CSE 484 / CSE M 584: Computer Security and Privacy

The End
(Anonymity, Side Channels, Emerging Technologies)

Spring 2016

Franziska (Franzi) Roesner

franzi@cs.washington.edu

Admin

- **Final Projects due** Monday @ 8pm
- Check out the rubric on the course website
  - E.g., don't forget to include one slide on legal and/or ethical issues
- Extra credit: review up to 2 other presentations
  - We will make them available by 10am on Tuesday

- Extra credit readings due today @ 8pm

Today: A Few Last Topics

- Finish anonymity
- Side channels
- Security for emerging technologies

Recall: Anonymity

- Tor (http://tor.eff.org)
  - Overlay circuit-based anonymity network
  - Best for low-latency applications such as anonymous Web browsing

- Mixminion (http://www.mixminion.net)
  - Network of mixes
  - Best for high-latency applications such as anonymous email

- Not: YikYak ☺

Using a Tor Circuit

- Client applications connect and communicate over the established Tor circuit.
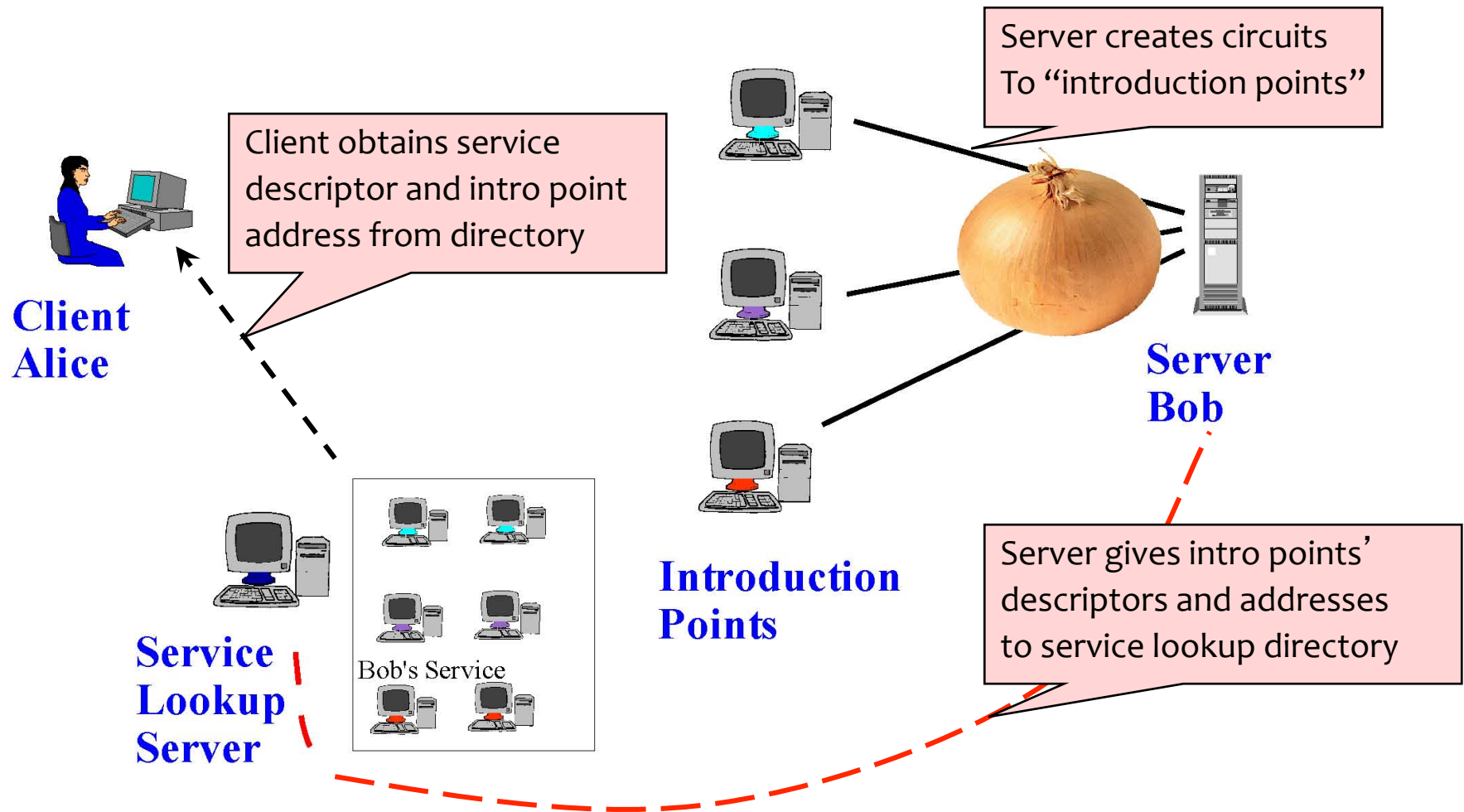

