InfoSec 101

Introduction to Information Security for (non-IT) Professionals

Fabian Lischka, Larry Salibra, Leonhard Weese

FCC, Hong Kong, 2015-02-26

v0.91 from 2015-02-23

Content

- Introduction
  - What can go wrong? Why should I care? Disclaimers
- Suggested Best Practices
  - Basics: Passwords, Phishing, Cloud Storage
  - Communication: Browsing, VPN, Email, Chat
  - Miscellaneous
- Questions

Introduction: What can go wrong?

- Threats
  - WFO (“Well funded organizations”) – maybe
    - NSA, GCHQ, China?
  - Criminals & Hackers (black hat)
    - Phishing

Introduction: Why should you care?

- You are dealing with sensitive information
  - You could be a target
  - Your communication could be monitored
  - Your data could be manipulated/deleted
- Protect:
  - Sources, safety, ability to operate, reputation
- Avoid:
  - Accidental disclosures/information leaks
  - Chilling effect on (potential) sources
    - If I were whistleblower, I'd much rather contact you via PGP

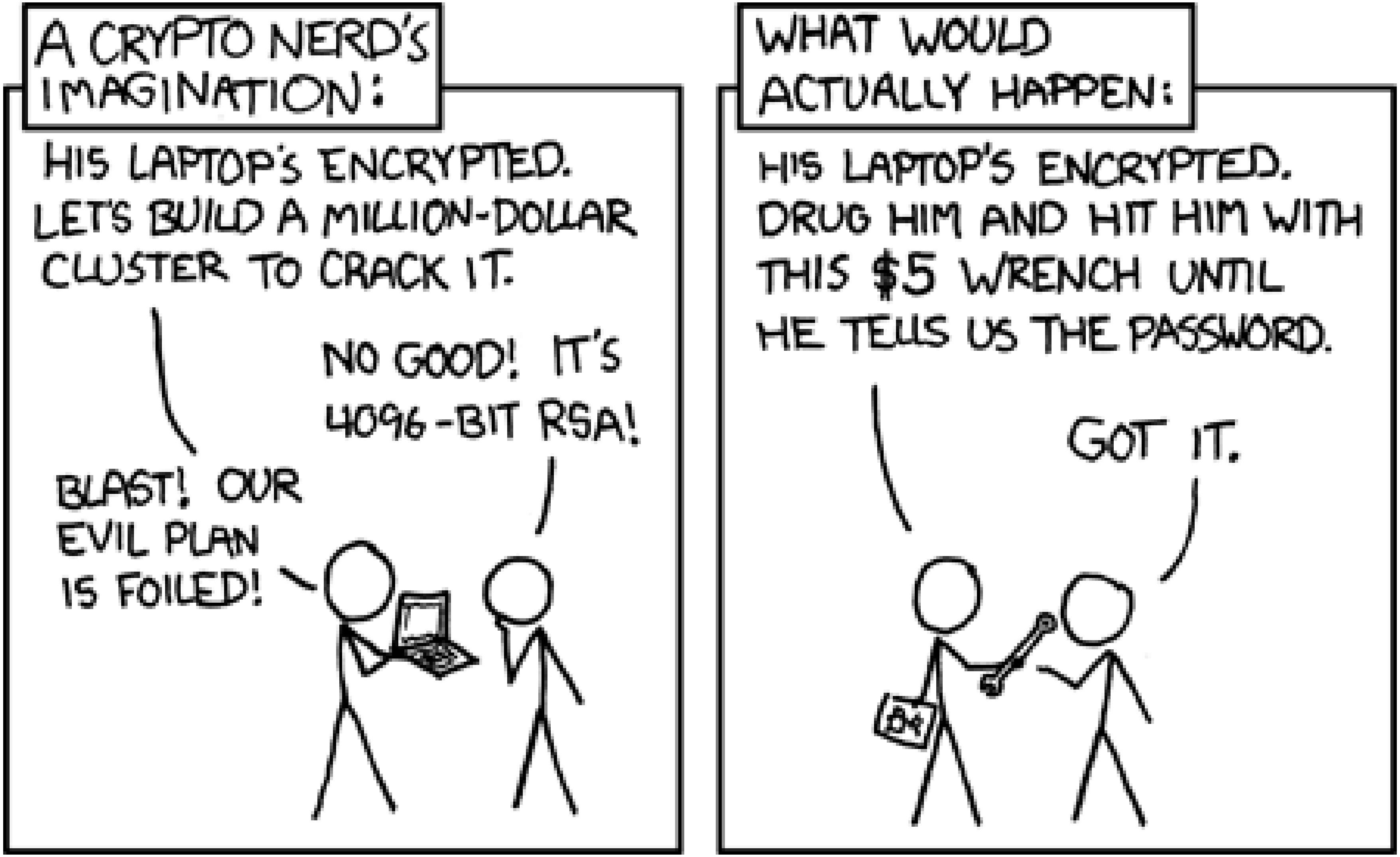
Introduction: Why should you care?

