP(Temporal Key Integrity Protocol)
- WPA
- 전환형 WPA/WPA2

이러한 프로토콜은 더 이상 안전하지 않으며 호환성, 안정성, 성능 및 보안상의 이유로 사용하지 않는 것이 좋습니다. 이들은 이전 버전과의 호환성을 위해서만 지원되며 향후 소프트웨어 버전에서 제거될 수 있습니다.

모든 Wi-Fi 구현에 있어서 가능한 한 가장 강력하고 안전하며 호환 가능한 Wi-Fi 연결을 제공하기 위해 개인용 WPA3 또는 기업용 WPA3 로 마이그레이션할 것을 권장합니다.

Wi-Fi 개인정보 보호

MAC 주소 무작위 생성

Wi-Fi 네트워크와 연결되지 않은 상태일 때 Wi-Fi 스캔을 수행하는 경우 Apple 플랫폼은 무작위 MAC 주소(매체 접근 제어)를 사용합니다. 이러한 스캔을 수행해 알려진 Wi-Fi 네트워크를 찾아 연결하거나, 위치 기반 미리 알림 또는 Apple 지도에서 위치 수정 시 지오펜스를 사용하는 앱에 대한 위치 서비스를 지원합니다. 선호하는 Wi-Fi 네트워크에 연결하려고 할 때 수행되는 Wi-Fi 스캔은 무작위가 아닙니다. Wi-Fi MAC 주소 무작위 생성 기능은 iPhone 5 및 이후 모델에서 지원됩니다.

기기가 Wi-Fi 네트워크와 연결된 상태가 아니며 기기의 프로세서가 잠자기 상태일 때 ePNO(향상된 선호하는 네트워크 오프로드) 스캔을 수행하는 경우 Apple 플랫폼은 무작위 MAC 주소를 사용합니다. ePNO 스캔은 지오펜스를 사용하는 앱에 대해 위치 서비스를 사용하는 경우에 실행됩니다(예를 들어 기기가 특정 장소 근처에 있는지 판단하는 위치 기반 미리 알림).

기기의 MAC 주소는 Wi-Fi 네트워크에 연결 해제된 경우에 변경되기 때문에 기기가 셀룰러 네트워크에 연결되어 있더라도 Wi-Fi 트래픽의 수동적 관찰자가 기기를 계속해서 추적하기 위해 MAC 주소를 사용할 수 없습니다. Apple은 Wi-Fi 제조업체에 iOS 및 iPadOS Wi-Fi 스캔은 무작위 MAC 주소를 사용하며 Apple이나 제조업체 모두 이러한 무작위 MAC 주소를 추측할 수 없다고 공지하였습니다.

iOS 14 이상, iPadOS 14 이상 또는 watchOS 7 이상 버전에서 iPhone, iPad 또는 Apple Watch에서 Wi-Fi 네트워크에 연결하는 경우, 네트워크별 고유한 무작위 MAC 주소로 자체 식별합니다. 이 기능은 사용자가 비활성화하거나 Wi-Fi 페이로드의 새로운 옵션을 사용하여 비활성화할 수 있습니다. 특정 상황에서는 기기가 실제 MAC 주소로 돌아갑니다.

자세한 정보는 Apple 지원 문서 iPhone, iPad 및 Apple Watch에서 비공개 Wi-Fi 주소 사용하기를 참조하십시오.

Wi-Fi 프레임 시퀀스 번호 무작위 생성

Wi-Fi 프레임은 저레벨 802.11 프로토콜에서 효과적이고 신뢰할 수 있는 Wi-Fi 통신을 위해 사용되는 시퀀스 번호를 포함합니다. 전송된 각 프레임에서 이러한 시퀀스 번호가 증가하기 때문에 Wi-Fi를 스캔하는 동안 전송된 정보를 동일한 기기에서 전송된 다른 프레임과 연관시키는 데 사용될 수 있습니다.

이를 방지하기 위해 MAC 주소가 새로운 무작위 주소로 변경될 때마다 Apple 기기는 시퀀스 번호를 무작위로 생성합니다. 여기에는 기기가 연결되어 있지 않은 동안에 새로운 스캔 요청마다 시퀀스 번호를 무작위로 생성하는 것이 포함됩니다. 이 무작위 생성은 다음 기기에서 지원됩니다.

- iPhone 7 및 이후 모델
- iPad 5세대 및 이후 모델
- Apple TV 4K 및 이후 모델
- Apple Watch Series 3 및 이후 모델
- iMac Pro 27(Retina 5K, 2017년) 및 이후 모델
- MacBook Pro 13(2018년) 및 이후 모델
- MacBook Pro 15(2018년) 및 이후 모델
- MacBook Air 13(Retina, 2018년) 및 이후 모델
- Mac mini(2018년) 및 이후 모델
- iMac 21.5(Retina 4K, 2019년) 및 이후 모델
- iMac 27(Retina 5K, 2019년) 및 이후 모델
- Mac Pro(2019년) 및 이후 모델

Wi-Fi 연결

Apple은 AirDrop 및 AirPlay에 사용되는 피어 투 피어 Wi-Fi 연결을 위한 무작위 MAC 주소를 생성합니다. 또한 무작위 주소는 iOS 및 iPadOS(SIM 카드 탑재)의 개인용 핫스팟과 macOS의 인터넷 공유에도 사용됩니다.

이러한 네트워크 인터페이스가 시작될 때마다 새로운 무작위 주소가 생성되고, 필요에 따라 각 인터페이스에 대한 고유 주소가 독립적으로 생성됩니다.

가려진 네트워크

Wi-Fi 네트워크는 **SSID(서비스 세트 식별자)**라는 네트워크 이름으로 식별됩니다. 일부 Wi-Fi 네트워크는 SSID를 가리도록 구성되며, 이 경우 무선 액세스 포인트에서 해당 네트워크의 이름을 브로드캐스트하지 않습니다. 이를 **가려진 네트워크**라고 합니다. 네트워크가 가려져 있는 경우, iPhone 6s 및 이후 모델의 기기에서 자동으로 감지합니다. 네트워크가 가려져 있는 경우, iOS 또는 iPadOS 기기는 요청에 포함된 SSID로 프로브를 보내며, 그렇지 않을 경우 보내지 않습니다. 이는 사용자가 이전에 연결했던 가려진 네트워크의 이름을 기기가 브로드캐스트하지 않도록 방지하여 사용자의 개인정보 보호를 확실히 보장합니다.

Bluetooth 보안

Apple 기기에는 Bluetooth Classic과 BLE(Bluetooth Low Energy) 등 두 종류의 Bluetooth가 있습니다. 두 버전의 Bluetooth 보안 모델에는 모두 다음과 같은 고유한 보안 기능이 포함됩니다.

- **페어링:** 하나 이상의 공유 비밀 키를 생성하는 프로세스
- **본딩:** 신뢰하는 기기 쌍을 형성하기 위해 페어링하는 동안 생성된 후속 연결에 사용하는 키를 저장하는 행위
- **인증:** 두 기기가 동일한 키를 가지고 있는지 확인
- **암호화:** 메시지 기밀성
- **메시지 무결성:** 메시지 위조 방지
- **단순 보안 페어링:** 수동 도청 방지 및 중간자 공격 방지

Bluetooth 버전 4.1은 Bluetooth Classic(BR/EDR) 물리적 전송에 보안 연결 기능을 추가했습니다.

각 Bluetooth 유형의 보안 기능은 다음과 같습니다.

지원	Bluetooth Classic	Bluetooth LE
페어링	P-256 타원 곡선	FIPS 승인 알고리즘(AES-CMAC 및 P-256 타원 곡선)
본딩	페어링 정보는 iOS, iPadOS, macOS, tvOS 및 watchOS 장치의 안전한 위치에 저장됨	페어링 정보는 iOS, iPadOS, macOS, tvOS 및 watchOS 장치의 안전한 위치에 저장됨
인증	FIPS 승인 알고리즘(HMAC-SHA256 및 AES-CTR)	FIPS 승인 알고리즘
암호화	컨트롤러에서 수행되는 AES-CCM 암호화 기법	컨트롤러에서 수행되는 AES-CCM 암호화 기법
메시지 무결성	메시지 무결성에 사용되는 AES-CCM	메시지 무결성에 사용되는 AES-CCM
단순 보안 페어링: 수동 도청 방지	ECDHE(Elliptic Curve Diffie-Hellman Exchange Ephemeral)	ECDHE(Elliptic Curve Diffie-Hellman Exchange)
단순 보안 페어링: 중간자(MITM) 공격 방지	두 가지 사용자 지원 숫자 방식: 숫자 비교 및 패스키 입력	두 가지 사용자 지원 숫자 방식: 숫자 비교 및 패스키 입력 모든 비-MITM 페어링 모드를 포함한 페어링에 사용자 응답이 필요함
Bluetooth 4.1 이상	iMac(2015년 후반) 및 이후 모델 MacBook Pro(2015년 전반) 및 이후 모델	iOS 9 이상 iPadOS 13.1 이상 macOS 10.12 이상 tvOS 9 이상 watchOS 2.0 이상
Bluetooth 4.2 이상	iPhone 6 및 이후 모델	iOS 9 이상 iPadOS 13.1 이상 macOS 10.12 이상 tvOS 9 이상 watchOS 2.0 이상

Bluetooth LE 개인정보 보호

사용자 개인정보 보호를 위해 BLE에는 주소 무작위 생성 및 교차 전송 키 파생이라는 두 가지 기능이 포함되어 있습니다.

주소 무작위 생성은 Bluetooth 기기 주소를 자주 변경하여 일정 기간 동안 BLE 기기 추적을 줄이는 기능입니다. 개인정보 보호 기능을 사용하는 기기를 알려진 기기에 다시 연결하려면 **개인 주소**라는 기기 주소를 다른 기기에서 확인할 수 있어야 합니다. 개인 주소는 페어링 진행 중에 교환된 기기의 ID 해결 키를 사용하여 생성됩니다.

iOS 13 이상, iPadOS 13.1 이상에서는 전송 간 링크 키를 파생하는 기능이 있으며 이를 **교차 전송 키 파생**이라고 합니다. 예를 들어, BLE로 생성된 링크 키를 사용하여 Bluetooth Classic 링크 키를 파생할 수 있습니다. 또한 Apple은 Bluetooth Core Specification 버전 4.1(Bluetooth Core Specification 5.1 참조)에 도입된 보안 연결 기능을 지원하는 기기에 대한 BLE 지원에 Bluetooth Classic을 추가했습니다.

iOS의 초광대역 보안

Apple이 설계한 새로운 U1 칩은 공간 인식에 초광대역 기술을 사용합니다. 이 기술로 iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max 및 이후 iPhone 모델에서 U1 칩이 탑재된 다른 Apple 기기를 정확하게 찾을 수 있습니다. 초광대역 기술은 동일한 기술을 사용하여, 지원되는 다른 Apple 기기에서 찾은 데이터를 무작위로 생성합니다.

- MAC 주소 무작위 생성
- Wi-Fi 프레임 시퀀스 번호 무작위 생성

단일 로그인 보안

단일 로그인

iOS 및 iPadOS는 단일 로그인(SSO)을 통해 기업 네트워크 인증을 지원합니다. SSO는 Kerberos 기반 네트워크에서 동작하여 서비스 접근에 허용된 사용자인지 인증합니다. SSO는 Safari 보안 세션에서부터 타사 앱에 이르기까지 수많은 네트워크 활동에 사용될 수 있습니다. 인증서 기반 인증(예: PKINIT) 또한 지원됩니다.

macOS는 Kerberos를 사용하는 기업 네트워크에 대한 인증을 지원합니다. 앱은 Kerberos를 사용하여 서비스 접근에 허용된 사용자인지 인증합니다. 또한 Kerberos는 Safari 보안 세션 및 네트워크 파일 시스템 인증에서부터 타사 앱에 이르기까지 수많은 네트워크 활동에 사용될 수 있습니다. 개발자 API의 앱 채택이 필요하더라도 인증서 기반 인증이 지원됩니다.

iOS, iPadOS 및 macOS SSO는 SPNEGO 토큰과 HTTP 합의 프로토콜을 사용하여 Kerberos 기반 인증 게이트웨이 및 Kerberos 티켓을 지원하는 Windows 통합 인증 시스템과 연동됩니다. SSO 지원은 오픈 소스 Heimdal 프로젝트를 기반으로 합니다.

iOS, iPadOS 및 macOS에서 다음과 같은 암호화 유형이 지원됩니다.

- AES-128-CTS-HMAC-SHA1-96
- AES-256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari가 SSO를 지원하여 표준 iOS 및 iPadOS 네트워크 API를 사용하는 타사 앱이 이를 사용해 구성을 설정할 수 있습니다. SSO를 구성하기 위해 iOS 및 iPadOS는 구성 프로파일 페이로드를 지원하여 MDM(모바일 기기 관리) 솔루션이 필요한 설정을 내려보낼 수 있도록 허용합니다. 이 설정에는 사용자 계정 이름(Active Directory 사용자 계정을 뜻함) 및 Kerberos 영역 설정과 SSO 사용을 허용할 앱 또는 Safari 웹 URL 구성을 포함합니다.

확장형 단일 로그인

앱 개발자는 SSO 확장 프로그램을 사용하여 자체 단일 로그인 구현을 제공할 수 있습니다. SSO 확장 프로그램은 기본 또는 웹 앱이 사용자 인증을 위해 일부 ID 공급자를 사용해야 할 때 호출됩니다. 개발자는 HTTPS로 리디렉션되는 유형과 시도/응답 매커니즘을 사용하는 유형(예: Kerberos)의 두 가지 확장 프로그램 유형을 제공할 수 있습니다. 이를 통해 OpenID, OAuth, SAML2 및 Kerberos 인증 체계를 확장형 단일 로그인에서 지원할 수 있습니다. SSO 확장 프로그램은 macOS 로그인 시 SSO 토큰을 가져오도록 허용하는 기본 SSO 프로토콜을 적용하여 macOS 인증을 지원할 수도 있습니다.

단일 로그인 확장 프로그램을 사용하기 위해 앱은 AuthenticationServices API를 사용하거나 운영 체제에서 제공하는 URL 차단 메커니즘을 사용할 수 있습니다. WebKit 및 CFNetwork는 모든 기본 앱 또는 WebKit 앱에 대한 단일 로그인을 매끄럽게 지원할 수 있는 차단 레이어를 제공합니다. 단일 로그인 확장 프로그램을 호출하려면 관리자가 제공하는 구성을 모바일 기기 관리(MDM) 프로파일을 통해 설치해야 합니다. 또한 리디렉션 유형 확장 프로그램은 관련 도메인 페이로드를 사용하여 지원하는 ID 서버가 자신의 존재를 인식하고 있음을 증명해야 합니다.