Client Initiator
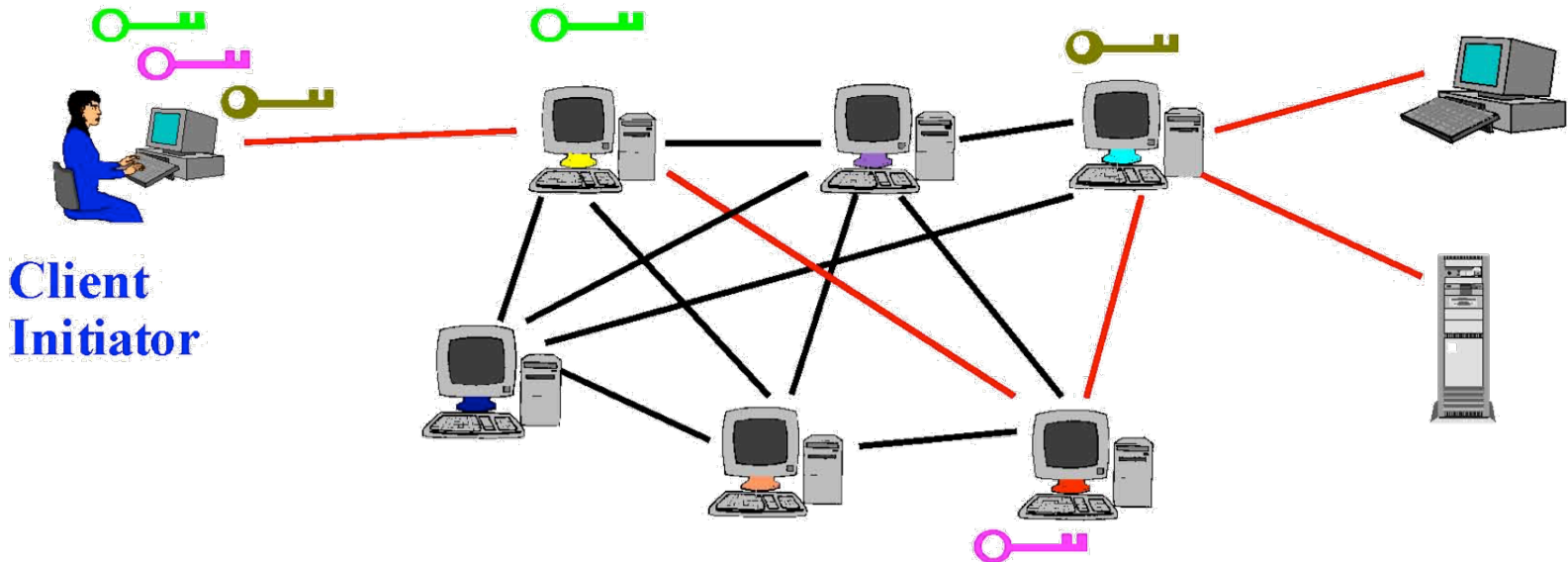
Tor Management Issues

- Many applications can share one circuit
  - Multiple TCP streams over one anonymous connection
- Tor router doesn't need root privileges
  - Encourages people to set up their own routers
  - More participants = better anonymity for everyone
- Directory servers
  - Maintain lists of active onion routers, their locations, current public keys, etc.
  - Control how new routers join the network
    - "Sybil attack": attacker creates a large number of routers
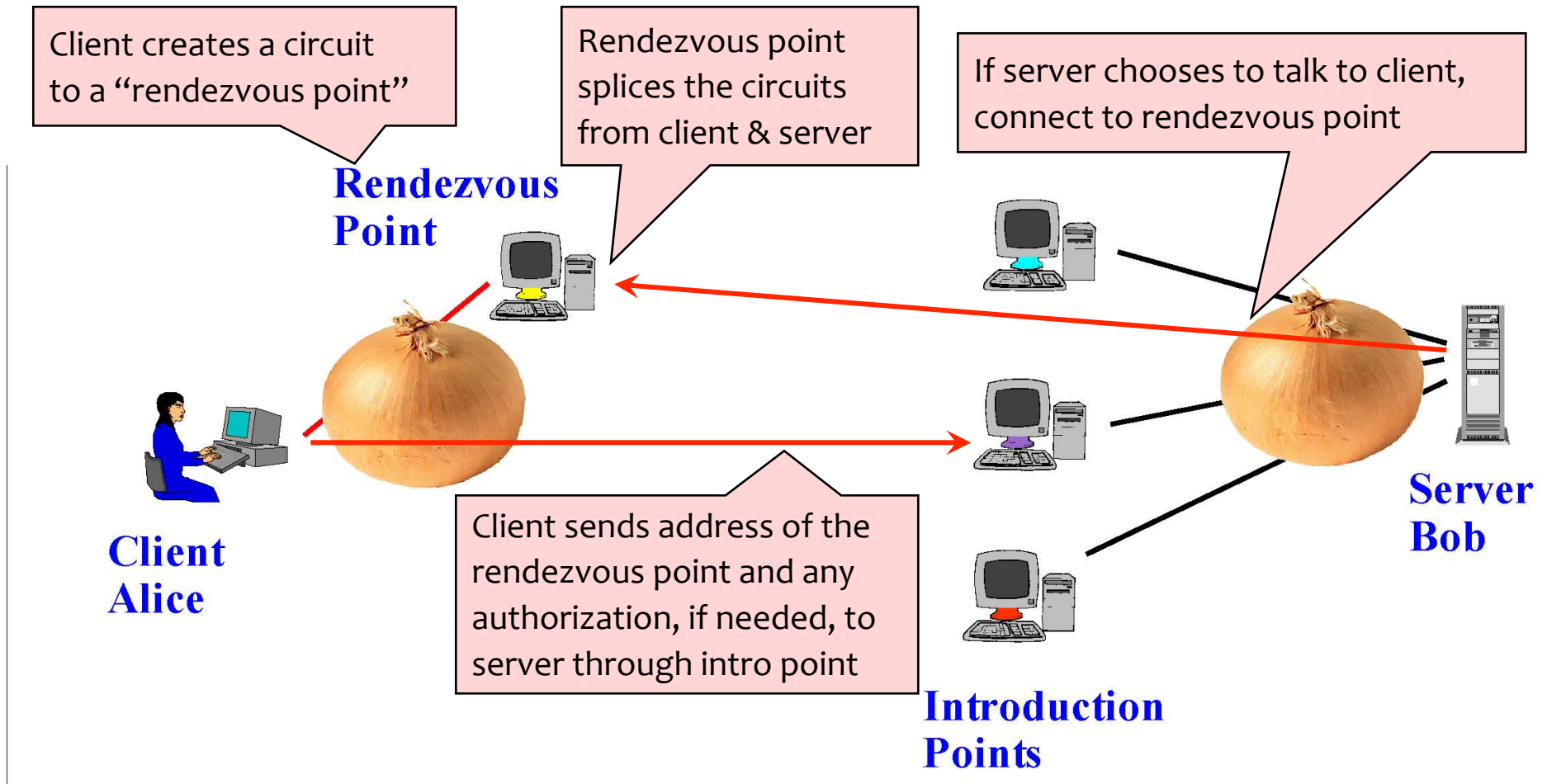 - Directory servers' keys ship with Tor code

Location Hidden Service

- **Goal:** deploy a server on the Internet that anyone can connect to without knowing where it is or who runs it

- Accessible from anywhere

- Resistant to censorship

- Can survive a full-blown DoS attack

- Resistant to physical attack
  - Can't find the physical server!

Creating a Location Hidden Server

Server creates circuits
To "introduction points"

Client obtains service
descriptor and intro point
address from directory

Client Alice

Server Bob

Service Lookup Server

Bob's Service

Introduction Points

Server gives intro points'
descriptors and addresses
to service lookup directory

Using a Location Hidden Server

Client creates a circuit to a "rendezvous point"

Rendezvous point splices the circuits from client & server

If server chooses to talk to client, connect to rendezvous point

Rendezvous Point

Client sends address of the rendezvous point and any authorization, if needed, to server through intro point

Client Alice

Server Bob

Introduction Points

Some Caution

- Tor isn't completely effective by itself
  - Tracking cookies, fingerprinting, etc.
  - Exit nodes can see everything!

