Hacker Intelligence Initiative, Monthly Trend Report #7

Enterprise Password Worst Practices

Nearly two years ago, Imperva published a report on 32 million breached passwords entitled "Consumer Password Worst Practices." Since then, successive breaches have highlighted consumers' inability to make sufficient password choices. Even a recent Google public ad campaign went bust when, in an effort to improve consumer password practices, the ad failed to make the right password recommendation. A Cambridge researcher pointed out that:

> *Google's example of a "very strong password" is '2bon2btitq', taken from the famous Hamlet quote "To be or not to be, that is the question". Empirically though, this is not a strong password, it's almost exactly average!*

When it comes to consumers implementing good passwords, we give up. Instead of consumers, responsibility rests on enterprises to put in place proper password security policies and procedures as a part of a comprehensive data security discipline. Passwords should be viewed by security teams as highly valuable data – even if PCI or other security mandates don't apply. We hope this paper guides enterprises to rectify poor password management practices.

For color and context, we present findings of our analysis of a recently exposed list of nearly 100,000 passwords following a data breach at FilmRadar.com, a website for film enthusiasts.

Obstacles

What is the right password policy to put in place? Two major obstacles impede enterprises today:

- **Hashing isn't enough**. Many organizations store passwords using a form of encryption, called cryptographic hash functions, often comprising the password's sole security measure. However, attackers do not attempt to directly attack the strength of the cryptographic measure. Rather, different methods exist which allow attackers to bypass the cryptographic measures – much like a burglar who doesn't bother to pick the lock but instead jumps the fence.
- **Many techniques and tools exist to help hackers crack passwords**. Password cracking tools are widely available. Some have actually been developed by the security community to help in the efforts of strengthening passwords, yet, like many white hat tools, they end up helping hackers. For example, using these readily available tools on the FilmRadar.com list, we were able to discover 77 of the 100 most popular passwords in less than ten minutes.

Passwords: *The Basics*

A password is a shared secret between a user and a service. When a user wants to connect to the service, she identifies with her user name (or any other form of account identifier) and proves her identity (i.e., authenticates) by providing the password. The service compares the provided password against what the user supplied during registration before granting the user access to the service.

Since passwords are the user's key to the service, organizations are wary of storing complete passwords. Instead, they choose to store a value which represents the password called a "digest". The password digest (a.k.a., a "password hash") is a mathematical transformation of the password which allows the comparison to the original password, but does not easily disclose the password itself. The most commonly used mathematical transformation is a cryptographic hash function called SHA-1. This function is strong enough so that there is no mathematical reverse function that takes the digest and reconstructs potential sources. However, when an enterprise fails to hash the passwords altogether, this is known as storing them "in the clear" and represents the most negligent practice possible.

Cryptographic Digests: *Not a Silver Bullet*

Contrary to common belief, cryptographic hash functions in general – whether they are SHA-1 or any other cryptographic function – are not impervious to hackers. The strength of a hash function, even if mathematically proven to be unbreakable, does not play a role in the cracking game. Instead of directly trying to attack the function, alternate methods exist which allow the adversary to bypass the cryptographic measures and guess the hashed passwords. There are two widely used techniques to crack passwords:

