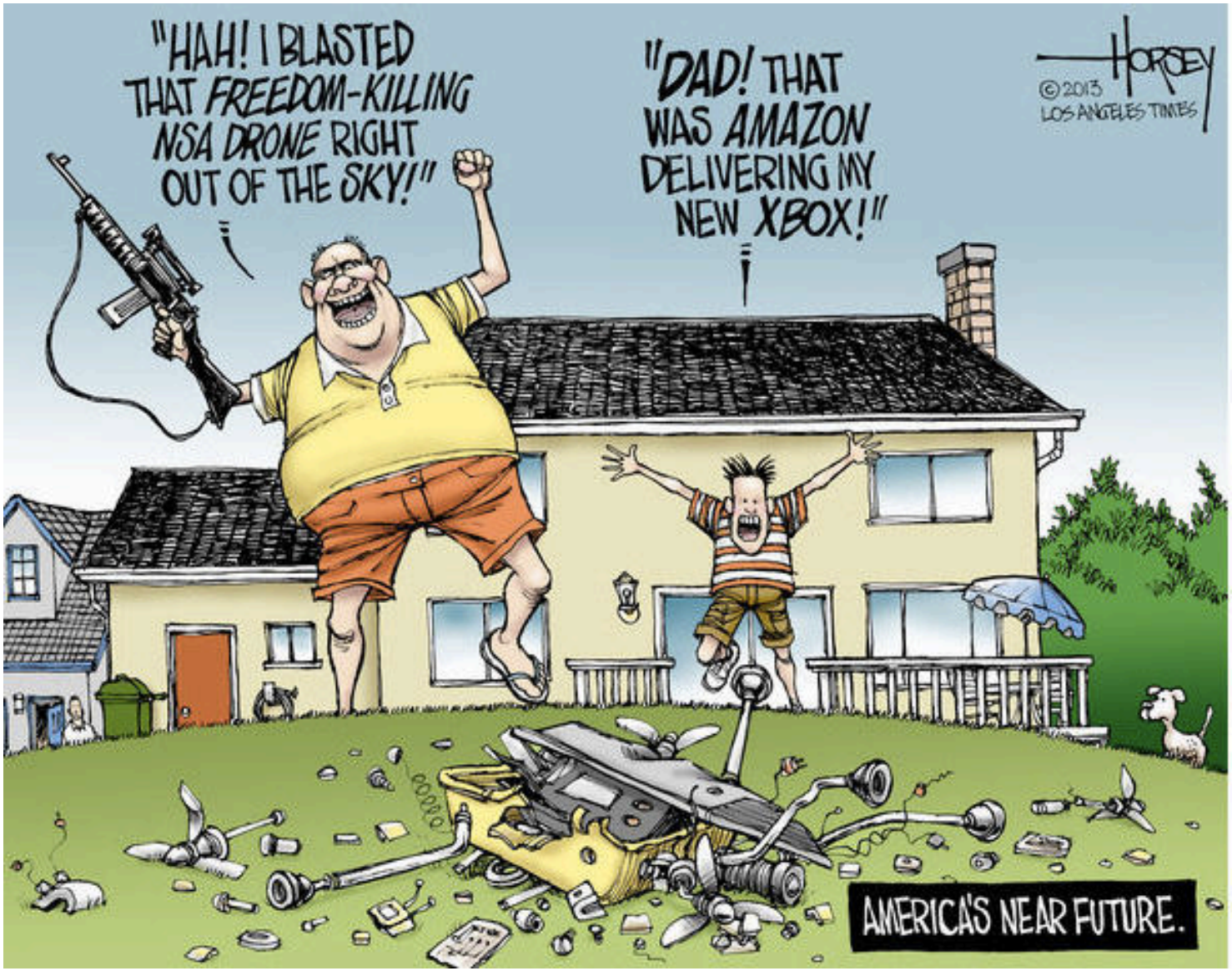
Lecture 18
Privacy, security, surveillance and self-defense



Privacy, security, surveillance, and self-defense

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

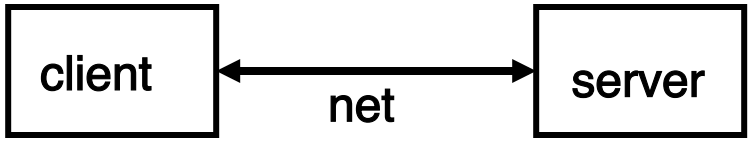
- what we should do about it as a society / country / institution / ...

