Password Management

Correct-Horse-Battery-Staple

Stephen "ToxicSauce" Walker-Weinshenker

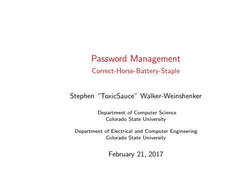
Department of Computer Science
Colorado State University

Department of Electrical and Computer Engineering
Colorado State University

February 21, 2017

2017-02-19

Password Management



Password Management
Correct-Horse-Battery-Staple

Stephen "ToxicSauce" Walker-Weinshenker

Department of Computer Science
Colorado State University

Department of Electrical and Computer Engineering
Colorado State University

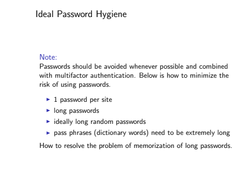
February 21, 2017

Ideal Password Hygiene

Note:
Passwords should be avoided whenever possible and combined with multifactor authentication. Below is how to minimize the risk of using passwords.

- 1 password per site
- long passwords
- ideally long random passwords
- pass phrases (dictionary words) need to be extremely long

How to resolve the problem of memorization of long passwords.



Ideal Password Hygiene

Note:
Passwords should be avoided whenever possible and combined with multifactor authentication. Below is how to minimize the risk of using passwords.

- 1 password per site
- long passwords
- ideally long random passwords
- pass phrases (dictionary words) need to be extremely long

How to resolve the problem of memorization of long passwords.

1. use multifactor auth, ssh keys or other auth methods whenever possible

Solution: Use a password management tool

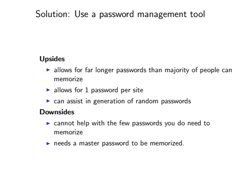
Upsides

- allows for far longer passwords than majority of people can memorize
- allows for 1 password per site
- can assist in generation of random passwords

Downsides

- cannot help with the few passwords you do need to memorize
- needs a master password to be memorized.

└Solution: Use a password management tool



Solution: Use a password management tool

Upsides

- allows for far longer passwords than majority of people can memorize
- allows for 1 password per site
- can assist in generation of random passwords

Downsides

- cannot help with the few passwords you do need to memorize
- needs a master password to be memorized.

1. Some tools can work with yubikeys or multifactor auth, but most still need a master password.

Creating Rememberable Passwords

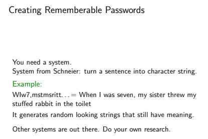
You need a system.
System from Schneier: turn a sentence into character string.

Example:

WIw7,mstmsritt. . . = When I was seven, my sister threw my stuffed rabbit in the toilet

It generates random looking strings that still have meaning.

Other systems are out there. Do your own research.



Creating Rememberable Passwords

You need a system.
System from Schneier: turn a sentence into character string.

Example:

WIw7,mstmsritt. . . = When I was seven, my sister threw my stuffed rabbit in the toilet

It generates random looking strings that still have meaning.

Other systems are out there. Do your own research.

Recommendations

WARNING!:
Please do your own research and draw your own conclusions. These are only recoomendations and should be taken with large amounts of salt. Software that is seen as secure today may be found to have gaping holes tomorrow.

Notice:
Using browser plugins can seriously compromise your password management program. Especially autofill plugins. Autotype plugins are better.

Recommendations

WARNING!:
Please do your own research and draw your own conclusions. These are only recoomendations and should be taken with large amounts of salt. Software that is seen as secure today may be found to have gaping holes tomorrow.

Notice:
Using browser plugins can seriously compromise your password management program. Especially autofill plugins. Autotype plugins are better.

Recommendations

Password Management

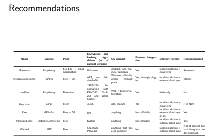
Stephen "ToxicSauce" Walker-Weinshenker

Name	License	Price	Encryption and hashing algorithms (as of current version)	OS support	Browser Integration	Delivery Format	Reccommended
1Password	Proprietary	$10-$30 + cloud subscription	Unknown	Android, iOS, macOS, Windows	Yes	local installation + cloud sync	Somewhat
Keepass and clones	GPLv2	Free + OS	AES, two fish, chacha20	Windows officially, others through ports	Yes, through plug-ins	local installation + external cloud sync	Mostly
LastPass	Proprietary	Freemium	"AES-256 bit encryption with PBKDF2 SHA-256 and salted hashes"	Web + browser integration	Yes	Web only	No
Keychain	APSL	Free?	3DES	iOS, macOS	Yes	local installation + cloud sync	Hell No!!
Pass	GPLv2+	Free + OS	gpg	anything	Not officially	local installation + external cloud sync or git	Yes
Password Safe	Artistic License 2.0	Free	twofish	anything	Not officially	local installation + external cloud sync	Yes
Warded	MIT	Free	Chacha20-Poly1305	anything that has a go compiler	No	local installation + external cloud sync	Not at present due to it being in active development.

Password Management

2017-02-19

└Recommendations



1. warded written by hexid in go
2. pass is very minimalistic, unix like
3. Password safe created by Bruce Scheier and currently developed by Rony Shapiro + open source community

Password Management

Stephen “ToxicSauce” Walker-Weinshenker

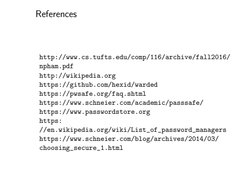
References

http://www.cs.tufts.edu/comp/116/archive/fall2016/npham.pdf
http://wikipedia.org
https://github.com/hexid/warded
https://pwsafe.org/faq.shtml
https://www.schneier.com/academic/passsafe/
https://www.passwordstore.org
https://en.wikipedia.org/wiki/List_of_password_managers
https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

2017-02-19

Password Management

└References



References

http://www.cs.tufts.edu/comp/116/archive/fall2016/npham.pdf
http://wikipedia.org
https://github.com/hexid/warded
https://pwsafe.org/faq.shtml
https://www.schneier.com/academic/passsafe/
https://www.passwordstore.org
https://en.wikipedia.org/wiki/List_of_password_managers
https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html