ECE 455: CYBERSECURITY

Lecture #12

Daniel Gitzel

In the news

- **Zero-click, wormable, remote code execution in Microsoft Teams**
  - Fixed 10/31/2020
  - Go take a look at this great write up:
    - https://github.com/oskarsve/ms-teams-rce

SIDE CHANNELS

Side Channel Attacks

- **Physical systems may emit information that tells us about their internal state**
  - EM Radiation (including light)
  - Sound (including vibration)
  - Temperature
  - Power Usage
  - Response Time

Side Channel Attacks

- **Attacks based on information that can be extracted from the physical implementation of a system, rather than breaking its theoretical properties**
  - Most commonly discussed in the context of crypto-systems
  - But also prevalent in many contexts

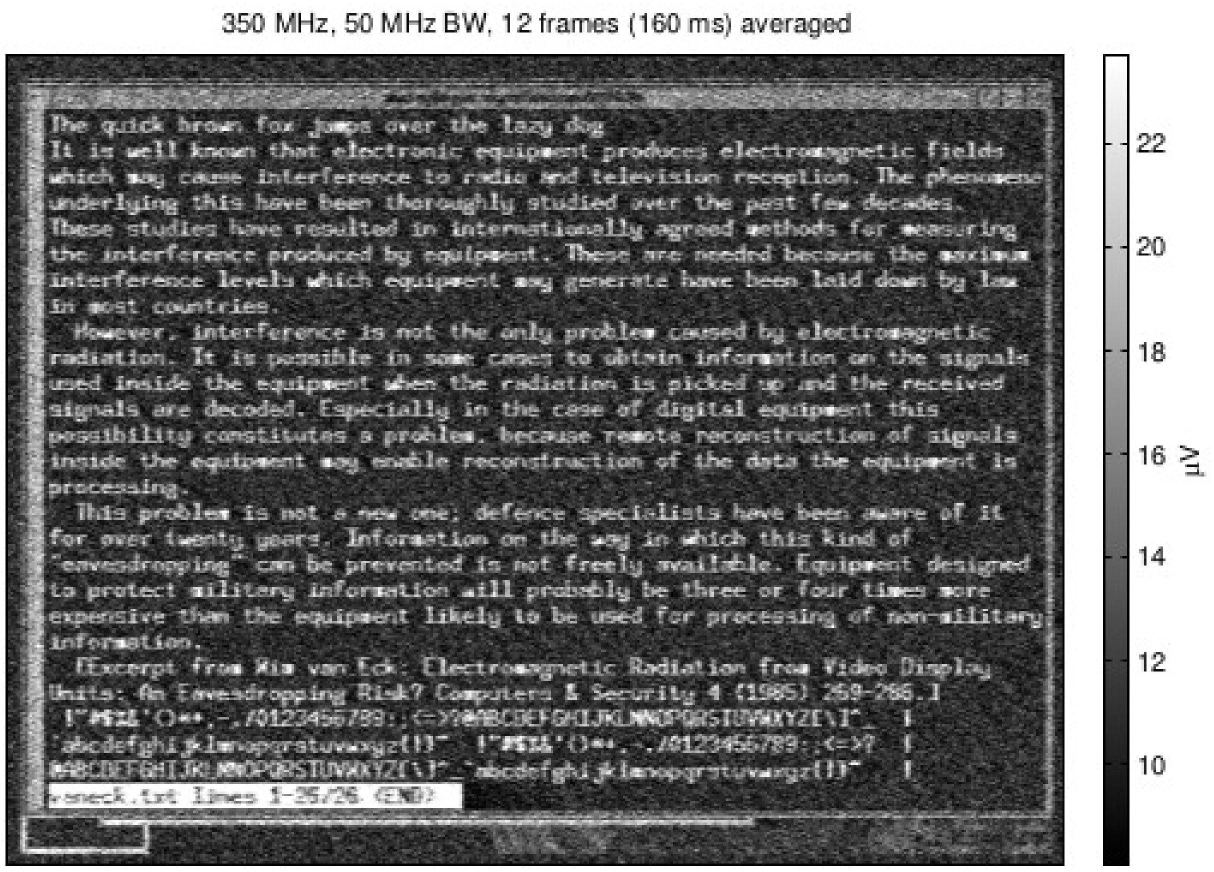
Examples (on Crypto-systems)