- 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)

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

Ransomware

An official website of the United States government. Here's how you know

MORE > SCAMS AND SAFETY FBI

SCAMS AND SAFETY

Protecting Your Kids | On The Internet | Common Scams And Crimes | Sex Offender R

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.

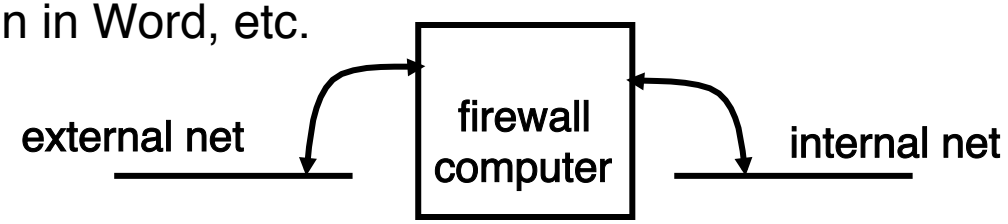
You can unknowingly download ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's embedded with malware.

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

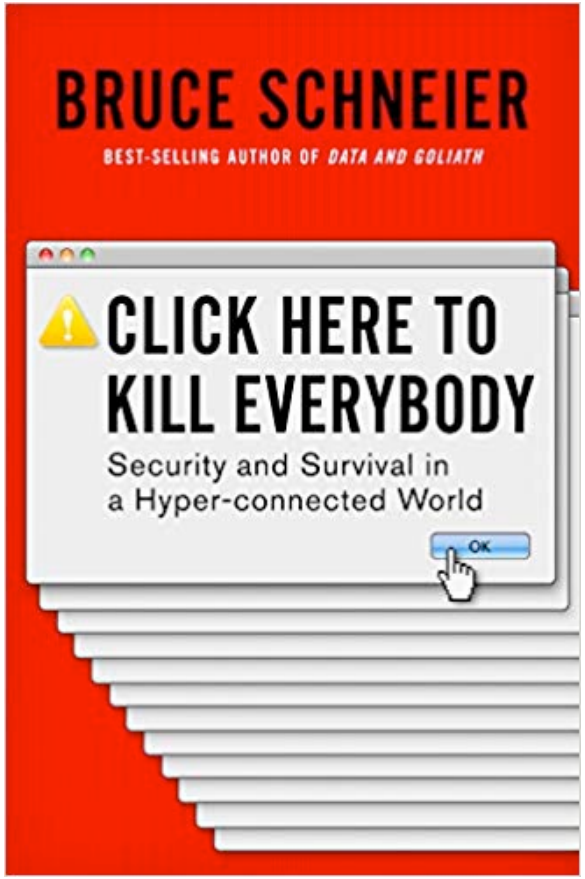
- use strong passwords; don’t share them across important accounts
- use 2-factor identification when available (e.g., Duo)
- cookies off, spam filter on, Javascript limited
- turn off previewers and HTML mail readers
- anti-virus software on and up to date
  - turn on macro virus protection in Word, 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