- “Even if the men in suits aren't after you, there are benefits to everyday crypto” – Jennifer Valentino DeVries, WSJ
- Learn to use it – might come in handy
  - Snowden revelations were delayed because Greenwald didn't have software or expertise
- Network effect
  - Communication tools more useful if more people use them
- Red flag
  - Help your fellow journalists: make security normal, a “default”, rather than a red flag

Introduction: Disclaimer

- Using certain tools can raise red flags
- Certain tools can be slow, clumsy, inconvenient
- Might require expertise, discipline
- Do not rely on this in life-and-death situations
  - Weakest link property
  - WFO will get in, if they really want to
    - PGP/GPG and certain other protocols seems unbroken
    - But: so many ways to get in

Introduction: Disclaimer


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.
$4

Best Practices: Contents

- Basics: Better…
  - Passwords (Protect against Phishing, Malware)
  - Disk Encryption
  - Cloud Storage
- Communication
  - Browsing, Tor
  - VPNs
  - Email, Chat/Voice
  - Whistleblowing
- Miscellaneous/Advanced

Best Practices: Passwords

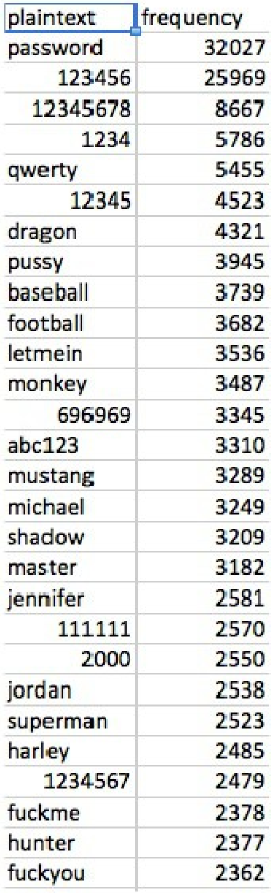
- Two basic ideas
  - Avoid bad passwords, use good passwords
  - Don't re-use the same password
- Unfortunately, these ideas conflict
- Solution: Password Managers

Best Practices: Passwords

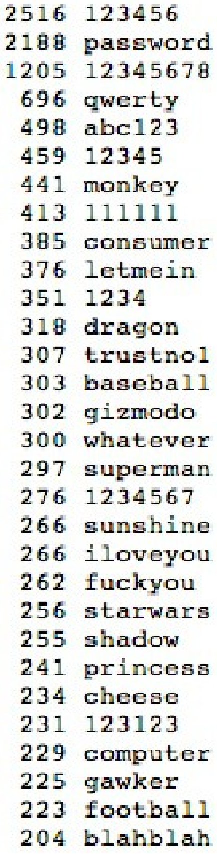
- Avoid bad passwords
  - Things you love (but so does everyone else)
    - Pets or significant others; Sports, sport teams, bands
    - Family, religion, love, sex (`696969`, `love`, `jesus`, `angel`, `lord`)
  - Words related to the site (eg `job`, `career`, `link` for linkedin)
  - Generally, dictionary words, unless multiple unusual ones
  - Patterns (`1234`, `qwerty`, `abcd`, `1qaz`)
- Don't rely on simple tricks, they're all well known!
  - Appending numbers, exclamation marks (`password123`): not secure
  - Simple substitutions (`p@55word`): not secure
  - Simple composition of common patterns (`ilovejesus123`): not secure

Best Practices: Passwords

- LinkedIn breach (2012), Gawker breach (2010)



plaintext	frequency
password	32027
123456	25969
12345678	8667
1234	5786
qwerty	5455
12345	4523
dragon	4321
pussy	3945
baseball	3739
football	3682
letmein	3536
monkey	3487
696969	3345
abc123	3310
mustang	3289
michael	3249
shadow	3209
master	3182
jennifer	2581
111111	2570
2000	2550
jordan	2538
superman	2523
harley	2485
1234567	2479
fuckme	2378
hunter	2377
fuckyou	2362



```
2516 123456
2188 password
1205 12345678
 696 qwerty
 498 abc123
 459 12345
 441 monkey
 413 111111
 385 consumer
 376 letmein
 351 1234
 318 dragon
 307 trustno1
 303 baseball
 302 gizmodo
 300 whatever
 297 superman
 276 1234567
 266 sunshine
 266 iloveyou
 262 fuckyou
 256 starwars
 255 shadow
 241 princess
 234 cheese
 231 123123
 229 computer
 225 gawker
 223 football
 204 blahblah
```

