InfoSec 101

Introduction to Information Security for (non-IT) Professionals

Fabian Lischka, Larry Salibra, Leonhard Weese

FCC, Hong Kong, 2015-02-26

v0.94 from 2015-02-24

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?

- Examples:
  - Film journalist in Syria: Gov't confiscated laptop
  - AP Twitter account hacked: Phishing
  - GCHQ captured journalists' emails (BBC, NYT, …)
  - Hackers used hotel Wi-Fi to steal executive's data
- Can our recommendations protect you?

Attack	Opportunistic	Targeted
Hackers/Criminals	Yes	Yes, likely
Gov't/WFO (NSA,...)	Yes (but red flag?)	Well....

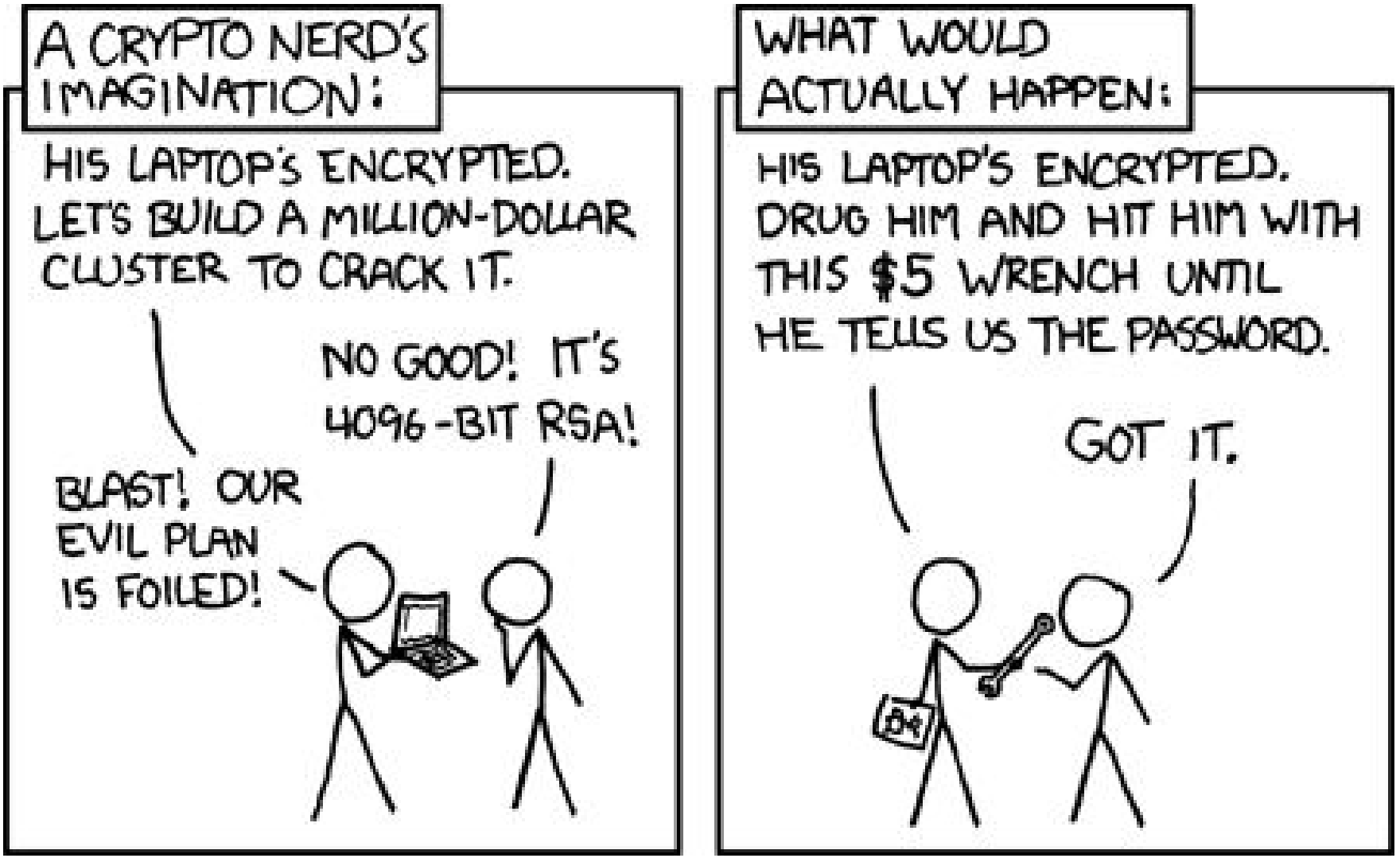
Introduction: Why should you care?

