Considerations and Resources for Practical Security

Evan Misshula

2018-02-25

what to expect

- a lot of this presentation is humorous
- real references at the end
- security is incremental
- perfect is the enemy of getting better

what this is not

- not about physical security
- not a tutorial
- not what to do if the FBI, CIA of FSB is after you

what we will cover some important security problems

- passwords

what we will cover some important security problems

- passwords
- ssh keys
- file security

what we will cover some important security problems

- passwords
- ssh keys
- file security
- email

what we will cover some important security problems

- passwords
- ssh keys
- file security
- email
- mobile/wifi

my exposure

my exposure

- I worked for three years for Center for Cybercrime Studies

my exposure

- I worked for three years for Center for Cybercrime Studies
- I took at the GC:
  - Secure Operating Systems
  - Advanced Penetration Testing

my exposure

- I worked for three years for Center for Cybercrime Studies
- I took at the GC:
  - Secure Operating Systems
  - Advanced Penetration Testing
- I went to Eastern Regional Security Camps for the US Cyberchallenge for 2011 and 2012

my exposure

- I worked for three years for Center for Cybercrime Studies
- I took at the GC:
  - Secure Operating Systems
  - Advanced Penetration Testing
- I went to Eastern Regional Security Camps for the US Cyberchallenge for 2011 and 2012
- I designed the curriculum for the High School for NSF/NSA Cybercamp at John Jay