운영 체제와 함께 제공되는 유일한 확장 프로그램은 Kerberos SSO 확장 프로그램입니다.

AirDrop 보안

AirDrop을 지원하는 Apple 기기는 Bluetooth LE와 Apple이 만든 피어 투 피어 Wi-Fi 기술을 사용해 파일 및 정보를 근처 기기(AirDrop을 지원하는 iOS 7 이상이 설치된 iOS 기기와 iPad 기기 및 OS X 10.11 이상이 설치된 Mac)에 보낼 수 있습니다. 인터넷 연결 또는 무선 액세스 포인트(AP)를 사용하지 않고 기기 간에 직접 통신하기 위해 Wi-Fi 무선 통신을 사용합니다. 이 연결은 TLS로 암호화됩니다.

AirDrop은 '연락처만'이 공유 기본값으로 설정되어 있습니다. 사용자는 AirDrop에서 '모두'로 설정해 모두와 공유하거나 기능을 완전히 끌 수도 있습니다. 조직에서는 MDM(모바일 기기 관리) 솔루션을 사용해 관리하는 기기 및 앱의 AirDrop 사용을 제한할 수 있습니다.

AirDrop 작동

AirDrop은 iCloud 서비스를 사용하여 사용자 인증을 지원합니다. 사용자가 iCloud에 로그인하면 2048비트 RSA 자격 증명이 기기에 저장되고 사용자가 AirDrop을 활성화하면 사용자의 Apple ID와 연결된 이메일 주소 및 전화번호를 기반으로 축소된 버전의 AirDrop 신원 해시가 생성됩니다.

사용자가 AirDrop을 사용해 항목을 공유하는 경우 전송하는 기기는 축소된 버전의 AirDrop 신원 해시가 포함된 BLE를 통해 AirDrop 신호를 보냅니다. AirDrop이 켜져 있으며 잠자기 상태가 아닌 근처의 다른 Apple 기기는 전송하는 기기가 응답하는 기기의 신원을 찾을 수 있도록 해당 신호를 감지하고 피어 투 피어 Wi-Fi를 사용하여 응답합니다.

'연락처만' 모드에서는 수신된 AirDrop의 축소된 신원 해시를 수신하는 기기의 연락처 앱에 있는 사람의 해시와 비교합니다. 해시가 일치하는 경우, 수신하는 기기는 해당 신원 정보로 피어 투 피어 Wi-Fi를 통해 응답합니다. 일치하는 해시가 없으면 기기가 응답하지 않습니다.

'모두' 모드에서 전반적으로 동일한 프로세스가 사용됩니다. 하지만 기기의 연락처 앱에 일치하는 결과가 없더라도 수신 기기는 응답합니다.

그런 다음, 발신 기기는 피어 투 피어 Wi-Fi를 사용하여 AirDrop 연결을 구축하며 이 연결을 사용하여 전체 신원 해시를 수신 기기로 보냅니다. 전체 신원 해시가 받는 사람의 연락처 앱에 있는 사람의 해시와 일치하는 경우, 수신 기기는 전체 신원 해시로 응답합니다.

해시가 검증되면 받는 사람의 이름과 사진(연락처 앱에 있는 경우)이 전송하는 사람의 AirDrop 공유 시트에 표시됩니다. 이는 iOS 및 iPadOS에서 '사람' 또는 '기기' 섹션에 표시됩니다. 검증되지 않거나 인증되지 않은 장치는 설정 > 일반 > 정보 > 이름에 정의된 기기 이름 및 실루엣 아이콘과 함께 발신자의 AirDrop 공유 시트에 표시됩니다. iOS 및 iPadOS의 경우 AirDrop 공유 시트의 '다른 사람' 섹션에 위치합니다.

그런 다음 발신 사용자가 공유할 상대를 선택할 수 있습니다. 사용자 선택에 따라 전송하는 기기에서는 수신하는 기기와 암호화된 연결(TLS)을 시작하여 iCloud 신원 인증서를 교환합니다. 인증서의 신원은 각 기기의 연락처 앱에서 확인됩니다.

인증서가 확인되면 수신하는 기기에서는 신원이 확인된 사용자 또는 기기에서 전송된 항목을 수신할지를 확인하게 됩니다. 수신자가 여럿일 경우 전송처마다 이 프로세스가 반복됩니다.

iPhone 및 iPad의 Wi-Fi 암호 공유 보안

Wi-Fi 암호 공유를 지원하는 iPhone 및 iPad 기기는 AirDrop이 Wi-Fi 암호를 한 기기에서 다른 기기로 전송하는 것과 유사한 메커니즘을 사용합니다.

사용자가 Wi-Fi 네트워크(요청자)를 선택하고 Wi-Fi 암호에 대한 메시지를 받으면 Apple 기기는 Wi-Fi 암호가 필요하다는 BLE(Bluetooth Low Energy) 알림을 표시합니다. 선택된 Wi-Fi 네트워크의 암호가 있으며 가까운 거리에 있고 잠자기 상태가 아닌 다른 Apple 기기는 BLE를 사용하여 요청하는 기기에 연결합니다.

Wi-Fi 암호(수여자)가 있는 기기는 요청자의 연락처 정보를 요구하며, 요청자는 AirDrop과 유사한 메커니즘을 사용하여 신원을 증명해야 합니다. 신원이 증명된 후 수여자는 요청자에게 암호를 전송합니다. 이는 네트워크에 연결할 때 사용할 수 있습니다.

조직에서는 MDM(모바일 기기 관리) 솔루션을 통해 관리하는 기기 및 앱의 Wi-Fi 암호 공유 사용을 제한할 수 있습니다.

macOS의 방화벽 보안

macOS에는 네트워크 접근 및 서비스 거부 공격으로부터 Mac을 보호하기 위해 내장된 방화벽이 있습니다. 시스템 설정 > 개인정보 보호 및 보안(macOS 13 이상), 시스템 환경설정의 보안 및 개인 정보 보호 패널(macOS 12 또는 이전 버전)로 이동하거나, 수동으로 설치되거나 MDM 솔루션에게서 제공받은 방화벽 페이로드와 함께 구성 프로파일을 사용하여 구성될 수 있습니다. 지원되는 구성은 다음과 같습니다.

- 앱에 관계없이 들어오는 모든 연결 차단.
- 내장 소프트웨어가 들어오는 연결을 자동으로 받도록 허용.
- 다운로드한 소프트웨어 및 서명된 소프트웨어가 들어오는 연결을 자동으로 수신하도록 허용.
- 사용자 지정 앱을 기반으로 한 접근 추가 또는 거부.
- Mac이 ICMP(Internet Control Message Protocol) 프로브 및 포트 스캔 요청에 응답하지 않도록 방지.

개발자 키트 보안

개발자 키트 보안 개요

Apple은 타사 개발자가 Apple 서비스를 확장할 수 있도록 많은 '키트' 프레임워크를 제공합니다. 이러한 프레임워크는 개인정보 보호 및 사용자 보안을 핵심으로 구축됩니다.

- HomeKit
- CloudKit
- SiriKit
- WidgetKit
- DriverKit
- ReplayKit
- ARKit

HomeKit 보안

HomeKit 통신 보안

HomeKit는 iCloud와 기기 보안 기능을 사용하여 Apple에 공개하지 않으면서도 개인 데이터를 보호하고 동기화할 수 있는 홈 자동화 인프라를 제공합니다.

HomeKit 신원 및 보안은 Ed25519 공개-개인 키 쌍을 기반으로 합니다. Ed25519 키 쌍은 사용자의 기기에 생성되며 HomeKit 신원으로 사용됩니다. 키 쌍은 사용자의 Apple 기기 및 HomeKit 액세서리 간 직접 통신을 인증하기 위해 HomeKit 액세서리 프로토콜(HAP)의 일부로 사용됩니다.

홈 허브가 있는 홈의 경우, 공유 홈의 구성원은 이 홈 허브를 통해 액세서리에 명령을 전달할 수 있습니다. 이러한 명령은 Apple Identity Service(IDS)를 사용하여 사용자의 기기에서 홈 허브로 종단간 암호화 및 인증되어 전송되며, 여기에서 HomeKit Accessory Protocol(HAP) 또는 스마트 홈 연결 표준인 Matter를 사용하여 관련 액세서리로 전달됩니다.

키체인에 저장되며 암호화된 키체인 백업에만 포함된 키는 iCloud 키체인을 사용하여 여러 기기에서 최신으로 유지됩니다.

HomeKit 액세서리 간의 통신

HomeKit 액세서리는 자체적으로 Ed25519 키 쌍을 생성해 Apple 기기와 통신합니다. 액세서리가 초기화 설정으로 복원되는 경우 새로운 키 쌍이 생성됩니다.

Apple 기기와 HomeKit 액세서리 간의 관계를 구축하기 위해, 키는 Secure Remote Password(SRP) 프로토콜(3072비트)을 사용하여 교환됩니다. 액세서리 제조업체에서 제공하는 8자리 코드인 키를 사용자의 기기에 입력하면 HKDF-SHA512에서 파생된 키와 함께 ChaCha20-Poly1305 AEAD를 사용하여 암호화됩니다. 액세서리의 MFi 인증은 설정 중에도 확인됩니다. MFi 칩이 탑재되지 않은 액세서리는 iOS 11.3 이상에서 소프트웨어 인증을 지원할 수 있습니다.

사용 중에 기기와 HomeKit 액세서리가 통신하면 위에서 설명한 프로세스를 통해 교환한 키를 사용하여 서로를 인증합니다. 각 세션은 STS(Station-to-Station) 프로토콜을 사용해 구축되며 세션별 Curve25519 키를 기반으로 HKDF-SHA512에서 파생된 키를 사용해 암호화됩니다. 이는 IP 기반 및 BLE(Bluetooth Low Energy) 액세서리에도 적용됩니다.

브로드캐스트 알림을 지원하는 BLE 기기의 경우 보안 세션으로 연결된 기기의 브로드캐스트 암호화 키를 통해 액세서리가 권한 설정됩니다. 이 키는 해당 액세서리의 상태 변경에 대한 데이터를 암호화하는 데 사용되며 이 데이터는 BLE 알림을 통해 알림으로 전송됩니다. 브로드캐스트 암호화 키는 HKDF-SHA512에서 파생된 키이며 데이터는 ChaCha20-Poly1305 AEAD 알고리즘을 사용하여 암호화됩니다. 브로드캐스트 암호화 키는 주기적으로 변경되며 HomeKit 데이터 보안에서 설명한 대로 iCloud를 사용하여 다른 기기에 업데이트됩니다.

Matter 액세서리로 통신하기

Matter 액세서리를 통한 신원 및 보안은 인증서에 기반합니다. Apple 홈의 경우, 신뢰 루트 인증 기관(CA)은 초기 사용자 기기('소유자')에서 생성되며, CA에 대한 개인 키는 해당 iCloud 키체인에 저장됩니다. 홈의 각 Apple 기기는 NIST P256을 사용하여 인증서 서명 요청(CSR)을 생성합니다. 이 CSR은 소유자의 기기에 포함되며,해당 CA 개인 키를 사용하는 기기에 대한 Matter 신원 인증서를 생성합니다. 그러고 나면 이 인증서는 사용자의 기기 및 액세서리 간 통신을 인증하는 데 사용됩니다.

Matter 액세서리는 자체적으로 NIST P256 키 쌍 및 CSR을 생성하며, 액세서리 페어링 중에 CA에서 인증서를 수신합니다. 키 쌍이 생성되기 전에, Matter 액세서리 및 홈 소유자의 기기는 액세서리 제조업체에서 제공하는 PIN을 통한 SPAKE2+ 프로토콜을 사용하여 키를 교환하며, 기기 인증 프로세스가 수행됩니다. 그런 다음 CSR 및 인증서는 AES-CCM 및 HKDF-SHA256에서 파생된 키를 사용하여 암호화된 채널을 통해 교환됩니다. 액세서리가 초기 설정으로 복구될 경우, 새로운 키 쌍 및 CSR이 생성되고, 페어링 중에 액세서리에 대해 새로운 인증서가 발급됩니다.

사용 중에 Apple 기기 및 Matter 액세서리가 통신하면, 각각 자체 인증서를 사용하여 서로를 인증합니다. 각 세션은 3단계(시그마) 프로토콜을 사용해 구축되며 세션별 P256 키를 기반으로 HKDF-SHA256에서 파생된 키를 사용해 암호화됩니다.

Apple 기기가 Matter 액세서리와 안전하게 통신하는 방법에 관한 정보는 Apple Developer 웹 사이트에서 iOS 16의 Matter 지원을 참조하십시오.

HomeKit 및 Siri

액세서리에 쿼리를 보내거나 액세서리를 제어하고 모드를 활성화시키기 위해 Siri를 사용할 수 있습니다. Siri는 홈 구성에 관해 최소한의 정보를 익명으로 제공받습니다. Siri가 명령을 인식하는데 필요한 방, 액세서리 및 모드의 이름이 제공됩니다. Siri에게 전송된 오디오는 특정 액세서리 또는 명령어를 나타낼 수 있지만 Siri 데이터는 HomeKit와 같은 Apple의 다른 기능과는 연결되지 않습니다.

Siri 지원 HomeKit 액세서리

사용자는 Siri 지원 액세서리에서 홈 앱을 사용하여 타이머, 알람, 인터컴 및 초인종과 같은 새로운 Siri 및 기타 HomePod 기능을 활성화할 수 있습니다. 이러한 기능이 활성화될 경우, 액세서리는 이러한 Apple 기능을 호스트하는 로컬 네트워크와 페어링된 HomePod과 함께 조정됩니다. HomeKit 및 AirPlay 프로토콜을 함께 사용하여 암호화된 채널을 통해 기기 간에 오디오가 교환됩니다.

'Siri야' 듣기가 켜져 있을 경우, 액세서리는 자체적으로 실행 중인 트리거 구문 감지 엔진을 사용하여 "Siri야"라는 구문을 듣습니다. 구문을 감지할 경우, 이 엔진은 HomeKit를 사용하여 페어링된 HomePod에 오디오 프레임을 직접 전송합니다. HomePod은 오디오를 다시 확인하고, 만약 구문이 트리거 문구를 포함하지 않을 경우 오디오 세션을 취소합니다.

Touch for Siri가 켜져 있을 경우, 사용자는 액세서리에서 지정 버튼을 눌러 Siri와 대화를 시작할 수 있습니다. 페어링된 HomePod에 오디오 프레임을 직접 전송합니다.

