

Lecture 18: Privacy, security, self-defense

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

- what can they do with the information?
- what can they do to you?
- what can go wrong?

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

- what can you do personally in the meantime?

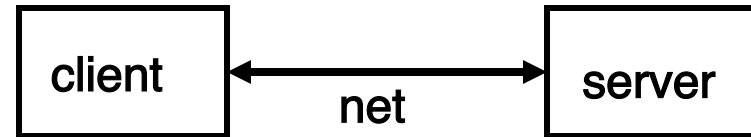
Privacy on the Web

- **what does a browser send with a web request?**
 - IP address, browser type, operating system type, other info
 - 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, Google, ...)
 - public records are really public
 - lots of big databases like phone books
 - log files everywhere
 - aggregators & data brokers 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
 - less so in the EU (GDPR, May 2018)

Potential security & privacy problems

- **attacks against client**

- release of client information, tracking
- adware, phishing, spyware, viruses, ransomware, ...
 - spyware: client sends info to server upon connection
 - viruses: run malware on client computer
- buggy/misconfigured browsers, etc., permit vandalism, theft, hijacking, ...



- **attacks against server**

- buggy/misconfigured servers, etc., permit break-in, data breach, vandalism, hijacking, ransomware, ...
- phishing
- denial of service attacks

- **attacks against information in transit**

- eavesdropping
 - encryption helps
- masquerading, man in the middle attacks
 - 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
 - and others
- **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

General Data Protection Regulation (GDPR) (May 2018)

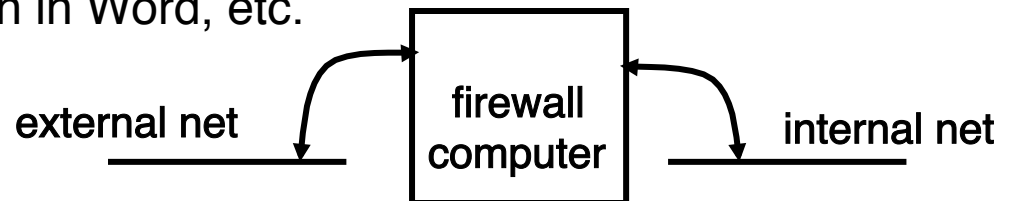
You have the right to:

- **information** about the processing of your personal data;
- **obtain access to** the personal data held about you;
- ask for incorrect, inaccurate or incomplete personal data to be **corrected**;
- request that personal **data be erased** when it's no longer needed or if processing it is unlawful;
- **object** to the processing of your personal data for marketing purposes or on grounds relating to your particular situation;
- request the **restriction** of the processing of your personal data in specific cases;
- receive your personal data in a machine-readable format and send it to another controller (**'data portability'**);
- request that decisions based on **automated processing** concerning you or significantly affecting you and based on your personal data are made by natural persons, not only by computers. You also have the right in this case to express your point of view and to contest the decision.

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights_en

Personal 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



VPN (Virtual Private Network)

- a protected connection from your computer to a private network
 - e.g., from your laptop at home to Princeton's network
 - as if you were on campus
- creates an encrypted "tunnel" from your computer to VPN host
- your traffic appears to come from / go to the VPN host, not you
 - needs a VPN client on your computer
 - e.g., Palo Alto Networks GlobalProtect at PU
- you can still be tracked by cookies, fingerprinting, etc.
- you have to trust the VPN client and host

