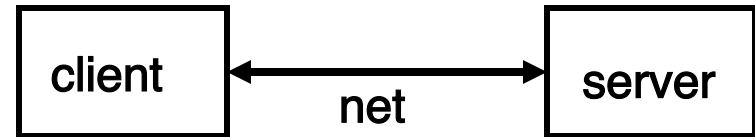# Lecture 17
Privacy and Security

Privacy, security, self-defense

- what can go wrong

- what you can do about it for yourself

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

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 (Sony, …)
    - often from unwise downloading
  - buggy/misconfigured browsers, etc., permit vandalism, theft, hijacking, ...
- **attacks against server**
  - client asks server to run a programs 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

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

- Ghostery disables Javascript trackers
- NoScript disables all Javascript

- uMatrix Origin
- Adblock Plus
- PrivacyBadger

Plug-ins, add-ons, extensions, etc.

- **programs that extend capabilities of browser** (and other programs)
  - browser provides an API and a protocol for data exchange
  - extension 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**
  - Javascript
    - compiled into instructions for a virtual machine
      - (like the Toy machine on steroids)
    - instructions are interpreted by virtual machine in browser

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)

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
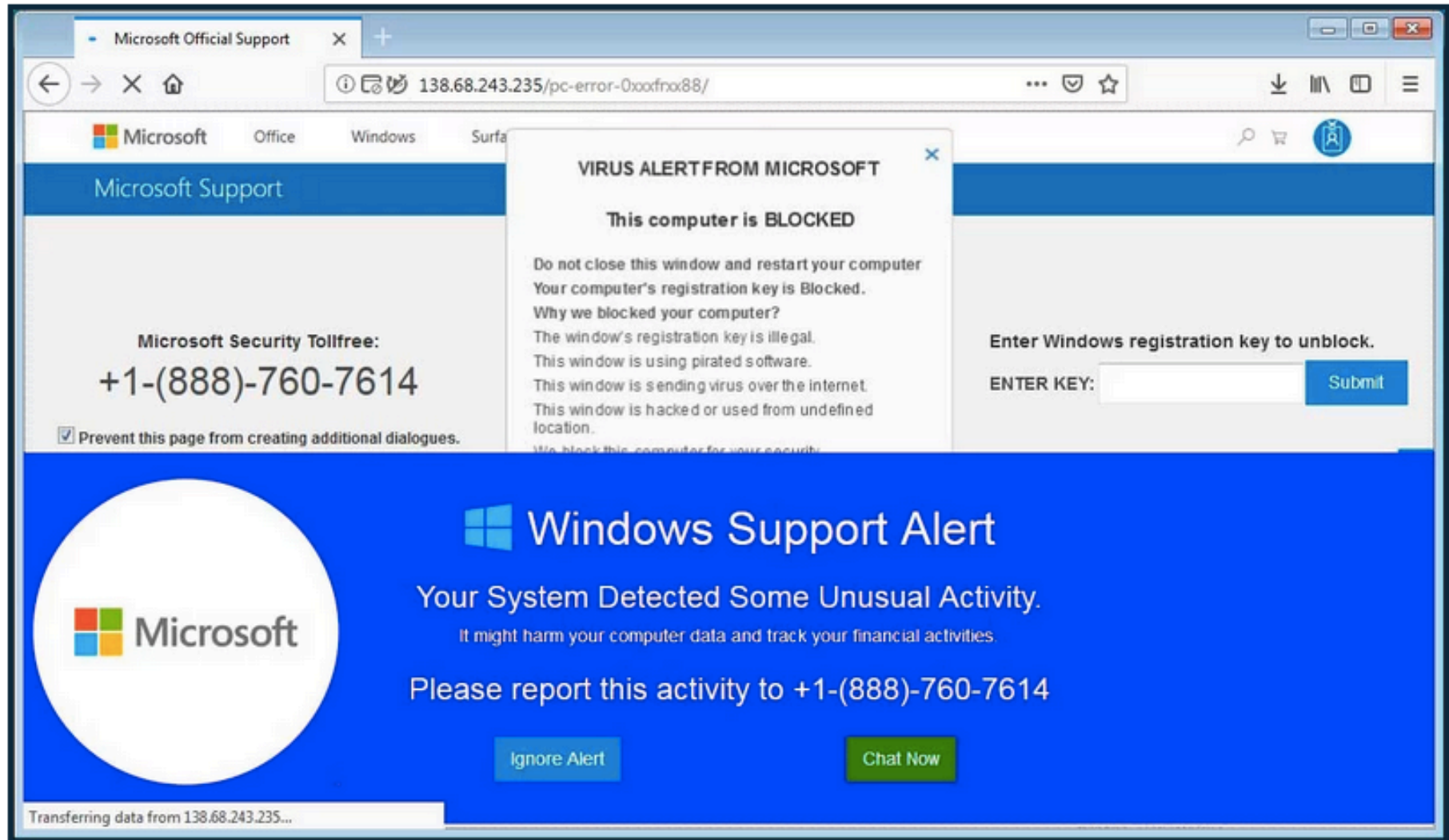
Worms and viruses

