Attacks on privacy

Kristjan Krips
Reminder about terminology

- Privacy vs anonymity
- Data vs information
- Confidentiality, integrity, availability (CIA)
- Software bug, vulnerability, exploit
- Threat, risk
Examples of leaks

#BREAKING: Aussies' private health records leaked by the Department of Health. [link](https://bit.ly/2BpE1uA)
Examples of tracking

- Exposing the Hidden Web: Third-Party HTTP Requests On One Million Websites (2015)
- I never signed up for this! Privacy implications of email tracking (2018)
- Third Party Tracking in the Mobile Ecosystem (2018)

Spy pixels in emails 'have become endemic'
bbc.in/3b75f1Q

4:46 AM · Feb 17, 2021 · SocialFlow
Examples of attacks

Highly unusual ransom case underway here in Finland: a private psychotherapy clinic was hacked, and the therapist notes for maybe even 40,000 patients were stolen. Now the attacker has emailed the victims, asking each for 200 € ransom in Bitcoin. #vastaamo
Examples of profit

The Conti ransomware leaks have unveiled Conti’s primary Bitcoin address.

From April 21st, 2017 - February 28th, 2022 Conti has received 65,498.197 BTC

That is 2,707,466,220.29 USD.
Who are the attackers?

- It largely depends on the context and on the assets that are being handled.
  - Competitors
  - State level actors
  - Cyber criminals
  - Script kiddies
  - Random bots

- In the context of an individual:
  - Service providers
  - Law enforcement agencies
  - Cyber criminals
  - Others
Motivation

● Raise awareness of different types of attacks
  ○ Be both knowledgeable and paranoid!

● Learn to defend yourself
  ○ However, you are not always in charge of your data.

● Solution:
  ○ Privacy enhancing technologies
HTTP cookies

- What kind of information do websites see about the visited users?
- How do cookies work?
Service providers and tracking

- Why are third-party cookies relevant in the context of privacy?
- How widespread is the issue?
  - Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on One Million Websites (2015)
  - A Day in the Life of Your Data (2021)
  - 'Spy pixels in emails have become endemic' (2021)

- How to defend yourself?
  - Measures integrated into browsers, browser extensions, configuration, more advanced options like Pi-Hole.

- What about the leakage of the session cookie?
  - Session fixation, session hijacking
Other means for tracking users across sessions

- IP address
- Browser fingerprint
- Behavioural profiling
- ETag
- Tracking pixels / beacons
- CNAME cloaking
- HTTP GET request parameters
- HTML5 local storage
- HSTS based fingerprinting
IP address

- **IP address**
  - Reveals location
  - Google: “what is my ip address”

- **Turn off location queries in browsers:**
  - Google Chrome: Settings -> Privacy and security -> Site Settings -> Location -> Blocked
  - Firefox: go to about:config and set
    - dom.webnotifications.enabled = false
    - geo.enabled = false

- **Mitigation measures: large organisations, proxies, VPN, Tor browser**

![Tor Browser screen shot]
Browser fingerprinting

● Browser fingerprint
  ○ [https://coveryourtracks.eff.org/](https://coveryourtracks.eff.org/)
  ○ Information about the browser configuration
  ○ Mitigation measures:
    ■ Browser with protective configuration: Tor browser, Brave browser
    ■ Extensions: NoScript, Privacy Badger, Disconnect

● Behavioural profiling
  ○ [https://paul.reviews/behavioral-profiling-the-password-you-cant-change](https://paul.reviews/behavioral-profiling-the-password-you-cant-change)
Image based tracking - ETag

- **ETag cache**
  - Works without:
    - Cookies
    - JavaScript
    - Knowing the IP
  - Based on image checksum (ETag), which is sent to the server to check if the cached image has changed.

- [https://lucb1e.com/randomprojects/cookielesscookies/](https://lucb1e.com/randomprojects/cookielesscookies/)
Image based tracking - Tracking pixels

- Transparent tracking pixels
  - Example

- Used both in webpages and in emails
  - Email: when was it read, which software was used, which IP, cookies
  - Used by spammers, marketers, phishers
  - [I never signed up for this! Privacy implications of email tracking](https://example.com) (2018)

- To detect view the source of your email.