- “Even if the men in suits aren't after you, there are benefits to everyday crypto”
  - Jennifer Valentino DeVries, WSJ
- Benefits:
  - Avoid chilling (potential) sources
    - Whistleblowers prefer PGP/SecureDrop
  - Learn to use it – might come in handy
    - Snowden revelations delayed
  - Network effect
  - Red flag: Help your fellow journalists

Introduction: Disclaimer

- Red flag!
- Inconvenient
- Requires some expertise, discipline
- Weakest link property
- Just basic stuff!
  - Do not rely on this in life-and-death situations
  - No protection against WFO, governments, etc.
    - However: PGP, some other protocols appear unbroken

Introduction: Disclaimer



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 ways hackers attack passwords:
  - Dictionary plus trial and error
  - Database breaches (LinkedIn)
- Two ideas to protect your passwords:
  - 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)
  - Words related to site
  - Dictionary words, patterns (`1234`, `qwerty`, `abcd`)
- Don't rely on simple tricks, they're all well known!
  - Appending: password123, password!
  - Substitutions: p@55word
  - Simple composition: password123angel!

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"):
  - 1st letter of long *passphrase*
- Example:
  - Wo hěn xǐhuān HK, IT security, and (sometimes) 9 hours sleep
  - **WhxHK,ITs&(st)9hs**
- Best Practices:
  - Creative, weird (possibly multi-language)
  - Avoid: catch phrase, song lyrics, quotes
  - Result should have at least 12 characters
  - Note: different keyboard layouts on other computers

Best Practices: Password Managers

- Purpose: Different passwords for different sites
  - Generate & Store
  - Protect with Master Password (Better be good! Better don't forget it!)
- What: App or browser addin, for computers, smart phones
- Recommended:
  - Apple only, simple: **iCloud Keychain**
  - Free, open source: **pwsafe,** or **KeePass** (more powerful, complicated)
  - Commercial solution with support: **1Password,** or **LastPass**
- Disadvantages:
  - Can be cumbersome (sync)
  - If compromised, all your paswords are exposed

Best Practices: Avoid Phishing

Best Practices: Avoid Phishing

- What: Fake email lures you to malicious website
  - "log in" on fake site, or hit by *drive-by* exploit
  - *Spearphishing*
- Pitfalls:
  - Visible: www.mybank.com, actually: www.phishy.net
  - Server: read right to left (this is bad: www.mybank.com.domain.bla.phishy.net/login.html)
- Prevention:
  - Don't click on that link!

Best Practices: Avoid Malware

- Rule of thumb: if it's thrust upon you, it's crap
- Trojan Horse
  - Alert: Your computer is infected!
  - Free flashlight app!
- Prevention:
  - Don't install that junk
  - Attachments, USB, etc.

