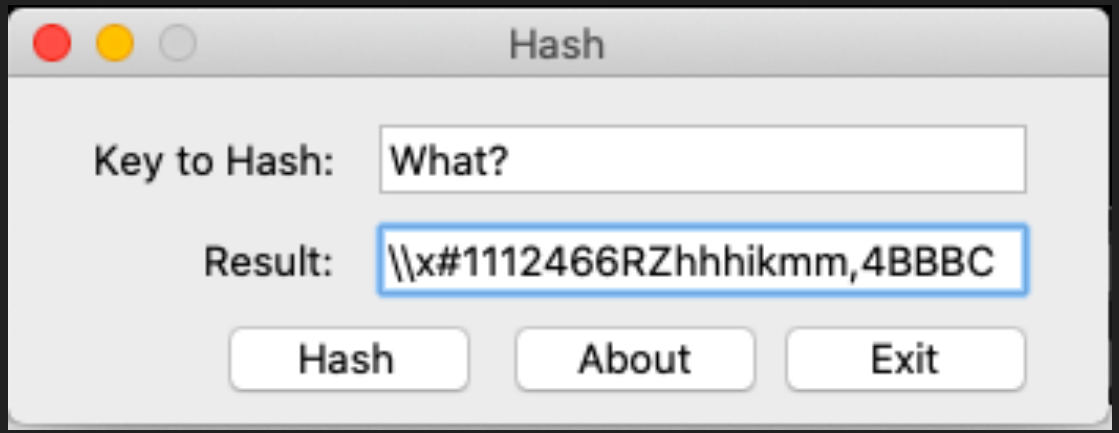
On the Effectiveness of Password Managers

Andrew Vella

How do I know when something is secure?

There is no way to design perfect security systems. Given enough time and effort, you can break into just about anything. But there are ways to make it tougher…

What comes to mind?



An example of encryption (with a few too many repeats!)

A Security System is Effective If:

It deters people from attempting. (ie “That looks hard to steal”)

It takes them a long time to break it… Like a trillion years

It requires an authentication method:

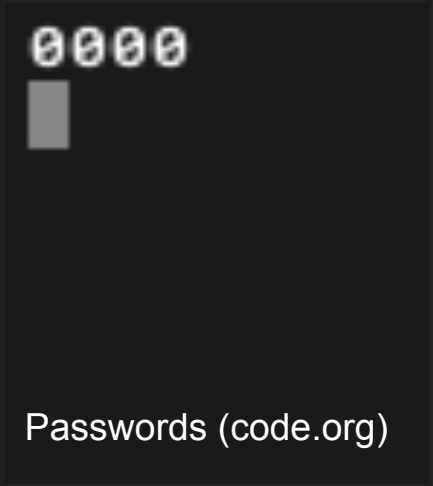
- Something you have
- Something you know
- Something unique about who you are

(ie “Hey I need your PIN, and your keys, and your eyeballs. That would be great!)

Pros and Cons of passwords

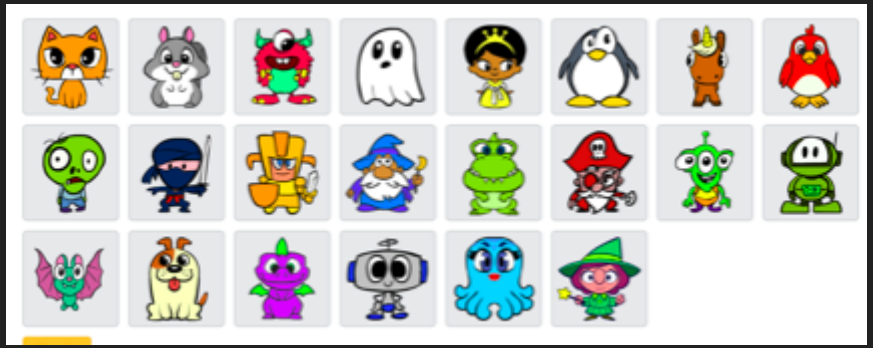
What are some of the pros and cons of a password system?

What comes to mind?



Passwords (code.org)

Brute Force Attack



Graphical

Passwords

PROS	CONS
Generally reliable within constraints (length, variation in characters)	Completely unreliable outside of constraints (too short, all numbers)
Easy for user to use and understand. It is an intuitive security device.	Easy for anyone who can get a hold of it. No way to verify identity without additional measures.
General Purpose: Can be implemented on a wide range of devices without specific sensors. (No expensive biometrics required)	Extremely Common: Methods to break passwords are widely known, implemented, and improved.
Can be recovered if lost	Recovery methods introduce vulnerability

I thought this presentation was about password managers

A password manager is only as strong as your strongest password!

Password managers encrypt sensitive information and store it in “the cloud” (which is a euphemism that does not describe the cloud in the least).

Information is decrypted via a private key. In this case the user creates a master password.

A master password is just a glorified password. That’s it. Get that, and you have all the info you could ask for. The password manager is compromised!

Can anyone do better?

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes by Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano evaluates security methods based on various criteria.

They describe 25 factors to be considered and weighted accordingly for the optimization of a particular scheme for security. In summary: here are a few.

Factors

Accessibility? Min physical or cognitive effort (carrying, typing, memory)

Is it vulnerable to impersonation? (security questions are weak to this)

Is it easy to deploy across servers, devices, and browsers?

Is recovery an option if the system is compromised?

Low cost of operation? Scaling?

Is the consent of the user required?

Theft? Phishing? Internal Observation (via a keylogger)?

Are internal errors likely?

How do password managers compare to alternatives?

Password Managers are a low effort, accessible, scalable solution. (That is, more passwords does not require more effort.) However, if the master password is acquired. There is virtually no way to recover from the damages.

Man-in-the-middle schemes employ a device between client and server for verification. They require the use of one time codes that need to be carried on your person. This allows security on a computer with malware, but it has a higher cost of operation and is not protected against theft or loss of the codes in your pocket. This also does not scale well.

Biometrics are useful in specific situations but are not generally a viable option alone. They are prone to error (open your eyes more, wash your hands, position the camera) and are not as accessible as other methods. Specific hardware is required which reduces deployability and increases cost of operation.

Graphical passwords are easy to learn, but they are not compatible with servers and they do not scale well. Great for kids. Not very secure. Choose the picture from the set is vulnerable to attack. Also not accessible to anyone with a vision impairment.

Conclusions

Ultimately, no alternative outmatches the benefits of a traditional password. Yes, they can be hard to remember. They can be a pain to make and update. However, they are deployable, accessible, and reliable.

The shortcomings of a traditional password can be dealt with via some augmentation. Stick a note on the monitor. Keep a book.

Get a password manager. (Install the browser extension, discover it does not work on your default browser, and once it works, do the thing you wanted to stop doing, now with higher stakes)