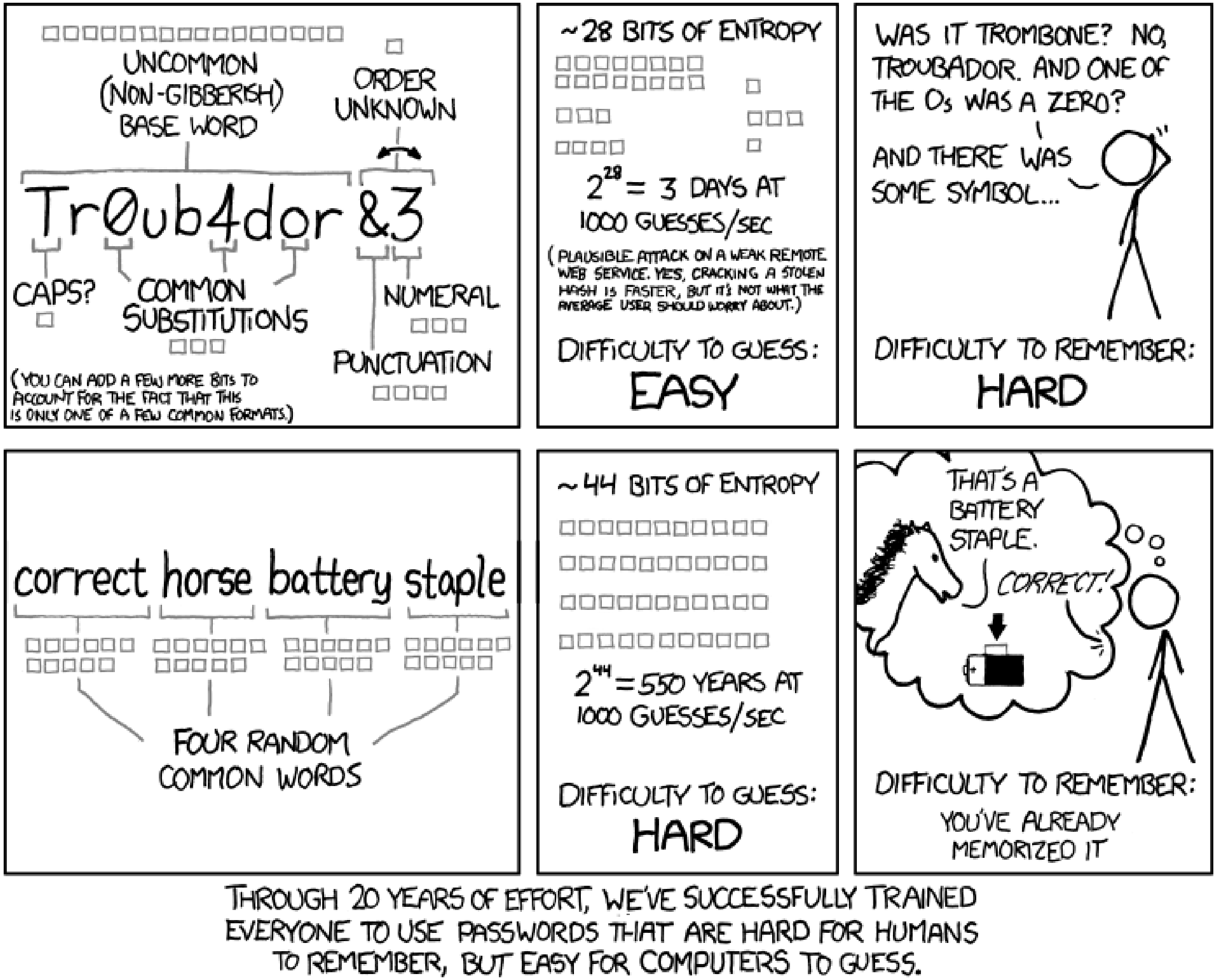
Best Practices: Passwords

- Good technique (“Schneier Scheme”):
  - Use 1st letter of words of a long sentence (the *passphrase*)
- Example:
  - Wo hěn xǐhuān HK, IT security, and (sometimes) 9 hours sleep
  - **WhxHK,ITs&(st)9hs**
- Best Practices:
  - Creative, weird, unique passphrase, possibly multi-language
  - Avoid catch phrase, song lyrics, movie quote. Make your own!
  - Long phrase, resulting in at least 12 characters
  - Include numbers, small/capital letters, symbols, etc.
  - Note: might see different keyboard layouts on other computers

Best Practices: Passwords

- Good technique:
  - Use 4 or 5 *randomly* selected words from a large dictionary
  - Maybe truncated at 5 or 4 characters
  - Number/symbol to separate them
- Example
  - Keelhaul, cleistogamy, evince, vacuum
  - **Keel3clei6evin9vacu**
- Best Practices
  - Random words, not some words that you like
  - Sufficiently many