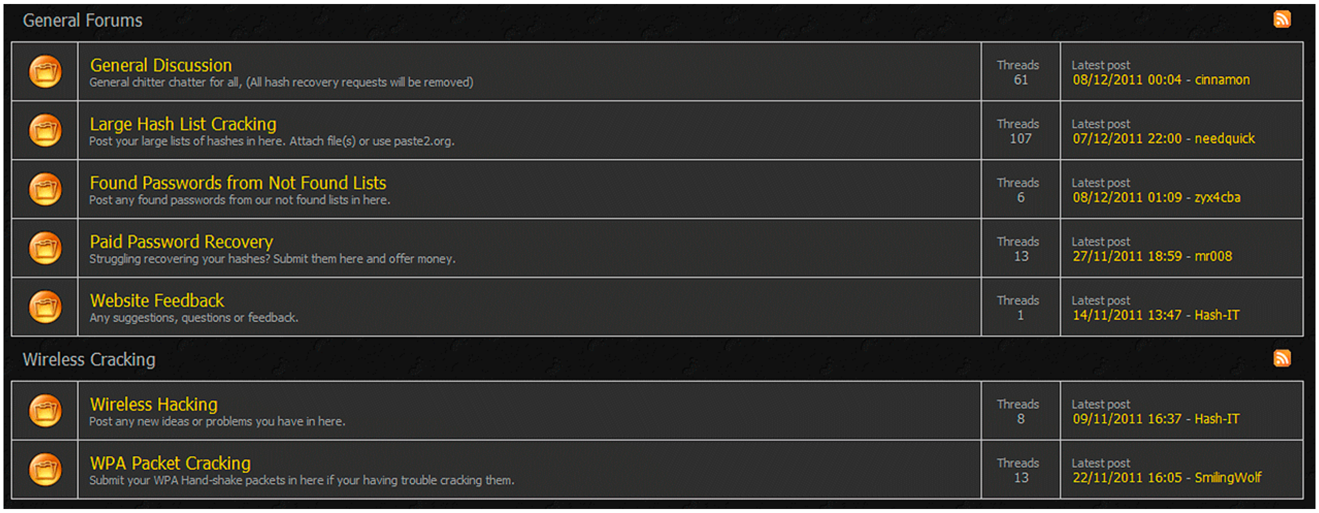
- **Rainbow tables** – These are pre-computed data sets containing hash values from nearly every combination of alphanumeric character up to a certain length. Although creating the rainbow tables is a lengthy process, they are created only once. In fact, hackers consider creating such tables a worth-while investment since after the rainbow tables are generated they can be used over and over again. One hacker website, for instance, developed 50 billion values for public use.
- **Dictionaries** – These are lists of common passwords together with a pre-calculated hash value. In this manner, a hacker can compare a digest with the pre-computed values. Dictionary attacks have proven to be an effective technique to crack passwords since many people have the tendency to use common passwords based on names, numerical or keyboard sequences. For example, in our previous analysis, we demonstrated that the most common password was '123456'.

Password Cracking Tools: *A Hacker Community Effort*

Password cracking tools – using rainbow tables and dictionaries – abound. With enough determination, a hacker can easily find tools and multiple dictionaries for password cracking. Most of these resources are free and available to anyone to download.

We list here some of the more popular ones:

- MD5 decrypter – This site offers online cracking (twelve passwords per request) based on 8.7 billion unique hash values. This site also offers a forum to upload large datasets for decryption. In particular, this tool clearly demonstrates the power of the hacker community as they work together to crack passwords. One of our recent HII reports highlighted how hackers leverage hacker forums as a collaboration platform to aid one another in attack efforts. This site is no different as one of its features is the ability to post a digest which will most likely be identified by other users. Site postings have shown that nearly all such requests were cracked successfully. In fact, we tried this out in our labs when we were stumped against digests we were not certain about. We found that the list of hashed passwords was updated with our unknown digests within a week following our original query.



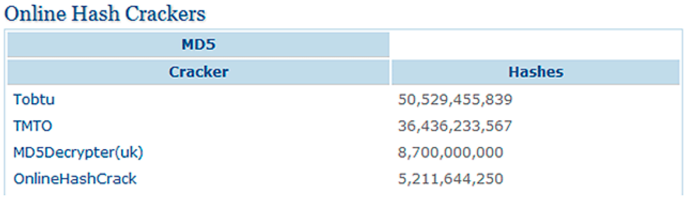
General Forums

Forum	Threads	Latest post
General Discussion General chitter chatter for all, (All hash recovery requests will be removed)	Threads 61	Latest post 08/12/2011 00:04 - cinnamon
Large Hash List Cracking Post your large lists of hashes in here. Attach file(s) or use paste2.org.	Threads 107	Latest post 07/12/2011 22:00 - needquick
Found Passwords from Not Found Lists Post any found passwords from our not found lists in here.	Threads 6	Latest post 08/12/2011 01:09 - zyx4cba
Paid Password Recovery Struggling recovering your hashes? Submit them here and offer money.	Threads 13	Latest post 27/11/2011 18:59 - mr008
Website Feedback Any suggestions, questions or feedback.	Threads 1	Latest post 14/11/2011 13:47 - Hash-IT

Wireless Cracking

Forum	Threads	Latest post
Wireless Hacking Post any new ideas or problems you have in here.	Threads 8	Latest post 09/11/2011 16:37 - Hash-IT
WPA Packet Cracking Submit your WPA Hand-shake packets in here if your having trouble cracking them.	Threads 13	Latest post 22/11/2011 16:05 - SmilingWolf