- **If your system behaves differently for secret key bits 1 vs. 0**
- **The system is emitting information**
  - Timing Attacks (caching, computation time, hardware)
  - Power Analysis (algorithm implementation, I/O)

Example Timing Attacks

- **RSA: Leverage key-dependent timings of modular exponentiations**
- **Block Ciphers: Leverage key-dependent cache hits/misses**
- **Example papers:**
  - RSA and Diffie-Hellman Timing Attacks
  - SSL Timing Attacks

RF interception



```
The quick brown fox jumps over the lazy dog
It is well known that electronic equipment produces electromagnetic fields
which may cause interference to radio and television reception. The phenomena
underlying this have been thoroughly studied over the past few decades.
These studies have resulted in internationally agreed methods for measuring
the interference produced by equipment. These are needed because the maximum
interference levels which equipment may generate have been laid down by law
in most countries.
  However, interference is not the only problem caused by electromagnetic
radiation. It is possible in some cases to obtain information on the signals
used inside the equipment when the radiation is picked up and the received
signals are decoded. Especially in the case of digital equipment this
possibility constitutes a problem, because remote reconstruction of signals
inside the equipment may enable reconstruction of the data the equipment is
processing.
  This problem is not a new one; defence specialists have been aware of it
for over twenty years. Information on the way in which this kind of
"eavesdropping" can be prevented is not freely available. Equipment designed
to protect military information will probably be three or four times more
expensive than the equipment likely to be used for processing of non-military
information.
  [Excerpt from Wim van Eck: Electromagnetic Radiation from Video Display
Units: An Eavesdropping Risk? Computers & Security 4 (1985) 269-286.]
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_  !
`abcdefghijklmnopqrstuvwxyz{|}~  !"#$%&'()*+,-./0123456789:;<=>?  !
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~   !
vaneck.txt lines 1-26/26 (END)
```

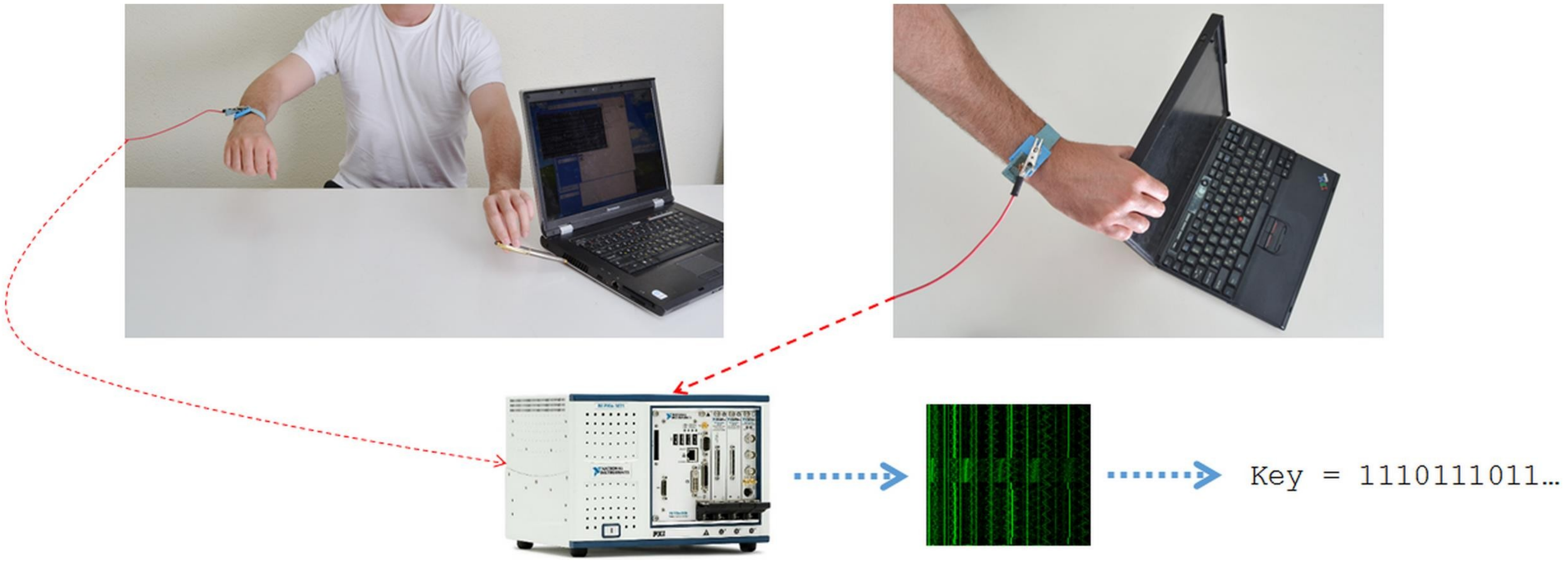
Figure 19.1: – RF signal from a Toshiba laptop reconstructed several rooms away, through three plasterboard walls (courtesy of Markus Kuhn [1104]).