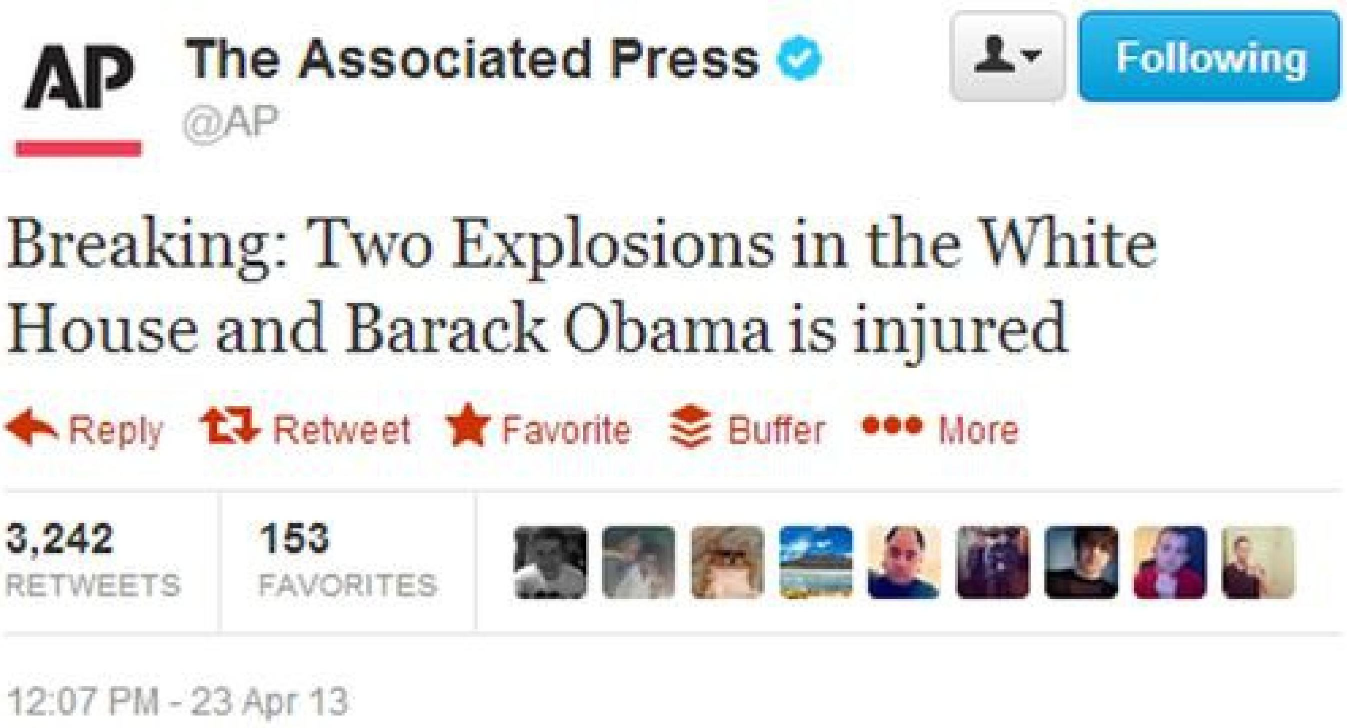
Best Practices: Passwords


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
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.

Best Practices: Password Managers

- Purpose: Use different (secure) passwords for different sites
  - Password Managers generate and store these passwords securely
  - Password Managers require one Master Password
    - Better be good! Better don't forget it!
- What: App or browser addin, available on computers, smart phones
- Recommended:
  - Apple only, simple: **iCloud Keychain**
  - Free, open source: **Password Safe/pwsafe,** or **KeePass**
  - Commercial solution with support: **1Password,** or **LastPass**
- Disadvantages:
  - Cumbersome, particularly sync between devices
  - If compromised, all your paswords are exposed

Best Practices: Avoid Phishing



The Associated Press
@AP

Breaking: Two Explosions in the White House and Barack Obama is injured

3,242 RETWEETS

153 FAVORITES

12:07 PM - 23 Apr 13

Best Practices: Avoid Phishing

- Phishing: Common and surprisingly effective attack
- What is it? Fake emails (colleague, bank, etc) lures you to malicious website
  - you "log in" with your real credentials on a fake site or are hit by “drive-by” exploit
- Note:
  - Link can have some legitimate text (http://www.mybank.com),
    but point somewhere else (http://phishingsite.xyz)
  - Server (whatever is before the first slash) must be read from right to left
    (this is a bad link: www.mybank.com.domain.bla.phishingsite.xyz/login.html)
- Prevention:
  - Be suspicious of unexpected, somewhat generic emails
  - Don't click on links in emails to "log in" somewhere. Type it in!
  - Examine *actual* links (not what's displayed)
  - Check exact name of the website, and the "lock" symbol
  - Never provide your password to anyone, except the *actual* website it's for