Client Initiator
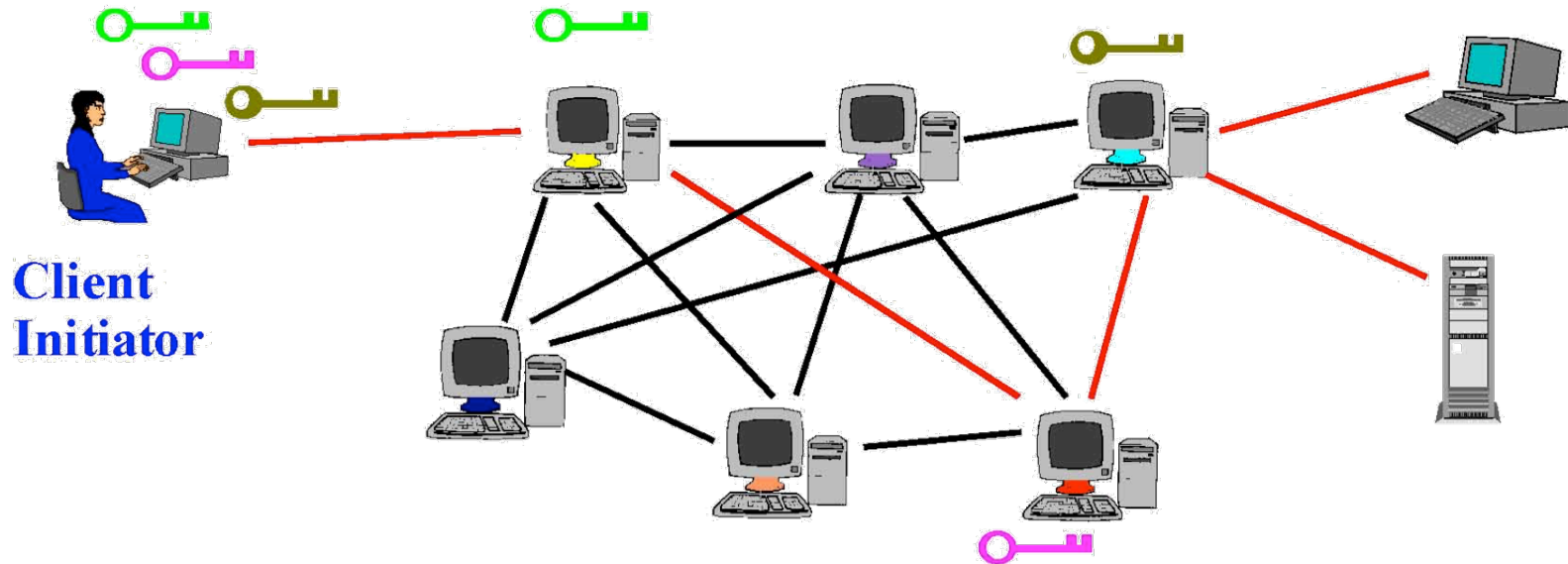
SIDE CHANNELS

Side Channel Attacks

- Attacks based on information that can be gleaned from the physical implementation of a system, rather than breaking its theoretical properties
  - Most commonly/devastatingly used against cryptosystems
  - But also prevalent in other contexts, e.g., due to widespread smartphone sensors

Cache-Based Side Channels

Type	Enc.	Year	Attack description		Victim machine	Samples	Crypt. key
Active Time-driven [9]	AES	2006	Final Round Analysis	UP	Pentium III	$2^{13.0}$	Full 128-bit key
Active Time-driven [30]	AES	2005	Prime+Evict (Synchronous Attack)	SMP	Athlon 64	$2^{18.9}$	Full 128-bit key
Active Time-driven [40]	DES	2003	Prime+Evict (Synchronous Attack)	UP	Pentium III	$2^{26.0}$	Full 56-bit key
Passive Time-driven [4]	AES	2007	Statistical Timing Attack (Remote)	SMT	Pentium 4 with HT	$2^{20.0}$	Full 128-bit key
Passive Time-driven [8]	AES	2005	Statistical Timing Attack (Remote)	UP	Pentium III	$2^{27.5}$	Full 128-bit key
Trace-driven [14]	AES	2011	Asynchronous Probe	UP	Pentium 4 M	$2^{6.6}$	Full 128-bit key
Trace-driven [29]	AES	2007	Final Round Analysis	UP	Pentium III	$2^{4.3}$	Full 128-bit key
Trace-driven [3]	AES	2006	First/Second Round Analysis	-	-	$2^{3.9}$	Full 128-bit key
Trace-driven [30]	AES	2005	Prime+Probe (Synchronous Attack)	SMP	Pentium 4 with HT	$2^{13.0}$	Full 128-bit key
Trace-driven [32]	RSA	2005	Asynchronous Probe	SMT	Xeon with HT	-	310-bit of 512-bit key

Table 1: Overview of cache-based side channel attacks: UP, SMT and SMP stand for uniprocessor, simultaneous multithreading and symmetric multiprocessing, respectively.