Best Practices: Disk Encryption

- Purpose: Protects the content of your laptop
- What: App, or embedded in operating system
- How:
  - Encrypts entire disk, decrypts on the fly
- Disadvantages:
  - Forget your password, say **Hasta la vista!**

Best Practices: Disk Encryption

- Smartphones:
  - Automatical (in latest versions: iOS 8, Android L)
- Computers:
  - OS X: FileVault
- External drives:
  - OS X: Format as encrypted disks (Disk Utility)

Best Practices: Deleting Data

- Modern computer, hard disk, flash drive:
  - Delete just moves data to trash folder
  - “Empty trash” only deletes "directory link"
  - Actual data is still there
- Prevention:
  - Chose "Secure Erase"
- Don't forget backups and cloud syncing!
  - Copies of data might still be around

Best Practices: Cloud Storage

- Be aware of what is in the cloud
- 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:
  - Data encrypted (with PGP) can be put on any cloud server (can't be decrypted without your private key)

Best Practices: Communication

Best Practices: Browsing

- Tracking
  - Search engines, social networks
  - Cookies
  - IP address
- Others on network might see what you browse
- 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/project X)
  - Use HTTPS (lock symbol), encrypts your traffic
  - Heed warnings about security certificates, else potential MITM

Best Practices: Browsing – Search

- Recommended for anonymous search:
  - **DuckDuckGo:** Can set as default eg in Safari
  - **Ixquick:** non-Google sources
  - **StartPage:** Google source
- Not recommended: Bing, Google, Yahoo
- DuckDuckG "Bangs": !s, !g, !v, !w

Best Practices: Browsing - Addons

- Recommended Tools:
  - **Adblock Plus:** Chrome, Firefox, IE, Opera, Safari.
    - Lets “acceptable ads” through by default, but can disable.
  - **AlwaysHTTPS:** Firefox, Chrome, Opera
    - Encrypts browsing to many sites.
  - **Ghostery:** Firefox, Chrome, Opera, Safari.
    - Stops trackers when browsing.
    - Uploads anonymized tracker data by default, but can disable.
  - **Privacy Badger:** Firefox, Chrome.
    - Stops trackers when browsing
- Similar: Adblock, Adblock Edge.

Best Practices: Browsing – Tor

- Tor
  - Routes through extra hops, encrypted, so:
    - website you visit does not know who it's talking to,
    - interceptors near you don't know what websites you visit
  - What: stand-alone application available for most platforms, based on Firefox
- Recommended: **Torbrowser** (OS X, Win), **OnionBrowser** (iOS), **Orbot** (Android)
- Disadvantages:
  - Slower
  - 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,* to a specific VPN server "somewhere"
  - From VPN server *unencrypted* to destination
- Protects from interception "nearby"
  - Internet Cafe, your ISP, your government (maybe)
- 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**. Strong commitment to security & privacy.
  - **ZenMate.** Free Browser addon.
    - *Only* browser goes through VPN, *not* Mail, Messenger, ...
- Test whether the VPN works correctly
  - Compare: www.ipleak.net with/without

Best Practices: Email & PGP

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

Best Practices: Email & PGP

- Standard: PGP/GPG
  - PGP = "Pretty Good Privacy": original (1991)
  - OpenPGP: open internet standard
  - GPG = "Gnu Privacy Guard": open source
- Purpose: Encrypt any text
- What:
  - Command line tool, but various apps available

Short Excursion: Encryption

- Encryption uses a *key*, and an *algorithm*
- Method:
  - *Plain Text* + key + algo = *ciphertext*
  - Send the ciphertext across
  - Ciphertext + key + algo = Plain Text
- Postal analogy
- Disadvantage:
  - Alice and Bob must have the same key

Short Excursion: Asymmetric Encryption

- *Awesome* mathemagic:
  - Keys for *encryption* and *decryption* need **not** be the same
  - Create key pair, publish half. Cannot reconstruct other
- 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
- Problems:
  - Key management, MITM (compare "finger prints" OOB)