Best Practices: Avoid Malware

- Rule of thumb: if it's free, it's crap.
- Trojan Horse
  - malicious software packaged to look like something desirable, tricking the user into actively installing it
  - Examples:
    - spammy websites claim that your computer is infected, & offer free "virus scanner" for download. Actually, this "virus scanner" is malware
    - a popular early Android app was a free flashlight app. However, it uploaded all the user's contact data, location, etc. to the provider, who sold it.
- Prevention:
  - Don't install arbitrary "disk cleaners", "search bars", etc.
  - Don't install anything unless necessary, and only from a trusted source
  - Don't open untrusted attachments
  - Don't plug in untrusted USB sticks

Best Practices: Disk Encryption

- Purpose: Protects the content of your laptop
  - when it's stolen
  - when it's in the hand of government/border control
- What: App, or embedded in the operating system
- How:
  - Encrpyts your entire harddrive, and
  - Decrypts what's needed on the fly
- Without Disk Encryption, can just take out harddisk from your laptop, and copy everything from it, without logging in
- Disadvantages: Might be ever so slightly slower on old hardware

Best Practices: Disk Encryption

- Smartphones:
  - Automatically enabled in iOS 8, and Android L
  - Can be set up for earlier Android versions
- Computers:
  - OS X: FileVault
  - Windows: ??
  - Careful: TrueCrypt appears to have some issues
- External Diskdrives:
  - OS X: Can be formatted as encrypted disks (Disk Utility), password can be stored in Keychain
  - Windows: ??

Best Practices: Deleting Data

- Modern computer:
  - Deleted Data is is just moved into the trash folder
  - When the trash folder is emptied, only the "directory link" is deleted
  - Actual data is still there
- Prevention:
  - Chose "Secure Erase"
- Don't forget backups and cloud syncing!

Best Practices: Cloud Storage

- Be aware of what is in the cloud
  - iOS/OS X keep your contacts, calendars, photos in iCloud
  - iCloud celebrity photo hack: most likely bad passwords & social engineering
- Suggested Tools:
  - Encrypted, but experimental: TorrentSync
  - Careful, only partial encryption: Dropbox, Google Drive, iCloud
  - Not recommended at all: 360 Cloud Disk, Baidu Cloud Disk, QQ Net Disk
- Note:
  - Whatever you encrypt yourself (with PGP) you can put on any cloud server; it can't be decrypted without your private key

Best Practices: Communication

Best Practices: Browsing

- Search engines, social networks track you (even on other sites)
  - Facebook is notified whenever you visit a site that has a "Like" button
- Cookies allow sites to identify you over time, across sites
- You might be uniquely identified by your browser alone (see Panopticlick)
- You and your location might be determined from your IP address (see IPLeak)
- Prevention:
  - Occasionally delete all cookies/history (careful: need to re-login)
  - Browse in Private mode ("porn mode")
  - Use different browsers for different tasks (private/job/sensitive)
  - Install some of the tools in the next section
- Notes:
  - Do not ignore warnings about security certificates. MITM ("men in the middle") attackers could read all your traffic (incl. Passwords)
  - Always use HTTPS, if possible, as it encrypts your traffic (lock symbol)

Best Practices: Browsing – Search

- Recommended Search Engines:
  - **DuckDuckGo:** Anonymous, unlogged search.
    - Can be set as default in many browsers, including Safari (OS X, iOS)
  - **Ixquick:** Anonymous, unlogged search, using non-Google sources
  - **StartPage:** Anonymous, unlogged search, using Google as the source
- Not recommended: Bing, Google, Yahoo
- DuckDuckG "Bangs": !s, !g, !v, !w

Best Practices: Browsing - Addons

- Recommended Tools:
  - **Adblock Plus:** Blocks ads when browsing. Android, Chrome, Firefox, IE, Opera, Safari. Lets "acceptable ads" through by default, but can disable.
  - **AlwaysHTTPS:** Encrypts your browsing with many websites. Firefox, Chrome, Opera.
  - **Ghostery:** Stops trackers when browsing. Uploads anonymized tracker data by default. Firefox, Chrome, Opera, Safari.
  - **Privacy Badger:** Stops advertisers and trackers when browsing. Firefox, Chrome.
- Similar: Adblock, Adblock Edge.