password problem

- different for each entity
- longer is better
- random is better

password problem

- different for each entity
- longer is better
- random is better

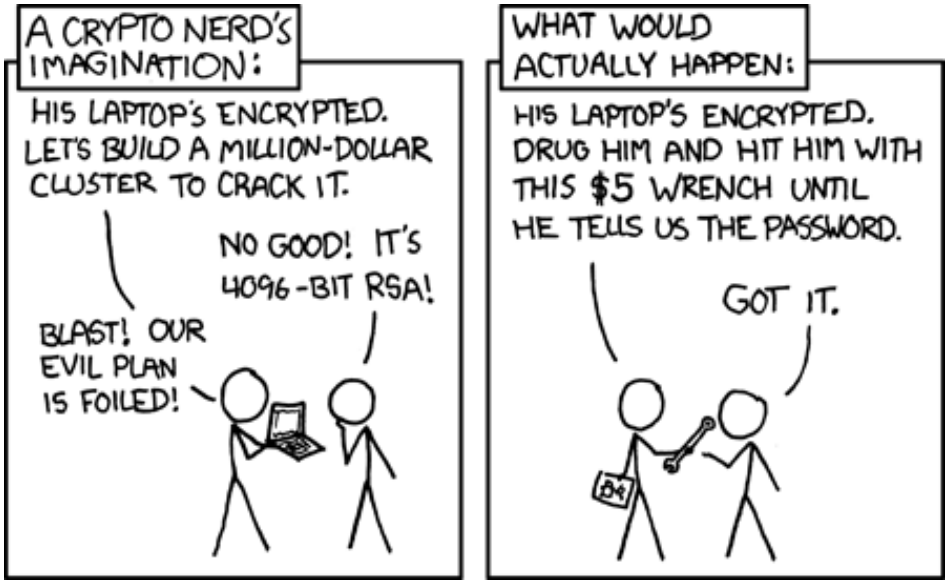
- humans need help

What we all think

What about a really good password

What about a really good password

or with a nerd's imagination



terrible implications

terrible implications

One more problem

- I will show you the solution I use
- But there is one more problem

too short

A small slide-show from intel on passwords

A small slide-show from intel on passwords

A small slide-show from intel on passwords

A small slide-show from intel on passwords

A small slide-show from intel on passwords

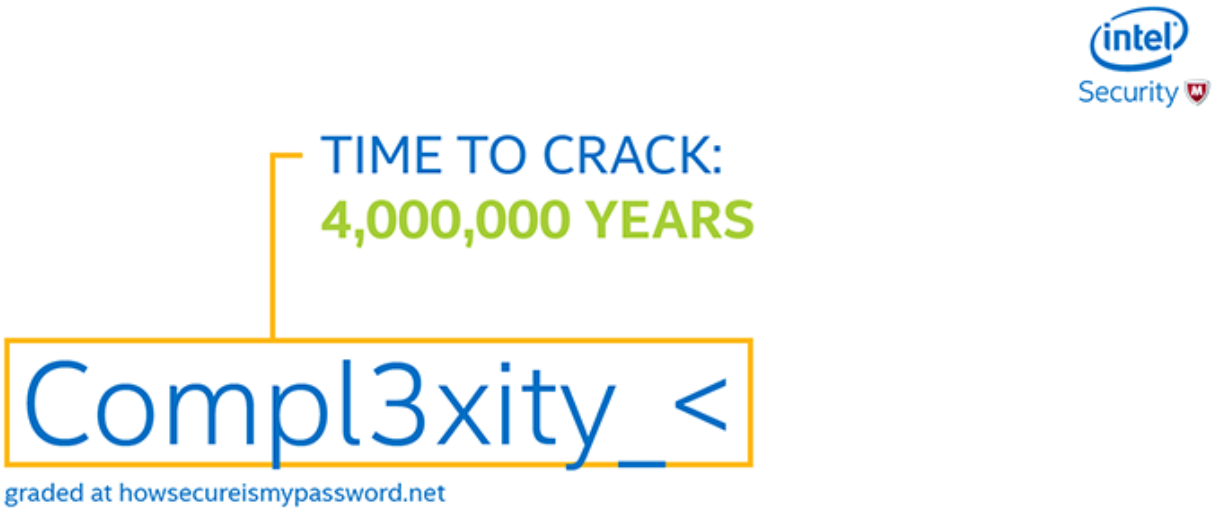
A small slide-show from intel on passwords

A small slide-show from intel on passwords

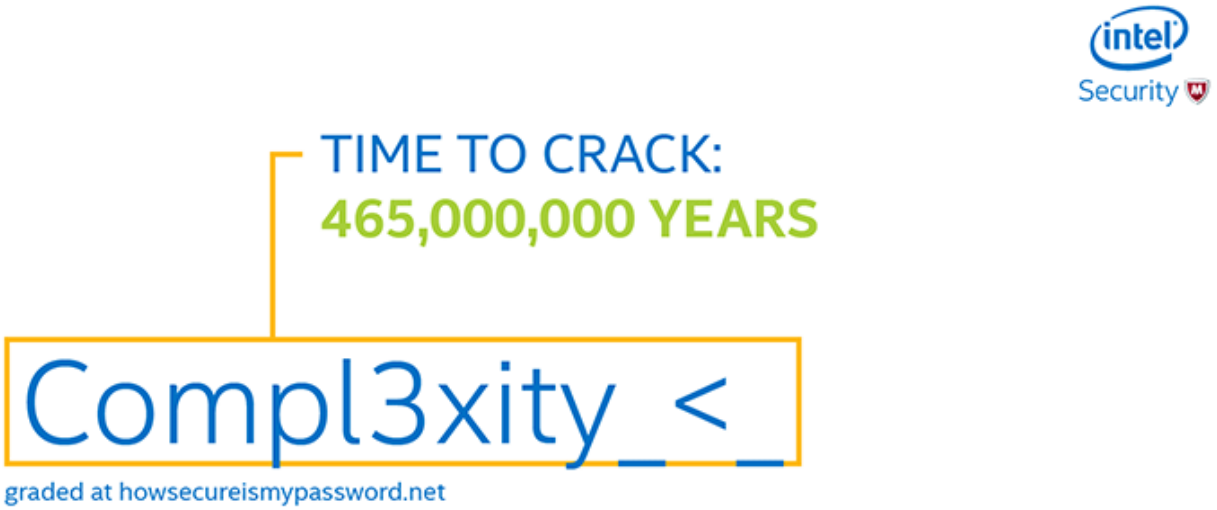
A small slide-show from intel on passwords

A small slide-show from intel on passwords

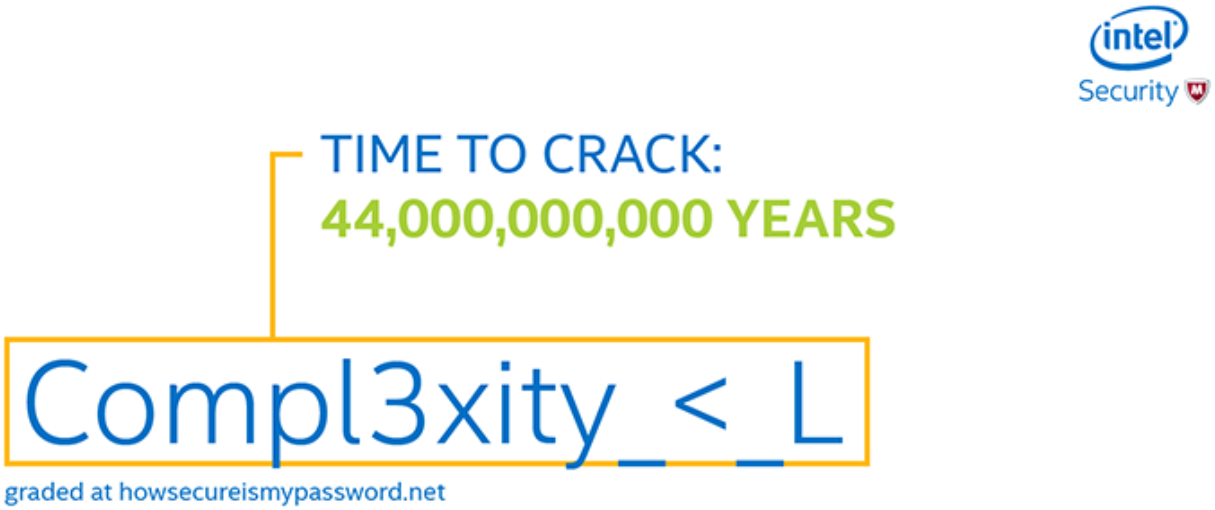
A small slide-show from intel on passwords