Siri 호출이 성공적으로 감지될 경우, HomePod은 Siri 서버에 오디오를 전송하고 HomePod이 HomePod 자체에 대한 사용자 호출에 적용된 것과 동일한 보안, 개인정보 보호 및 암호화 안전 장치를 사용하여 사용자의 요구를 충족합니다. Siri에 오디오 응답이 있을 경우 Siri 응답이 AirPlay 오디오 채널을 통해 액세서리로 전송됩니다. 일부 Siri 요청은 사용자가 더 많은 옵션을 듣고 싶은지와 같은 추가적인 정보를 요구합니다. 이 경우 액세서리는 사용자에게 메시지를 전달하라는 지시를 받고, 추가적인 오디오가 HomePod에 스트리밍됩니다.

액세서리에는 LED 표시기와 같이 현재 듣고 있음을 사용자에게 알려주는 시각 표시기가 필요합니다. 액세서리는 오디오 스트리밍에 대한 접근을 제외하면 Siri 요청의 목적을 알 수 없으며, 어떤 사용자 데이터도 액세서리에 저장되지 않습니다.

HomeKit 데이터 보안

새로운 HomeKit 아키텍처로 업그레이드(iOS 16.2 및 iPadOS 16.2에서 사용 가능)된 홈의 경우, HomeKit 데이터는 iCloud 및 iCloud 키체인을 사용하는 사용자의 Apple 기기 간에 안전하게 동기화됩니다. 이 과정 중에 HomeKit 데이터는 iCloud 종단간 암호화를 사용하여 암호화되며 Apple은 여기 접근할 수 없습니다.

HomeKit에서 처음으로 홈을 생성한 사용자('소유자')나 편집 권한을 가진 사용자만이 새로운 사용자를 추가할 수 있습니다. 새로운 사용자의 공개 키를 통해 소유자의 기기가 액세서리를 구성하므로 액세서리가 새로운 사용자로부터 인증을 받고 명령을 받을 수 있습니다. 편집 권한을 가진 사용자가 새로운 사용자를 추가하면 작업을 완료하기 위하여 해당 프로세스가 홈 허브로 위임됩니다.

홈 데이터 및 앱

사용자는 개인정보 보호 설정에서 앱의 홈 데이터 접근을 제어할 수 있습니다. 앱이 홈 데이터를 요청하는 경우, 연락처 앱, 사진 앱에 접근하거나 다른 iOS, iPadOS 및 macOS 데이터 소스가 동작하는 방법과 유사하게 사용자에게 접근 승인을 요청합니다. https://developer.apple.com/homekit/에서 HomeKit 개발자 설명서에서 설명하는 것과 같이, 사용자가 승인하는 경우 앱은 방의 이름, 액세서리의 이름, 각 액세서리가 있는 방에 접근할 수 있습니다.

로컬 데이터 저장 공간

HomeKit는 홈, 액세서리, 모드 및 사용자에 대한 정보를 사용자의 Apple 기기에 저장합니다. 이 데이터는 데이터 보호 클래스인 Protected Until First User Authentication을 사용하여 Data Vault에 저장됩니다. HomeKit 데이터는 로컬 백업에서 백업되지 않습니다.

HomeKit를 통한 라우터 보안 향상

사용자는 HomeKit를 지원하는 라우터를 통해 홈 네트워크의 보안을 향상할 수 있습니다. 이 라우터를 사용하면 사용자는 HomeKit 액세서리가 로컬 네트워크 및 인터넷에 대해 가지는 Wi-Fi 접근을 관리할 수 있습니다. 또한 라우터는 PPSK(비공개 PSK) 인증을 지원하여 액세서리별로 전용 키를 사용해 Wi-Fi 네트워크에 해당 액세서리를 추가할 수 있으며 필요한 경우 해지할 수 있습니다. PPSK 인증을 통해 주요 Wi-Fi 암호를 액세서리에 공개하지 않으며, 액세서리의 MAC 주소가 변경되어도 라우터에서 안전하게 식별할 수 있어 보안을 강화할 수 있습니다.

홈 앱을 사용하면 사용자가 다음과 같이 액세서리 그룹의 액세스 제한을 구성할 수 있습니다.

- **제한 없음:** 인터넷 및 로컬 네트워크에 제한 없이 연결할 수 있습니다.
- **자동:** 기본 설정입니다. 액세서리 제조업체에서 Apple에 제공하는 인터넷 사이트 및 로컬 포트 목록에 따라 인터넷 및 로컬 네트워크 접근을 허용합니다. 이러한 목록에는 액세서리가 올바르게 작동하는 데 필요한 모든 사이트 및 포트가 포함됩니다. (리스트가 제공되지 않을 경우 '제한 없음' 상태로 설정됩니다.)
- **홈으로 제한:** HomeKit가 로컬 네트워크에서 액세서리를 찾고 제어하는 데 필요한 연결(홈 허브에서 원격 제어를 지원하기 위한 연결 포함)을 제외하고 인터넷이나 로컬 네트워크에 액세스할 수 없습니다.

PPSK는 HomeKit에서 자동으로 생성되는 액세서리별 개인용 WPA2 암호문구로, 보안에 강력합니다. 액세서리가 나중에 홈에서 제거되면 해지됩니다. PPSK는 홈에서 HomeKit 라우터로 구성된 HomeKit를 통해 액세서리가 Wi-Fi 네트워크에 추가될 때 사용됩니다. 이러한 추가는 Wi-Fi 자격 증명에'홈 앱의 액세서리 설정 화면에서 **관리되는 HomeKit**'로 반영됩니다. 라우터를 추가하기 전에 Wi-Fi 네트워크에 추가된 액세서리는 액세서리가 PPSK를 지원하는 경우 이를 사용하도록 재구성되고 그렇지 않은 경우 기존 자격 증명을 유지합니다.

추가적인 보안책으로 사용자는 라우터 제조업체의 앱을 사용하여 HomeKit 라우터를 구성해야 하며, 이를 통해 앱에서 사용자가 라우터에 액세스할 권한이 있으며, 라우터를 홈 앱에 추가할 수 있는 사용자라는 것을 확인해야 합니다.

HomeKit 카메라 보안

IP 주소(인터넷 프로토콜 주소)를 지닌 HomeKit 카메라는 비디오 및 오디오 스트림에 접근하는 로컬 네트워크 상의 iOS, iPadOS, tvOS 및 macOS 기기로 스트림을 직접 전송합니다. 스트림은 기기와 IP 카메라(인터넷 프로토콜 카메라)에서 무작위로 생성한 키를 사용하여 암호화됩니다. 이 키는 안전한 HomeKit 세션을 통해 카메라로 교환됩니다. 기기가 로컬 네트워크상에 없는 경우 암호화된 스트림은 홈 허브를 통해 기기로 릴레이됩니다. 홈 허브는 기기와 IP 카메라 간에 릴레이하는 기능만 할 뿐 스트림의 암호화를 해제하지 않습니다. 앱이 사용자에게 HomeKit IP 카메라 비디오 보기를 표시하면 HomeKit는 독립된 시스템 프로세스에서 비디오 프레임을 안전하게 렌더링합니다. 이로 인해 해당 앱에서는 해당 비디오 스트림에 접근하거나 스트림을 저장할 수 없습니다. 또한 앱은 이 스트림의 스크린샷을 캡처할 권한이 없습니다.

HomeKit 보안 비디오

HomeKit는 비디오 콘텐츠가 Apple이나 제3자에게 노출되는 일 없이 HomeKit IP 카메라로 클립을 녹화하고, 분석하고, 볼 수 있는 종단간 보안과 비공개 메커니즘을 제공합니다. IP 카메라에서 움직임이 감지되면 홈 허브 역할을 하는 Apple 기기로 직접 비디오 클립이 전송되며, 여기에는 해당 홈 허브 기기와 IP 카메라 간의 전용 로컬 네트워크 연결이 사용됩니다. 로컬 네트워크 연결은 홈 허브와 IP 카메라 간의 HomeKit 세션을 통해 전송된 세션별 HKDF-SHA512에서 파생된 키 쌍으로 암호화됩니다. HomeKit는 중요한 이벤트가 발생할 경우 홈 허브에서 오디오 및 비디오 스트림의 암호화를 해제하여 로컬에서 비디오 프레임을 분석합니다. 중요한 이벤트가 감지되면 HomeKit는 무작위로 생성된 AES256 키로 구성된 AES-256-GCM을 사용해 비디오 클립을 암호화합니다. HomeKit는 또한 각 클립의 포스터 프레임을 생성하며, 이 포스터 프레임은 동일한 AES256 키를 사용하여 암호화됩니다. 암호화된 포스터 프레임과 오디오 및 비디오 데이터는 iCloud 서버에 업로드됩니다. 암호화 키를 포함한 각 클립의 관련 메타데이터는 iCloud 종단간 암호화를 사용하여 CloudKit에 업로드됩니다.

HomeKit는 얼굴 식별을 위해 iCloud 종단간 암호화를 사용하여 특정 인물의 얼굴을 분류하는 데 사용되는 모든 데이터를 CloudKit에 저장합니다. 저장된 데이터에는 이름 등 각 인물에 대한 정보와 해당 인물의 얼굴을 나타내는 이미지가 포함됩니다. 이러한 얼굴 이미지는 사용자의 사진에서 가져오거나(사용자가 선택한 경우) 이전에 분석된 IP 카메라 비디오에서 수집될 수 있습니다. HomeKit 보안 비디오 분석 세션은 이 분류 데이터를 사용하여 IP 카메라로부터 직접 수신하는 보안 비디오 스트림에서 얼굴을 식별하고 앞에서 언급한 클립 메타데이터에 해당 식별 정보를 포함합니다.

카메라의 클립을 보는 데 홈 앱을 사용하면 iCloud에서 데이터가 다운로드되며, 스트림 암호화 해제에 사용된 키의 래핑은 iCloud 종단간 암호화를 사용하여 로컬에서 해제됩니다. 암호화된 비디오 콘텐츠는 서버에서 스트리밍되며 iOS 기기의 로컬에서 암호화를 해제한 후 뷰어에 표시됩니다. 각 비디오 클립 세션은 하위 섹션으로 나뉘어지며, 각 하위 섹션은 고유한 키를 사용하여 콘텐츠 스트림을 암호화합니다.

Apple TV와 HomeKit 보안

HomeKit는 일부 타사 리모컨 액세서리를 Apple TV에 안전하게 연결하고 사용자 프로파일을 홈의 Apple TV 소유자에게 추가하는 것을 지원합니다.

Apple TV에서 타사 리모컨 액세서리 사용하기

일부 타사 리모컨 액세서리는 홈 앱을 통해 추가된 Apple TV에 HID(Human Interface Design) 이벤트 및 Siri 오디오를 제공합니다. 리모컨은 보안 세션을 통해 HID 이벤트를 Apple TV로 전송합니다. 사용자가 Siri 전용 버튼을 사용하여 리모컨의 마이크를 활성화하면 Siri 지원 TV 리모컨이 오디오 데이터를 Apple TV로 전송합니다. 리모컨은 전용 로컬 네트워크 연결을 사용하여 오디오 프레임을 Apple TV로 직접 전송합니다. 로컬 네트워크 연결은 Apple TV와 TV 리모컨 간의 HomeKit 세션을 통해 전송된 키쌍에서 파생된 세션별 HKDF-SHA512로 암호화됩니다. HomeKit는 Apple TV의 오디오 프레임을 암호화 해제하고 오디오 프레임을 Siri 앱으로 전송하며, Siri 앱에서는 오디오 프레임을 모든 Siri 오디오 입력과 동일한 개인정보 보호 방식으로 처리합니다.

HomeKit 홈의 Apple TV 프로파일

HomeKit 홈 사용자가 자신의 프로파일을 홈의 Apple TV 소유자에게 추가하면 TV 프로그램, 음악 및 팟캐스트에 접근할 수 있습니다. Apple TV에서에서 프로파일 사용과 관련된 각 사용자 설정은 iCloud 종단간 암호화를 사용하여 소유자의 iCloud 계정에 공유됩니다. 데이터는 각 사용자의 소유이며, 소유자에게는 읽기 전용으로 공유됩니다. 홈의 각 사용자는 홈 앱에서 이 값을 변경할 수 있으며, 소유자의 Apple TV는 이 설정을 사용합니다.

설정이 켜져 있는 경우 사용자의 iTunes 계정을 Apple TV에서 사용할 수 있습니다. 설정이 꺼져 있는 경우 해당 사용자에 대한 모든 계정 및 데이터가 Apple TV에서 삭제됩니다. 첫 CloudKit 공유는 사용자의 기기에서 시작되며, 보안 CloudKit 공유를 설정하기 위한 토큰은 홈 사용자 간에 데이터를 동기화하는데 사용되는 것과 동일한 보안 채널을 통해 전송됩니다.

iOS, iPadOS 및 watchOS용 SiriKit 보안

Siri는 앱 확장 프로그램 시스템을 사용하여 타사 앱과 통신할 수 있습니다. 기기에서 Siri는 사용자의 연락처 정보 및 기기의 현재 위치에 접근할 수 있습니다. 하지만 Siri가 보호되는 데이터를 앱에 제공하기 전에 앱의 사용자 제어 접근 권한을 확인합니다. 이 권한에 따라 Siri는 사용자가 원래 말한 내용과 관련된 부분만 앱 확장 프로그램으로 전달합니다. 예를 들어, 연락처 정보에 대한 접근 권한이 없는 앱이라면 Siri는 "지불 앱으로 엄마한테 10,000원 지불해"와 같은 사용자 요청이 있는 경우에도 관계 정보를 해당 앱에 제공하지 않습니다. 이 경우에 앱은 '엄마'라는 단어만 볼 수 있습니다.

하지만 사용자가 연락처 정보 접근 권한을 앱에 부여한 경우, 사용자의 엄마에 관해 분석된 정보를 받을 수 있습니다. "오빠가 훌륭해라고 엄마한테 메시지 앱으로 문자 보내"와 같이 관계가 메시지 본문에 언급되는 경우에 Siri는 앱의 접근 허용 여부에 상관없이 '오빠'를 관계 정보로 처리하지 않습니다.

SiriKit 지원 앱은 사용자 연락처의 이름과 같은 앱 전용 또는 사용자 전용 용어를 Siri에 보낼 수 있습니다. 이 정보는 Siri의 음성 인식과 자연어 이해 기능이 해당 앱에서 사용되는 어휘를 인식하도록 하며, 임의의 식별자와 관련이 있습니다. 이러한 사용자 설정 정보는 식별자가 사용되는 동안이나 사용자가 설정에서 앱의 Siri 통합을 비활성화하기 전까지 또는 SiriKit 지원 앱이 제거되기 전까지 사용할 수 있습니다.

"RideShareApp을 사용해서 엄마 집까지 안내해 줘"와 같이 말하는 경우, 해당 요청은 사용자 연락처의 위치 데이터가 필요합니다. Siri는 위치 또는 연락처 정보에 대한 앱의 접근 권한 설정에 관계없이 해당 요청에 대해서만 앱 확장 프로그램에 필요한 정보를 제공합니다.