Best Practices: Browsing – Tor

- Tor routes all your traffic through a few extra hops, encrypted, so that
  - the website you are visiting does not know who it's talking to, and
  - interceptors near you don't know what websites you're visiting
- What: stand-alone application available for most platforms, based on Firefox
- Recommended: **Torbrowser** (OS X, Win), **OnionBrowser** (iOS), **Orbot** (Android)
- Disadvantages:
  - Can be rather slow
  - final hop in the clear

Best Practices: Browsing – Tor

- Best Practices:
  - Do not divulge private information when using Tor
    - Don't log into any website (Facebook, etc.)
    - Don't use your real name, or google yourself
  - Don't open documents downloaded through Tor while online
  - More! See Tor documentation
- ".onion" only accessible with a Tor browser
  - *Example:* DuckDuckGo: 3g2upl4pq6kufc4m.onion

Best Practices: VPNs

- Virtual Private Network: from your device
  - *encrypted* all the way to a specific VPN server "somewhere"
  - from VPN server *unencrypted* to its destination
- Protects from interception "nearby"
  - Internet Cafe, your ISP, local government
- Allows to circumvent censorship
    - When traveling in certain jurisdictions
    - Might have to enable advanced options for that

Best Practices: VPNs

- Many providers, but no free lunch
  - expect to pay for good service (about USD 5/month)
- Recommended:
  - **AirVPN**. Excellent VPN, strong commitment to security & privacy. Run by activists in Italy. Three connections per account. Unix, OS X, Win, iOS, Android.
  - **ZenMate**: Free Browser add-on. Routes only browser traffic through a VPN, *not* other apps (Mail, Messenger, etc.). Chrome, FireFox, Opera.
- To test whether the VPN works correctly:
  - Visit ipleak.net with/without VPN active
  - Compare what IP address and location it reports

Best Practices: Email & PGP

- Basic Idea:
  - Encrypt your message including attachments into some blob (the *ciphertext*)
  - Send that blob via email
- Note: Meta data is *not* encrypted, can be intercepted / manipulated
  - Sender, recipient
  - Subject line
  - Length
  - Time and frequency of mails

Best Practices: Email & PGP

- The standard is PGP/GPG
  - PGP = "Pretty Good Privacy": original implementation (1991)
  - OpenPGP: open internet standard
  - GPG = "Gnu Privacy Guard": open source implementation
- Purpose: PGP/GPG takes arbitrary text and encrypts it, using asymmetric encryption
- What:
  - Command line tool, but
  - Various apps available, including utilities that integrate with existing email programs

Short Excursion: Encryption

- Encryption uses a key, and an algorithm
- Method:
  - *Plain Text + key + algo = ciphertext*
  - Send the ciphertext across (even a non-secured line)
  - Ciphertext + key + algo = Plain Text
- Evil Eve doesn't understand anything, if she doesn't have key
- Postal analogy:
- Disadvantages:
  - Alice and Bob must have the same key. They must have met once before, and agreed on a key.

Short Excursion: Asymmetric Encryption

- Asymmetric encryption is *awesome* mathemagic:
  - Keys for *encryption* and *decryption* need **not** be the same
  - Create a key pair, publish one half. Other half cannot be reconstructed!
- Method:
  - Plain Text + Bob's public key + algo = ciphertext
  - Send the ciphertext across (even a non-secured line)
  - Ciphertext + Bob's private key + algo = Plain Text
- Evil Eve doesn't understand anything, if she doesn't have Bob's private key.
- Problems:
  - Key management, MITM (comparing "finger prints")

Best Practices: Email & PGP

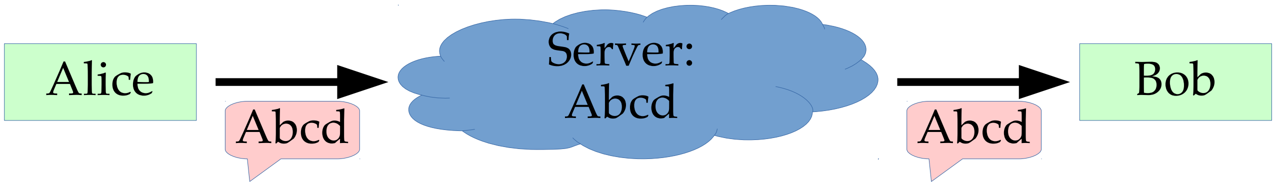
- Recommended:
  - GPG4Win. GPG for Windows
  - GPGTools. GPG on OS X Mail.
  - IPGMail: GPG for iOS.
- For key management, consider keybase.io
- Not recommended for sensitive information:
  - Normal email

