Easy digital security for everyday life

10 weird tricks the NSA doesn't want you to know

SIPB Cluedump, 8 December 2016

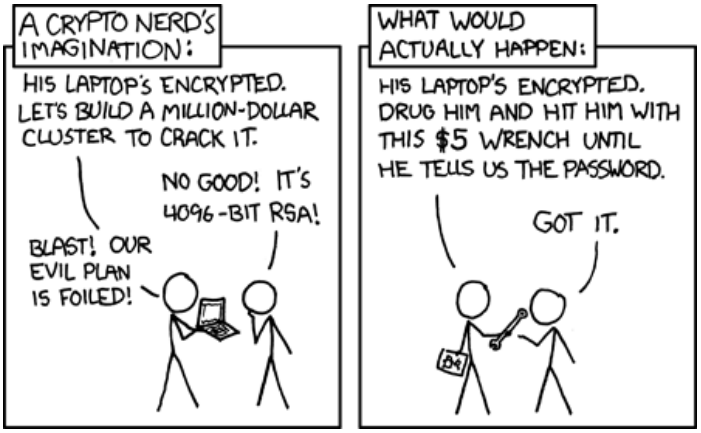
Anish Athalye (aathalye), Merry Mou (mmou), Sam Dukhovni (dukhovni)

So why I am here, and why should I care?

- People who should care about security
  - cryptonuts
  - journalists
  - activists
  - researchers in dangerous situations
  - anyone who has any reason for the police to not be fond of you
  - people who care about / are friends with those who actually need the security, in order to help provide covering traffic and normalize security culture
  - YOU!
- https://haveibeenpwned.com/

Defining Your Threat Model

- Understand your circumstances
  - Who's (possibly) after you?
  - What do they want?
  - What are their capabilities?
- Define your needs/values
  - confidentiality, privacy, anonymity, anti-surveillance
  - integrity, authenticity
  - availability


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Before we go on...

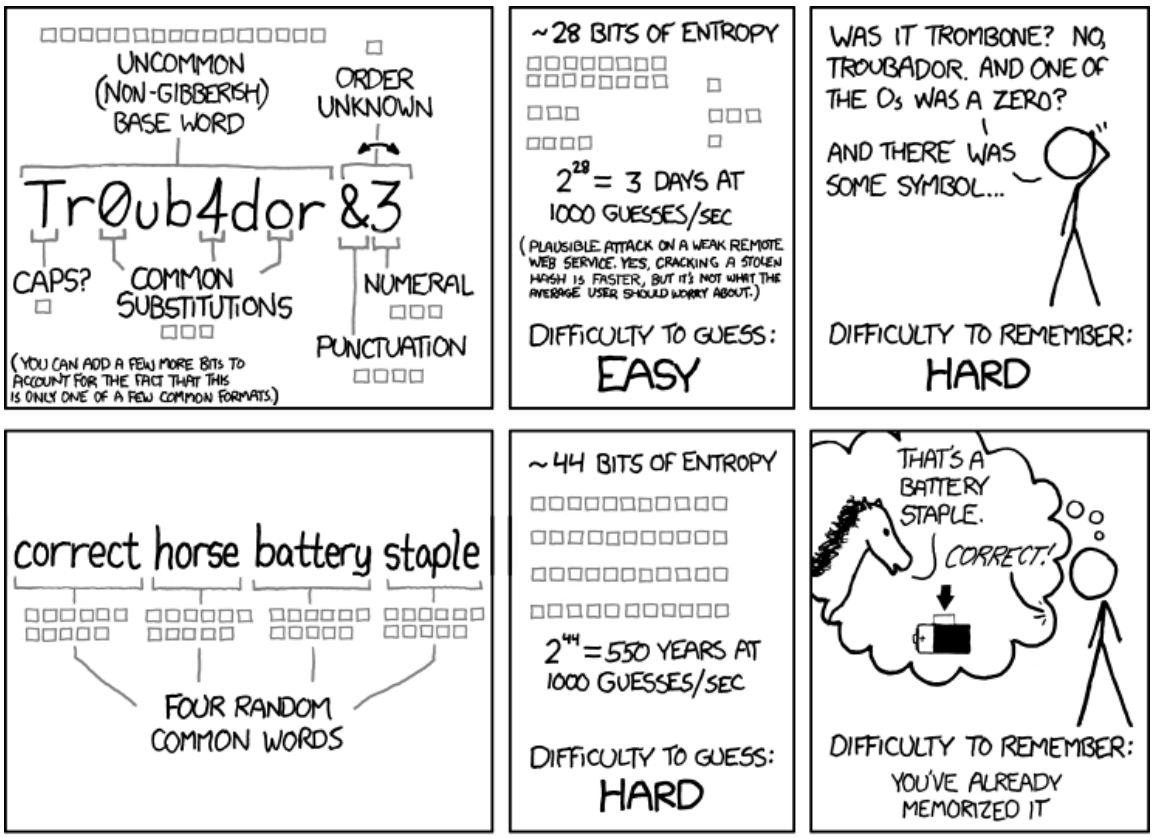
- Security can be overwhelming, and winning is hard
- Choose your battles by defining your threat model
- Even a little security is better than no security, so it's okay if you don't do everything we talk about today, just do whatever you can
- Our recommendations are our own, based on our experiences, general knowledge, and understanding of the general student's threat model

