Consumer Password Worst Practices

The Imperva Application Defense Center (ADC)

Summary

In December 2009, a major password breach occurred that led to the release of 32 million passwords[1]. Further, the hacker posted to the Internet[2] the full list of the 32 million passwords (with no other identifiable information). Passwords were stored in cleartext in the database and were extracted through a SQL Injection vulnerability[3]. The data provides a unique glimpse into the way that users select passwords and an opportunity to evaluate the true strength of these as a security mechanism. In the past, password studies have focused mostly on surveys[4]. Never before has there been such a high volume of real-world passwords to examine.

The Imperva Application Defense Center (ADC) analyzed the strength of the passwords.

[1] http://www.rockyou.com/help/securityMessage.php
[2] The posting of the passwords on igigi.baywords for rockyou-com-passwords-list has been removed
[3] http://www.techcrunch.com/2009/12/14/rockyou-hacked/
[4] http://blog.absolute.com/passwords-are-not-enough/

The shortness and simplicity of passwords means many users select credentials that will make them susceptible to basic, brute force password attacks. Furthermore, studies show[5,6,7] that about one half of the users use the same (or very similar) password to all websites that require logging in. Ironically, the problem has changed very little over the past twenty years. In 1990, a study of Unix password security revealed that password selection is strikingly similar to the 32 million breached passwords[8]. Just ten years ago, hacked Hotmail passwords showed little change[9]. This means that the users, if allowed to, will choose very weak passwords even for sites that hold their most private data. Worse, as hackers continue to rapidly adopt smarter brute force password cracking software, consumers and companies will be at greater risk. To quantify the issue, the combination of poor passwords and automated attacks means that in just 110 attempts, a hacker will typically gain access to one new account on every second or a mere 17 minutes to break into 1000 accounts.

Key Findings

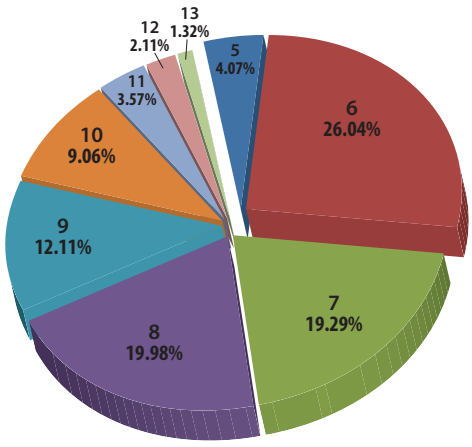
- About 30% of users chose passwords whose length is equal or below six characters.
- Moreover, almost 60% of users chose their passwords from a limited set of alpha-numeric characters.
- Nearly 50% of users used names, slang words, dictionary words or trivial passwords (consecutive digits, adjacent keyboard keys, and so on). The most common password among Rockyou.com account owners is "123456".

Analysis

NASA provides the following recommendations[10] for strong password selection. The ADC used NASA's standards to help benchmark consumers' password selection:

1. Recommendation: *It should contain at least eight characters*.

The ADC analysis revealed that just one half of the passwords contained seven or less characters. (Rockyou.com current minimal password length requirement is five). A staggering 30% of users chose passwords whose length was equal to or below six characters.

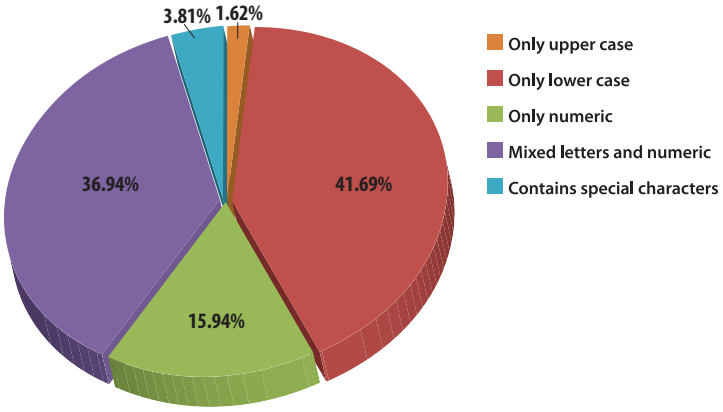


Password Length Distribution

[5] http://www.telegraph.co.uk/technology/news/6125081/Security-risk-as-people-use-same-password-on-all-websites.html
[6] http://www.readwriteweb.com/archives/majority_use_same_password.php
[7] http://www.thetechherald.com/articles/Internet-users-still-using-same-password-for-all-Web-sites/4816/
[8] http://www.klein.com/dvk/publications/passwd.pdf
[9] http://www.switched.com/2009/10/07/hotmail-scam-reveals-most-common-password-123456/
[10] http://www.nasa.gov/centers/dryden/pdf/89163main_train_timesheet.pdf

2. Recommendation: ***It should contain a mix of four different types of characters—upper case letters, lower case letters, numbers, and special characters such as !@#$%^&*,;" If there is only one letter or special character, it should not be either the first or last character in the password.***

The ADC analysis showed that almost 60% of users chose their passwords from within a limited set of characters. About 40% of the users use only lowercase characters for their passwords and about another 16% use only digits. Less than 4% of the users use special characters.