- **old threat, new technologies**
  - new connectivity makes them more dangerous
- **basic problem: running someone else's software on your machine**
  - bugs and ill-advised features make it easier
- **operates by hiding executable code inside something benign**
  - e.g., .EXE file or script in mail or document, downloaded content
  - USB drive or other attractive medium
- **Melissa, ILoveYou, Anna Kournikova viruses use Visual Basic**
  - applications (Word, Excel, Powerpoint, Outlook) have VB interpreter
  - a document like a .doc file or email message can contain a VB program
  - opening the document causes the VB program to be run

- **virus detectors**
  - scan for suspicious patterns, suspicious activities, changes in files
  - this is a real arms race

Bots, botnets, etc.

- bots: software robots running automated tasks over Internet
  - e.g., web spider collecting web page info for search engines

- botnet: collection of "zombie" computers that can be controlled remotely
  - most often Windows PCs
  - infected via viruses, worms, trojan horses, etc.
  - controlled by chat protocol, web page visits, peer to peer
  - exploits include denial of service attacks, spam, click fraud, adware, spyware, ...

Microsoft Support scan

Data breaches in 2020 (Wikipedia)

|				
Betsson Group	2020	unknown	gaming	unknown
CheckPeople	2020	56,000,000	background check	unknown
Clearview AI	2020	3,000,000,000 (Number of photos obtained)	information technology	hacked
Instagram	2020	200,000,000	social network	poor security
Koodo Mobile	2020	unknown	mobile carrier	hacked
Marriott International	2020	5,200,000	hotel	poor security/inside job
Nintendo (Nintendo Account)	2020	160,000	gaming	hacked
SlickWraps	2020	377,428	phone accessories	poor security
Tetrad	2020	120,000,000	market analysis	poor security
TikTok	2020	42,000,000	social media	poor security
Virgin Media	2020	900,000	mobile carrier	accidentally exposed
Wawa (company)	2020	30,000,000	retail	hacked
YouTube	2020	4,000,000	social media	poor security
Unknown agency (believed to be tied to United States Census Bureau)	2020	200,000,000	financial	accidentally published
National Health Information Center (NCZI) of Slovakia	2020	391,250	healthcare	poor security

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

external net   firewall
                      computer   internal net
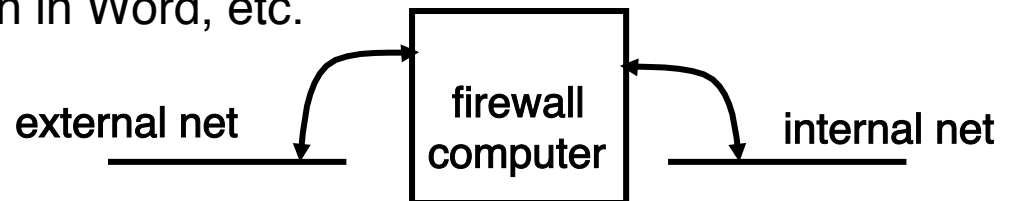
Internet of Things

- 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
- usually no incentive to improve
- usually no mechanism to upgrade or update