Now for the 10 weird - aka relatively low effort - things!

- Authentication
- Internet browsing
- Hardware

0) Install software updates!

1) Get a password manager



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

1) Password security: basics

- Password entropy
  - Password generation model
  - `# bits of entropy = log_2(# possibilities)`
  - Ex: 4 dictionary words: `log_2(150000^4) = 69 bits`
  - Ex: 8 random letters (lower case or upper case): `log_2(52^8) = 46 bits`
- Diceware
- Unique passwords

1) Password managers

- Currently accepted a best practice in security community
- Remember a single strong master password, randomly generate the rest
- Browser plugins
    - Makes life easier for you, also helps prevent phishing attacks

1) Password managers: recommendations

- KeePassX
  - https://ssd.eff.org/en/module/how-use-keepassx

2) Use 2-Factor authentication

2) 2-Factor Authentication

- Something you know (password) + something you have (token)
- SMS, TOTP, U2F
- At least use 2FA for the services you really care about

3) Don't use biometrics

3) Biometrics: don't use them

- Can't change things once biometrics are compromised
- Your fingerprint isn't protected by the Constitution
  - You're protected against revealing passwords under the Fifth Amendment (right against self-incrimination)

Internet browsing

- Network connections
- Browsers
- Browser extensions
- Online applications
- Encrypted chat
- Anonymous browsing

4) Use a secure web browser

4) Browsers: recommendations

- Firefox is nice, open source, has lots of helpful security browser extensions

- Opera has a free VPN - useful if your internet connection is being spied on
- Google Chrome has sandboxing and gets automatic security updates
- Chromium is a free-software version of Chrome, no automatic updates

5) Use browser extensions that help enforce good security habits

5) Browser extensions

- uBlock Origin: blocks scripts serving advertisements; you can also use it to make a "malicious ad" blocklist
    - Not AdBlock Plus
    - **NOT uBlock**
- HTTPS Everywhere: tries to use an encrypted connection whenever it can, verifies certificates of websites you visit
- NoScript (Firefox only): blocks javascript, Flash, etc, except on pages you've explicitly decided to trust
    - Can do the same thing in Chrome/Chromium Settings menu ("Show advanced settings..." -> Privacy -> Content Settings)
- Privacy Badger: detects and blocks ads/trackers
- Be careful when installing browser extensions! Check the distributor, check what permissions it requires