"By exploiting side channels that arise from shared CPU caches, researchers have demonstrated attacks extracting encryption keys of popular cryptographic algorithms such as AES, DES, and RSA."
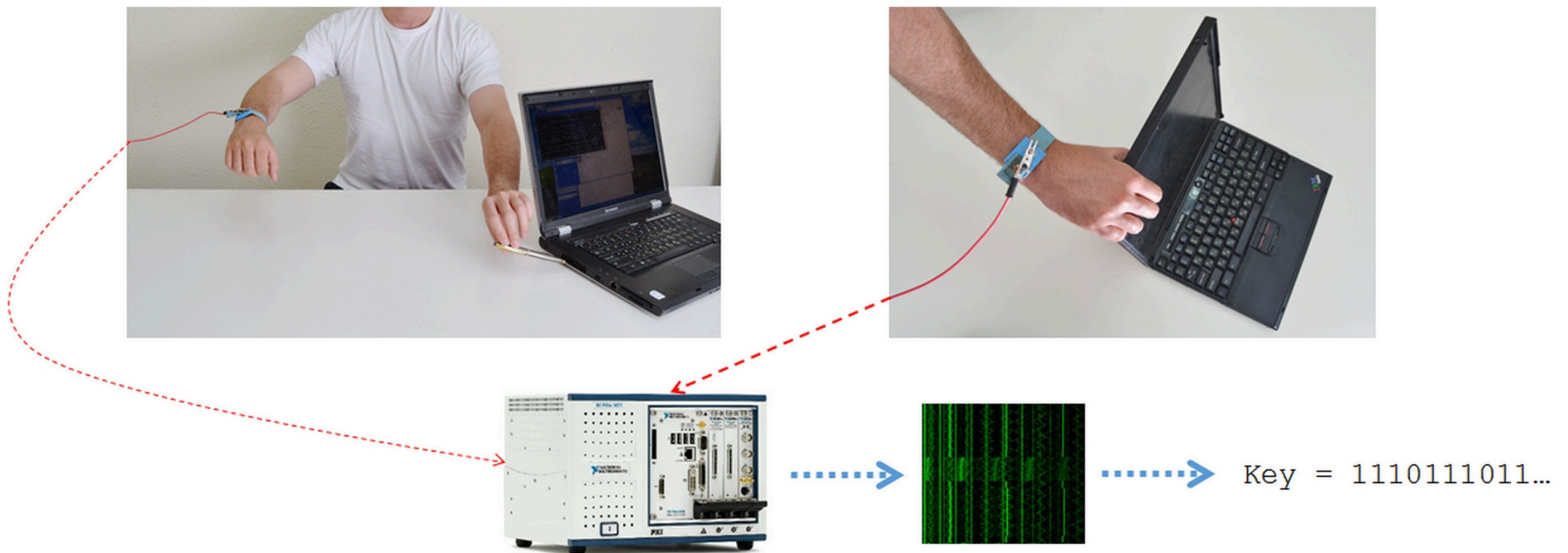
Kim et al. "STEALTHMEM: System-Level Protection Against Cache-Based Side Channel Attacks in the Cloud" USENIX Security 2012

Others (on Cryptosystems)
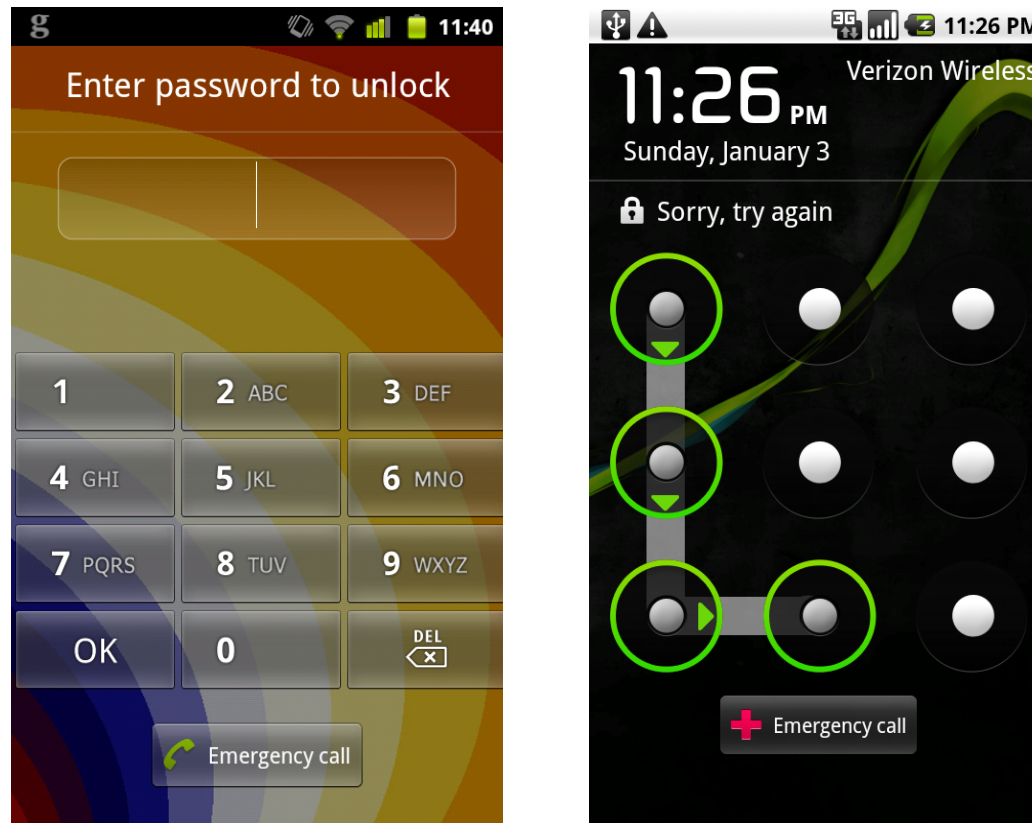
- Timing attacks
- Power analysis
- Etc.

If you do something different for secret key bits 1 vs. 0, attacker can learn something…

