enisa

European Network
and Information
Security Agency

Password security: a joint effort between end-users and service providers

Password security: a joint effort between end-users and service providers

Just halfway through 2012, data leaks have already exposed millions of users' sensitive personal data including password information. ENISA is reminding service providers to follow best practices to better protect sensitive data.

In the cyber world individuals are commonly identified by username and password. To avoid identity theft and other security issues, people have to keep their passwords safe. Online service providers who are storing usernames and passwords are expected to do the same. But problems arise when security is compromised at either end of the chain.

On the Internet a range of resources and recommendations are available to improve security. This includes specific guidance on passwords, how long they should be, what level of complexity should be used. In addition there are numerous guides available for service providers on how to build more secure authentication systems. In spite all this, successful attacks are continuing with reports of passwords and other confidential data being disclosed.

These breaches not only provided access to personal information but also compromised other password protected services with stolen credentials being reused to attack other web sites, as people often use the same passwords for different accounts.

In recent months, millions of citizens have had their personal information compromised:

Company	Accounts affected	Reference	Date
LinkedIn	6 500 000	http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/ http://nakedsecurity.sophos.com/2012/06/06/linkedin-confirms-hack-over-60-of-stolen-passwords-already-cracked/	6/6/2012
EHarmony	1 500 000	http://advice.eharmony.com/blog/2012/06/06/update-on-compromised-passwords/	6/7/2012
Formspring	420 000 +	http://blog.formspring.me/2012/07/urgent-change-your-formspring-password/	10/7/2012

Yahoo Voice	400 000 +	http://news.yahoo.com/450-000-yahoo-passwords-just-got-hacked-might-155505805.html?_esi=1 http://www.guardian.co.uk/technology/2012/jul/12/yahoo-voice-hack-attack-passwords-stolen	12/7/2012
Android Forums	1 000 000 +	http://phandroid.com/2012/07/12/android-forums-security-breach-change-your-passwords-penetration-tester-wanted/ http://www.zdnet.com/android-forums-hacked-1-million-user-credentials-stolen-7000000817/	12/7/2012
NVIDIA	400 000 +	http://www.nvidia.com/content/forums/index.html	13/7/2012
Gamigo	8 240 000	http://www.zdnet.com/8-24-million-gamigo-passwords-leaked-after-hack-7000001403/	24/7/2012

In the light of these attacks, ENISA is reminding service providers that the occurrence of breaches and their impact could be reduced by the following well established recommendations.

Service Providers: Protect your users, protect their passwords!

1. Properly store password information

Service providers should **never store a password in plaintext**. Only cryptographic versions of the passwords (cryptographic hashes or digests) should be stored.

But even with this level of security, attackers, by making use of widely available password dictionaries and precomputed hash lists, are cracking password hashes with high efficiency rates. Recently, attackers have easily cracked 3 million passwords from a LinkedIn password hashes leak. Leaked hashes later are later used to "grow" existing password dictionaries and tables, making further attacks even more efficient.

As technology advances, older hashing algorithms (crypt, MD5, SHA-1, plus others) are becoming quicker to compute and should be replaced by more complex and attack-resistant algorithms. Today, **every password hash algorithm should employ a further layer of security by implementing salt and multiple iterations** over the initial hash (e.g. BCrypt, Salted SHA-256).

2. Prevent data leaks

Hashes should not only be attack resistant: as with any sensitive information, they must also be stored in a secure environment that makes data leaks more unlikely. In the past years, most online data breaches were accomplished using SQL injection attacks. Service providers should defend themselves against these attacks by implementing a proper SDLC (Software

Development Life Cycle), taking special care of validation methods for inputs, parameters and variables.
The efficiency of the security controls should be checked regularly with audits and penetration tests.

3. Secure your authentication

Every password-based authentication scheme should rely on a proper **password policy** enforcing password requirements (e.g. minimum length, complexity, renewal frequency) adapted to the sensitivity of the service provided. A more secure online authentication system should rely on a combination of mechanisms which reduces the success rate of an online attack. Login **attempts throttling** mechanisms like CAPTCHA and per-source limitation, further increase the security of an online authentication system and prevent automated attacks.

When providing access to sensitive or critical information, service providers should implement **two-factor authentication schemes**. By using smartphone as a second factor (e.g. SMS one-time password, dedicated mobile application) the security of a login process is strengthened.

4. Notify in case of breach

In cases of personal data breaches, existing European legislation already requires all telecommunications service providers to notify their competent national authorities and the individuals affected. The forthcoming reform of the data protection framework will soon introduce a general obligation of notification.

Notifications about data breaches will contribute in the long term to better data protection. End users will receive all relevant information related to incidents involving their personal data, while the competent authorities (typically data protection authorities) will have an overview of data leaks in their countries. This will allow them to further enhance guidelines and recommendations for storing and transmitting data.

References and Advisories:

https://krebsonsecurity.com/2012/06/ how-companies-can-beef-up-password-security
http://news.techworld.com/security/3331283/barclays-97-percent-of-data-breaches-still-due-to-sql-injection/

http://www.verizonbusiness.com/about/events/2012dbir/index.xml

https://www.trustwave.com/global-security-report

http://throwingfire.com/storing-passwords-securely/

http://blog.moertel.com/articles/2006/12/15/never-store-passwords-in-a-database

https://www.owasp.org/index.php/Authentication_Cheat_Sheet

https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

Tell your users: Protect yourself, protect your passwords!

Password security is also the user's responsibility. Therefore, ENISA is also advising service providers to remind their users that a secure password is their best and often only way to efficiently protect their data from attackers. The following advice will help them to make it harder for an attacker to access personal data:

password
123456
12345678
1234
letmein
12345
qwerty
dragon
696969
football
baseball
mustang
michael
pussy
abc123
monkey
master
jennifer

Worst (most common) passwords in 2012

Source xato.net

- Do not to reuse the same password for multiple accounts.
  Attackers often try to re-use compromised passwords to access other services.
- If a password is stolen, it must immediately be changed. In case the same password or a variation of the same password has been used for another online account, they must also be changed.
- Use complex passwords longer than 8 characters which contain alpha-numeric and special characters (e.g. characters a-z, A-Z, 0-9 along with '.,&@:?!()$#/\)
  A long password does not mean it is hard to remember: four random common words mixed with special characters make a password strong and easy to remember.
- Regularly change passwords for online accounts.
- Make use of passwords managers.
  Passwords managers are software that chooses and manages passwords for you.
- Take advantage of service providers that offer two-factor authentication.
  A two factor authentication involves two things, such as something you know (like a password) and something you have (e.g. a one-time password sent to a mobile phone). When possible, use this secure form of authentication to access important services.

More advice on choosing strong passwords:

- http://www.google.com/goodtoknow/online-safety/passwords/
- http://www.microsoft.com/en-gb/security/online-privacy/passwords-create.aspx
- www.getsafeonline.org/nqcontent.cfm?a_id=1127
- http://xkcd.com/936/