4-23-2014

Password Best Practices

Debbie Ginsberg
IIT Chicago-Kent College of Law Library, dginsberg@kentlaw.iit.edu

Password Best Practices

April 23, 2014
Deborah Ginsberg & Heather Banks

What is Heartbleed?

Heartbleed is a serious software flaw that allows hackers to bypass password protections and access information on a computer server. The attack cannot be targeted to specific kinds of data (like passwords), but instead is limited to small amounts of random information. However, by attacking the computer many times, a hacker can eventually obtain useful information like passwords. It is not clear if hackers exploited the flaw before it was discovered.

Should I change my passwords?

Many sites were affected, but you should not change your password on sites that have not been fixed (otherwise, your password could still be discovered).

- Check to see if a particular site was affected: https://filippo.io/Heartbleed/
- Check to see if a particular site has been fixed: http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/

Bad passwords you should never use

Common passwords

Many users make the mistake of never changing their default passwords from generics like “password” or “123456.”

- The 25 Worst Passwords of 2013: http://splashdata.com/press/worstpasswords2013.htm
- 500 passwords you should never use (some are “adult” words): http://www.bmyers.com/public/1958.cfm

Dangerous habits

- Do not use personal information such as birthdates, places you have lived, or family names - Ginsberg2014 would not be a good password.
- Do not reuse the same password on multiple sites.
- Do not use short passwords (under 8 characters).
- Do not use only lowercase letters.
- Do not share passwords with others.
- Do not use your username in your password.

Create strong passwords

Good habits

- Use uppercase, lowercase, and numbers. Note that some systems do not work well with "special characters" (e.g. punctuation) while others require such characters.
- Create long passwords - at least 8 characters (10 or more is better).
- Change passwords every few months.
- Substitute numbers for letters (Carolina becomes Carol1na or, even better, Carol8na (1 for "i" can be too obvious). To make this password more effective, add numbers or another word: Carol8a732.

(Relatively) simple mnemonics

- Create a prefix or a suffix that you can use with all of your passwords. For example, you could use "Gard8N" as your prefix, and then add the passwords you can remember easily to that prefix: Gard8[password1], Gard8N[password2], Gard8N[password3].
- Use phrases (you can add additional characters between words to make it even stronger): ILikePastaAndSauce could also be I1Like1Pasta1And1Sauce.
- You can also use the first letters of a phrase (with additional characters like numbers): I1L1P1A1S1.

Password generators

Many sites will generate random passwords for you.

- Strong Password Generator (creates very strong, but hard to remember passwords) http://strongpasswordgenerator.com/
- XKPasswd: (creates passwords that are easier to remember) https://www.xkpasswd.net/c/index.cgi

Test password strength

- **Telepath Words** - how easily can your password be guessed? https://telepathwords.research.microsoft.com/
- **How Secure Is Your Password** - how easily can your password be hacked? https://howsecureismypassword.net/

Password management tools

These sites remember your passwords so that you do not have to.

- Lastpass (lastpass.com) -- basic service is free; there is a $12/yearly fee to use on mobile devices.
- 1Password (https://agilebits.com/onepassword) -- $25 per license for computers, iOS app is $8.99, Android app is free.
- Keepass (http://keepass.info/) -- free, but requires a PC emulator to use on Macs. Does not have its own mobile app, but there are mobile apps that work with Keepass.

Two-factor authentication

To keep your accounts safe even if your password is discovered, consider using two-factor authentication. With this tool, you use your regular password to access an account, and then use a second password that is sent to you by phone or by text.

For example, to access your home Gmail with two-factor authentication:

1. Login to gmail.com as usual.
2. Google will send you a text message with a randomly generated second password.
3. Use the second password to access Gmail.

Two-factor authentication is not provided automatically. You will need to set it up for each service you wish to use it with.

Services that use two-factor authentication: http://twofactorauth.org/

Even two-factor authentication has its limits - it would not have protected against Heartbleed, for example.

Note: Two-factor authentication is not available for Chicago-Kent Gmail accounts. You can use it for your personal Gmail account.

Hardware authentication

You may have seen (or even own) fingerprint scanners on mobile devices. This prevents hacking using software but users have reported that it can cause problems with access.

Have I been hacked?

- **Have I Been Pwned?** - check to see if one of your user IDs been compromised - https://haveibeenpwned.com/
  The site will tell you which service may have been compromised.

CLC's Best Practices Page

CLC has posted a few techniques to keep your computer and data safe:
http://kentlaw.iit.edu/current-students/information-technology/best-practices