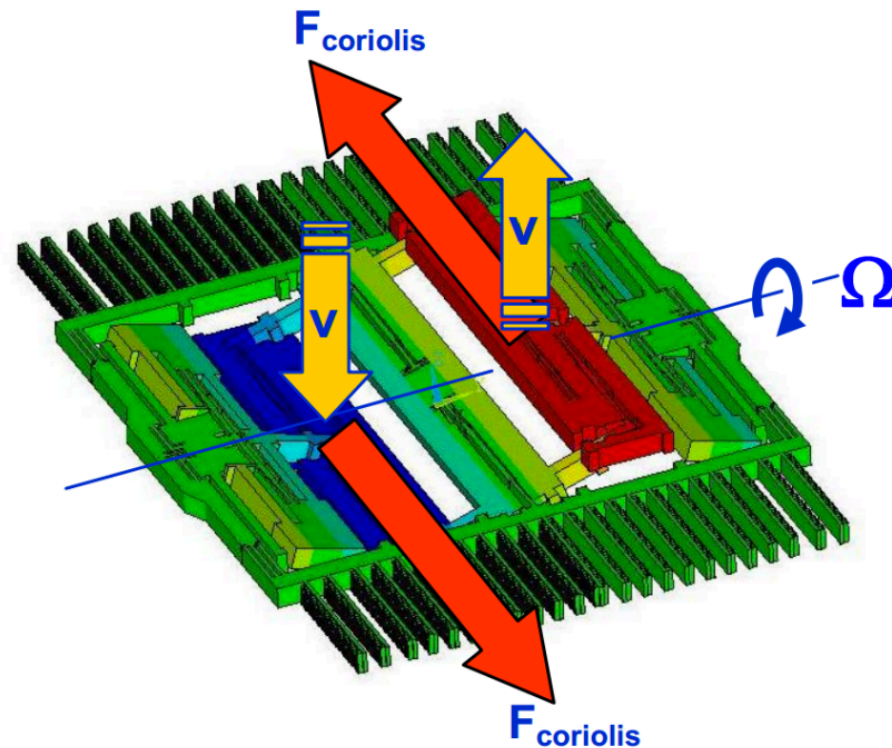# Key Extraction via Electric Potential

Genkin et al. "Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks On PCs" CHES 2014
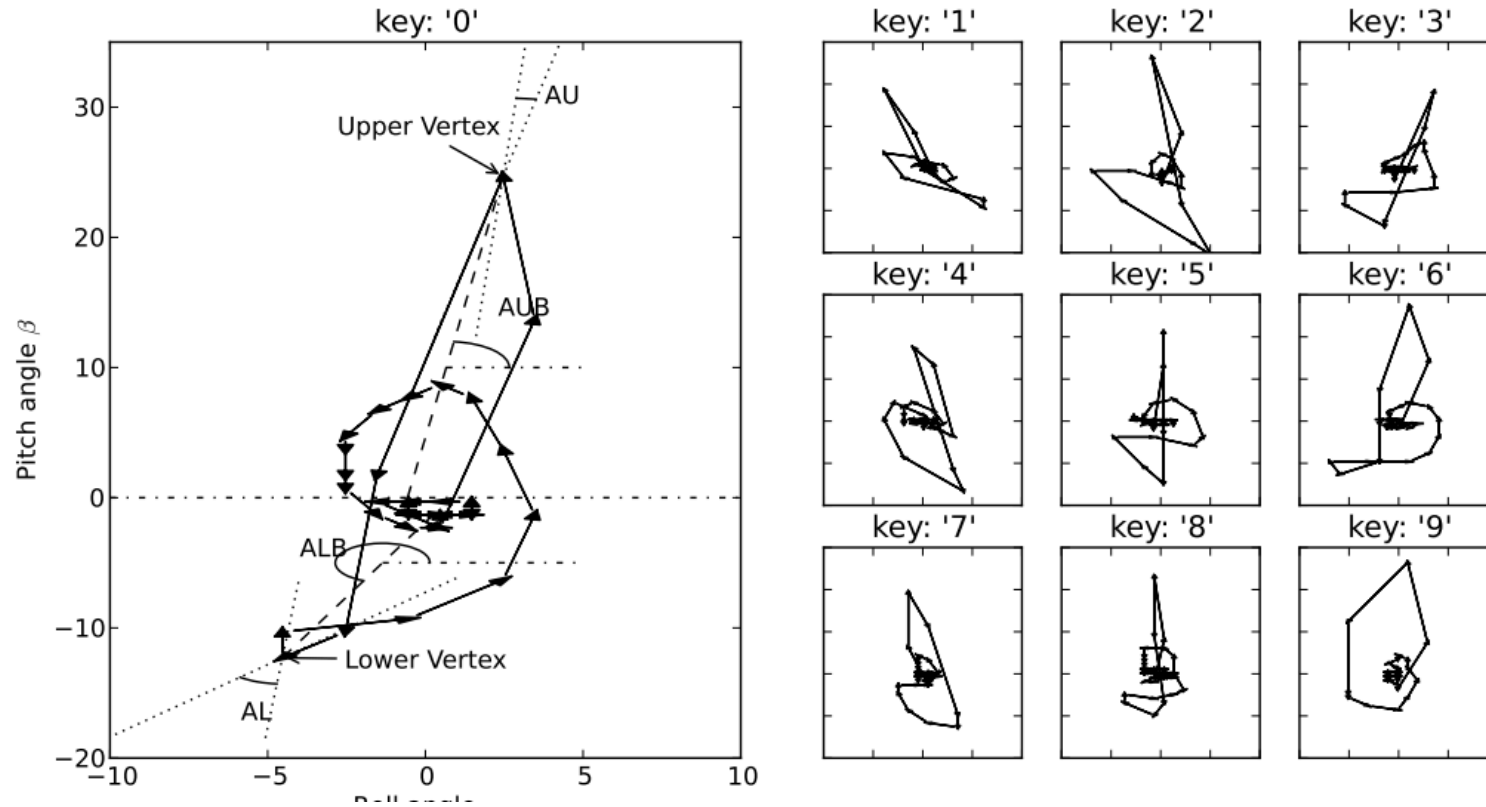
Accelerometer Eavesdropping

Aviv et al. "Practicality of Accelerometer Side Channels on Smartphones" ACSAC 2012

Gyroscope Eavesdropping

Michalevsky et al. "Gyrophone: Recognizing Speech from Gyroscope Signals" USENIX Security 2014

