InfoSec 101

Introduction to Information Security for (non-IT) Professionals

Fabian Lischka, Larry Salibra, Leonhard Weese

FCC, Hong Kong, 2015-02-26

V0.96.L from 2015-02-25

Content

- Introduction
  - Disclaimers
- Suggested Best Practices
  - Basics: Passwords, Phishing
  - Communication: Browsing, VPN, Email, Chat
- 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....

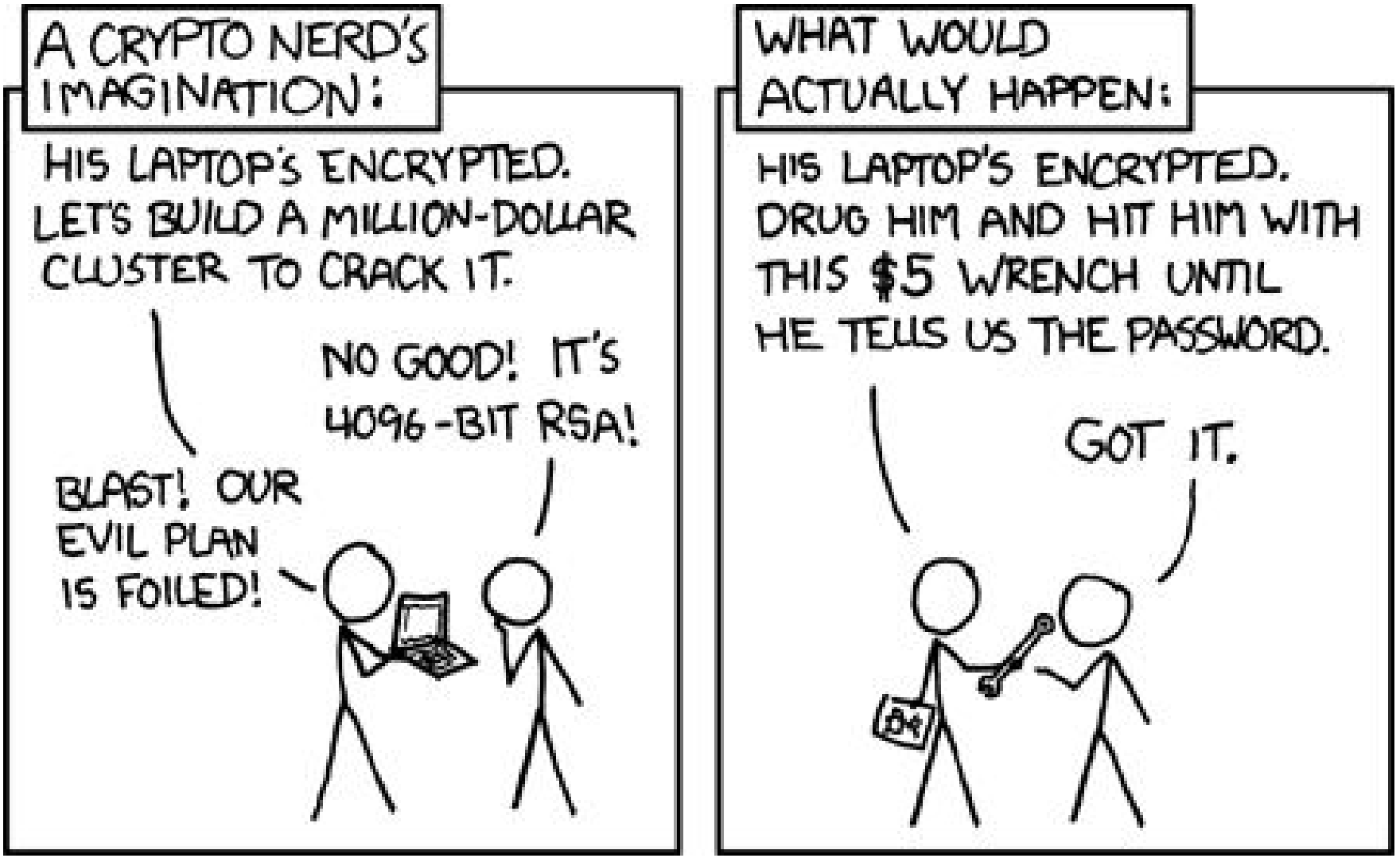
Introduction: Why should you care?