WidgetKit 보안

WidgetKit는 개발자가 위젯 및 시계 컴플리케이션을 제공하려고 사용하는 프레임워크입니다. 해당 컴플리케이션은 민감한 정보를 표시할 수 있으며 이는 화면 상시표시가 있는 기기에서 특히 잘 보일 수 있습니다.

iOS에서 사용자들은 잠금 화면 또는 화면 상시표시에서 민감한 데이터를 표시할지 여부를 구성할 수 있습니다. 설정 > Face ID 및 암호의 '잠겨 있는 동안 접근 허용'에서 잠금 화면 위젯의 데이터 접근을 비활성화할 수 있습니다.

Apple Watch에서 사용자들은 설정 > 디스플레이 및 밝기 > 화면 상시표시 > 민감한 컴플리케이션 가리기를 선택해 화면 상시표시에서 민감한 데이터를 표시할지 여부를 구성할 수 있습니다. 또한 모든 컴플리케이션 또는 개인 컴플리케이션의 수정된 콘텐츠를 표시할 수 있습니다.

사용자가 비공개 콘텐츠를 가리려는 경우, WidgetKit이 위치 지정자 또는 수정을 렌더링합니다. 수정을 구성하려면 개발자는 다음을 수행해야 합니다.

1. `redacted(reason:)` 콜백을 적용하십시오.

2. `privacy` 속성을 읽으십시오.

3. 사용자 설정 위치 지정자 보기를 제공하십시오.

개발자는 `unredacted()` 보기 변경자로 보기를 수정하지 않은 상태로 렌더링할 수도 있습니다.

예를 들어, 전체 위젯 콘텐츠의 개인정보를 보호해야 하는 경우, 개발자는 개인 보기를 개인정보 보호로 표시하는 대신에 위젯 확장 프로그램에 데이터 보호 기능을 추가할 수 있습니다. 선택한 개인정보 보호 수준과 일치하도록 기기를 잠금 해제할 때까지 WidgetKit는 위젯 콘텐츠 대신에 위치 지정자를 표시합니다. 개발자는 Xcode에서 위젯 확장 프로그램의 데이터 보호 기능을 활성화한 다음, 제공하려는 개인정보 보호 수준에 적합한 값으로 `Data Protection` 권한을 설정해야 합니다.

- `NSFileProtectionComplete`
- `NSFileProtectionCompleteUnlessOpen`

WidgetKit는 기기가 암호로 잠겨 있을 때 이러한 위젯의 콘텐츠를 가리며, 사용자가 기기를 재시동한 후에 인증할 때까지 위치 지정자를 표시합니다. 또한 이러한 iOS 위젯은 Mac에서 iPhone 위젯으로 사용할 수 없습니다.

macOS용 DriverKit 보안

DriverKit는 사용자가 자신의 Mac에 기기 드라이버를 생성하는 것을 개발자가 허용하도록 하는 프레임워크입니다. DriverKit로 구축된 드라이버는 커널 확장 프로그램이 아니라 사용자 공간에서 실행되어 시스템 보안 및 안정성을 향상합니다. 이는 더 쉽게 설치할 수 있도록 하며 macOS의 안정성 및 보안을 향상합니다.

사용자가 앱을 다운로드하기만 하면(시스템 확장 프로그램 또는 DriverKit를 사용할 때 설치 프로그램은 필요하지 않음) 확장 프로그램은 필요할 때에만 활성화됩니다. 이는 /시스템/라이브러리 또는 /라이브러리에 설치하기 위해 관리자 권한이 필요한 여러 사례에서 kexts를 대치합니다.

커널 확장 프로그램이 필요한 보안 앱, 기기 드라이버, 클라우드 저장 공간 솔루션, 네트워킹을 사용하는 IT 관리자는 시스템 확장 프로그램에 구축된 새로운 버전을 사용할 것을 권장합니다. 이러한 새로운 버전은 공격 표면을 줄이면서 Mac에서의 커널 패닉 확률을 크게 감소시킵니다. 이러한 새로운 확장 프로그램은 사용자 공간에서 실행되며 설치에 있어서 특별한 권한을 필요로 하지 않고 번들링 앱이 휴지통으로 이동되면 자동으로 제거됩니다.

DriverKit 프레임워크는 I/O 서비스, 기기 매칭, 메모리 디스크립터 및 디스패치 큐용 C++ 클래스를 제공합니다. 또한 I/O 관련 숫자, 모음, 문자열 유형 및 기타 일반적인 유형을 정의합니다. 사용자는 이를 USBDriverKit 및 HIDDriverKit와 같은 제품군 전용 드라이버 프레임워크와 함께 사용합니다. 시스템 확장 프로그램 프레임워크를 사용하여 드라이버를 설치하고 업그레이드합니다.

iOS 및 iPadOS의 ReplayKit 보안

ReplayKit는 개발자가 앱에 녹화 및 라이브 방송 기능을 추가할 수 있도록 하는 프레임워크입니다. 또한, 사용자가 기기의 전면 카메라와 마이크를 사용하여 녹화 영상과 라이브 방송에 주석을 달 수 있게 합니다.

동영상 녹화

동영상 녹화에는 다음과 같이 여러 가지 보안 계층이 구축되어 있습니다.

- **권한 요청 알림:** 녹화를 시작하기 전에 ReplayKit가 사용자 동의 요청 알림을 나타내 사용자가 화면을 녹화하고 마이크와 전면 카메라를 사용하는 목적을 사용자가 확인하도록 합니다. 이 알림은 앱 프로세스마다 한 번씩 나타나며 앱이 8분 이상 백그라운드에서 실행되는 경우 알림이 다시 나타납니다.
- **화면 및 오디오 캡처:** 화면 및 오디오 캡처는 앱 프로세스가 아닌 ReplayKit의 데몬 replayd에서 이루어집니다. 이로 인해 녹화된 콘텐츠는 앱 프로세스에서 절대 접근할 수 없습니다.
- **앱 내 화면 및 오디오 캡처:** 이는 권한 요청 알림에 의해 보호되는 앱이 비디오 및 샘플 버퍼를 가져오도록 허용합니다.
- **동영상 생성 및 저장:** 동영상 파일은 ReplayKit의 보조 시스템에서만 접근할 수 있는 디렉토리에 작성되며 다른 앱에서는 절대 접근할 수 없습니다. 이 때문에 타사 개발자는 사용자의 동의 없이 녹화 영상을 사용할 수 없습니다.
- **최종 사용자 미리보기 및 공유:** 사용자는 ReplayKit에서 제공된 사용자 인터페이스를 통해 동영상을 미리 보거나 공유할 수 있습니다. 해당 사용자 인터페이스는 iOS 확장 프로그램 인프라를 통해 프로세스 밖에서 제공되며 생성된 동영상 파일에 대한 접근 권한을 가집니다.

ReplayKit 방송

동영상 방송에는 다음과 같이 여러 가지 보안 계층이 구축되어 있습니다.

- **화면 및 오디오 캡처:** 방송 중의 화면 및 오디오 캡처 메커니즘은 `replayd`에서 사용하는 동영상 녹화 메커니즘과 동일합니다.
- **방송 확장 프로그램:** 타사 서비스에서 ReplayKit 방송에 참여하려고 하는 경우 com.apple.broadcast-services 엔드포인트로 구성된 아래와 같은 두 개의 새로운 확장 프로그램을 생성해야 합니다.
  - 사용자가 방송을 설정하도록 하는 사용자 인터페이스 확장 프로그램
  - 비디오 및 오디오 데이터를 서비스의 백엔드 서버로 업로드하는 업로드 확장 프로그램

이 아키텍처는 방송되는 비디오 및 오디오 콘텐츠에 대한 권한을 호스팅 앱에서 가질 수 없도록 합니다. ReplayKit 및 타사 방송 확장 프로그램만 접근할 수 있습니다.

- **방송 선택기:** 방송 선택기로 사용자는 제어 센터를 통해 접근 가능한 동일한 시스템 정의 사용자 인터페이스를 사용하여 앱에서 직접 시스템 방송을 실행할 수 있습니다. 사용자 인터페이스는 프라이빗 API를 통해 구현되며 ReplayKit 프레임워크 내장 확장 프로그램입니다. 또한, 호스팅 앱 외부의 프로세스입니다.
- **업로드 확장 프로그램:** 방송 중에 비디오와 오디오를 처리하기 위해 타사 방송 서비스에서 구현하는 확장 프로그램은 Raw 포맷으로 인코딩되지 않은 샘플 버퍼를 사용합니다. 처리 모드에서 비디오 및 오디오 데이터는 직렬화되어 직접 XPC 연결을 통해 타사 업로드 확장 프로그램에 실시간으로 전달됩니다. 비디오 데이터는 비디오 샘플 버퍼에서 IOSurface 대상체를 추출하여 인코딩된 다음, XPC 개체로 안전하게 인코딩되어 XPC를 통해 타사 확장 프로그램으로 전송되어 다시 IOSurface 대상체로 안전하게 디코딩됩니다.

iOS 및 iPadOS의 ARKit 보안

ARKit는 개발자가 앱이나 게임에서 증강 현실 환경을 제작할 수 있도록 하는 프레임워크입니다. 개발자는 iOS 또는 iPadOS 기기의 전면이나 후면 카메라를 사용하여 2D 또는 3D 요소를 추가할 수 있습니다.

Apple은 개인정보 보호를 염두에 두고 카메라를 설계했으며 타사 앱이 카메라에 접근하려면 반드시 사용자의 동의를 받아야 합니다. iOS 및 iPadOS에서 사용자가 앱에 접근 권한을 부여하면, 해당 앱은 전면 및 후면 카메라의 실시간 영상에 접근할 수 있습니다. 카메라 사용에 투명성이 없는 앱은 카메라를 사용할 수 없습니다.

카메라로 촬영한 사진 및 비디오에는 촬영 날짜, 장소, 심도, 오버캡처와 같은 다른 정보가 포함될 수 있습니다. 사용자가 카메라 앱으로 촬영한 사진과 비디오에 위치 정보를 포함하지 않으려는 경우, 설정 > 개인정보 보호 > 위치 서비스 > 카메라에서 언제든지 이 설정을 변경할 수 있습니다. 사용자가 사진과 비디오를 공유할 때 위치 정보를 포함하지 않으려는 경우, 공유 시트의 옵션 메뉴에서 위치를 끌 수 있습니다.

사용자의 AR 경험을 더 효과적으로 포지셔닝하기 위해 ARKit를 사용하는 앱은 다른 카메라 앱에서 월드 트래킹 또는 얼굴 추적 정보를 사용할 수 있습니다. 월드 트래킹은 물리적 공간에 대한 상대적 위치를 결정하기 위해 사용자 기기에서 알고리즘을 사용하여 이러한 센서 정보를 처리합니다. 지도 앱에서 월드 트래킹은 광학적 방위 감지와 같은 기능을 활성화합니다.

보안 기기 관리

보안 기기 관리 개요

iOS, iPadOS, macOS, tvOS 및 watchOS는 유연한 보안 정책과 쉽게 시행하고 관리할 수 있는 설정을 지원합니다. 이를 통해 회사는 기업 정보를 보호하고 직원들이 개인 기기를 사용하더라도(예: BYOD(개인 기기 사용) 프로그램) 기업의 요구 사항을 준수하도록 할 수 있습니다.

조직은 MDM 솔루션으로 구현된 MDM(모바일 기기 관리) 프레임워크를 사용하여 암호 요구 사항을 적용하고, 설정을 구성하고, 기능을 제한하고, 관리되는 기기에서 기업 데이터를 원격으로 삭제할 수도 있습니다. 이를 통해 직원들이 개인 기기를 사용하여 데이터에 접근할 때에도 기업 데이터를 안전하게 보호할 수 있습니다.

iPhone 및 iPad용 페어링 모델 보안

iOS 및 iPadOS는 페어링 모델을 사용하여 호스트 컴퓨터에서 기기로의 접근을 제어합니다. 페어링은 기기와 그에 연결된 호스트 간에 신뢰 관계를 구축합니다. 연결된 호스트는 공개 키 교환을 통해 나타납니다. 또한 iOS 및 iPadOS는 이 신뢰 관계의 서명을 사용하여 연결된 호스트에서 데이터 동기화와 같은 추가 기능을 사용할 수 있습니다. iOS 9 이상 버전에서는 서비스에 다음과 같은 사항이 적용됩니다.

- 페어링이 필요한 서비스는 사용자가 기기를 잠금 해제한 후에만 시작될 수 있습니다.
- 기기의 잠금이 최근에 해제되지 않으면 서비스가 시작되지 않습니다.
- 사진 동기화 등의 서비스를 시작하려면 기기의 잠금을 해제해야 할 수 있습니다.

페어링 과정을 진행하려면 사용자가 기기를 잠금 해제하고 호스트에서 보낸 페어링 요청을 승인해야 합니다. iOS 9 이상에서 사용자가 암호를 입력하면 호스트 및 기기가 2048비트 RSA 공개 키를 교환 및 저장합니다. 그러면 기기에 저장된 Escrow keybag의 잠금을 해제하는 256비트 키가 호스트에 주어집니다. 교환된 키는 암호화된 SSL 세션을 시작하는 데 사용됩니다. 기기가 보호된 데이터를 호스트로 전송하거나 서비스(iTunes 또는 Finder 동기화, 파일 전송, Xcode 개발 등)를 시작하기 전에 이 세션을 시작해야 합니다. 이 암호화된 세션을 모든 통신에 사용하려면 기기가 Wi-Fi를 통해 호스트에 연결되어야 하므로, 미리 USB를 통해 페어링되어야 합니다. 또한 페어링을 사용하면 여러 진단 기능을 사용할 수도 있습니다. iOS 9에서 페어링 기록이 6개월 이상 사용되지 않았다면 그 기록은 만료됩니다. iOS 11 이상에서는 이 기간이 30일로 줄었습니다.

com.apple.mobile.pcapd와 같은 특정 진단 서비스는 USB를 통해서만 작동할 수 있습니다. 추가적으로 com.apple.file_relay 서비스를 설치하려면 Apple이 서명한 구성 프로파일이 필요합니다. iOS 11 이상에서 Apple TV는 SRP(Secure Remote Password) 프로토콜을 사용하여 무선으로 페어링을 구축할 수 있습니다.

사용자는 '네트워크 설정 재설정 또는 위치 및 개인정보 보호 재설정' 옵션을 사용하여 신뢰하는 호스트 목록을 지울 수 있습니다.

MDM(Mobile Device Management)

MDM(Mobile Device Management) 보안 개요

Apple 운영 체제는 조직에서 배포된 일정 규모의 Apple 기기를 안전하게 구성 및 관리할 수 있도록 해주는 MDM(모바일 기기 관리)을 지원합니다.