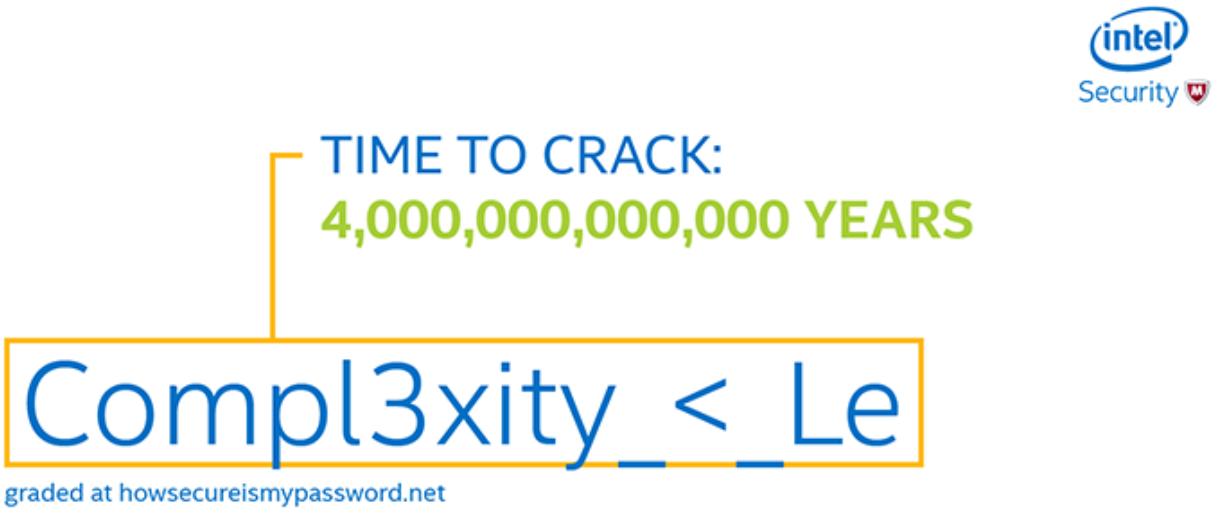
A small slide-show from intel on passwords



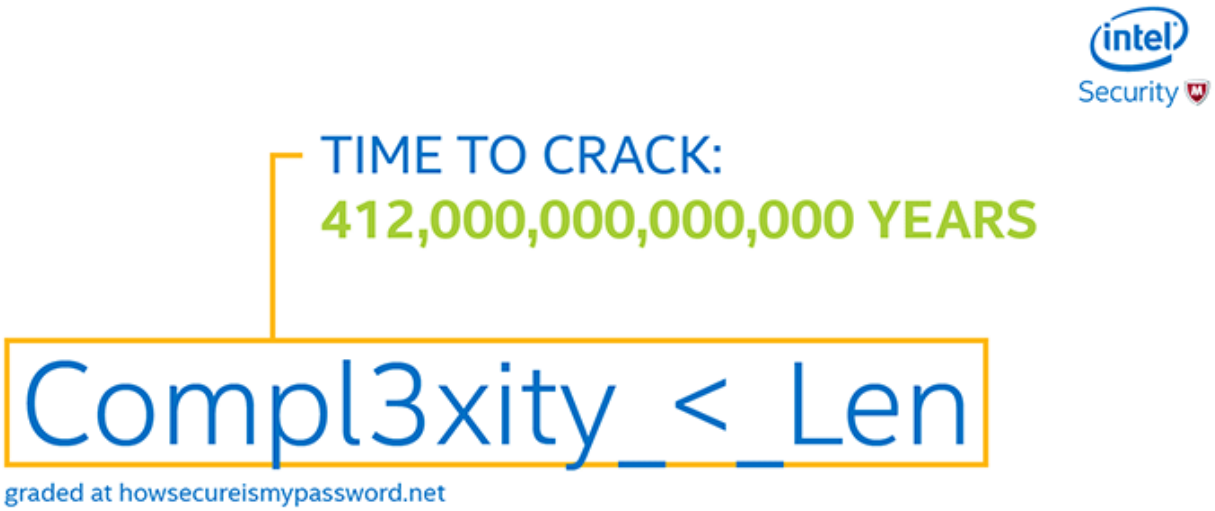
A small slide-show from intel on passwords