- “Even if the men in suits aren't after you, there are benefits to everyday crypto”
  - Jennifer Valentino DeVries, WSJ
- Benefits:
  - Relieved / confident sources
  - Practice
  - Network effect
  - Red flag: Help your fellow journalists

Introduction: Disclaimer

- Red flag!
- Requires discipline
- Weakest link property
- Only introduction!
  - Do not rely on this in life-and-death situations
  - No protection against WFO, governments, etc.

Introduction: Disclaimer



Best Practices: Passwords

- 3 Attacks:
  - Dictionary + trial and error
  - Database breaches (LinkedIn, Gawker, …)
  - “I lost my password”
- 3 Counter measures:
  - Good passwords!
  - No re-use
  - No security questions
- Problem: Conflict
- Solution: Password Managers

Best Practices: Passwords

- Bad passwords
  - What you love
  - Words related to site
  - Dictionary words, patterns (`1234`, `qwerty`, `abcd`)
- Tricks: 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**
- Good technique ("xkcd scheme"):
  - 4 or 5 randomly selected words
  - Example: Keelhaul, cleistogamy, evince, vacuum
    → **Keel3clei6evin9vacu**

Best Practices: Password Managers

- Purpose: Different passwords for different sites
  - Master Password
- Recommended:
  - Apple only, simple: **iCloud Keychain**
  - Free, open source: **pwsafe,** or **KeePass**
  - Commercial, with support: **1Password,** or **LastPass**
- Disadvantages:
  - Compromise

Best Practices: Avoid Phishing

Best Practices: Avoid Phishing, Malware

- Fake email lures you to malicious website
  - "log in" on fake site, or hit by *drive-by* exploit
  - *Spearphishing*
- Pitfalls:

  1) www.mybank.com → www.phishy.net
  2) www.mybank.com.domain.bla.phishy.net
- Prevention:
  - Don't click!
  - Don't install!

Best Practices: Disk Encryption

- Purpose: Protect data on your laptop
  - Hotel, stolen, border
- Forget your password, say **Hasta la vista!**
- Available:
  - Smartphones: Automatic (on latest: iOS 8, Android L)
  - OS X: FileVault
  - Windows: BitLocker
- External drives:
  - OS X: Format as encrypted disks (Disk Utility)

Best Practices: Browsing

- You leave a massive data trail
  - Search engines, social networks
  - Cookies
  - IP address
- Recommended Tools:
  - **Adblock Plus**
  - **AlwaysHTTPS**
  - **Ghostery**
  - **Privacy Badger**

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 – Tor

- Tor
  - Routes through extra hops, encrypted
  - **Torbrowser** (OS X, Win), **OnionBrowser** (iOS), **Orbot** (Android)
  - .onion, eg 3g2upl4pq6kufc4m.onion (DuckDuckGo)
- Best Practices:
  - Do not divulge private information
  - Don't open documents while online
- Disadvantages:
  - Slower
  - Final hop in the clear

Best Practices: VPNs

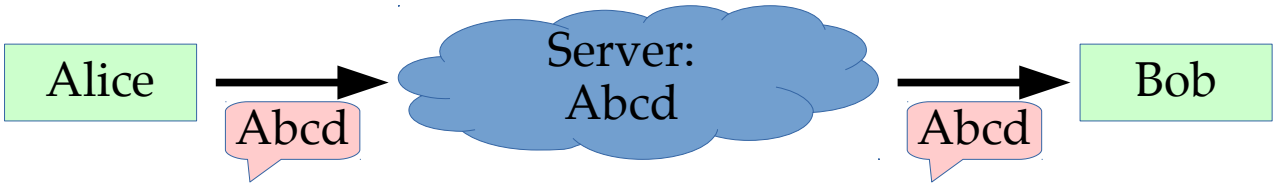
- One extra hop:
  - From device e*ncrypted* to VPN server "somewhere"
  - From VPN server *unencrypted* to destination
- Benefits:
  - Protects from interception "nearby"
  - Allows to circumvent censorship
- Recommended:
  - **AirVPN**
  - **ZenMate.** Free. *Only* browser
- Test: www.ipleak.net with / without