MDM이 안전하게 작동하는 방법

MDM 기능은 구성, 무선 등록 및 Apple 푸시 알림 서비스(APNS) 같은 운영 체제 기술을 기반으로 합니다. 예를 들어, APNS는 보안 연결을 통해 직접 MDM 솔루션과 통신할 수 있도록 기기를 깨우고 트리거하는 데 사용됩니다. 기밀 또는 소유권 정보는 APNS을 통해 전송되지 않습니다.

MDM을 사용하여 IT 부서는 기업 또는 교육 환경에 Apple 기기를 등록하고, 무선으로 설정을 구성 및 업데이트하고, 정책 준수 여부를 감독하고, 소프트웨어 업데이트를 관리하며, 관리형 기기를 원격으로 삭제하거나 잠글 수도 있습니다.

iOS 13, iPadOS 13.1 및 macOS 10.15 이상에서 Apple 기기는 '개인 기기 사용' BYOD 프로그램을 위해 특별히 설계된 새로운 사용자 등록 옵션을 지원합니다. 사용자 등록 기능은 관리형 데이터를 암호화하여 따로 저장함으로써 기업 데이터의 보안 수준을 높이면서도 사용자에게 기기에 대한 자율성을 제공합니다. 이는 BYOD 프로그램에 대한 사용자 경험, 보안 및 개인정보 보호의 균형을 유지하는 데 더욱 효과적입니다. 이와 유사한 데이터 분리 메커니즘이 iOS 17, iPadOS 17 및 macOS 14 이상의 계정 기반 기기 등록에 추가되었습니다.

등록 유형

- **사용자 등록:** 사용자 등록은 사용자 소유의 기기용으로 설계되었으며 관리형 Apple ID와 통합되어 기기에 사용자 ID를 설정합니다. 등록을 시작하려면 관리형 Apple ID가 필요하며 사용자가 성공적으로 인증해야 등록이 완료됩니다. 관리형 Apple ID는 사용자가 이미 로그인한 개인 Apple ID와 함께 사용할 수 있습니다. 관리형 앱 및 계정은 관리형 Apple ID를 사용하고 개인 앱 및 계정은 개인 Apple ID를 사용합니다.
- **기기 등록:** 기기 등록을 사용하면 조직은 사용자가 수동으로 기기를 등록하도록 한 다음, 기기 지우기 등 다양한 측면에서 기기 사용을 관리할 수 있습니다. 또한 기기 등록에는 기기에 적용 가능한 더 큰 구성 세트 및 제한이 있습니다. 사용자가 등록 프로파일을 제거하면 해당 등록 프로파일을 기반으로 하는 모든 구성, 설정 및 관리형 앱이 함께 제거됩니다. 사용자 등록과 마찬가지로 기기 등록도 관리형 Apple ID로 통합할 수 있습니다. 이 계정 기반 기기 등록을 사용하면 개인 Apple ID와 함께 관리형 Apple ID를 사용할 수 있으며 기업 데이터를 암호화해 분리합니다.
- **자동 기기 등록:** 자동 기기 등록을 사용하면 조직은 기기를 상자에서 꺼내는 순간부터 기기를 구성하고 관리할 수 있습니다. 이러한 기기를 **감독 중인 기기**라고 하며 사용자가 MDM 프로파일을 제거하지 못하도록 하는 옵션을 선택할 수 있습니다. 자동 기기 등록은 조직 소유의 기기용으로 설계되었습니다.

기기 제한사항

관리자가 제한사항을 활성화하여(일부 경우에는 비활성화) 사용자가 MDM 솔루션에 등록된 iPhone, iPad, Mac, Apple TV 또는 Apple Watch의 특정 앱, 서비스 또는 기능을 이용하지 못하도록 제한할 수 있습니다. 제한사항은 구성의 일부인 제한사항 페이로드에 있는 기기로 전송됩니다. iPhone에서 특정 제한사항은 페어링된 Apple Watch에도 반영됩니다.

암호 설정 관리

기본적으로 iOS, iPadOS, watchOS에서 사용자의 암호는 숫자 PIN으로 설정됩니다. Face ID 또는 Touch ID를 지원하는 iPhone 및 iPad 기기의 기본 암호 길이는 6자리이며, 최소 길이는 4자리입니다. 길고 복잡한 암호는 추측하거나 해킹하기 어렵기 때문에 이를 사용할 것을 권장합니다.

관리자는 MDM을 사용하거나 iOS 및 iPadOS, Microsoft Exchange에서 복잡한 암호 요구 사항 및 기타 정책을 적용할 수 있습니다. macOS 암호 정책 페이로드를 수동으로 설치할 경우, 관리자 암호가 필요합니다. 암호 정책의 경우 특정한 길이의 암호나 특정 조합 또는 속성에 부합하는 암호를 요구합니다.

Apple Watch는 기본적으로 숫자 암호를 사용합니다. 관리형 Apple Watch에 적용된 암호 정책에 숫자가 아닌 문자를 사용해야 하는 경우, 페어링된 iPhone을 사용해 기기를 잠금 해제해야 합니다.

구성 적용

구성은 MDM 솔루션에서 관리형 기기에 대해 정책과 제한사항을 전달 및 관리하는 데 사용하는 기본 방식입니다. 조직이 많은 수의 기기를 구성하려 하거나 많은 수의 기기에 복잡한 맞춤형 이메일 설정, 네트워크 설정 또는 인증서를 전달하려는 경우 구성이 가장 안전한 방식입니다.

구성

구성은 특정 구조를 따르는 XML 프로파일 또는 json 포맷 파일이며 설정 및 승인 정보를 Apple 기기에 로드하는 페이로드로 구성되었습니다. 구성은 설정, 계정, 제한 및 자격 증명 구성을 자동화합니다. 이러한 파일은 MDM 솔루션 또는 Mac용 Apple Configurator에서 생성하거나 수동으로 생성할 수 있습니다. 조직이 구성을 Apple 기기로 보내기 전에 먼저 등록 프로파일을 사용하여 기기를 MDM 솔루션에 등록해야 합니다.

참고: Mac용 Apple Configurator는 iPhone, iPad 및 Apple TV에서 구성 프로파일을 관리할 때만 사용할 수 있습니다.

등록 프로파일

등록 프로파일은 기기에 대해 지정된 MDM 솔루션에 해당 기기를 등록하는 MDM 페이로드가 있는 구성입니다. 이를 통해 MDM 솔루션은 명령 및 구성을 기기에 전송하고 기기의 특정 양상을 쿼리할 수있습니다. 사용자가 등록 프로파일을 제거하면 모든 구성, 설정 및 등록 유형 및 사용된 구성에 따라 해당 등록 프로파일을 기반으로 하는 관리형 앱도 함께 제거됩니다. 기기에는 한 번에 한 개의 등록 프로파일만 존재할 수 있습니다.

예시 구성

구성에는 지정할 수 있는 특정 페이로드의 다음과 같은 설정이 다수 포함되어 있습니다.

- 암호 정책
- 기기 기능 제한(예: 카메라 비활성화)
- 네트워크 및 VPN 설정
- Microsoft Exchange 설정
- Mail 설정
- 계정 설정
- LDAP 디렉토리 서비스 설정
- CalDAV 캘린더 서비스 설정
- 자격 증명 및 ID
- 인증서
- 소프트웨어 업데이트

프로파일 서명 및 암호화

구성 프로파일은 서명하여 출처를 검증하고 암호화하여 무결성을 확인하고 콘텐츠를 보호할 수 있습니다. iOS 및 iPadOS의 구성 프로파일은 3DES 및 AES128을 지원하는 RFC 5652에 지정된 CMS(암호 메시지 구문)를 사용하여 암호화됩니다.

프로파일 설치

구성은 MDM 솔루션을 사용해 기기에 설치하거나 사용자가 직접 설치할 수 있습니다. 또는 Mac용 Apple Configurator를 사용해 iOS, iPadOS 및 tvOS 기기에 구성을 배포할 수 있습니다. 일부 구성은 MDM 솔루션을 사용해 설치해야 합니다. 프로파일을 제거하는 방법에 대한 자세한 정보는 Apple 플랫폼 배포의 모바일 기기 관리 개요를 참조하십시오.

참고: 감독 중인 기기에서는 구성 프로파일도 기기에 잠길 수 있습니다. 이는 구성 프로파일이 제거되는 것을 방지하거나 암호만으로 구성 프로파일 제거를 허용하기 위해 설계되었습니다.

자동 기기 등록

사용자에게 기기를 할당하기 전에 조직은 직접 기기를 만지거나 기기를 먼저 준비할 필요 없이 자동으로 MDM(모바일 기기 관리) 솔루션에 iOS, iPadOS, macOS 및 tvOS 기기를 등록할 수 있습니다. 서비스 중 하나에서 Apple School Manager, Apple Business Manager 또는 Apple Business Essential에 등록한 후, 관리자는 서비스 웹 사이트에 로그인하여 해당 프로그램을 MDM 솔루션에 링크합니다. 그런 다음, 구입한 기기가 MDM을 통해 사용자에게 할당됩니다. 기기 구성 프로세스 중에 기기는 Apple 서버에 할당된 MDM이 있는지 조회하고, 있는 경우 MDM 솔루션에 연결하여 등록을 수행합니다. 자동 기기 등록 및 호환되는 MDM 솔루션을 사용하면 조직에서 다음과 같은 보안 조치를 적용할 수 있습니다.

- 기기를 활성화할 때 Apple 기기의 설정 지원에서 사용자가 초기 설정 단계의 일부로 인증을 수행하도록 설정
- 제한된 접근 권한이 포함되어 있는 임시 구성을 제공하며 민감한 데이터에 접근하는 경우 추가적인 기기 구성 요청
- 기기를 등록하기 전에 최소 운영 체제의 실행 요청
- Mac 컴퓨터에 FileVault 활성화 강제 적용

기기가 MDM으로 등록한 후, 모든 구성, 제한사항 또는 제어 설정이 자동으로 설치됩니다.

기기 설정 지원에서 특정 단계를 제거하면 설정 과정을 더욱 단순하게 만들어 사용자가 기기를 더욱 빠르게 사용할 수도 있습니다. 단계를 건너뛰는 경우, 개인정보 보호 설정이 더 많이 사용됩니다. 예를 들어, 위치 서비스를 구성하는 패널을 건너뛰면 해당 서비스는 설정 지원 중에 활성화되지 않습니다.

관리자는 또한 사용자가 기기에서 MDM 프로파일을 제거할 수 있는지를 제어하고 기기를 사용하는 동안 구성 및 제한사항이 설정되어 있는지 확인할 수도 있습니다.

Apple School Manager, Apple Business Manager 및 Apple Business Essential

Apple School Manager, Apple Business Manager 및 Apple Business Essential은 조직이 직접 Apple에서 구입했거나 프로그램에 참여하는 Apple 공인 대리점 및 이동통신사를 통해 구입한 Apple 기기에 배포할 수 있는 IT 관리자용 서비스입니다.

해당 서비스를 MDM 솔루션과 함께 사용하는 경우 IT 관리자는 사용자를 위한 설정 절차를 단순화하고, 기기 설정을 구성하고, 세 서비스에서 구입한 앱 및 책을 배포할 수 있습니다. Apple School Manager의 경우 직접 또는 SFTP를 사용하여 SIS(Student Information Systems)와 통합할 수 있으며, 세 서비스는 모두 디렉토리 동기화 및 연합 인증을 지원하기 때문에 조직의 신원 제공자(IdP)를 기반으로 계정을 자동으로 권한 설정, 업데이트 및 권한 설정 해제할 수 있습니다.

Apple은 ISO/IEC 27001 및 27018 표준을 준수하는 인증을 유지하여 Apple 고객이 규제 및 계약 의무를 이행할 수 있도록 합니다. 이러한 인증은 고객에게 범위 내의 시스템에 대한 Apple의 개인정보 보호 및 정보 보안 관행에 있어서 독자적 증명을 제공합니다. 자세한 정보는 Apple 플랫폼 인증의 Apple internet services security certifications를 참조하십시오.

참고: 특정 국가 또는 지역에서 Apple 프로그램을 사용할 수 있는지 알아보려면 Apple 지원 문서 교육 기관 및 기업용 Apple 프로그램과 결제 방법의 사용 가능 여부를 참조하십시오.

기기 감독

감독을 통해 일반적으로 기기를 조직에서 소유하고 있음을 나타낼 수 있고, 조직은 기기의 구성 및 제한사항을 추가로 제어할 수 있습니다. 자세한 정보는 Apple 플랫폼 배포의 Apple 기기 감독에 관하여를 참조하십시오.

감독은 자동 기기 등록을 사용할 때 기기에서 자동으로 활성화됩니다.

활성화 잠금 보안

Apple이 활성화 잠금을 시행하는 방법은 해당 기기가 iPhone 또는 iPad인지, Apple Silicon이 탑재된 Mac 또는 Apple T2 보안 칩이 탑재된 Intel 기반 Mac인지에 따라 달라집니다.

iPhone 및 iPad에서의 동작

iPhone 및 iPad 기기에서 활성화 잠금은 iOS 및 iPadOS 설정 지원에서 Wi-Fi 선택 화면 이후의 활성화 절차를 통해 시행됩니다. 기기에서 활성화를 감지하면 Apple 서버에 활성화 인증서를 요청합니다. 활성화 잠금으로 잠긴 기기는 이 시점에서 활성화 잠금을 활성화한 사용자의 iCloud 자격 증명을 입력하도록 사용자에게 요청합니다. iOS 및 iPadOS 설정 지원에서는 유효한 인증서를 받아야만 다음 단계로 이동합니다.

Apple Silicon이 탑재된 Mac에서의 동작

Apple Silicon이 탑재된 Mac의 경우 LLB에서 해당 기기에 유효한 LocalPolicy가 있는지 확인하고 LocalPolicy 정책 재전송 방지 값이 보안 저장 장치 구성 요소에 저장된 값과 일치하는지 확인합니다. 저레벨 부트로더(LLB)는 다음과 같은 경우에 복구용 OS로 시동합니다.

- 현재 사용하는 macOS에 대한 LocalPolicy가 없는 경우
- 해당 macOS에 대해 LocalPolicy가 유효하지 않은 경우
- LocalPolicy 재전송 방지 값이 보안 저장 장치 구성 요소에 저장된 해시 값과 일치하지 않는 경우

복구용 OS에서는 Mac 컴퓨터가 활성화되어 있지 않은지 감지하고 활성화 서버와 통신하여 활성화 인증서를 요청합니다. 기기가 활성화 잠금으로 잠겨 있는 상태라면 복구용 OS에서는 현재의 활성화 잠금을 활성화한 사용자의 iCloud 자격 증명을 입력하도록 사용자에게 요청합니다. 유효한 활성화 인증서를 받으면 활성화 인증서 키를 사용하여 RemotePolicy 인증서를 받습니다. Mac 컴퓨터는 LocalPolicy 키와 RemotePolicy 인증서를 사용하여 유효한 LocalPolicy를 생성합니다. LLB 펌웨어는 유효한 LocalPolicy가 없는 경우 macOS로의 시동을 허용하지 않습니다.