More Gyroscope

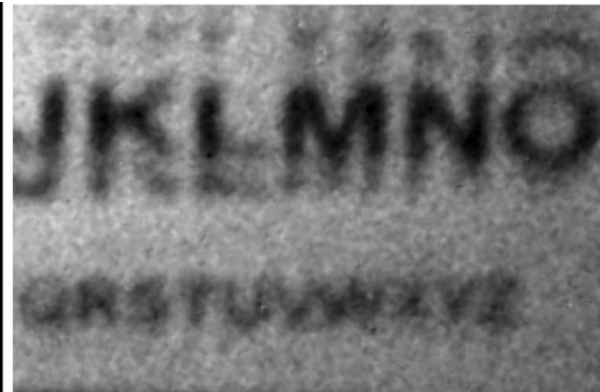Chen et al. "TouchLogger: Inferring Keystrokes On Touch Screen From Smartphone Motion" HotSec 2011
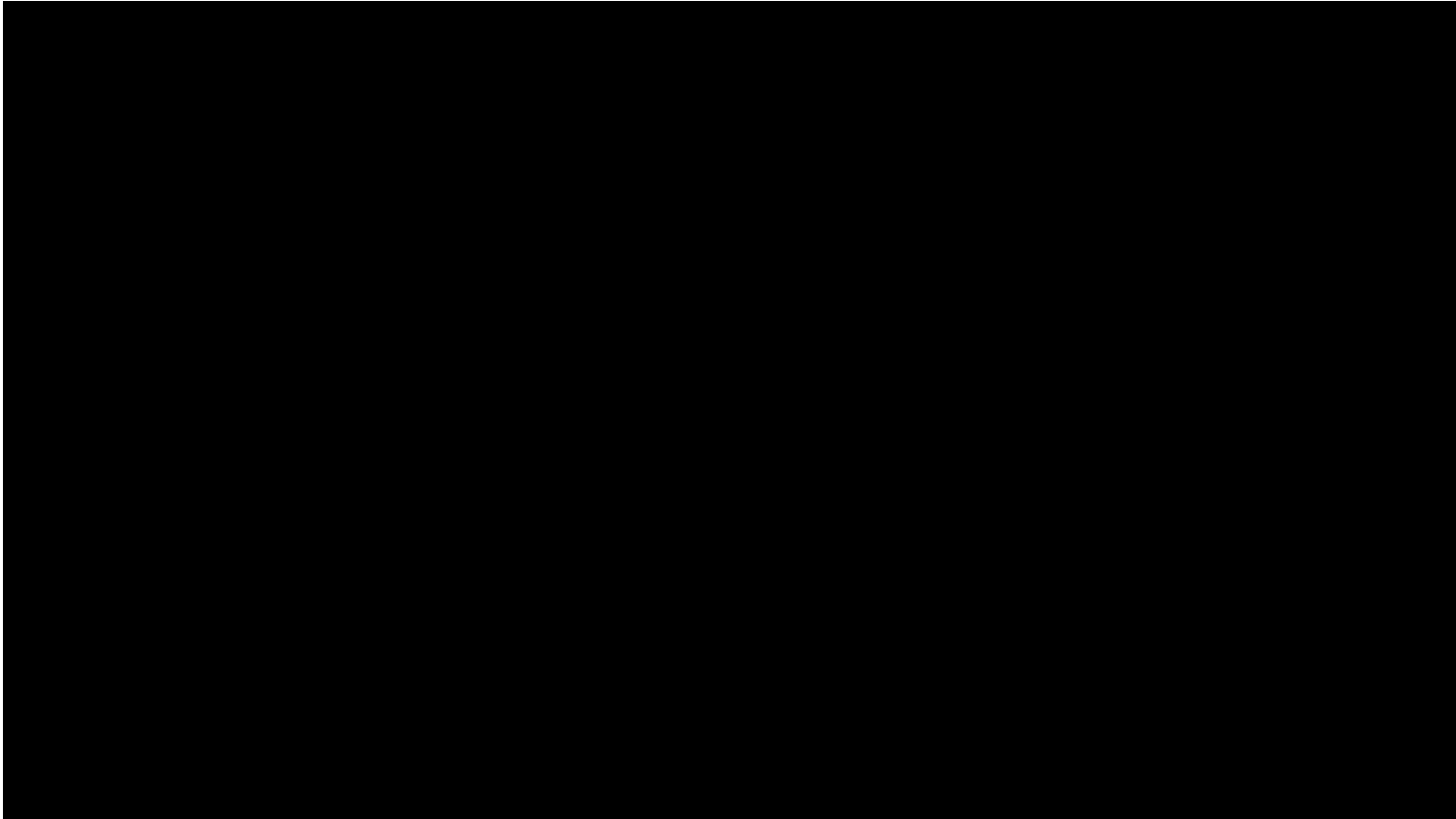
Keyboard Eavesdropping

Zhuang et al. "Keyboard Acoustic Emanations Revisited" CCS 2005
Vuagnoux et al. "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards" USENIX Security 2009

Compromising Reflections

CSE 484 / CSE M 584 - Spring 2016
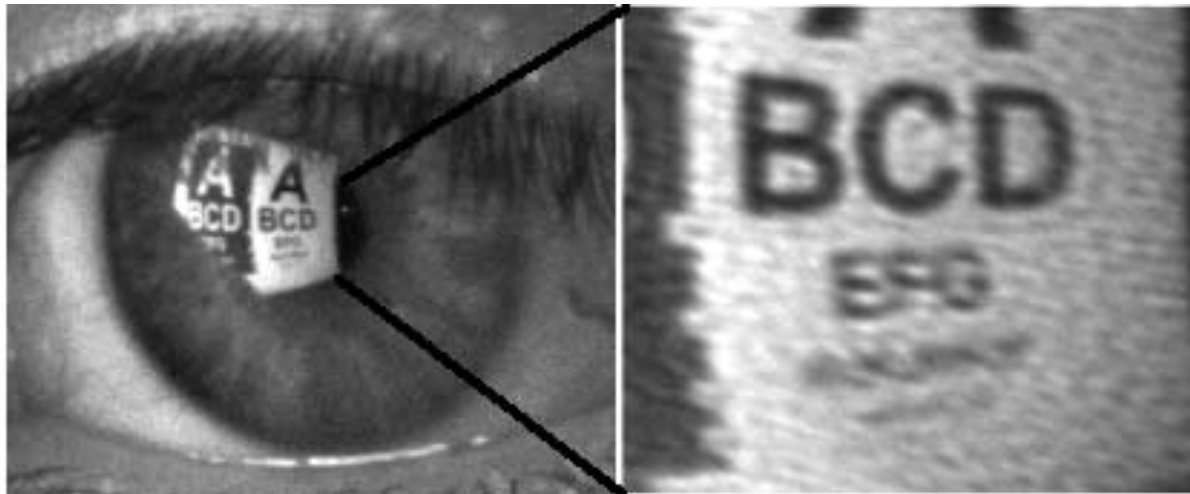
Audio from Video