Best Practices: Email & GPG

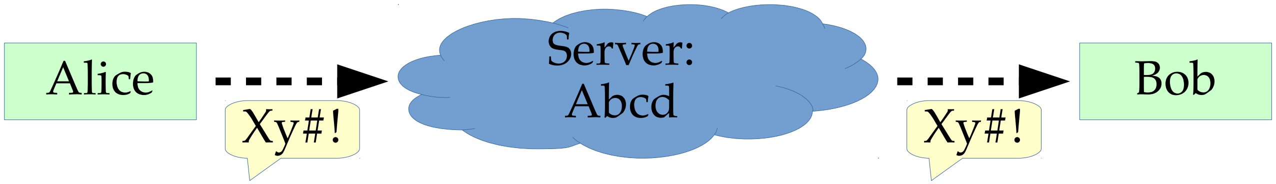
- Use generic subject ("cat pictures")
- Key generation:
  - 4096 bits, RSA
  - Expiry date, say 2 years
    - Allows to retire key
    - Can always extend, link to new key
  - Strong passphrase
- Beware of drafts stored in clear text on the mail server
  - Either enable "encrypt drafts", or go off-line while composing sensitive emails

Short Excursion: Levels of Security

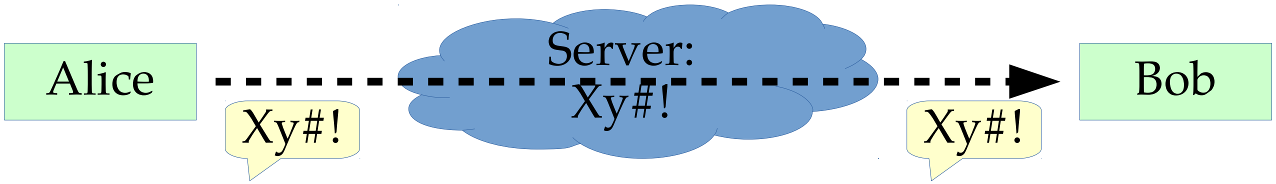
- Can send message across:
  - Unencrypted



  - Partially



  - End-to-End



Best Practices: Chat

- Most apps are crap, but there are good & free alternatives!
- Weaknesses:
  - Meta data (with whom do you chat how often)
  - MITM (man in the middle attack)
    - Solution: Out-of-band key comparison

Best Practices: Chat

- Recommended (End-to-end encrypted):
  - **iMessage**: Closed Source. Apple only.
  - **Telegram**: only “Secret Chat” end-to-end. Closed source. Smartphone, Desktop
  - **TextSecure**: Open source. Android, but iOS version on the way.
  - **Threema**: Closed source. Not free. Smartphone.
- Recommended (advanced!):
  - **Adium**: OTR chat for OS X. A bit clunky.
  - **Pidgin + OTR**: OTR chat for Windows.
  - **ChatSecure**: OTR chat for iOS, Android. A bit clunky.
- Only partial encryption: AIM, Blackberry Messenger, Facebook Chat, IRC, Line, Telegram non-secret & groups, WhatsApp, Yahoo Messenger
- Not recommended: Firechat, Google Hangout, Google Talk, ICQ, Kik, Kaoko, QQ, Snapchat, Viber, WeChat, Whisper. SMS.

Best Practices: Voice

- Recommended:
  - Signal (iOS), Redphone (Android)
    - Free, encrypted calls
- Only partial encryption:
  - Google Hangout (Voice/Video)
- Not recommended:
  - Normal phone calls
  - Skype

Best Practices: Whistleblowing

- Recommended: SecureDrop
- Purpose: Confidential communication between journalist and source
- What: Stand-alone software package, running on a server
- How:
  - Contact news organization's “SecureDrop” *via Tor*
  - Choose a pseudonym
  - Drop documents securely
  - Follow up/Communicate using pseudonym
- Your organization can set up an instance of the software on a server
- Example: Contact *The Guardian* at 33y6fjyhs3phzfjj.onion

Best Practices: Miscellaneous

Miscellaneous: Information Leaks

- Your phone is a tracking device
  - Cell phone provider knows where it is, smart phone knows where it is
- If you hand out info, you might reveal more than you thought
  - Phone number, email can be googled: what to they reveal?
  - Reverse Image Search (TinEye, Google)
    - See whether a picture appears elsewhere on the net, eg Facebook, LinkedIn, Twitter, or your employer's website
  - Images contain embedded information (EXIF data)
    - Might contain the time and location the picture was taken (McAfee case)
    - Tools available to remove that information (EXIF strippers, metadata scrubbers)
      - Recommended (but maybe a bit complicated): ExifTool. Windows, OS X, UNIX
- Your IP address can lead to your ISP, and then to you.
- Cookies on your browser can identify you across sites

Miscellaneous: Multiple Accounts

- Recommended: Separate accounts on your computer
  - Work
  - Private
  - Project XYZ
- Use shared folders to move information between them in a controlled matter
- Disadvantage:
  - Have to re-enter passwords etc.
- Advantage:
  - Makes information leaks less likely