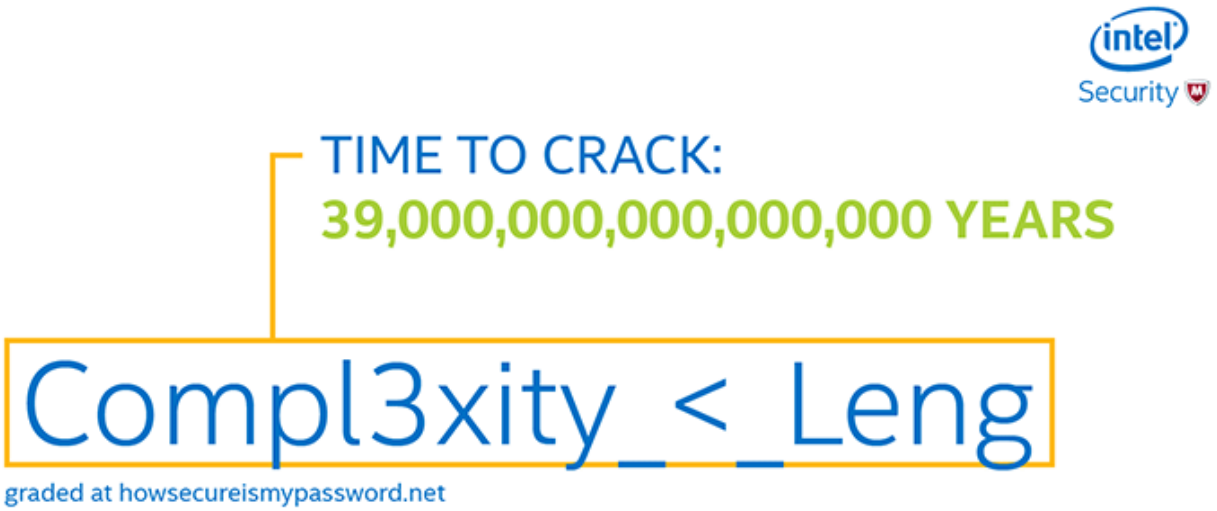
A small slide-show from intel on passwords



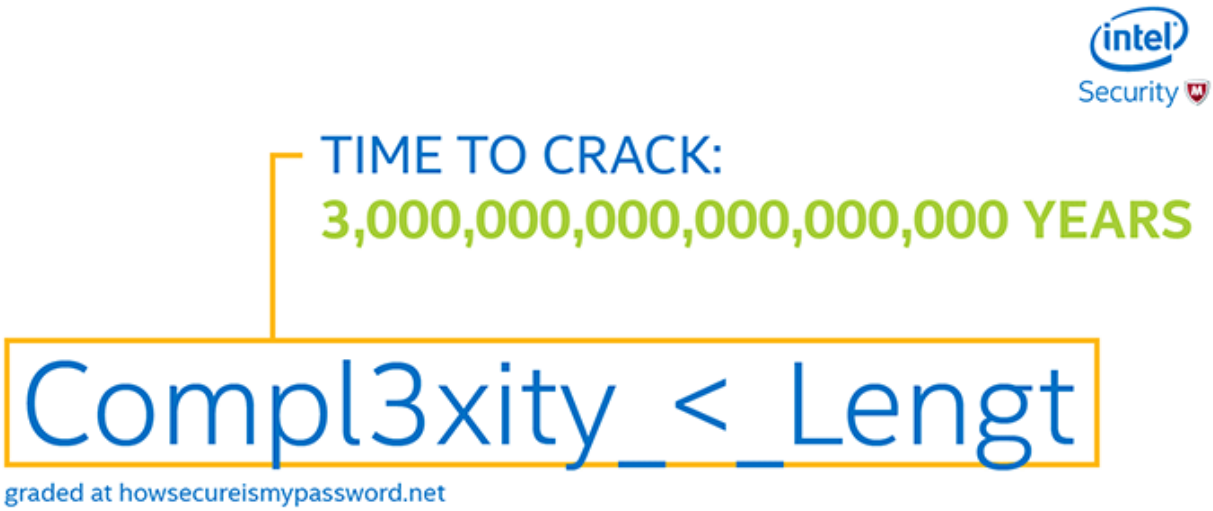
A small slide-show from intel on passwords