Short Excursion: Encryption

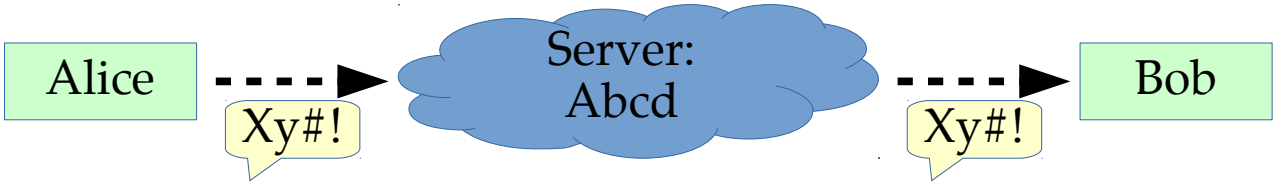
- Encryption:
  - *Plain Text + key + algo = ciphertext*
  - Transmit/store ciphertext
  - Ciphertext + key + algo = Plain Text
- Disadvantage: must have same key
- Solution: Asymmetric (aka Public Key)
- Problems:
  - Key management, MITM ("finger prints" OOB)

Short Excursion: Levels of Security

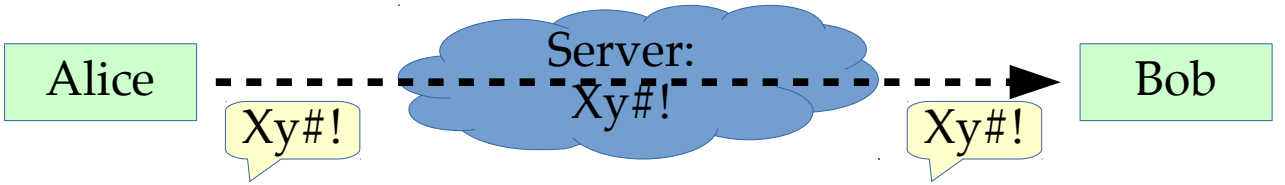
- Can send message across:
  - Unencrypted



  - Partially



  - End-to-End



Best Practices: Email & PGP

- Standard: PGP/GPG to encrypt any text
  - PGP: original (1991), GPG: open source
  - Both implement OpenPGP
- Command line tool, but various apps available
- Recommended:
  - **GPG4Win:** GPG for Windows
  - **GPGTools:** GPG for OS X, with Mail integration.
  - **IPGMail:** GPG for iOS.
- For key management, consider keybase.io

Best Practices: Email & PGP

- Note: Meta data *not* encrypted
  - Sender, recipient, subject, length, time, frequency of mails

    → 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

Best Practices: Chat

- Recommended (End-to-end encrypted):
  - **iMessage** (Apple only)
  - **Telegram** ("Secret Chat")
  - **TextSecure** (Android)
  - **Threema**
- MITM attack: Out-of-band key comparison
- Not recommended: Anything else. SMS.

Best Practices: Voice

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

Miscellaneous: Information Leaks

- Your phone is a tracking device
- You might reveal more than you thought
  - Phone number, email can be googled
  - Reverse Image Search (TinEye, Google)
  - Images: EXIF
    - Recommended (but complicated): **ExifTool**
- IP address → ISP → you
- Cookies

Miscellaneous: Multiple Accounts

- Recommended: Separate accounts on your computer
  - Work
  - Private
  - Project XYZ
- Shared folders
  - move information 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:
  - One layer broken, still secure
- 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

Best Practices: More

- Not covered:
  - Deleting Data
  - Cloud Storage
  - Whistleblowing (“SecureDrop”)
- Please check

  http://fabianlischka.github.io/InfoSec101

Finally: Advanced Steps

- Highly sensitive information → *much more* careful, systematic, paranoid
- Tools:
  - OpSec
  - VMs (Virtual Machines)
  - Tails (The amnesic incognito live system)

Questions?

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