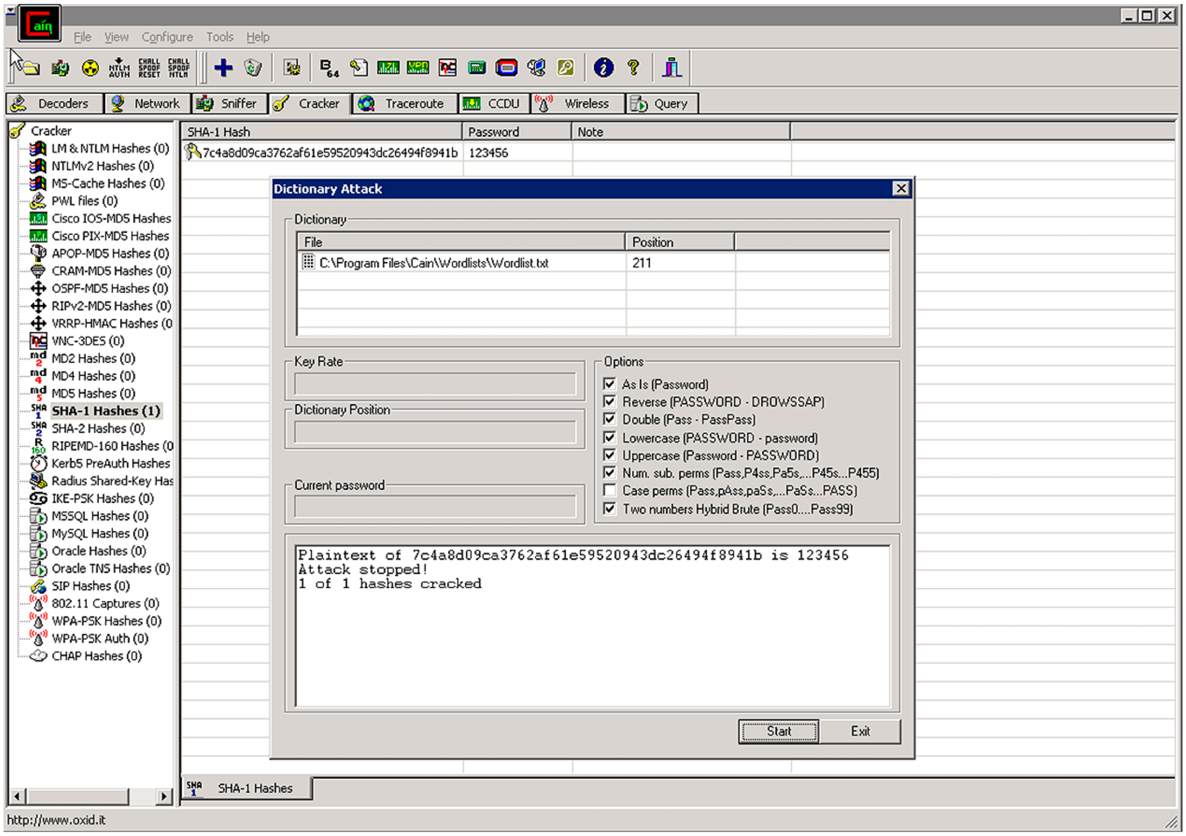
- Cyberwar Zone – This site provides lists of common used passwords such as Disney characters, film actors, common family names and even Chinese words. Also, there are rainbow tables with 50 billion hash values.



Online Hash Crackers

MD5	
Cracker	Hashes
Tobtu	50,529,455,839
TMTO	36,436,233,567
MD5Decrypter(uk)	8,700,000,000
OnlineHashCrack	5,211,644,250

- › Cain and Able – This site hosts a password recovery tool which offers various methods for cracking passwords, including a dictionary of common passwords.