Best Practices: Email & PGP

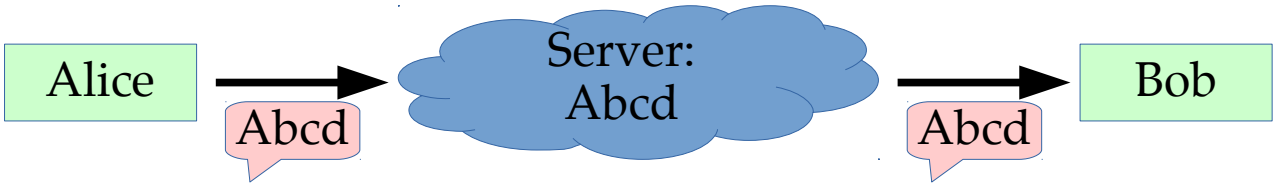
- Recommended:
  - **GPG4Win:** GPG for Windows
  - **GPGTools:** GPG for OS X, with Mail integration.
  - **IPGMail:** GPG for iOS.
- For key management, consider keybase.io
- Not recommended for sensitive information:
  - Normal email

Best Practices: Email & PGP

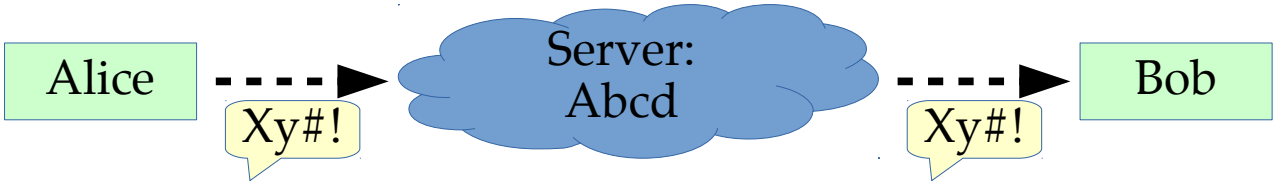
- Use generic subject ("cat pictures")
- Key generation:
  - 4096 bits, RSA
  - Expiry date, say 2 years
    - Allows to retire key
    - Can always extend, link to new key
  - Strong passphrase
- Beware of drafts stored in clear text on the mail server
  - Either enable "encrypt drafts", or go off-line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

Short Excursion: Levels of Security

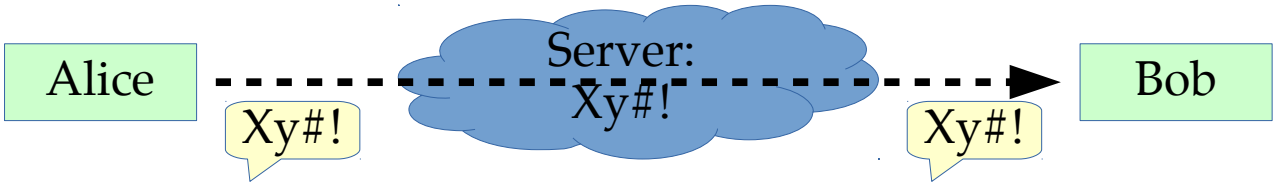
- Can send message across:
  - Unencrypted



  - 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. Open source. Smartphone, Desktop
  - **TextSecure**: Open source. Android, but iOS version on the way.
  - **Threema**: Closed source. Not free. Smartphone.
- Recommended (Advanced, a bit complicated):
  - **Adium**: OTR chat for OS X.
  - **Pidgin + OTR**: OTR chat for Windows.
  - **ChatSecure**: OTR chat for iOS, Android.
- 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 journalist ↔ 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 SecureDrop on a server)
- Example: Contact *The Guardian* at 33y6fjyhs3phzfjj.onion

Best Practices: Miscellaneous

Miscellaneous: Information Leaks

- Your phone is a tracking device
  - Provider knows where phone is, smart phone knows where phone 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): can reveal name etc.
    - Finds picture on net, eg Facebook, LinkedIn, Twitter, employer
  - Images contain embedded information (EXIF data)
    - Time, location the picture was taken (McAfee case)
    - Tools 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: “meet”, “Carl”, “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/