6) Use online applications that you trust

6) Other online applications, search engines

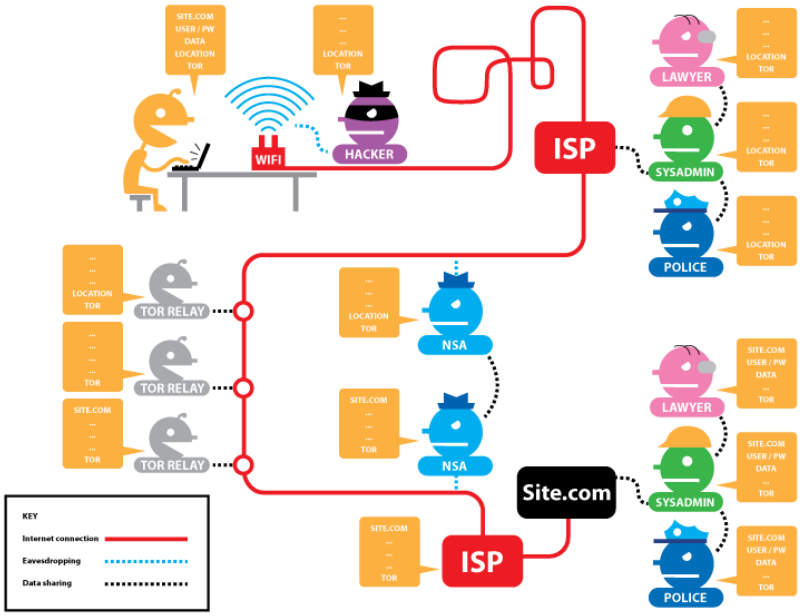
- DuckDuckGo.com: privacy-respecting search engine
- Framasoft.org: central homepage for many privacy-respecting webapps, such as Framadate.org (like WhenIsGood), Framapad.org (like Google Docs)

7) If you care, use anonymous browsing

7) Anonymous Browsing with Tor

- Tor is an anonymizing network that routes your traffic through a series of different volunteer-run servers, so no single eavesdropper can tell where it's really going
- https://www.torproject.org/

7) Anonymous Browsing with Tor



7) Anonymous Browsing with Tor

- The easiest way to use Tor is with the Tor Browser, a modified version of Firefox with Tor built in
- https://www.torproject.org/projects/torbrowser.html.en
- The Tor Browser also includes NoScript and HTTPS Everywhere
- There's a simple slider to configure how secure vs. usable you want the Tor Browser to be
    - Click on the onion logo, and select "Privacy and Security Settings"

8) Use end-to-end encrypted communication

8) Encrypted communication

- The Ideal: End to End Encryption
  - only the 2 people communicating (at the "ends") can read the messages
  - Intermediate servers can't read anything

8) Encrypted communication: recommendations

- Signal
  - App for iOS and Android phones, super-easy to set up and use
  - On Android, can set it as default SMS app

9) Backup early, often, and to completion - especially your security stuff, etc.

9) Backups

- Backups are good for you in general.
- In case your laptop dies / is stolen.
- Make them (encrypted!). Regularly.
- Specifically for purposes regarding security, back up your gpg (`~/.gnupg`), ssh keys (`~/.ssh`), password manager files (e.g. your `*.kdbx` file for KeePassX)

9) Backups: recommended steps

- Get an external harddrive
- Backup using
  - Mac OS: Time Machine (check the box for encrypted backups)
  - Ubuntu: rsnapshot on an encrypted (e.g. LUKS) disk

10) Secure your hardware

10) Hardware tracking

- Before you lose your phone/laptop/etc., install a device tracking application
- Enables device tracking + remote wipe

- Mac OS / iOS: Find My iPhone
- Android: Android Device Manager
- Open source, works on all major OSes, but requires some more tech saavy: Prey (preyproject.com)

10) Full Disk Encryption

- Do it so that if someone gets physical access to your machine, they can't also read your files
- When entering the United States, Customs and Border Protection can temporarily detain you, seize your devices, and image them. They can do this without a warrant, and they can do this if you are a citizen. Turn your stuff off before you go through customs.

- Mac - enable FileVault
- Ubuntu - easiest to set up LUKS (Linux Unified Key Setup) when you initially install Ubuntu / format your disks. Frontend is cryptsetup(8). (Don’t forget to encrypt your swap partition!)

Acknowledgements

- Benjamin Barenblat (bbaren)
- SIPB

Resources

- Slides at https://git.io/easy-security
- EFF Surveillance Self Defense https://ssd.eff.org/
- https://www.cryptoparty.in/
- http://www.slashgeek.net/2012/06/15/how-to-be-completely-anonymous-online/
- https://onlinesafety.feministfrequency.com/en
- https://tech.safehubcollective.org/cybersecurity/
- riseup.net