SHA-1 Hash	Password	Note
7c4a8d09ca3762af61e59520943dc26494f8941b	123456	

Dictionary

File	Position
C:\Program Files\Cain\Wordlists\Wordlist.txt	211

Key Rate

Dictionary Position

Current password

Options

- ☑ As Is (Password)
- ☑ Reverse (PASSWORD - DROWSSAP)
- ☑ Double (Pass - PassPass)
- ☑ Lowercase (PASSWORD - password)
- ☑ Uppercase (Password - PASSWORD)
- ☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- ☐ Case perms (Pass,pAss,paSs,...PaSs...PASS)
- ☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
Plaintext of 7c4a8d09ca3762af61e59520943dc26494f8941b is 123456
Attack stopped!
1 of 1 hashes cracked
```

- › John the Ripper – This site contains a password cracking tool includes a dictionary of common passwords.

Lessons from the Real Life: *The Analysis of 100,000 Digests*

A couple of months ago, a data breach at FilmRadar.com exposed 95,167 hashed user passwords. Like many online services, FilmRadar stored the passwords in a digested format, using the SHA1 hash function, hoping to guarantee confidentiality. However, storing the user passwords as a cryptographic digest is just not enough. To prove just how weak this type of security measure is, we analyzed the FilmRadar passwords using both rainbow and dictionary attacks. Using publicly available tools, we could:

- › **Uncover 77 of the 100 most popular passwords in less than ten minutes using rainbow tables through an online service.** Interestingly, this also gave us insight to the power of collaboration amongst the hacker community. We observed that when hackers struggled to find corresponding passwords, it usually took just a week for the community to contribute updates.
- › **Guess nearly 5% of all passwords on the list in less than two days by using dictionaries.** Lesson one: Using various dictionaries from multiple resources, hackers can still figure out passwords even though the process is slow. Lesson two: The bigger the dataset, the more common passwords it contains, the faster the hacking. A smaller dataset – or even just non-common passwords – would make cracking much slower if not impossible.

Out of the top 15 passwords (see *Table 1*), there was only one which we were not able to guess. Once again, uncovering password lists provides ample fodder regarding user password practices:

- The 100 most common passwords in the list constitute ~10% of the entire list.
- Human nature forces associations between the passwords with the service. Consider the most popular password, 'Blink123'. Most likely, this was influenced by the movie Blink.
- The most common password in the RockYou 32 million password dictionary, '123456', was displaced on the FilmRadar list. However, common sequences remain a popular choice. As the list shows, nearly all passwords end with a numeric sequence.
- Many of the uncovered passwords are listed in common dictionaries.

Table 1: 15 Most Common Password from FilmRadar.com

Password popularity rank	Password	Number of Occurrences
1	Blink123	1578
2	Greatday1	441
3	Gendut80	436
4	Sample123	420
5	Baobao87	375
6	Matttt24	309
7	Speak2me	261
8	ABcd1234	252
9	[not found]	245
10	abcd1234	215
11	Sara2000	194
12	blueU1234	179
13	Tgold1973	165
14	Hello123	146
15	Timetoget1	144

Defeating Rainbow Tables: *Salting*

We were able to analyze the FilmRadar password digests as they simply used a cryptographic hash function. This is a common practice. In fact, a Booz Allen breach in July showed that they relied only on the SHA-1 hash function as their password security mechanism. An analysis of the Booz Allen breach appears in our blog where we demonstrated how security measures can easily be defeated using rainbow tables.

How can organization defeat rainbow table attacks? An effective measure is called "salting." A salt value is a random value pre-pended to the password before it gets encrypted. In this manner, the computational time required to break weak passwords increases exponentially. For example, a salt of just a three bit length increases the storage and pre-computation time of rainbow tables eightfold.

To be clear, salting does not make the passwords hack-proof. However, this is not a concern as the point is to increase the cost of guessing the password. This is a simple measure for the organization to employ. By contrast, it represents a costly investment for the commercial hacker.

Mitigation

Passwords are a convenient authentication method. Yet, stored incorrectly and they can cause a lot of hassle in the event of a breach. To begin with, hash functions protect only strong passwords while naïve hashing (without a salt) exposes passwords to rainbow table attacks.

Advice to users is to choose strong passwords. The rest is up to the business. What should site owners do to mitigate the effectiveness of crackers?

- **Allow users to choose longer passwords which are easier to remember.** We recommend passphrases. Passphrases provide the necessary length yet do not require the user to write down the secret on a note left on the worker's desk.
- **Enforce strong password policy.** This doesn't mean just applying restriction on the character types but also by comparing against dictionaries used by attackers. In fact, Hotmail recently banned the usage of common passwords. This also means defining and banning site-specific passwords, like FilmRadar's 'Blink123'. Likewise, numerical or keyboard sequences need to be banned altogether.
- **Use salted digests.** As mentioned in the previous section, a salted value should increase the cost of guessing the password so that financially-motivated hackers will not make such an investment.

Hacker Intelligence Initiative Overview

The Imperva Hacker Intelligence Initiative goes inside the cyber-underground and provides analysis of the trending hacking techniques and interesting attack campaigns from the past month. A part of Imperva's Application Defense Center research arm, the Hacker Intelligence Initiative (HII), is focused on tracking the latest trends in attacks, Web application security and cyber-crime business models with the goal of improving security controls and risk management processes.

Imperva
3400 Bridge Parkway, Suite 200
Redwood City, CA 94065

Tel: +1-650-345-9000
Fax: +1-650-345-9004
www.imperva.com