Lecture 18
Privacy, security, surveillance and self-defense

"Hah! I blasted that freedom-killing NSA drone right out of the sky!"

"Dad! That was Amazon delivering my new XBox!"

© 2013 Horsey
Los Angeles Times

America's Near Future.
Privacy, security, surveillance, and self-defense

- who is watching you?
- how are they watching?
- what can they learn?
- what can go wrong?

- what we should do about it as a society / country / institution / ...

- what you can do about it for yourself in the meantime
Privacy on the Web

• what does a browser send with a web request?
  – IP address, browser type, operating system type
  – referrer (URL of the page you were on)
  – cookies

• what do "they" know about you?
  – whatever you tell them, implicitly or explicitly (e.g., Facebook)
  – public records are really public
  – lots of big databases like phone books
  – log files everywhere
  – aggregators collect a lot of information for advertising
  – spyware, key loggers and similar tools collect for nefarious purposes
  – government spying is everywhere

• who owns your information?
  – in the USA, they do; you don't
  – much less so in the EU (GDPR, May 2018)
Potential security & privacy problems

• **attacks against client**
  - release of client information, tracking
    cookies: client remembers info for subsequent visits to same server
  - adware, phishing, spyware, viruses, ...
    spyware: client sends info to server upon connection
    often from unwise downloading
  - buggy/misconfigured browsers, etc., permit vandalism, theft, hijacking, ...

• **attacks against server**
  - client asks server to run a program when using cgi-bin
    server-side programming has to be careful
  - buggy code on server permits break-in, theft, vandalism, hijacking, …
  - denial of service attacks

• **attacks against information in transit**
  - eavesdropping
    encryption helps
  - masquerading
    needs authentication in both directions
How to cut down on tracking

- turn off all cookies
  - at least turn off third-party cookies
- use Firefox or Safari (or Edge) instead of Chrome
- use DuckDuckGo instead of Google search

- use extensions to disable advertising and tracking
  - Ghostery disables Javascript trackers
  - uMatrix Origin reduces / eliminates advertisements
  - Adblock Plus removes advertisements
  - DuckDuckGo Privacy Essentials
  - PrivacyBadger
  - NoScript disables all Javascript

- move to the EU or California
Extensions, plug-ins, add-ons, etc.

- programs that extend capabilities of browser (and other programs)
  - browser provides an API and a protocol for data exchange
  - extensions often for ad blocking and reduction of tracking
  - a plug-in focuses on specific application area
    - e.g., documents, pictures, sound, movies, scripting language, ...
  - may exist standalone as well as in plug-in form
  - e.g., Acrobat Reader, Flash, Quicktime, Windows Media Player, ...

- scripting languages interpret downloaded programs in a browser
  - Javascript is the main such language
    - compiled into instructions for a virtual machine
      - (like the Toy machine on steroids)
      - instructions are interpreted by virtual machine in browser

- browser extensions are written in Javascript
  - e.g., Ghostery, AdBlock, ..., NoScript
## Data breaches in 2021 (Wikipedia)

<table>
<thead>
<tr>
<th>Entity</th>
<th>Year</th>
<th>Records</th>
<th>Organization type</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ancestry.com</td>
<td>2021</td>
<td>300,000</td>
<td>web</td>
<td>poor security</td>
</tr>
<tr>
<td>Ankle &amp; Foot Center of Tampa Bay, Inc.</td>
<td>2021</td>
<td>156,000</td>
<td>healthcare</td>
<td>hacked</td>
</tr>
<tr>
<td>AOL</td>
<td>2021</td>
<td>92,000,000</td>
<td>web</td>
<td>inside job, hacked</td>
</tr>
<tr>
<td>AOL</td>
<td>2021</td>
<td>20,000,000</td>
<td>web</td>
<td>accidentally published</td>
</tr>
<tr>
<td>Apple, Inc./BlueToad</td>
<td>2021</td>
<td>12,367,232</td>
<td>tech, retail</td>
<td>accidentally published</td>
</tr>
<tr>
<td>Apple</td>
<td>2021</td>
<td>275,000</td>
<td>tech</td>
<td>hacked</td>
</tr>
<tr>
<td>Apple Health Medicaid</td>
<td>2021</td>
<td>91,000</td>
<td>healthcare</td>
<td>poor security</td>
</tr>
<tr>
<td>CyberServe</td>
<td>2021</td>
<td>1,107,034</td>
<td>hosting provider</td>
<td>hacked</td>
</tr>
<tr>
<td>T-Mobile</td>
<td>2021</td>
<td>45,000,000</td>
<td>telecom</td>
<td>hacked</td>
</tr>
<tr>
<td>Twitch</td>
<td>2021</td>
<td>unknown</td>
<td>tech</td>
<td>hacked</td>
</tr>
<tr>
<td>Microsoft Exchange servers</td>
<td>2021</td>
<td>unknown</td>
<td>software</td>
<td>zero-day vulnerabilities</td>
</tr>
<tr>
<td>Health Service Executive</td>
<td>2021</td>
<td>unknown</td>
<td>healthcare</td>
<td>unknown</td>
</tr>
<tr>
<td>Atraf</td>
<td>2021</td>
<td>unknown</td>
<td>dating</td>
<td>hacked</td>
</tr>
</tbody>
</table>
Ransomware

Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.

You can unknowingly download ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that’s embedded with malware.

Once the code is loaded on a computer, it will lock access to the computer itself or data and files stored there. More menacing versions can encrypt files and folders on local drives, attached drives, and even networked computers.

Most of the time, you don’t know your computer has been infected. You usually discover it when you can no longer access your data or you see computer messages letting you know about the attack and demanding ransom payments.
Defenses

• use strong passwords; don’t share them across important accounts
• use 2-factor identification when available (e.g., Duo)
• cookies off, spam filter on, Javascript limited
• turn off previewers and HTML mail readers
• anti-virus software on and up to date
  – turn on macro virus protection in Word, etc.
• run spyware detectors
• use a firewall
• try less-often targeted software
• be careful and suspicious all the time
  – don't view attachments from strangers
  – don't view unexpected attachments from friends
  – don't just read/accept/click/install when requested
  – don't install file-sharing programs
  – be wary when downloading software
Internet of Things

- you thought it was bad with computers
- phones made it worse
- and now it's the Internet of Things

- lots and lots of Things
- most have very poor security
  - e.g., hard-coded unchangeable passwords
- no firewalls or virus scanners
- often very naive users
- usually no incentive to improve
- usually no mechanism to upgrade or update

"It used to be that things had computers in them. Now they are computers with things attached to them."
Thing architecture

Maybe, maybe not

Processor (CPU)

Display/screen

Mouse, keyboard, touchpad

Network, likely by wireless

Primary memory (RAM)

Secondary storage (hard disk, SSD)

Other devices, such as CD/DVD, camera, speakers, microphone, ...

Sensors; often actuators
Lots of Things

- **home**
  - web cams, baby monitors, ...
  - lights, thermostats, door locks, ...
  - TV, appliances, ...
- **personal services and gadgets**
  - games & toys, e-readers, watches, Fitbit, ...
  - Alexa, Siri, Google Voice, ...
- **cars, trains, planes, drones**
- **medical devices and instruments**
- **infrastructure**
  - power plants and grid, traffic lights, transportation,
  - phones & communications systems, ...
- **manufacturing, shipping, ...**
- **police & military systems**
- . . .