Davis et al. "The Visual Microphone: Passive Recovery of Sound from Video" SIGGRAPH 2014
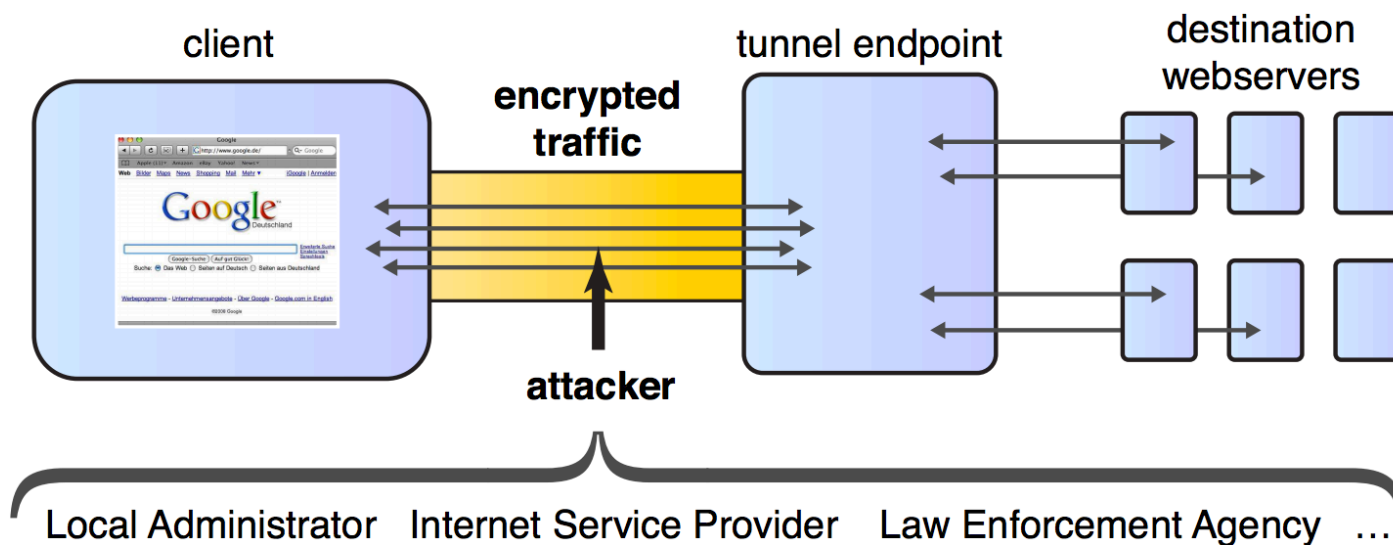
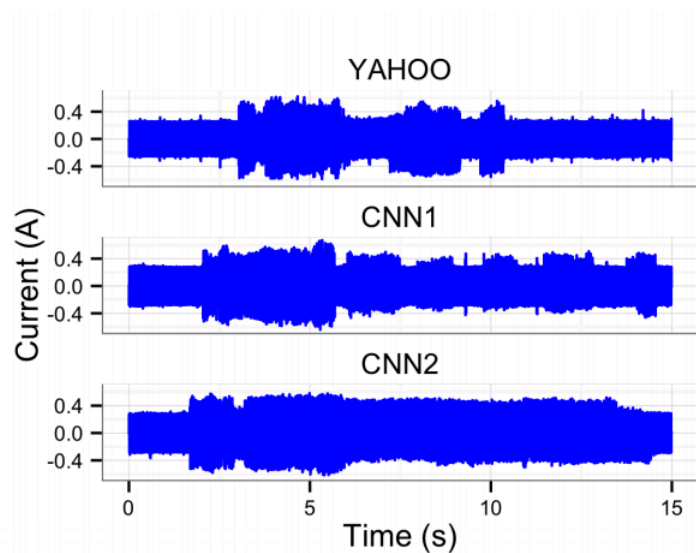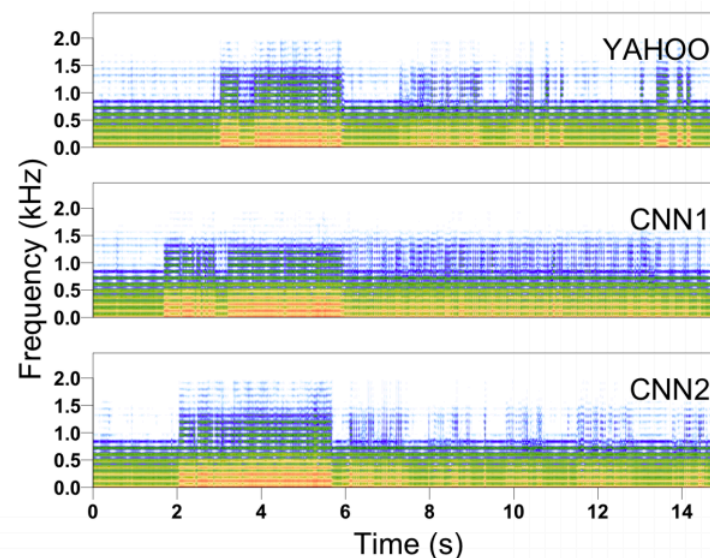# Identifying Web Pages: Traffic Analysis

Figure 1: Website fingerprinting scenario and conceivable attackers

Herrmann et al. "Website Fingerprinting: Attacking Popular Privacy Enhancing Technologies with the Multinomial Naïve-Bayes Classifier" CCSW 2009

Identifying Web Pages: Electrical Outlets

(a) Time-domain plots

(b) Spectrogram plots

Fig. 1: Time- and frequency-domain plots of several power traces as a MacBook loads two different pages. In the frequency domain, brighter colors represent more energy at a given frequency. Despite the lack of obviously characteristic information in the time domain, the classifier correctly identifies all of the above traces.

Clark et al. "Current Events: Identifying Webpages by Tapping the Electrical Outlet" ESORICS 2013
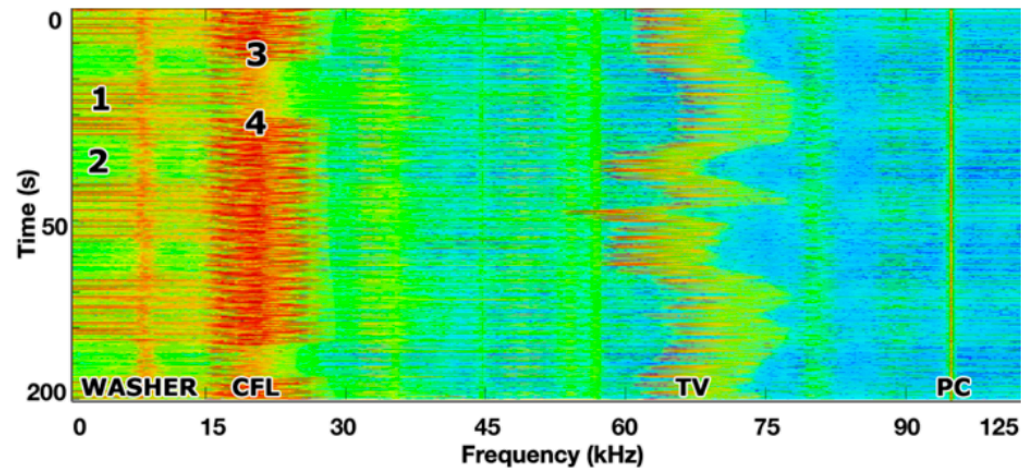
Powerline Eavesdropping

Figure 1: Frequency spectrogram showing various electrical appliances in the home. Washer cycle on (1) and off (2). CFL lamp turning off briefly (3) and then on (4). Note that the TV's (Sharp 42" LCD) EMI shifts in frequency, which happens as screen content changes.