- Mitigation:
  - Prevent email client from loading images.
  - Use text-based email readers (Alpine, Mutt)
  - Configure email client to only display plaintext messages / disable all HTML
  - [(Don't) Return to Sender: How to Protect Yourself From Email Tracking](https://example.com) (2019)
CNAME cloaking

- Lets go over this method in more detail
- Bypass ad blockers by moving to the DNS level

Tracker company asks a website to create a subdomain for the website that works as an alias for the tracking site.
  - Difficult to enumerate the subdomains that might be used as CNAME aliases.
  - Used to target specific users like the ones using Safari browser
  - CNAME Cloaking, the dangerous disguise of third-party trackers

Mitigation
  - uBlock for Firefox, Brave browser, Pi-hole
  - ?? Google Chrome ?? -- testing in lab showed that uBlock works in some cases
CNAME cloaking

● Examples:
  ○ 16ao.mathon.fr
  ○ f7ds.liberation.fr

● How to check for CNAME aliases?
  ○ Windows:
    ■ nslookup -q=CNAME 16ao.mathon.fr
  ○ Linux
    ■ host -t cname 16ao.mathon.fr
Network level interception - overview

- DNS queries are often in plaintext
- TLS does not protect the metadata

- Network level attacker sees visited websites and metadata
  - IP addresses
  - Time
  - Amount of exchanged data

- Bluetooth: lots of vulnerabilities
- Wifi: WPA2 might be broken
- Cellular networks: 2G is broken, SS7 is broken
Network level interception - surveillance

- www.submarinecablemap.com
Network level interception - OCSP queries

- Online Certificate Status Protocol (OCSP)
  - Used to check whether a digital certificate is valid
  - However, the OCSP query is sent in plaintext

- In 2020 it was revealed that macOS made OCSP queries about developer certificates when applications were launched. However, many developers only have one application, thus the query uniquely identified the launched application.
  - Your Computer Isn't Yours
  - Does Apple Track Every Mac App You Run? OCSP Explained
Network level interception - man-in-the-middle attacks

- Browser extensions
- DNS based attacks

- Legitimate attacks by corporate networks and antivirus software
  - Needs access to the end-user device
  - Breaks security properties offered by TLS
  - Is surprisingly widespread, reaching double digits in percentage of overall traffic
  - The Security Impact of HTTPS Interception (2017)

- Cell tower level interception and fake base stations
  - Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks (2019)
Various topics - voting privacy

● Elections have to be simultaneously transparent and provide vote secrecy.

● Verifiability vs coercion resistance
  ○ It should be possible to verify that the election result is calculated from the ballots.
  ○ Voter should be able to verify that her vote was included in the tally.
  ○ Identity has to be separated from the vote.
  ○ Voter should not be able to prove how she voted.

● I-voting ballots
  ○ Have to be encrypted
  ○ Identities are usually separated with the help of mix-nets
  ○ Coercion-free voting environment can not be guaranteed
Various topics - voting privacy

- **Paper ballots**
  - Double envelope system
  - Voting booth no longer guarantees privacy due to cameras, fingerprints.

- **Technology can also affect voting booths.**
  - It is possible to listen how the vote was cast.
  - The image shows a spectrogram displaying the sound of writing numbers 5, 7, 8
Various topics - voting privacy

- Voting machines
  - Side-channels can leak how the vote was cast: [Studying the Nedap/Groenendaal ES3B voting computer](#)

- Internet voting
  - Voting device has to be trusted.
  - Verification device has to be trusted.
  - If code voting is used, the printing houses have to be trusted.
  - Cryptographic means are used to anonymise ballots.
Various topics - tracking in the physical world

- Loyalty cards
- Payments
- Mobile service providers
- CCTV cameras
- Smartphone apps
- Printer tracking
- Smart speakers with microphones
- Smart watches
Various topics - smart speakers (2019)

- Amazon Workers Are Listening to What You Tell Alexa
- Apple apologizes for Siri audio recordings, announces privacy changes going forward
- Amazon Echo’s privacy issues go way beyond voice recordings
- https://lightcommands.com/
- Illustration by XKCD
  - https://xkcd.com/1807/
Optimistic plan for the lab

- Manipulation of cookies
- Viewing and removing EXIF data with `exiftool`
- Restoring deleted files with `Recuva`
- Trying out man-in-the-middle attacks with `Burp Suite`
- Trying out `Wireshark`
- Trying out different OSINT tools
  - search engines
  - reverse image search
  - `Shodan`
  - `Maltego`
  - `https://spyse.com/`
  - `https://osintframework.com/`