A small slide-show from intel on passwords

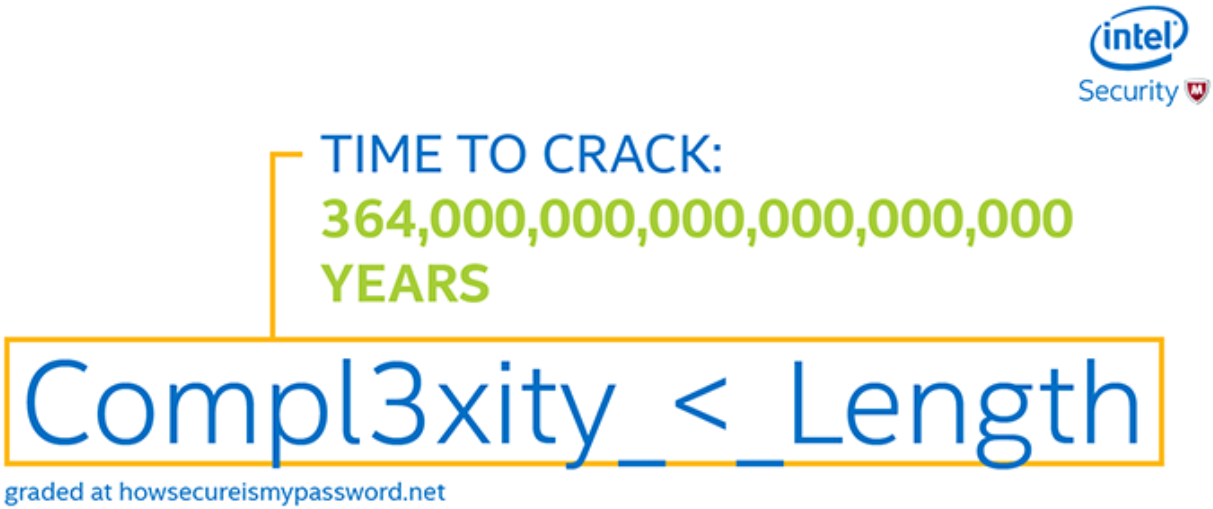


A small slide-show from intel on passwords

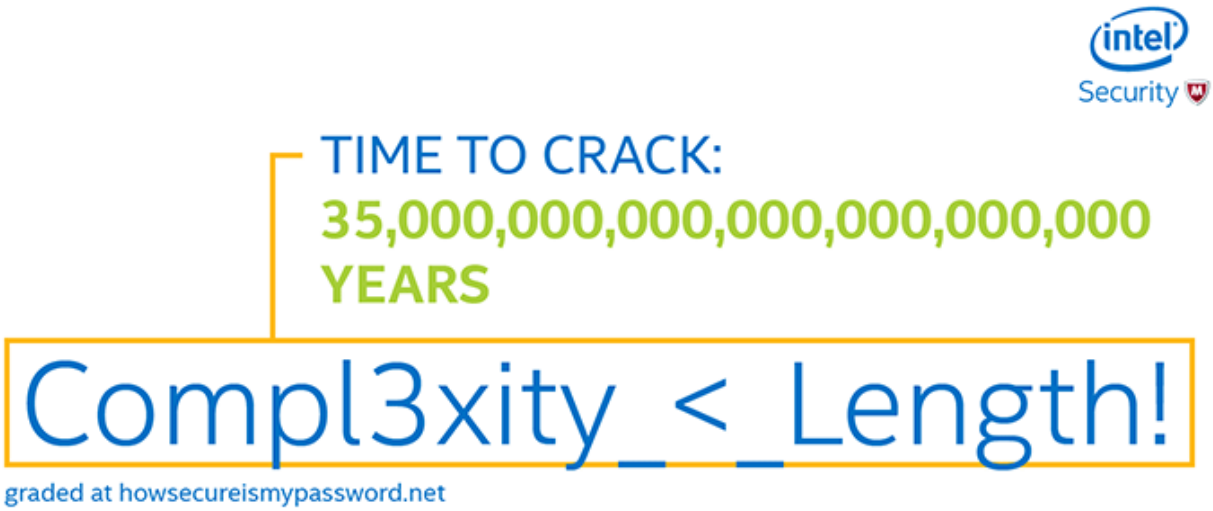


A small slide-show from intel on passwords

:PROPERTIES: :BEAMER$_{env}$: frame :END:x

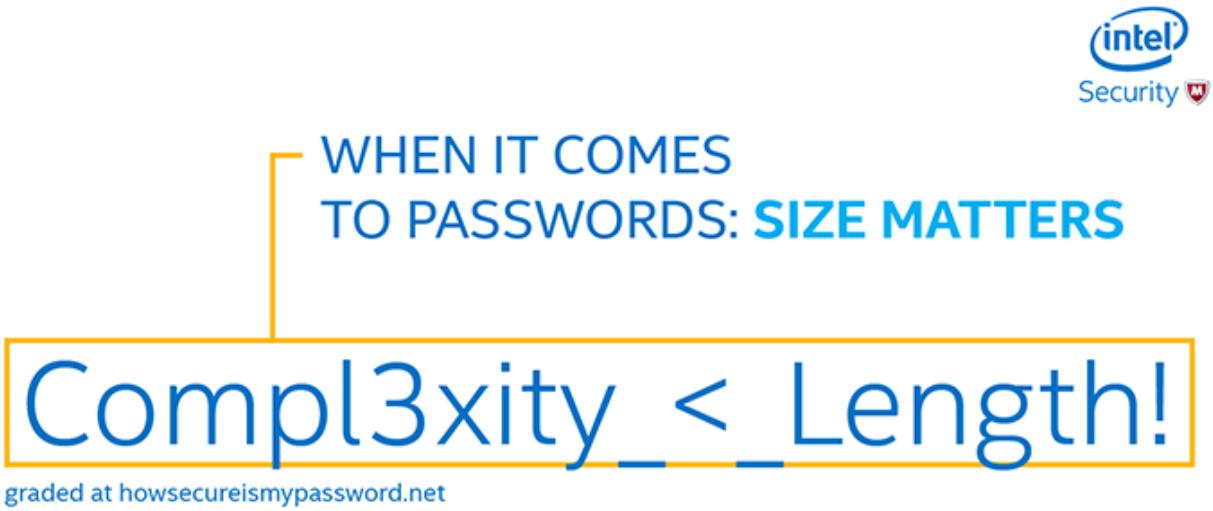


A small slide-show from intel on passwords

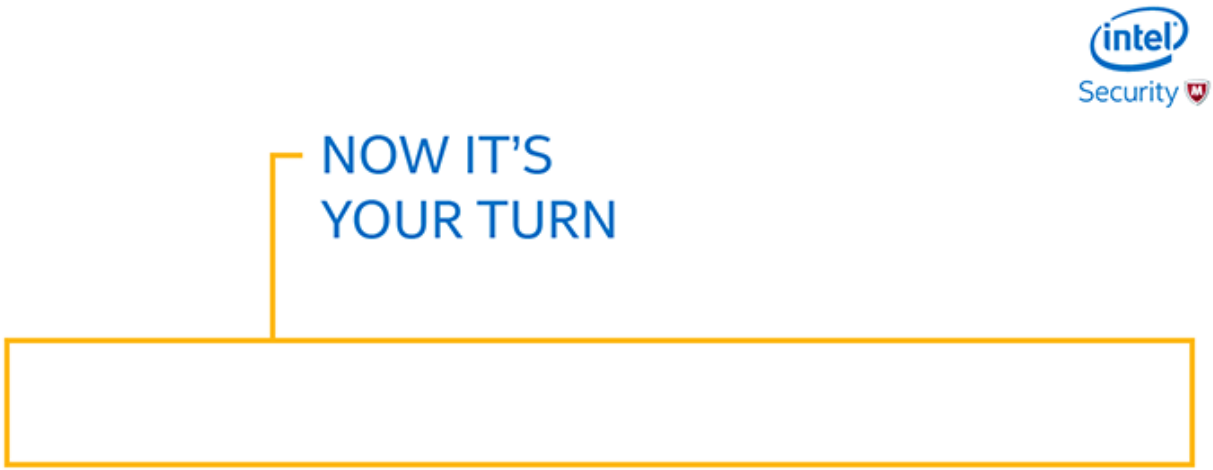


A small slide-show from intel on passwords

A small slide-show from intel on passwords



A small slide-show from intel on passwords



A small slide-show from intel on passwords

#PASSWORDDAY

So the problem for IT

So how does everyone do it?

Tutorials on ssh keys

- OS X and Linux
  - Search: standard unix password manager
  - `https://www.passwordstore.org/`
- Windows
  - Search: keeper
  - `https://keepersecurity.com/personal.html`

How a password manager works

- one very strong password
- it keeps all of your other usernames and passwords
- it generates long random passwords
- you login by copying and pasting from your manager to the website

How a password manager works

- one very strong password
- it keeps all of your other usernames and passwords
- it generates long random passwords
- you login by copying and pasting from your manager to the website

