Protect Yourself on Public Networks

Benjamin Toll
benjamintoll.com
benjam72@yahoo.com

Topics

- Passwords
- Metadata
- Web Browsing
- Communication
  - Email
  - Text
  - VoIP
  - Chat
- Public Wi-Fi
- Machine Security

Foreword: Security Mindset

- Security is hard
- Security is often not convenient
- Security is a process not a purchase
  - Always upgrade software
  - Join mailing lists to know when intrusions happen and patches are available
  - There is no silver bullet
- Always be learning

Passwords

- Security
  - Don’t...
    - Use the same password for more than one account
    - Use dictionary words, song lyrics, i.e, any common text in the public domain
    - Don’t ever give it to anyone!
  - Password Manager
    - LastPass
    - KeePass
    - stymie
  - Two-Factor Authentication
- Strength
  - Information entropy
  - Diceware
- Attack Vectors
  - Dictionary attacks (Fail2Ban, salts)
  - Rainbow tables (salts)
  - Network sniffing (encryption)
- Red flag if the site or admin can give you a forgotten password!

Metadata

- What is it?
  - Data about data
  - Everything except actual message
    - Timestamps
    - Location
    - Sender and receiver
- Why is it important to remove it?
  - Can create an accurate profile:
    - Likes and dislikes (preferences)
    - Professional and personal relationships
    - Movements (location)
    - Health
- View and strip metadata before posting or uploading a document or photo
  - ExifTool
  - Metadata Anonymisation Toolkit (MAT)
  - PDF Redact Tools
  - peepdf

Before we talk about web browsing...

- What is TLS (https)?
- What is public-key cryptography?
- What are digital certificates? Why do we need them?
- What is end-to-end encryption? How is it different from TLS?

Web Browsing

- Use Tor Browser
  - Browse anonymously
  - Avoid DNS leaks
- Install security browser plugins (but not if using Tor Browser!)
  - HTTPS Everywhere
  - Privacy Badger
  - uBlock
- Turn off JavaScript or at least use stricter safety settings
- Turn off 3rd-party cookies
- Downloads
  - Use a sandbox environment to mitigate malware
    - Virtual machine (i.e., VirtualBox)
    - chroot
    - Tails
  - Verify downloads by MD5, SHA, GPG signature
- Check shortened URLs (i.e., bitly) with CheckShortURL
- Don’t click through to sites with a bad cert unless you absolutely know what you’re doing!

Communication

Email

- GPG
- Thunderbird
  - Enigmail
  - TorBirdy
- Email client shouldn't render HTML or automatically load images and other remote media
  - Prevents recent EFAIL attack
  - Prevents tracking (i.e., 1x1 image used to know an email has been opened)
- Disable auto-download of attachments
- Open MS Office and PDF attachments in Google Drive or some online service that essentially recreates the document as an image
- Thwart phishing attacks
  - Hover over link to see destination
  - Browse to domain instead of clicking on link
  - Call to verify authenticity

Text and VoIP

- Signal
- WhatsApp
- Set disappearing messages if paranoid
- Verify keys
  - In person
  - On phone if person is known

Chat

- Pidgin with OTR

Public Wi-Fi

- Tails
  - Live operating system, provides a secure sandbox environment
- VPN
  - Be very selective when choosing a public VPN service!
    - Service will know your details and may not scrub logs after a reasonable amount of time.
      - IP address
      - Sites visited
    - May cooperate with law enforcement without making you aware.
    - If served a secret FISA court order cannot legally disclose this.
      - https://www.calyxinstitute.org/projects/canary-watch
      - https://canarywatch.org/
- SSH Tunneling (Dynamic Port Forwarding)

```
1. ssh -fCND 1080 www.example.com
2. Configure browser (or system settings) to direct traffic to port 1080.
```

- GNU MAC Changer
  - Dynamically change MAC address when joining public network
- Tor Browser
  - Browse anonymously
  - Avoid DNS leaks

Machine Security

- Disk encryption
- File-system level encryption
- TrueCrypt, et al.
- Encrypt tar archives
- Secure file deletion
  - BleachBit
  - shred

Recommended Links

- Schneier on Security
- A Few Thoughts on Cryptographic Engineering
- Khan Academy
  - Internet 101
  - Journey Into Cryptography
- Debian Security Mailing Lists
  - debian-security
  - debian-security-announce

References

- Free Software Foundation
- Freedom of the Press Foundation
- Riseup
- Surveillance Self-Defense (EFF)

FIN

Benjamin Toll
benjamintoll.com
benjam72@yahoo.com