"It used to be that things had computers in them.
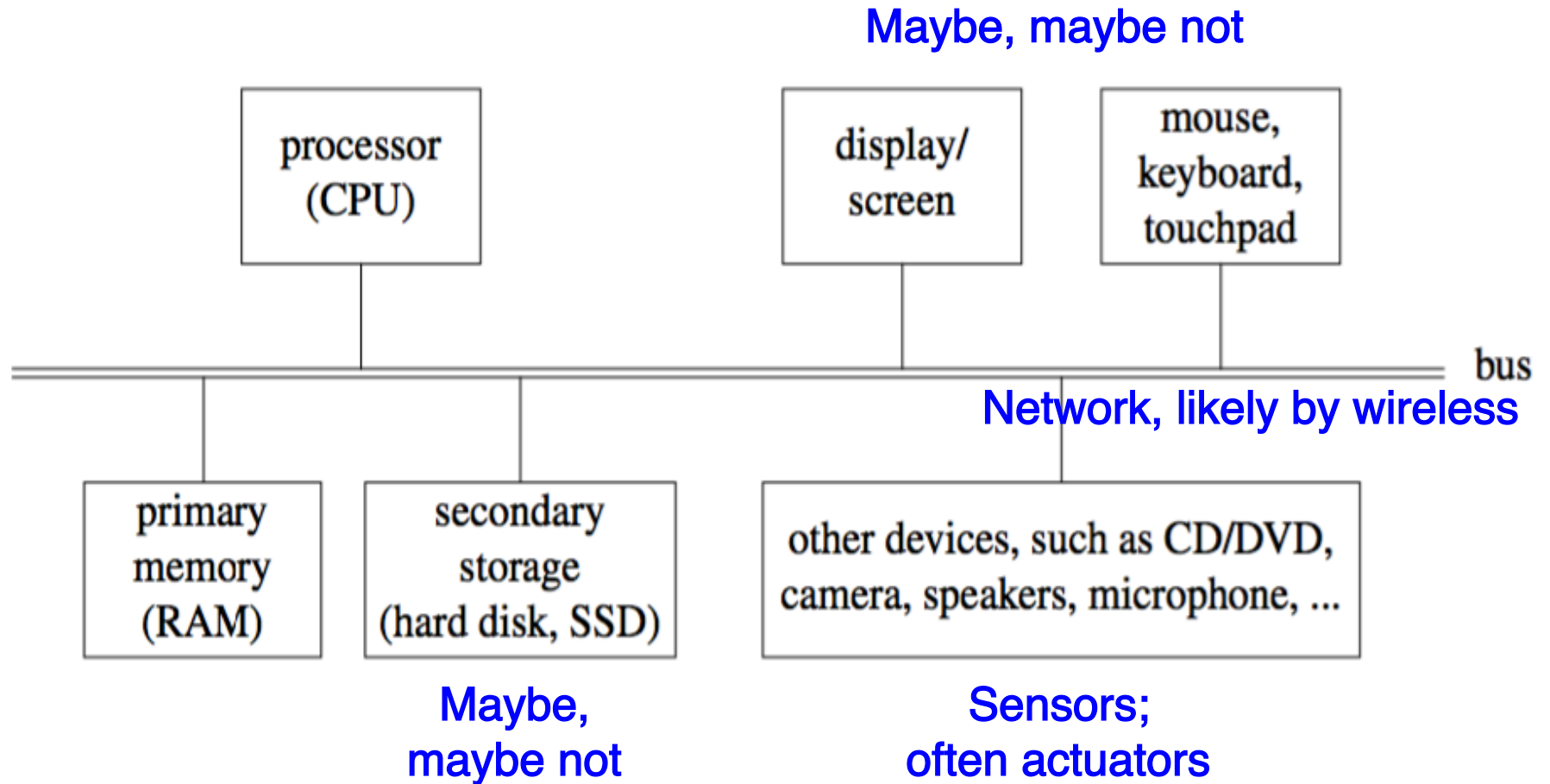Now they *are* computers with things attached to them."
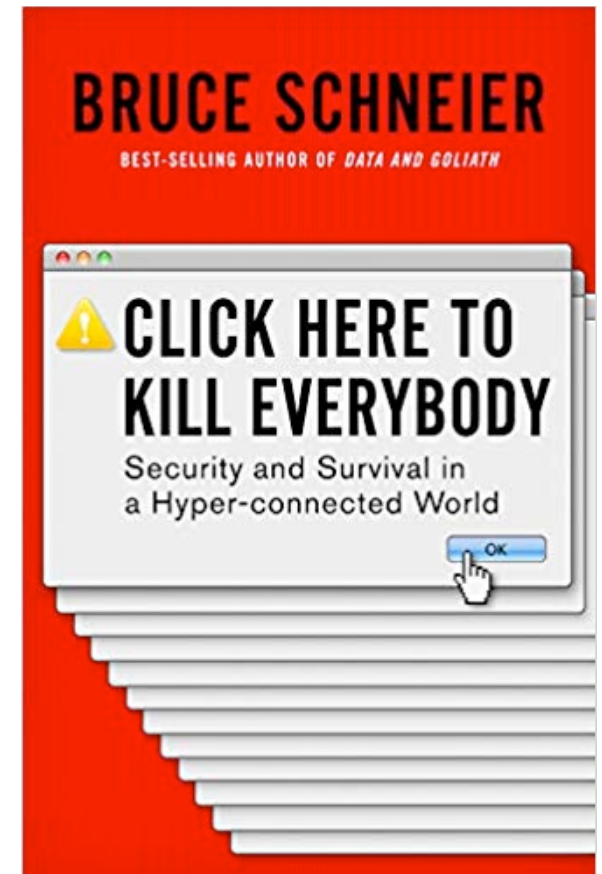
Internet of Things

- vacuum tubes => transistors => integrated circuits
- magnetic cores => integrated circuits
- mechanical disks => solid state drives
- copper wire => fiber optics
- wired Ethernet => wireless

- smaller, cheaper, faster, better => lots of things
- things + wireless + Internet => Internet of Things

"And as computers continue to get smaller and cheaper, they're being embedded into more things, and more things are turning into computers."

Thing architecture

Maybe, maybe not

processor (CPU)

display/ screen

mouse, keyboard, touchpad

bus

Network, likely by wireless

primary memory (RAM)

secondary storage (hard disk, SSD)

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

Maybe, maybe not

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**
- **. . .**