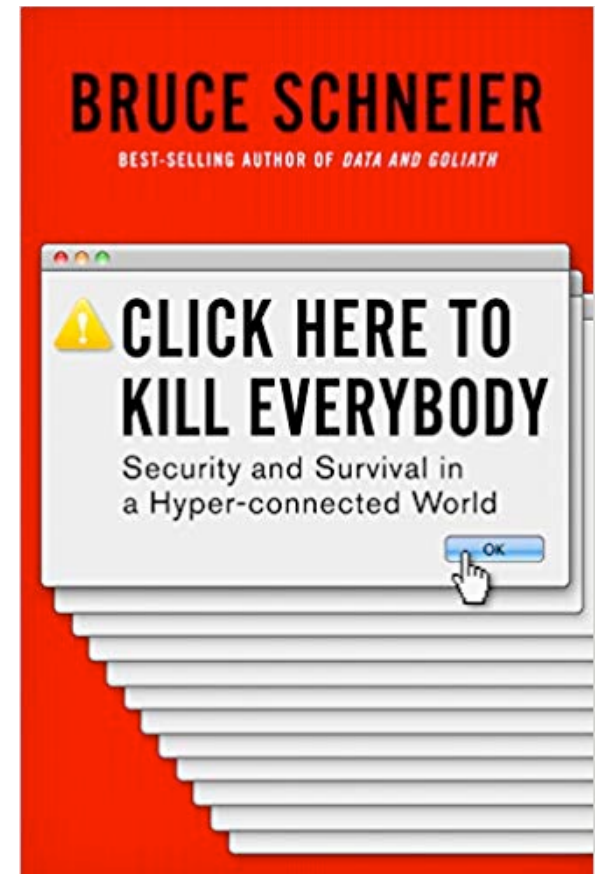
Internet of Things

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

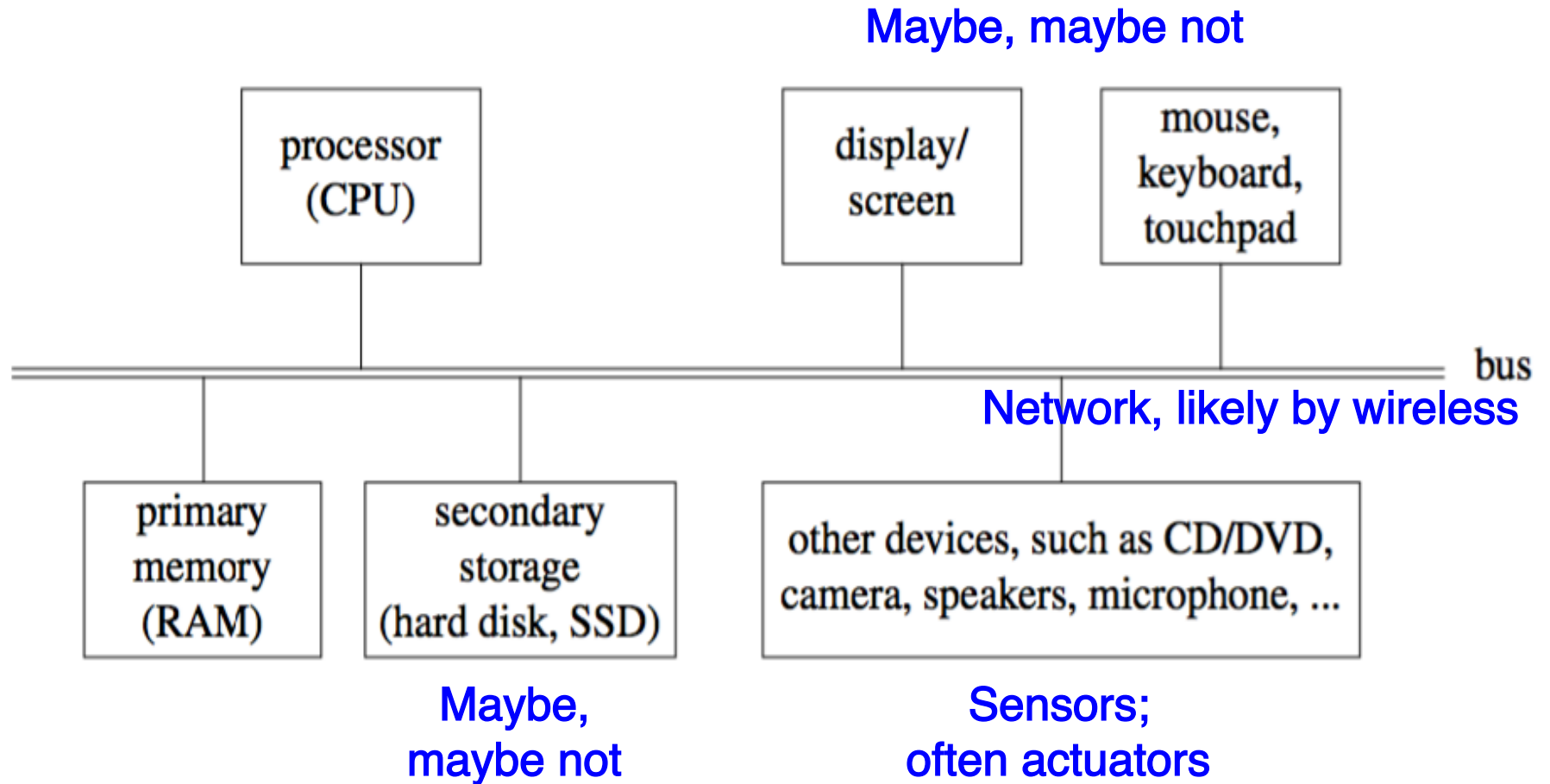
- lots and lots of Things
- most have very poor security
 - e.g., hard-coded unchangeable passwords
- no firewalls or virus scanners
- often very naive users
- usually no incentive to improve
- usually no mechanism to upgrade or update

"It used to be that things had computers in them.

Now they *are* computers with things attached to them."



Thing architecture



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
- . . .

firetvstick + echo dot
Hands-free control of your Fire TV



Cheez-It Dash Button
Amazon
\$4.99 ✓Prime



Pop-Tarts Dash Button
Amazon
\$4.99 ✓Prime



The Internet of ransomware things...