- Don't lose your laptop

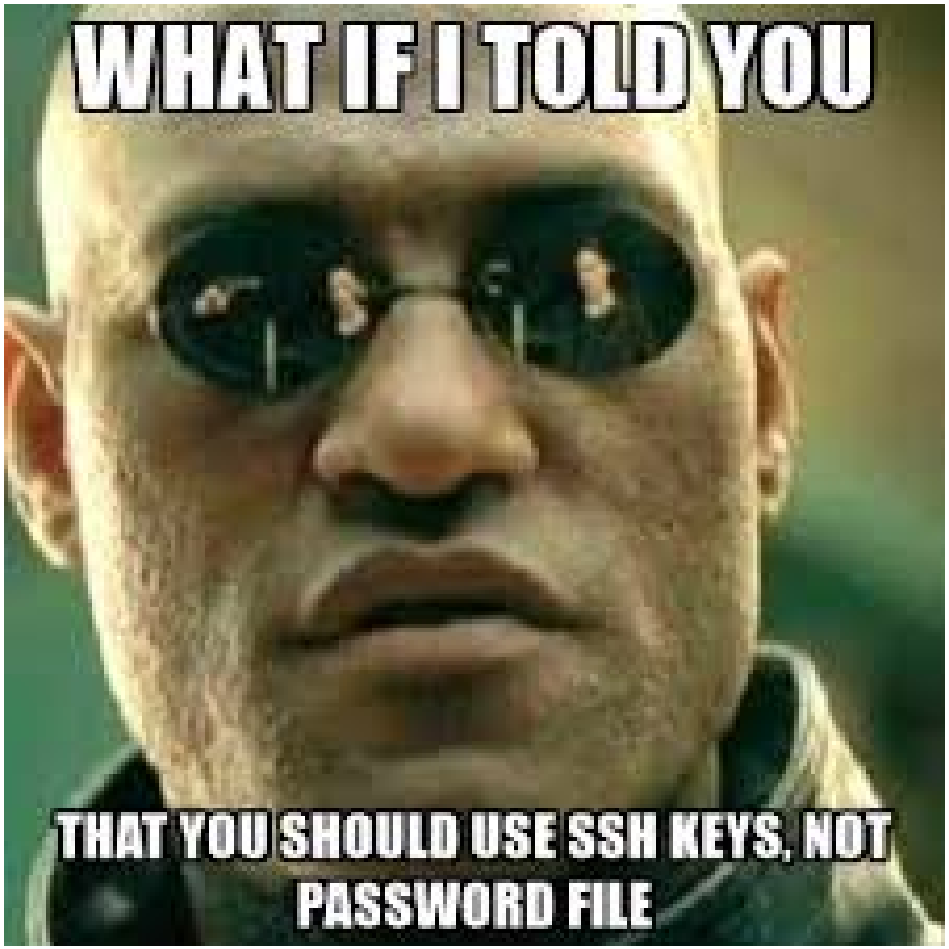
Keys

- ssh keys are a pair of two large numbers
  - call one: public
  - call the other: private
    - that multiply to a very large number
- That very large number is only divisible each of these
- It is equivelent to a 670 random character password

Tutorials on ssh keys

- OS X
  - Search: osx generate ssh keys
  - `https://help.github.com/articles/generating-a-new-ssh-key-and-adding-it-to-the-ssh-agent/`
- Windows
  - Search: windows generate ssh keys
  - `https://www.digitalocean.com/community/tutorials/how-to-use-ssh-keys-with-putty-on-digitalocean-droplets-wi`
- Linux
  - Search: ubuntu generate ssh keys
    - `https://help.ubuntu.com/community/SSH/OpenSSH/Keys`

So


WHAT IF I TOLD YOU
THAT YOU SHOULD USE SSH KEYS, NOT PASSWORD FILE

And now:


YOU GET AN SSH KEY
AND YOU GET AN SSH KEY
EVERYBODY GETS AN SSH KEY

But of course:

File security

- We can use our keys to encode a file even if the whole drive is not
  - The encoded file is called *Ciphertext*