Intel 기반 Mac 컴퓨터에서의 동작

T2 칩이 탑재된 Intel 기반 Mac의 경우 컴퓨터가 macOS로 시동하도록 허용하기 전에 T2 칩 펌웨어가 유효한 활성화 인증서가 있는지 확인합니다. T2 칩에서 로드한 UEFI 펌웨어는 T2 칩으로부터 기기의 활성화 상태를 쿼리하고 유효한 활성화 인증서가 없는 경우에 macOS 대신 복구용 OS로 시동하도록 합니다. 복구용 OS에서는 Mac이 활성화되어 있지 않은지 감지하고 활성화 서버와 통신하여 활성화 인증서를 요청합니다. 기기가 활성화 잠금으로 잠겨 있는 상태라면 복구용 OS에서는 현재의 활성화 잠금을 활성화한 사용자의 iCloud 자격 증명을 입력하도록 사용자에게 요청합니다. UEFI 펌웨어는 유효한 활성화 인증서가 없는 경우 macOS로의 부팅을 허용하지 않습니다.

관리형 분실 모드 및 원격으로 지우기

관리형 분실 모드는 감독 중인 기기가 도난 당한 경우 해당 기기의 위치를 찾기 위해 사용하는 기능입니다. 기기를 찾으면 원격으로 기기를 잠그거나 지울 수 있습니다.

관리형 분실 모드

iOS 9 이상이 설치된 감독 중인 iOS 또는 iPadOS 기기를 분실하거나 도난당한 경우, MDM(모바일 기기 관리) 관리자가 기기에서 원격으로 분실 모드(관리형 분실 모드라고 함)를 활성화할 수 있습니다. 관리형 분실 모드가 활성화되면 현재 사용자가 로그아웃되며 기기는 잠금 해제할 수 없게 됩니다. 기기를 발견하면 연락할 전화번호를 표시하는 것과 같이 관리자가 직접 입력한 메시지를 화면에 표시합니다. 관리자는 또한 해당 기기의 현재 위치를 송신하도록 요청할 수 있습니다(위치 서비스가 꺼져 있는 경우에도 위치 송신 가능). 또한 원하는 경우 사운드도 재생할 수 있습니다. 관리형 분실 모드를 나갈 수 있는 유일한 방법으로는 관리자가 관리형 분실 모드를 끄는 것인데, 이 경우 해당 사용자는 관리형 분실 모드가 꺼진 것을 잠금 화면이나 홈 화면에 표시되는 알림으로 확인할 수 있습니다.

원격으로 지우기

iPhone, iPad, Mac, Apple TV 및 Apple Watch 기기는 관리자가 또는 사용자가 원격으로 지워서 모든 데이터를 읽을 수 없도록 만들 수 있습니다.

MDM이나 iCloud에서 원격으로 지우기 명령을 실행하면 기기는 MDM 솔루션에 명령을 확인하고 삭제를 수행합니다. Microsoft Exchange ActiveSync를 통한 원격 지우기는 기기가 명령을 수행하기 전에 Microsoft Exchange Server를 통해 명령을 확인합니다.

다음 경우에는 원격 지우기를 수행할 수 없습니다.

- 사용자 등록
- 사용자 등록이 설치된 계정에 Microsoft Exchange ActiveSync 사용
- 기기가 감독 중인 기기인 경우에 Microsoft Exchange ActiveSync 사용

사용자는 설정(iPhone 및 iPad) 또는 시스템 설정(Mac)을 사용해 소유하고 있는 지원되는 기기를 지울 수도 있습니다. 그리고 언급한 바와 같이 암호 입력에 여러 번 실패한 경우 iPhone, iPad 및 Apple Watch 기기가 자동으로 지워지도록 설정할 수 있습니다.

즉시 원격 지우기는 Apple Silicon이 탑재된 Mac 컴퓨터 및 Apple T2 보안 칩이 탑재된 Mac 컴퓨터에서 사용할 수 있거나 FileVault가 켜져 있는 경우에 사용 가능합니다. 즉시 원격 지우기는 미디어 키를 안전하게 폐기하는 방법으로 이루어집니다.

iPadOS의 공유 iPad 보안

공유 iPad는 iPad 배포에 사용되는 다중 사용자 모드입니다. 이는 사용자별 문서와 데이터를 계속 구분하는 동시에 iPad를 공유할 수 있도록 합니다. 모든 사용자에게는 각자의 개인용 저장 위치가 할당되며 이는 사용자의 자격 증명으로 보호되는 Apple 파일 시스템(APFS) 볼륨으로 실행됩니다. 공유 iPad를 사용하려면 조직이 발급하고 소유하는 관리형 Apple ID 사용할 필요가 있습니다.

공유 iPad를 사용하면 사용자는 여러 사용자가 사용하도록 구성된 모든 조직 소유 기기에 로그인할 수 있습니다. 사용자의 데이터는 별도의 디렉토리에 분할되어 있습니다. 각 홈 디렉토리는 각자의 데이터 보호 도메인에 있으며 UNIX 권한 및 샌드박스로 보호됩니다. iPadOS 13.4 이상에서 사용자는 임시 세션에도 로그인할 수 있습니다. 사용자가 임시 세션에서 로그아웃하면 사용자의 APFS 볼륨이 삭제되며 할당된 공간은 시스템에 반환됩니다.

공유 iPad에 로그인하기

공유 iPad에 로그인할 때 기본 및 연합 관리형 Apple ID가 모두 지원됩니다. 연합 계정을 처음 사용할 때 사용자는 ID 공급자(IdP)의 로그인 포털로 안내됩니다. 인증이 완료되면 관리형 Apple ID를 백업하기 위해 임시 접근 토큰이 발급되며 기본 관리형 Apple ID 로그인 프로세스와 유사한 로그인 프로세스가 진행됩니다. 로그인하면 공유 iPad의 설정 지원은 기기의 로컬 데이터를 보호하고 향후 로그인 화면을 인증하기 위한 암호(자격 증명)를 설정하라는 메시지를 사용자에게 표시합니다. 사용자가 연합 계정을 사용하여 관리형 Apple ID로 한 번 로그인하고, 이후로는 암호로 기기를 잠금 해제하는 단일 사용자 기기와 마찬가지로, 공유 iPad에서 사용자는 연합 계정을 사용하여 한 번 로그인하고 그 다음부터는 설정된 암호를 사용합니다.

사용자가 연합 인증 없이 로그인하면 관리형 Apple ID는 SRP 프로토콜을 사용하여 Apple IDS(Identity Service)로 인증됩니다. 인증에 성공하면 해당 기기에 특정한 임시 접근 토큰을 부여받습니다. 사용자가 해당 기기를 사용한 적이 있는 경우, 로컬 사용자 계정을 이미 가지고 있으며 동일한 인증서를 사용하여 잠금 해제됩니다.

사용자가 이전에 기기를 사용하지 않았거나 임시 세션 기능을 사용 중인 경우, 공유 iPad는 새로운 UNIX 사용자 ID, 사용자 개인 데이터를 저장하는 APFS 볼륨 및 로컬 키체인을 프로비저닝합니다. APFS 볼륨이 생성될 때 사용자에게 저장 공간이 할당되기 때문에 새로운 볼륨을 생성할 공간이 부족할 수 있습니다. 이러한 경우 시스템은 클라우드에 데이터 동기화를 완료한 기존 사용자를 식별하고 새로운 사용자가 로그인할 수 있도록 기기에서 해당 사용자를 제거합니다. 모든 기존 사용자가 클라우드 데이터 업로드를 완료하지 않은 경우 새로운 사용자는 로그인에 실패합니다. 새로운 사용자가 로그인하려면 한 사용자의 데이터 동기화가 완료될 때까지 기다리거나, 데이터 손실의 위험을 감수하고 관리자가 기존 사용자 계정을 강제로 삭제하도록 요청해야 합니다.

기기가 인터넷에 연결되어 있지 않으면(예: 사용자에게 Wi-Fi 액세스 포인트가 없는 경우) 며칠의 정해진 기한 동안 로컬 계정이 인증될 수 있습니다. 이 경우 기존 로컬 계정 또는 임시 세션이 있는 사용자만 로그인할 수 있으며, 로컬 계정이 있더라도 해당 기한이 지나면 온라인으로 인증해야 합니다.

사용자의 로컬 계정이 잠금 해제되거나 새로 생성된 상태에서 원격으로 인증되었다면 Apple 서버에서 발급한 임시 토큰은 iCloud 로그인을 승인하는 iCloud 토큰으로 변환됩니다. 그런 다음, 사용자의 설정이 복원되고 사용자의 문서와 데이터가 iCloud로부터 동기화됩니다.

사용자 세션이 진행 중이고 기기가 인터넷에 연결되어 있는 경우, 문서 및 데이터가 생성되거나 수정되면 iCloud에 저장됩니다. 또한 해당 사용자가 로그아웃하는 경우, 백그라운드 동기화 메커니즘을 통해 변경 사항을 iCloud나 NSURLSession 배경 세션을 사용하는 기타 웹 서비스로 푸시합니다. 해당 사용자의 백그라운드 동기화가 완료되면 APFS 볼륨은 마운트 해제되며 사용자가 다시 로그인해야만 다시 마운트할 수 있습니다.

임시 세션은 iCloud와 데이터를 동기화하지 않으며, Box 또는 Google Drive와 같은 타사 동기화 서비스에 로그인할 수는 있지만 임시 세션이 종료될 때 데이터를 계속 동기화할 수 있는 기능은 없습니다.

공유 iPad에서 로그아웃하기

사용자가 공유 iPad에서 로그아웃하면 해당 사용자의 User keybag이 즉시 잠기며 모든 앱이 종료됩니다. 새로운 사용자가 로그인할 경우 속도를 높이기 위해 iPadOS는 일부 일반적인 로그아웃 동작을 일시적으로 미루고 새로운 사용자에게 로그인 윈도우를 표시합니다. 이 시간 동안(약 30초) 사용자가 로그인하면 공유 iPad가 새로운 사용자 계정에 로그인하는 과정으로 인해 미뤘던 정리 작업을 수행합니다. 또한 공유 iPad가 대기 상태인 경우 미뤘던 정리 작업을 수행합니다. 다른 로그아웃이 발생할 때와 마찬가지로 이 정리 단계 동안에 로그인 윈도우가 재시작됩니다.

임시 세션이 종료되면, 공유 iPad는 전체 로그아웃 절차를 수행하고 임시 세션의 APFS 볼륨을 즉시 삭제합니다.

Apple Configurator 보안

Mac용 Apple Configurator는 관리자가 USB(또는 Bonjour를 통해 페어링된 tvOS 기기)로 Mac에 연결된 한 대에서 수십 대에 이르는 iOS, iPadOS 및 tvOS 기기를 사용자에게 제공하기 전에 쉽고 빠르게 구성하도록 하는 유연하고 안전한 기기 중심 설계를 갖추고 있습니다. 관리자는 Mac용 Apple Configurator로 소프트웨어를 업데이트하고, 앱과 구성 프로파일을 설치하고, 기기 배경화면을 변경하거나 배경화면의 이름을 변경하고, 기기 정보 및 문서를 내보내는 등의 작업을 수행할 수 있습니다.

Mac용 Apple Configurator는 Apple Silicon 및 Apple T2 보안 칩이 탑재된 Mac 컴퓨터를 되살리거나 복원할 수 있습니다. 이 방법으로 Mac을 되살리거나 복원한 경우, 운영 체제(macOS, Apple Silicon의 복구용 OS 또는 T2용 sepOS)의 최신 마이너 업데이트를 포함하는 파일이 Apple 서버에서 다운로드되고 Mac에 직접 설치됩니다. 성공적으로 되살리거나 복원한 다음, 해당 파일은 Apple Configurator를 실행 중인 Mac에서 삭제됩니다. 사용자는 Apple Configurator 외부에서 이 파일을 검사하거나 사용할 수 없습니다.

또한 관리자는 기기를 Apple, Apple 공인 대리점 또는 공인 이동통신사에서 직접 구입하지 않은 경우에도 Mac용 Apple Configurator 또는 iPhone용 Apple Configurator를 사용하여 기기를 Apple School Manager, Apple Business Manager 및 Apple Business Essential에 추가할 수 있습니다. 관리자가 수동으로 등록된 기기를 설정할 경우, 해당 기기는 이 서비스 중 하나에 등록되고 필수 감독 및 MDM(모바일 기기 관리) 등록을 거친 다른 모든 기기처럼 동작합니다. 직접 구입하지 않은 기기의 경우, 사용자는 30일의 임시 기간 동안 이 서비스 중 하나 또는 감독 및 MDM에서 기기를 제거할 수 있습니다.

조직은 기기를 설정하는 동안 인터넷에 연결된 호스트 Mac에 연결하는 방법으로 Mac용 Apple Configurator를 사용하여 어떤 인터넷 연결도 이루어지지 않은 iOS, iPadOS 및 tvOS 기기를 활성화할 수도 있습니다. 관리자는 Wi-Fi 또는 셀룰러 네트워크에 연결하지 않아도 앱, 프로파일, 문서 등 필요한 구성으로 기기를 복원하고, 활성화하고, 준비할 수 있습니다. 이 기능은 관리자가 테더링되지 않은 활성화 중에 일반적으로 요구되는 기존 활성화 잠금 요구 사항을 우회할 수 없도록 합니다.

스크린 타임 보안

스크린 타임은 성인 및 자녀가 앱, 웹 사이트 등을 사용한 시간을 관리하는 내장 기능입니다. 스크린 타임의 사용자는 성인과 (관리를 받는) 자녀로 나눌 수 있습니다.

스크린 타임은 새로운 시스템 보안 기능은 아니지만 기기 간에 수집 및 공유되는 데이터의 개인정보 보호 및 보안을 스크린 타임이 보호하는 방법에 대해 이해할 필요가 있습니다. 스크린 타임은 iOS 12 이상, iPadOS 13.1 이상, macOS 10.15 이상 및 watchOS 6 이상의 일부 기능에서 사용할 수 있습니다.

아래의 표는 스크린 타임의 주요 기능을 설명합니다.