Enev et al.: Televisions, Video Privacy, and Powerline Electromagnetic Interference, CCS 2011

SECURITY FOR EMERGING TECHNOLOGIES

Emerging Technologies
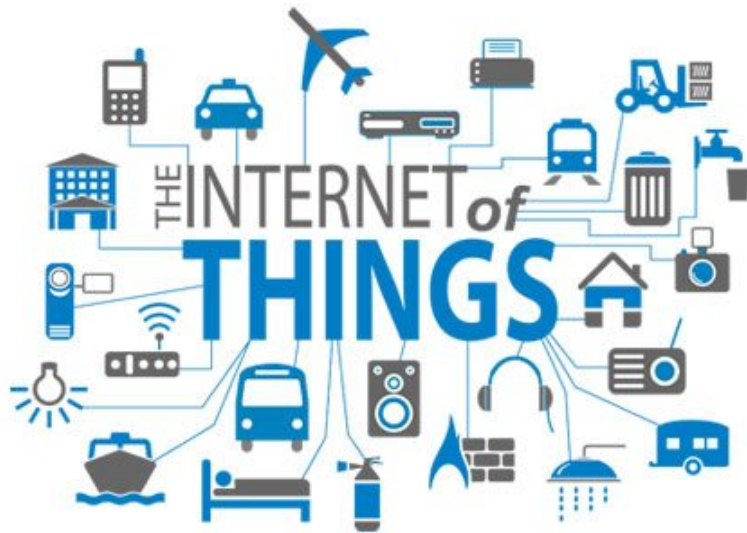
Augmented Reality

Synthetic Biology

Brain-Computer Interfaces

Case Study: Augmented Reality

- Input (sensor data) privacy
  - For users
  - For bystanders
- Output (display) security

- New challenges in AR context due to:
  - Need for ubiquitous sensing.
  - Multiple applications displaying virtual objects interacting with the user's view of the real world.

Challenge: Sensor Data Privacy

Seattle dive bar becomes first to ban Google Glasses over privacy fears
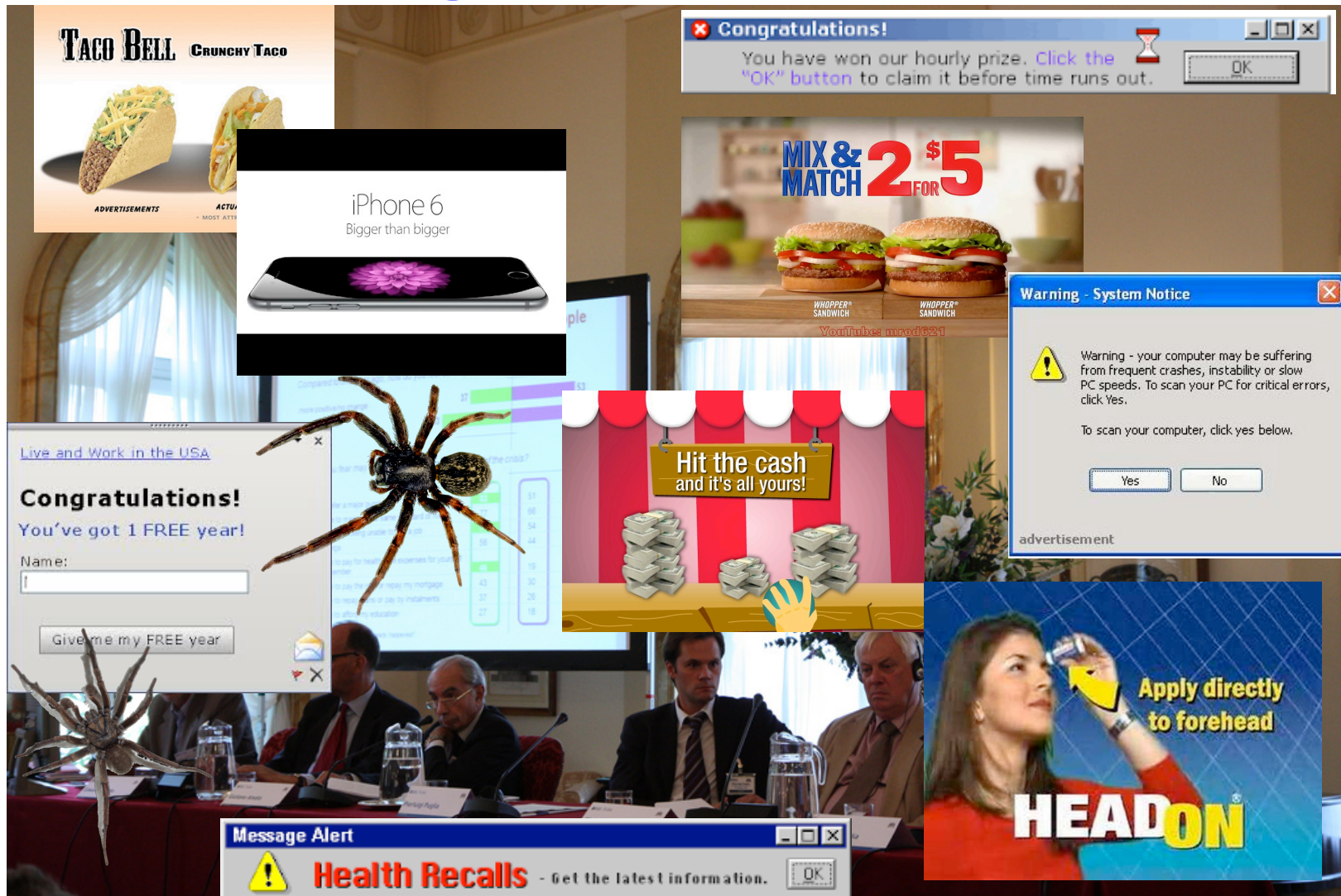
By NINA GOLGOWSKI

PUBLISHED: 00:43 EST, 10 March 2013 | UPDATED: 02:16 EST, 10 March 2013

Challenge: How can AR system manage applications' access to sensitive sensor data?

Challenge: Output Security

Challenge: Output Security

WRAP-UP

This Quarter

- Overview of:
    - Security mindset
    - Software security
    - Cryptography
    - Web security
    - Web privacy
    - Malware
    - Mobile platform security
    - Usable security
    - Physical security
    - Anonymity
    - Side channels
    - Emerging technologies (briefly!)

Lots We Didn't Cover…

- Deep dive into any of the above topics
- (Most) network security
- (Most) recent attacks/vulnerabilities
- (Most) specific protocols (e.g., Kerberos)
- Spam
- Social engineering
- Cryptocurrencies (e.g., Bitcoin)
- Other emerging technologies (e.g., home automation, brain-computer interfaces, synthetic biology, …)
- …

Thanks for a great quarter!

- Yay summer ☀️
- But also 😢

- Please fill out course evaluation:
  https://uw.iasystem.org/survey/161040

- Interested in research? Email me.