Miscellaneous: Defense in Depth

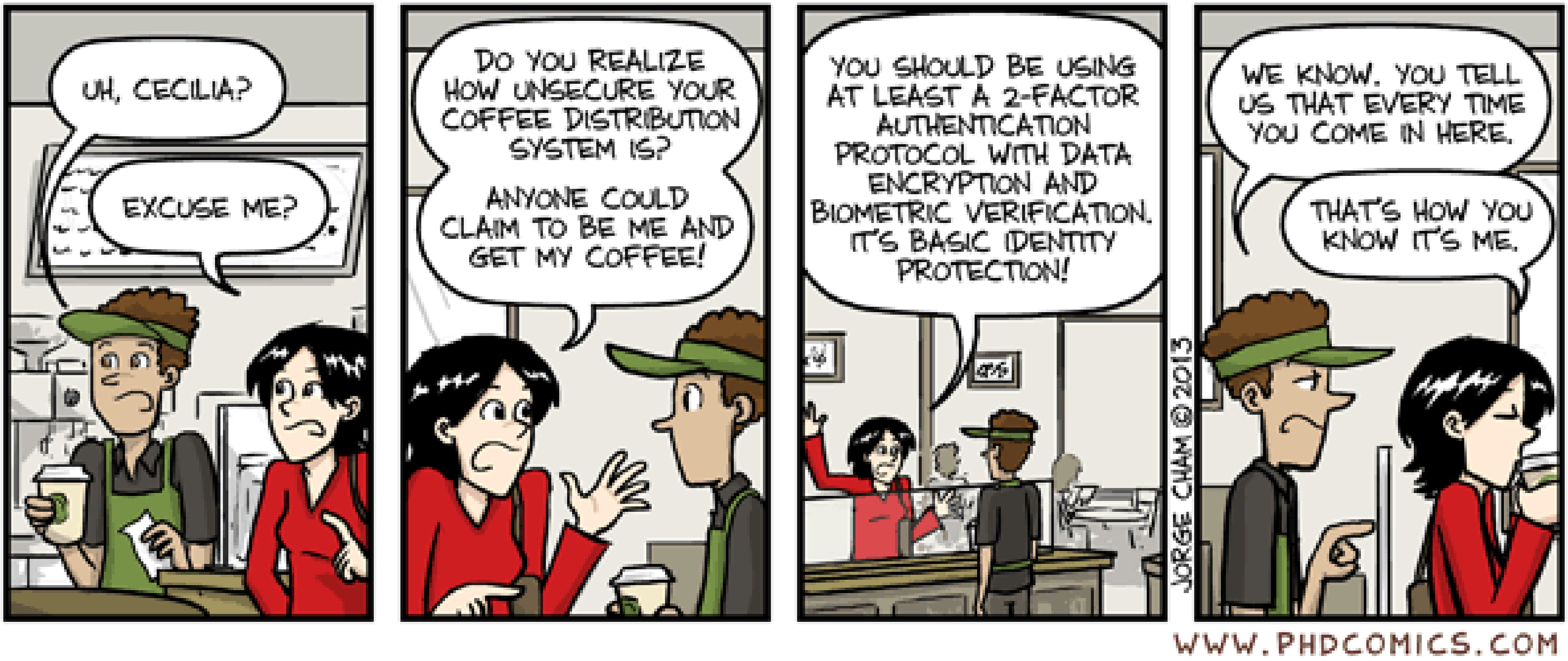
- Multiple layers of protection might be best
- If the adversary breaks one layer, the information is still protected
- Examples:
  - Agree on code words for sensitive entities
  - Cut message in many pieces, transmit...
    - … part on iMessage, part on Signal/Redphone, part on Telegram, part on Wickr, part on phone: “let's meet”, “Sunday”, “10 am”, “Wagyu Lounge”, “red shoes”
  - Use TOR over a VPN
  - Etc.

Finally: Advanced Steps

- If you have highly sensitive information, you'll need to be way more careful, systematic, paranoid.
- Research:
  - OpSec
  - VMs (Virtual Machines)
  - Tails (The amnesic incognito live system)
- Remember:
  - If they want to get you, they will.

Questions?

- More resources & links: http://fabianlischka.github.io/InfoSec101/


UH, CECILIA?
EXCUSE ME?
DO YOU REALIZE HOW UNSECURE YOUR COFFEE DISTRIBUTION SYSTEM IS?
ANYONE COULD CLAIM TO BE ME AND GET MY COFFEE!
YOU SHOULD BE USING AT LEAST A 2-FACTOR AUTHENTICATION PROTOCOL WITH DATA ENCRYPTION AND BIOMETRIC VERIFICATION. IT'S BASIC IDENTITY PROTECTION!
WE KNOW. YOU TELL US THAT EVERY TIME YOU COME IN HERE.
THAT'S HOW YOU KNOW IT'S ME.
JORGE CHAM © 2013
WWW.PHDCOMICS.COM