기능	지원되는 운영 체제
사용 데이터 보기	iOS iPadOS macOS
추가 제한사항 시행	iOS iPadOS macOS watchOS
웹 사용 제한 설정	iOS iPadOS macOS
앱 시간 제한 설정	iOS iPadOS macOS watchOS
다운타임 구성	iOS iPadOS macOS watchOS

자신의 기기 사용을 관리하는 사용자의 경우 스크린 타임 제어 및 사용 데이터는 CloudKit 종단간 암호화를 사용하여 동일한 iCloud 계정에 연결된 기기 간에 동기화될 수 있습니다. 기기 간 동기화를 사용하려면 사용자의 계정에 이중 인증이 활성화되어 있어야 합니다(동기화는 기본적으로 켜져 있음). 스크린 타임은 이전 버전의 iOS 및 iPadOS의 제한 기능 및 이전 버전의 macOS의 유해 콘텐츠 차단 기능을 대체합니다.

iOS 13 이상, iPadOS 13.1 이상 및 macOS 10.15 이상에서 스크린 타임 사용자와 관리되는 자녀는 그들의 iCloud 계정에 이중 인증이 활성화되어 있는 경우, 기기 간의 사용량을 자동으로 공유합니다. 사용자가 Safari 기록을 지우거나 앱을 삭제할 경우, 해당하는 사용 데이터가 해당 기기 및 모든 동기화된 기기에서 제거됩니다.

부모 및 스크린 타임

부모는 iOS, iPadOS 및 macOS 기기에서 스크린 타임을 사용하여 자녀의 사용 내용을 확인하고 제어할 수도 있습니다. 부모가 iCloud 가족 공유에서 가족 대표인 경우, 사용 데이터를 보고 자녀의 스크린 타임 설정을 관리할 수 있습니다. 부모가 스크린 타임을 켜면 자녀에게 알림이 나타나며 자녀도 자신의 사용 내용을 볼 수 있습니다. 부모가 자녀의 스크린 타임을 켠 경우, 자녀가 설정을 변경할 수 없도록 암호를 설정해야 합니다. 성년이 되면(국가 또는 지역에 따라 성년이 되는 나이가 다를 수 있음) 자녀는 이 모니터링을 끌 수 있습니다.

사용 데이터 및 구성 설정은 종단간 암호화된 Apple IDS(Identity Service) 프로토콜을 사용하여 부모와 자녀의 기기 간에 전송됩니다. 암호화된 데이터는 수신 기기에서 읽기 전까지 IDS 서버에 잠시 저장됩니다(예: iPhone 또는 iPad가 꺼져 있다가 켜진 경우). 이 데이터는 Apple이 읽을 수 없습니다.

스크린 타임 분석

사용자가 iPhone 및 Watch 분석 공유를 켜면 Apple이 사용자의 스크린 타임 사용 방식을 이해하는 데 도움이 되는 다음과 같은 익명의 데이터가 수집됩니다.

- 설정 지원을 사용하는 도중 또는 그 이후에 설정에서 스크린 타임 켜짐 여부
- 카테고리 사용에 제한을 생성한 이후 변경 여부(90일 이내)
- 스크린 타임 켜짐 여부
- 다운타임 활성화 여부
- '시간 연장 요청하기' 쿼리가 사용된 횟수
- 앱 시간 제한의 수
- 사용자 유형 및 보기 유형별(로컬, 원격, 위젯)로 스크린 타임 설정에서 사용자가 사용량을 본 횟수
- 사용자 유형별 사용자가 제한을 무시한 횟수
- 사용자 유형별 사용자가 제한을 삭제한 횟수

Apple은 특정한 앱 또는 웹 사용 데이터를 수집하지 않습니다. 사용자가 스크린 타임 사용 정보에서 앱 목록을 볼 때 해당 앱 아이콘을 App Store에서 바로 가져오며 이 요청에서 어떠한 데이터도 저장하지 않습니다.

용어집

고급 암호화 표준(AES) 데이터를 비공개로 유지하기 위해 암호화하는 데 사용되는 글로벌 암호화 표준.

권한 설정 프로파일 iOS 또는 iPadOS 기기에 앱을 설치하고 테스트하도록 허용하는 권한과 항목 세트를 포함하는 Apple이 서명한 .plist 파일(프로퍼티 리스트). 개발 권한 설정 프로파일은 개발자가 임시 배포를 위해 선택한 기기의 목록을 표시합니다. 배포 권한 설정 프로파일은 기업이 개발한 앱의 앱 ID를 포함합니다.

데이터 보호 지원되는 Apple 기기용 파일 및 키체인 보호 메커니즘. 앱이 파일과 키체인 항목을 보호하는 데 사용하는 API를 지칭하기도 합니다.

메모리 컨트롤러 SoC(system on chip)와 SoC(system on chip)의 주 메모리 간의 인터페이스를 제어하는 SoC(system on chip)의 보조 시스템.

미디어 키 안전하고 즉각적인 삭제 기능을 제공하는 암호화 키 계층의 일부. iOS, iPadOS, tvOS, watchOS에서 미디어 키는 데이터 볼륨의 메타데이터를 래핑합니다(따라서 미디어 키가 없으면 파일별 키에 접근할 수 없어 데이터 보호를 통해 보호되는 파일에 액세스할 수 없음). macOS에서 미디어 키는 키 재료, 모든 메타데이터, FileVault로 보호된 볼륨의 데이터를 래핑합니다. 어느 쪽이든 미디어 키를 삭제하면 암호화된 데이터에 액세스할 수 없게 됩니다.

보안 저장 장치 구성 요소 변경이 불가능한 RO 코드, 하드웨어 난수 발생기, 암호화 엔진 및 물리적 변형 감지 기능을 사용하여 설계된 칩입니다. 지원되는 기기의 경우, Secure Enclave가 재전송 방지 값 저장 장치의 보안 저장 장치 구성요소와 연결됩니다. 재전송 방지 값을 읽고 업데이트하기 위해, Secure Enclave 및 저장 장치 칩이 해당 재전송 방지 값에 단독으로 접근하는 보안 프로토콜을 사용합니다. 이 기술에는 보안 보장이 다른 여러 세대가 있습니다.

복구 모드 사용자의 기기를 인식하지 못하는 경우에 여러 Apple 기기를 복원하기 위해 사용하는 모드로서 사용자가 운영 체제를 다시 설치할 수 있도록 합니다.

삭제할 수 있는 저장 장치(Effaceable Storage) NAND 저장 공간의 전용 영역, 암호화 키를 저장하는 데 사용되며 직접 주소를 지정하고 안전하게 삭제됩니다. 공격자가 기기를 물리적으로 소유하는 경우에 보호를 제공하지는 않지만 삭제할 수 있는 저장 장치(Effaceable Storage)에 보관된 키를 키 계층의 부분으로 사용하여 빠른 삭제를 진행하여 전방향 안전성을 제공합니다.

소프트웨어 시드 비트 UID에서 키를 생성할 때 UID에 추가되는 Secure Enclave AES 엔진의 전용 비트. 각 소프트웨어 시드 비트는 그에 해당하는 잠금 비트가 있습니다. 해당하는 잠금 비트가 설정되어 있지 않은 경우 Secure Enclave Boot ROM 및 운영 체제가 독립적으로 각 소프트웨어 시드 비트의 값을 변경합니다. 잠금 비트가 설정되면 소프트웨어 시드 비트와 잠금 비트 모두 수정할 수 없습니다. Secure Enclave가 재시동되면 소프트웨어 시드 비트와 그에 해당하는 잠금이 재설정됩니다.

시스템 보조 프로세서 무결성 보호(SCIP) 보조 프로세서 펌웨어의 변경을 방지하기 위해 설계된 Apple이 사용하는 메커니즘.

시스템 소프트웨어 승인 하드웨어에 내장된 암호화 키와 온라인 서비스를 결합하여, 업그레이드 시 지원되는 기기에 맞는 합법적 Apple 소프트웨어만 제공 및 설치되도록 확인하는 프로세스.

암호 파생 키(PDK) 사용자 암호와 장기 SKP 키 및 Secure Enclave의 UID를 연결하여 파생된 암호화 키.

융선 흐름 각도 매핑 지문의 일부에서 추출한 융선의 방향과 너비의 수학적 표현.

저레벨 부트로더(LLB) 2단계 부트 아키텍처를 사용하는 Mac 컴퓨터에서, LLB는 Boot ROM에 의해 호출되고 차례로 보안 시동 체인의 부분으로 iBoot를 로드하는 코드를 포함합니다.

키 래핑 한 키를 다른 키로 암호화하는 방법. iOS 및 iPadOS는 RFC 3394와 같이 NIST AES 키 래핑을 사용함.

키체인 암호, 키 및 기타 민감한 자격 증명 정보를 저장하고 검색하기 위해 Apple 운영 체제와 타사 앱이 사용하는 인프라와 API 세트.

탱글링 사용자의 암호가 암호화 키로 전환되어 기기의 UID로 강화되는 과정. 이 과정은 무작위 대입 공격은 정해진 기기에서 수행되므로 속도가 제한되어 탱글링과 동시에 수행될 수 없음을 보장합니다. 탱글링 알고리즘은 PBKDF2입니다. PBKDF2는 PRF(의사 난수 함수)로서 각 반복에 대해 기기 UID와 키로 연결된 AES를 사용합니다.

파일 시스템 키 클래스 키를 포함하여 각 파일의 메타데이터를 암호화하는 키. 삭제할 수 있는 저장 장치(Effaceable Storage)에 보관되어 기밀성 유지보다는 빠른 삭제를 진행할 수 있습니다.

파일별 키 파일 시스템에서 파일을 암호화하기 위해 데이터 보호가 사용하는 키. 파일별 키는 클래스 키로 래핑되고 파일의 메타데이터에 저장됨.

AES 암호화 엔진 AES를 구현하는 전용 하드웨어 구성 요소.

AES-XTS 저장 매체를 암호화하는 작업을 의미하는 AES 모드(IEEE 1619-2007에 정의됨).

APNS(Apple 푸시 알림 서비스) 푸시 알림을 Apple 기기에 전달하는 Apple이 제공하는 전 세계적인 서비스.

Apple 보안 포상금 최신 출시 운영 시스템 및 최신 하드웨어(관련이 있는 경우)에 영향을 미치는 취약점을 보고한 연구원에게 Apple에서 주는 보상.

Apple 파일 시스템(APFS) iOS, iPadOS, tvOS, watchOS 및 macOS 10.13 이상을 사용하는 Mac 컴퓨터용 기본 파일 시스템. APFS는 강력한 암호화, 공간 공유, 스냅샷, 빠른 디렉토리 크기 조정 및 향상된 파일 시스템 기본 기능을 제공합니다.

Apple Business Manager 간편한 웹 기반의 IT 관리자용 포털로, Apple이나 프로그램에 참여하는 Apple 공인 대리점 또는 이동통신사를 통해 조직이 직접 구입한 Apple 기기를 빠르고 능률적으로 배포할 수 있는 방법을 제공합니다. 사용자에게 기기를 할당하기 전에 조직은 기기를 직접 조작하거나 먼저 준비할 필요 없이 자동으로 MDM(모바일 기기 관리) 솔루션에 기기를 등록할 수 있습니다.

Apple IDS(Identity Service) 키와 기기 주소를 찾는 데 사용되는 iMessage 공개 키, APNS 주소, 전화번호 및 이메일 주소가 포함된 Apple 디렉토리.

Apple School Manager 간편한 웹 기반의 IT 관리자용 포털로, Apple이나 프로그램에 참여하는 Apple 공인 대리점 또는 이동통신사를 통해 조직이 직접 구입한 Apple 기기를 빠르고 능률적으로 배포할 수 있는 방법을 제공합니다. 사용자에게 기기를 할당하기 전에 조직은 기기를 직접 조작하거나 먼저 준비할 필요 없이 자동으로 MDM(모바일 기기 관리) 솔루션에 기기를 등록할 수 있습니다.

ASLR(Address Space Layout Randomization) 소프트웨어 버그가 공격하기 어렵도록 만드는 운영 체제에 채용된 기술. 메모리 주소와 오프셋을 예측할 수 없게 하여 악성 코드가 이 값을 하드 코드할 수 없습니다.

Boot Camp 지원되는 Mac 컴퓨터에서 Microsoft Windows의 설치를 지원하는 Mac 유틸리티.

Boot ROM 기기가 처음 시동될 때 기기의 프로세서가 실행하는 최초의 코드. 프로세서의 필수불가결한 부분으로서 Apple이나 공격자가 변경할 수 없습니다.

BPR(Boot Progress Register) 소프트웨어가 기기의 부트 모드(DFU(기기 펌웨어 업데이트) 모드 및 복구 모드 등)를 확인하는 데 사용되는 SoC(system on chip) 하드웨어 플래그 세트. BPR 플래그가 설정되면 지울 수 없습니다. 이 플래그는 이후에 소프트웨어가 신뢰할 수 있는 시스템 상태 표시기로 사용됩니다.

CKRecord CloudKit에 저장되거나 CloudKit에서 가져온 데이터가 들어 있는 키 값 쌍의 사전.

Data Vault 요청된 앱 자체가 샌드박스되어 있는지와 관계 없이, 데이터에 대한 무단 접근으로부터 보호하기 위해 커널로 강화된 메커니즘.

DFU(기기 펌웨어 업그레이드) 모드 기기의 Boot ROM 코드가 USB를 통해 복구되도록 대기하는 모드. DFU 모드에서는 화면이 검은색으로 표시되지만 iTunes 또는 Finder를 실행 중인 컴퓨터에 연결하는 즉시 다음 메시지가 표시됩니다. 'Finder(또는 iTunes)가 복구 모드에 있는 (iPhone 또는 iPad)를 발견했습니다. Finder(또는 iTunes)와 함께 사용하기 전에 이 (iPhone 또는 iPad)를 복원해야 합니다.'

DMA(직접 메모리 접근) 하드웨어 하위 시스템이 CPU를 우회하여 주 메모리에 직접 접근할 수 있는 기능.

ECDHE(Elliptic Curve Diffie-Hellman Exchange Ephemeral) 타원 곡선 기반 키 교환 메커니즘. ECDHE는 비밀 키가 두 당사자 간의 메시지를 엿보는 사람에게 노출되지 않도록 차단하는 방식으로 두 당사자가 비밀 키에 대해 동의할 수 있도록 합니다.

ECDSA(Elliptic Curve Digital Signature Algorithm) 타원 곡선 암호화 기반 디지털 서명 알고리즘.

ECID(Exclusive Chip Identification) 각 iPhone 또는 iPad의 프로세서별로 고유한 64비트 식별자.

eSPI(Enhanced Serial Peripheral Interface) 동기식 직렬 통신용으로 설계된 일체형 버스.

Gatekeeper macOS에서 신뢰하는 소프트웨어만이 사용자의 Mac에서 실행되도록 보장하는 기술입니다.

GID(그룹 ID) UID와 비슷하지만 한 클래스의 모든 프로세서에 공통입니다.

HMAC 암호화 해시 기능을 사용한 해시 기반 메시지 인증 코드입니다.