Password Length Distribution

In fact, after evaluating the passwords against two of NASA's recommendations only 0.2% of Rockyou.com users have a password that could be considered as strong password:

- Eight characters or longer
- Contain a mixture of special characters, numbers and both lower and upper case letters.

3. Recommendation: ***It should not be a name, a slang word, or any word in the dictionary. It should not include any part of your name or your e-mail address*.**

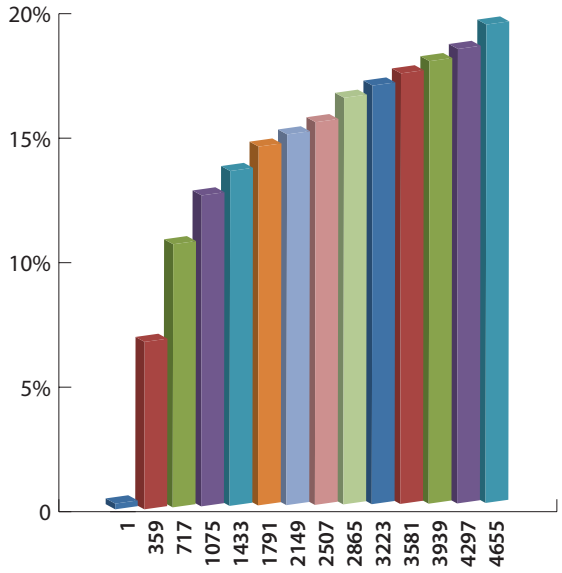
Almost all of the 5000 most popular passwords, that are used by a share of 20% of the users, were just that—names, slang words, dictionary words or trivial passwords (consecutive digits, adjacent keyboard keys, and so on). The most common password among Rockyou.com account owners is "123456". The runner up is "12345". The following table depicts the top 20 common passwords in the database list:

Rank	Password	Number of Users with Password (Absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Rank	Password	Number of Users with Password (Absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

Password Popularity—Top 20

If a hacker would have used the list of the top 5000 passwords as a dictionary for brute force attack on Rockyou. com users, it would take only one attempt (per account) to guess 0.9% of the users passwords or a rate of one success per 111 attempts. Assuming an attacker with a DSL connection of 55KBPS upload rate and that each attempt is 0.5KB in size, it means that the attacker can have 110 attempts per second. At this rate, a hacker will gain access to one new account every second or just less than 17 minutes to compromise 1000 accounts. And the problem is exponential. After the first wave of attacks, it would only take 116 attempts per account to compromise 5% of the accounts, 683 attempts to compromise 10% of accounts and about 5000 attempts to compromise 20% of accounts.
The following diagram depicts the expected effectiveness of attacks using a small, carefully chosen, attack dictionary:



Accumulated Percent of Dictionary Attack Success

Recommendations

Users

1. Choose a strong password for sites you care for the privacy of the information you store. Bruce Schneir's advice is useful: "take a sentence and turn it into a password. Something like "This little piggy went to market" might become "tlpWENT2m". That nine-character password won't be in anyone's dictionary."[11]
2. Use a different password for all sites—even for the ones where privacy isn't an issue. To help remember the passwords, again, following Bruce Schneier's advice is recommended: "If you can't remember your passwords, write them down and put the paper in your wallet. But just write the sentence—or better yet—a hint that will help you remember your sentence."[12]
3. Never trust a 3rd party with your important passwords (webmail, banking, medical etc.).

[11] http://www.guardian.co.uk/technology/2008/nov/13/internet-passwords
[12] ibid

Administrators

1. Enforce strong password policy—if you give the users a choice, it is very likely that they would choose weak passwords.
2. Make sure passwords are not transmitted in clear text. Always use HTTPS on login.
3. Make sure passwords are not kept in clear text. Always digest password before storing to DB.
4. Employ aggressive anti-brute force mechanisms to detect and mitigate brute force attacks on login credentials. Make these attacks too slowly for any practical purposes even for shorter passwords. You should actively put obstacles in the way of a brute-force attacker—such as CAPTCHAs, computational challenges, etc.
5. Employ a password change policy. Trigger the policy either by time or when suspicion for a compromise arises.
6. Allow and encourage passphrases instead of passwords. Although sentences may be longer, they may be easier to remember. With added characters, they become more difficult to break.

About Imperva

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline compliance.

© Copyright 2014, Imperva
All rights reserved. Imperva and SecureSphere are registered trademarks of Imperva.
All other brand or product names are trademarks or registered trademarks of their respective holders. WP-WORSTPRACTICES-PASSWORDS-0314.1