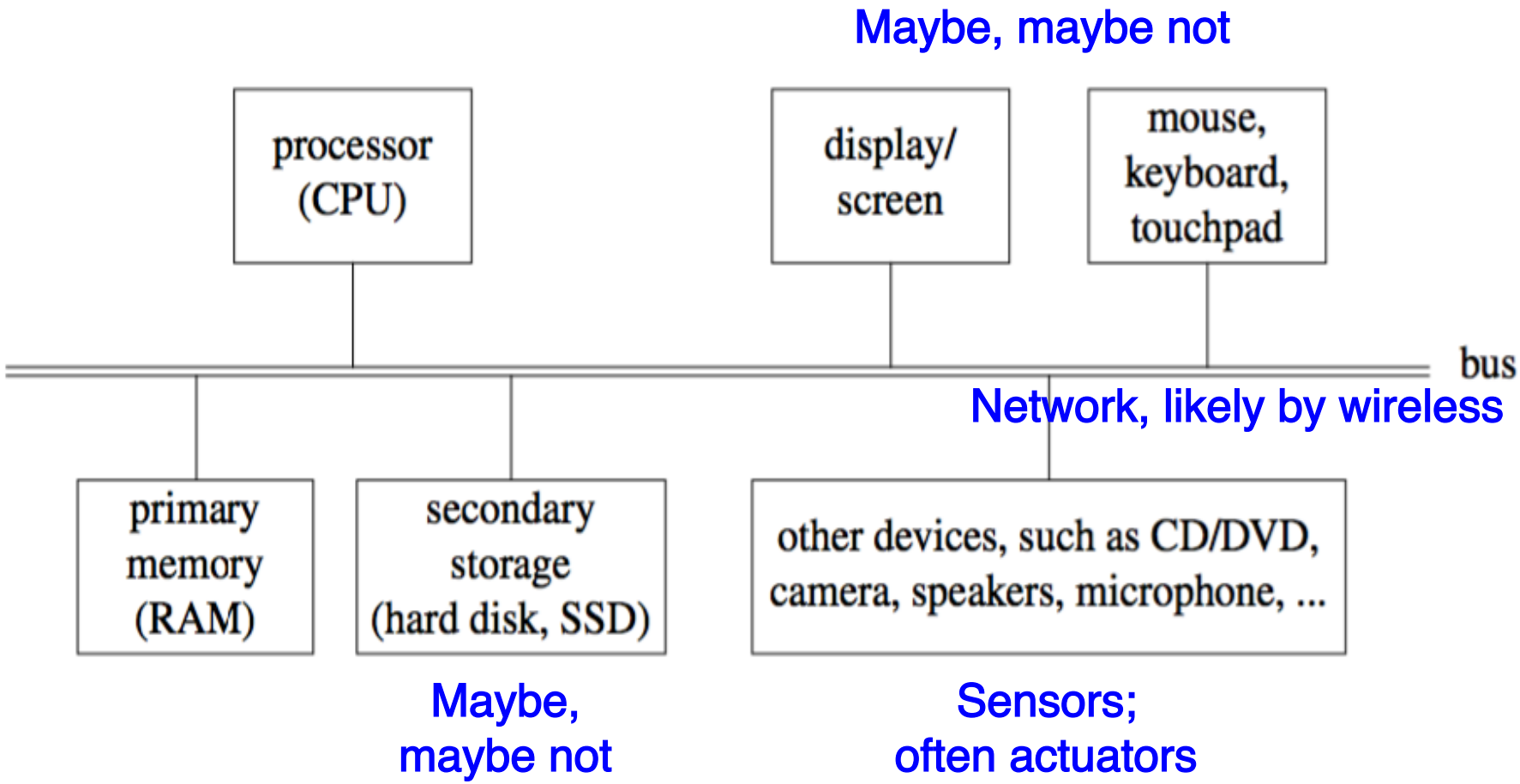
- you thought it was bad with computers
- phones made it worse
- and now it's the Internet of Things

- lots and lots of Things
- most have very poor security
  - e.g., hard-coded unchangeble 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

Cheez-It Dash Button
Amazon
$4.99 Prime

Pop-Tarts Dash Button
Amazon
$4.99 Prime

- 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
- . . .