HSM(하드웨어 보안 모듈) 디지털 키 보호 및 관리에 전문화된 변경 방지 컴퓨터.

iBoot 모든 Apple 기기에서 사용 가능한 Stage 2 부트로더. 보안 시동 체인의 부분으로 XNU를 로드하는 코드. SoC(system on chip) 생성에 따라 iBoot는 저레벨 부트로더로 로드되거나 Boot ROM에서 직접 로드될 수 있습니다.

IC(집적 회로) **마이크로칩**으로 알려짐.

IOMMU(입력/출력 메모리 관리 유닛) 입력/출력 메모리 관리 유닛. 다른 입력/출력 기기 및 주변 기기의 주소 공간에 대한 접근을 제어하는 통합 칩의 하위 시스템.

JTAG(Joint Test Action Group) 프로그래머와 회로 개발자들이 사용하는 표준 하드웨어 디버깅 도구.

keybag 클래스 키의 모음을 저장하는 데 사용되는 데이터 구조. 각 유형(User, Device, System, Backup, Escrow 및 iCloud 백업)에는 다음과 같은 동일한 포맷이 있습니다.

헤더에 포함된 내용: 버전(iOS 12 이상에서 4로 설정), 유형(시스템, 백업, 에스크로 또는 iCloud 백업), Keybag UUID, HMAC(Keybag이 서명된 경우), 클래스 키를 래핑하는 데 사용되는 방법(솔트 및 반복 횟수에 따라 UID 또는 PBKDF2를 사용하여 탱글링)

클래스 키의 목록: 키 UUID, 클래스(파일 또는 키체인 데이터 보호), 래핑 유형(UID 파생 키 전용, UID 파생 키와 암호 파생 키), 래핑된 클래스 키, 비대칭 클래스의 공개 키

MDM(모바일 기기 관리) 관리자가 등록된 기기를 원격으로 관리할 수 있는 서비스. 기기가 등록되면 관리자는 네트워크를 통해 MDM 서비스를 사용하여 설정을 구성하고 사용자 상호 작용 없이 기기에서 다른 작업을 수행할 수 있습니다.

NAND 비휘발성 플래시 메모리.

sepOS L4 마이크로커널의 Apple 맞춤형 버전을 기반으로 하는 Secure Enclave 펌웨어.

SKP(봉인 키 보호) 시스템 소프트웨어의 측정값 및 하드웨어에만 있는 키(예: Secure Enclave의 UID)로 암호화 키를 보호하거나 또는 **봉인**하는 데이터 보호 기술.

SoC(system on chip) 여러 구성요소를 단일 칩으로 통합한 집적 회로(IC). 응용 프로그램 프로세서, Secure Enclave 및 기타 보조 프로세서는 SoC의 구성요소입니다.

SSD 컨트롤러 저장 매체(SSD)를 관리하는 하드웨어 보조 시스템.

UEFi(Unified Extensible Firmware Interface) 펌웨어 펌웨어와 컴퓨터의 운영 체제를 연결하는 BIOS 대체 기술.

UID(고유 ID) 제조 시 각 프로세서에 각인되는 256비트 AES 키. 펌웨어나 소프트웨어가 읽을 수 없고 프로세서의 하드웨어 AES 엔진만 사용할 수 있습니다. 실제 키를 받기 위해 공격자는 프로세서의 실리콘에 대해 매우 복잡하고 고가의 물리적 공격을 마운트해야 합니다. UID는 UDID 뿐만 아니라 기기의 모든 식별자와 관련이 없습니다.

URI(Uniform Resource Identifier) 웹 기반의 리소스를 식별하는 문자 스트링.

xART eXtended Anti-Replay Technology의 약자. 물리적 저장 장치 아키텍처를 기반으로 하는 재전송 방지 기능을 통해 Secure Enclave에 대해 암호화되고 인증된 영구 저장 장치를 제공하는 서비스 집합입니다. 보안 저장 장치 구성 요소를 참조하십시오.

XNU Apple 운영 체제의 핵심 커널. 신뢰받는 것으로 간주되어 코드 서명, 샌드박스, 권한 검사 및 ASLR(Address Space Layout Randomization) 같은 보안책을 시행합니다.

XProtect macOS의 서명 기반 악성 코드 탐지 및 제거용 내장 안티바이러스 기술.

문서 수정 내역

문서 수정 내역

2024년 5월

추가된 주제:

- spih(Cryptex1 Image4 매니페스트 해시)
- stng(Cryptex1 생성)
- 메시지 앱 및 IDS용 BlastDoor
- 차단 모드 보안
- App Store 보안에 관하여
- WidgetKit 보안

업데이트된 주제:

- Apple 플랫폼 보안 소개
- Apple SoC 보안
- Secure Enclave
- Face ID, Touch ID, 암호
- 얼굴 인식 보안
- Face ID 및 Touch ID의 용도
- 여분의 전원으로 익스프레스 카드 사용
- 운영 체제 무결성
- 안전하게 데이터 연결 활성화하기
- iPhone 및 iPad의 액세서리 확인하기
- watchOS의 시스템 보안
- 암호
- 데이터 보호 개요
- 데이터 보호용 Keybag
- 대체 시동 모드에서의 보호 키
- 공격에 대한 사용자 데이터 보호
- macOS에서 FileVault 관리

- iOS 및 iPadOS의 앱 보안 개요
- macOS의 Gatekeeper 및 런타임 보호
- 관리형 Apple ID 보안
- iCloud 암호화
- 계정 복구 연락처 보안
- 유산 관리자 보안
- iCloud 키체인 보안 개요
- 키체인 동기화 보안
- iCloud 키체인용 에스크로 보안
- 카드 권한 설정 보안 개요
- Apple Pay에 신용 카드 또는 체크 카드 추가하기
- Apple Pay를 사용하여 카드로 결제하기
- Apple Card 보안
- Tap to Pay on iPhone 보안
- Apple 지갑을 사용한 접근
- 액세스 키 유형
- Apple 지갑의 ID
- Apple 지갑 ID의 보안
- 개발자 키트 보안 개요
- HomeKit 통신 보안
- MDM(Mobile Device Management) 보안 개요
- 구성 적용

2022년 12월

추가된 주제:

- iCloud용 고급 데이터 보호

업데이트된 주제:

- iCloud 보안 개요
- iCloud 암호화
- iCloud 백업의 보안
- 계정 복구 연락처 보안
- 유산 관리자 보안

2022년 5월

다음에 대한 내용이 업데이트됨:

- iOS 15.4
- iPadOS 15.4
- macOS 12.3
- tvOS 15.4
- watchOS 8.5

추가된 주제:

- 페어링된 복구용 OS 제한 사항
- LOVE(Local Operating System Version)
- 건강 공유
- 계정 복구 연락처 보안
- 유산 관리자 보안
- Tap to Pay on iPhone 보안
- Apple 지갑을 사용한 접근
- 액세스 키 유형
- Apple 지갑의 ID
- Siri 지원 HomeKit 액세서리

업데이트된 주제:

- Touch ID가 탑재된 Magic Keyboard
- Face ID, Touch ID, 암호
- 얼굴 인식 보안
- 여분의 전원으로 익스프레스 카드 사용
- Apple Silicon이 탑재된 Mac의 시동 모드
- Apple Silicon이 탑재된 Mac용 LocalPolicy 파일의 콘텐츠
- 서명된 시스템 볼륨 보안
- watchOS의 시스템 보안
- Apple 보안 리서치 기기
- Apple 파일 시스템의 역할
- 사용자 데이터에 대한 앱 접근 방지
- macOS의 앱 보안 개요
- macOS에서의 악성 코드로부터 보호
- iCloud 보안 개요
- 키체인 동기화 보안
- iCloud 키체인 복구 보안
- Apple Pay를 사용하여 카드로 결제하기

- Apple Pay의 비접촉식 패스
- Apple Pay로 카드 사용 불가능 상태
- Apple Card 신청
- Apple Cash 보안
- Apple 지갑에 교통 카드 및 전자머니 카드 추가하기
- 보안된 Apple Messages for Business
- FaceTime 보안
- iOS의 차 키 보안
- Apple Configurator 보안

제거된 주제:

- HomeKit 액세서리 및 iCloud

2021년 5월

다음에 대한 내용이 업데이트됨:

- iOS 14.5
- iPadOS 14.5
- macOS 11.3
- tvOS 14.5
- watchOS 7.4

추가된 주제:

- Touch ID가 탑재된 Magic Keyboard.
- Secure Enclave에 대한 보안 의사 및 연결.
- 자동 잠금 해제 및 Apple Watch.
- CustomOS Image4 Manifest Hash(coih).

업데이트된 주제:

- 여분의 전원으로 익스프레스 카드 사용에 두 가지 새로운 익스프레스 모드 거래 방식을 추가함.
- Secure Enclave 기능 요약을 편집함.
- smb3(보안 멀티 시동)에 소프트웨어 업데이트 콘텐츠를 추가함.
- SKP(봉인 키 보호)에 콘텐츠를 추가함.

2021년 2월

다음에 대한 내용이 업데이트됨:

- iOS 14.3
- iPadOS 14.3
- macOS 11.1
- tvOS 14.3
- watchOS 7.2

추가된 주제:

- 메모리 안전 iBoot 구현
- Apple Silicon이 탑재된 Mac의 시동 프로세스
- Apple Silicon이 탑재된 Mac의 시동 모드
- Apple Silicon이 탑재된 Mac의 시동 디스크 보안 정책 제어
- LocalPolicy 서명 키 생성 및 관리
- Apple Silicon이 탑재된 Mac용 LocalPolicy 파일의 콘텐츠
- 서명된 시스템 볼륨 보안
- Apple 보안 리서치 기기
- 암호 모니터링
- IPv6 보안
- iOS의 차 키 보안

업데이트된 주제:

- Secure Enclave
- 하드웨어 마이크 연결 해제
- Intel 기반 Mac용 복구용 OS 및 진단 환경
- Mac 컴퓨터의 직접 메모리 접근 보호
- macOS에서 안전하게 커널 확장하기
- 시스템 무결성 보호
- watchOS의 시스템 보안
- macOS에서 FileVault 관리
- 저장된 암호에 접근할 수 있는 앱 권한
- 암호 보안 권장 사항
- Apple Cash 보안
- 보안된 Apple Messages for Business
- Wi-Fi 개인정보 보호
- 활성화 잠금 보안
- Apple Configurator 보안

2020년 4월

다음에 대한 내용이 업데이트됨:

- iOS 13.4
- iPadOS 13.4
- macOS 10.15.4
- tvOS 13.4
- watchOS 6.2

업데이트 내용:

- 하드웨어 마이크 연결 해제에 iPad 마이크 연결 해제 내용이 추가되었습니다.
- 사용자 데이터에 대한 앱 접근 방지에 Data Vault가 추가되었습니다.
- macOS에서 FileVault 관리하기 및 명령어 라인 도구가 업데이트되었습니다.
- macOS에서의 악성 코드로부터 보호에 악성 코드 제거 도구 내용이 추가되었습니다.
- iPadOS의 공유 iPad 보안이 업데이트되었습니다.

2019년 12월

iOS 보안 설명서, macOS 보안 개요 및 Apple T2 보안 칩 개요 통합

다음에 대한 내용이 업데이트됨:

- iOS 13.3
- iPadOS 13.3
- macOS 10.15.2
- tvOS 13.3
- watchOS 6.1.1

개인정보 보호 제어, Siri 및 Siri 제안, Safari 지능형 추적 방지 기능이 제거되었습니다. 해당 기능에 대한 최신 정보를 확인하려면 https://www.apple.com/kr/privacy/ 페이지를 참조하십시오.

2019년 5월

iOS 12.3에 대한 내용이 업데이트됨

- TLS 1.3 지원
- AirDrop 보안에 대한 설명 개정
- DFU 모드 및 복구 모드
- 액세서리 연결 시 암호 요구 사항

2018년 11월

iOS 12.1에 대한 내용이 업데이트됨

- 그룹 FaceTime

2018년 9월

iOS 12에 대한 내용이 업데이트됨

- Secure Enclave
- OS 무결성 보호
- 여분의 전원으로 익스프레스 카드 사용
- DFU 모드 및 복구 모드
- HomeKit TV 리모컨 액세서리
- 비접촉식 패스
- 학생 ID 카드
- Siri 제안
- Siri 단축어
- 단축어 앱
- 사용자 암호 관리
- 스크린 타임
- 보안 인증 및 프로그램

2018년 7월

iOS 11.4에 대한 내용이 업데이트됨

- 생체 인증 정책
- HomeKit
- Apple Pay
- 비즈니스 채팅
- iCloud에 메시지 보관
- Apple Business Manager

2017년 12월

iOS 11.2에 대한 내용이 업데이트됨

- Apple Pay Cash

2017년 10월

iOS 11.1에 대한 내용이 업데이트됨

- 보안 인증 및 프로그램
- Touch ID/Face ID
- 공유 메모
- CloudKit 종단간 암호화
- TLS 업데이트
- Apple Pay, 웹에서 Apple Pay로 결제하기
- Siri 제안
- 공유 iPad

2017년 7월

iOS 10.3에 대한 내용이 업데이트됨

- Secure Enclave
- 파일 데이터 보호
- Keybag
- 보안 인증 및 프로그램
- SiriKit
- HealthKit
- 네트워크 보안
- Bluetooth
- 공유 iPad
- 분실 모드
- 활성화 잠금
- 개인정보 보호 제어

2017년 3월

iOS 10에 대한 내용이 업데이트됨

- 시스템 보안
- 데이터 보호 클래스
- 보안 인증 및 프로그램
- HomeKit, ReplayKit, SiriKit
- Apple Watch
- Wi-Fi, VPN
- 단일 로그인
- Apple Pay, 웹에서 Apple Pay로 결제하기
- 신용 카드, 체크 카드 및 선불 카드 권한 설정
- Safari 제안

2016년 5월

iOS 9.3에 대한 내용이 업데이트됨

- 관리형 Apple ID
- Apple ID 이중 인증
- Keybag
- 보안 인증
- 분실 모드, 활성화 잠금
- 보안 메모
- Apple School Manager
- 공유 iPad

2015년 9월

iOS 9에 대한 내용이 업데이트됨

- Apple Watch 활성화 잠금
- 암호 정책
- Touch ID API 지원
- A8의 데이터 보호가 AES-XTS 사용함
- 자동 소프트웨어 업데이트를 위한 Keybag
- 인증서 업데이트
- 기업 앱 신뢰 모델
- Safari 책갈피를 위한 데이터 보호
- 앱 전송 보안
- VPN 사양
- HomeKit용 iCloud 원격 접근
- Apple Pay 적립 카드, Apple Pay 카드 발급처 앱
- Spotlight 기기 내 인덱스
- iOS 페어링 모델
- Apple Configurator 2
- 제한사항

저작권

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com

KH028-00780