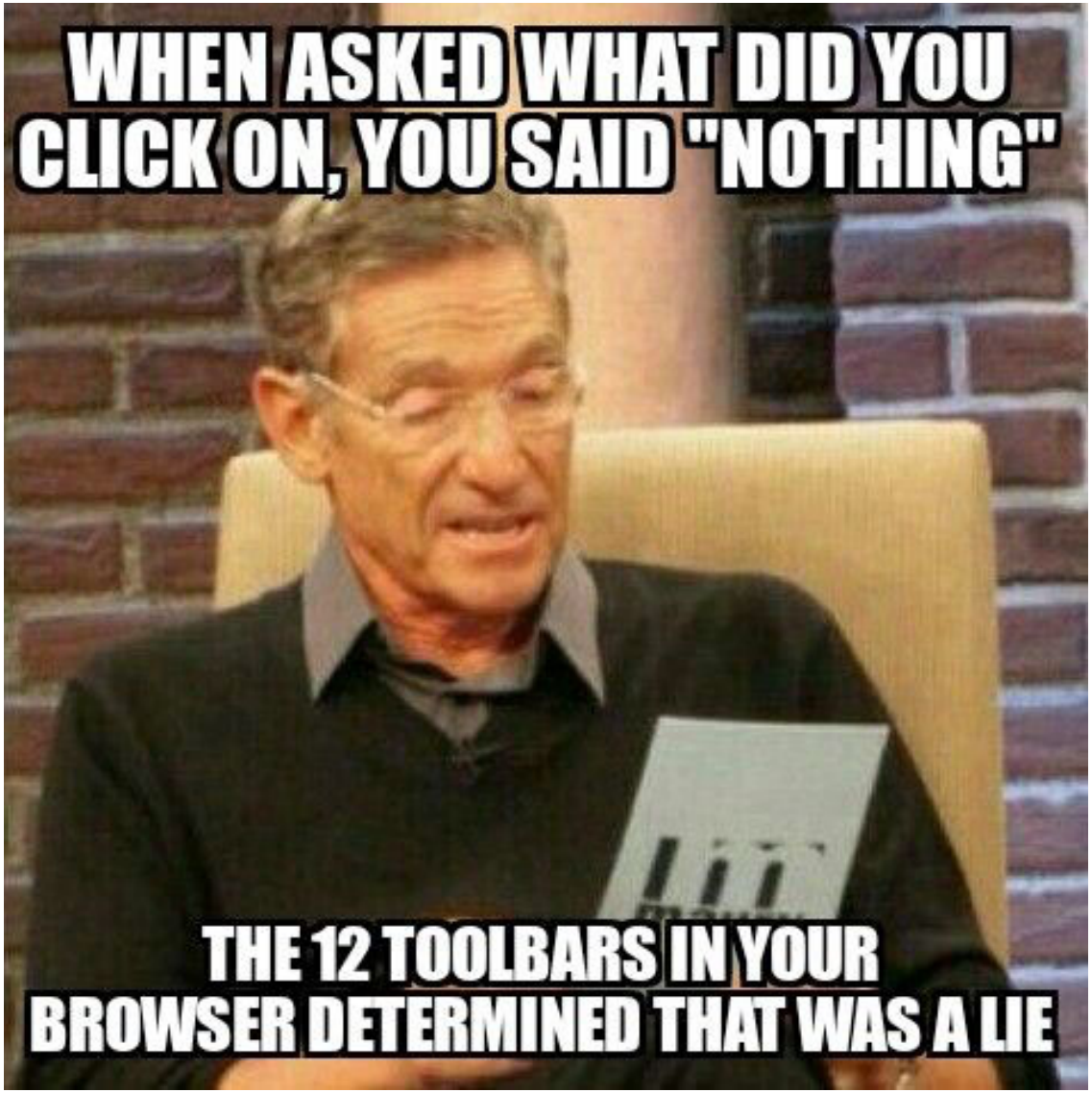
File security

- We can use our keys to encode a file even if the whole drive is not
  - The encoded file is called *Ciphertext*
- We can also use our private key to encode email
  - gmail has plugins to automatically use our private keys so all email is encrypted

File security

- We can use our keys to encode a file even if the whole drive is not
  - The encoded file is called *Ciphertext*
- We can also use our private key to encode email
  - gmail has plugins to automatically use our private keys so all email is encrypted
- search: gmail encrypted email
  - `https://support.google.com/mail/answer/6330403?hl=en`

Basic email security



Check before you click

1. Did this come from someone you know?
2. What is file extension?
   - don't click on anything that "pdf.exe", "docx.exe", "pptx.exe"
3. Videos (Adobe Flash) can execute arbitrary code on your computer

Check before you click

1. Did this come from someone you know?
2. What is file extension?
   - don't click on anything that "pdf.exe", "docx.exe", "pptx.exe"
3. Videos (Adobe Flash) can execute arbitrary code on your computer

1. Do not ever watch porn on a computer you need to keep secure

Mobile/wifi

- Don't do your banking at Starbucks on their wifi

Mobile/wifi

- Don't do your banking at Starbucks on their wifi
- Anything you share in plaintext is vulnerable

Mobile/wifi

- Don't do your banking at Starbucks on their wifi
- Anything you share in plaintext is vulnerable
- Don't let your phone automatically connect
  - hackers use strong signals to get a shot at your mobile data

Great resources on security

- Verne Paxson
  - `http://www.icir.org/vern/`
- Avinash Kak
  - `https://engineering.purdue.edu/kak/compsec/Lectures.html`