RF Interception

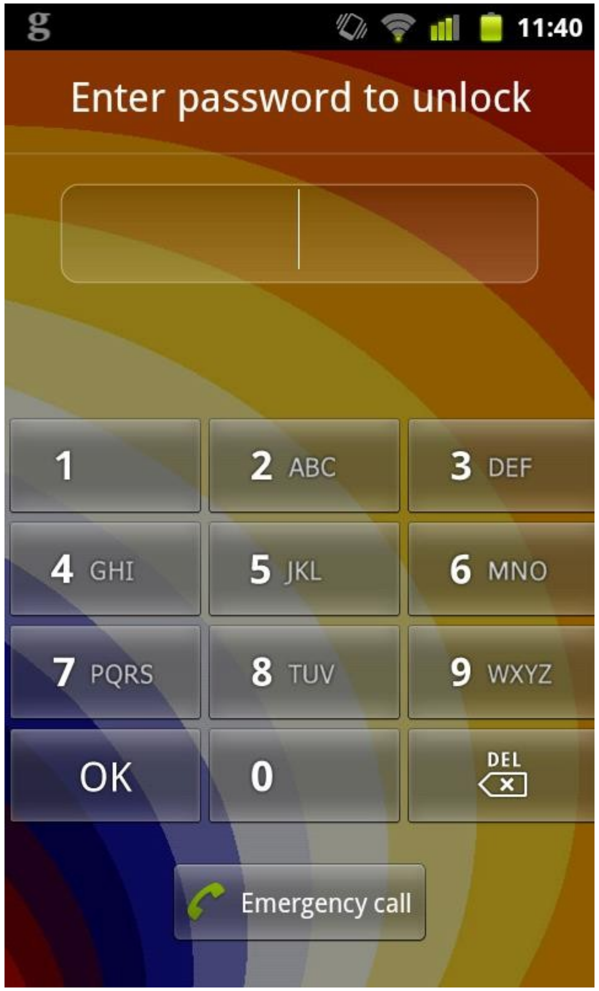
- **Assume 2MHz video data carrier frequency (in cable)**
- **Broadcast RF which modulates and mixes with video data (non-linear mixing)**
- **Aliased signal is rebroadcast and demodulated by receiver**
- **Accidental/environmental radio sources can be used:**
  - Cell phone/Wifi/etc.
  - Ship/Aircraft Radar (used by Soviets to listen into US Guam spy station)

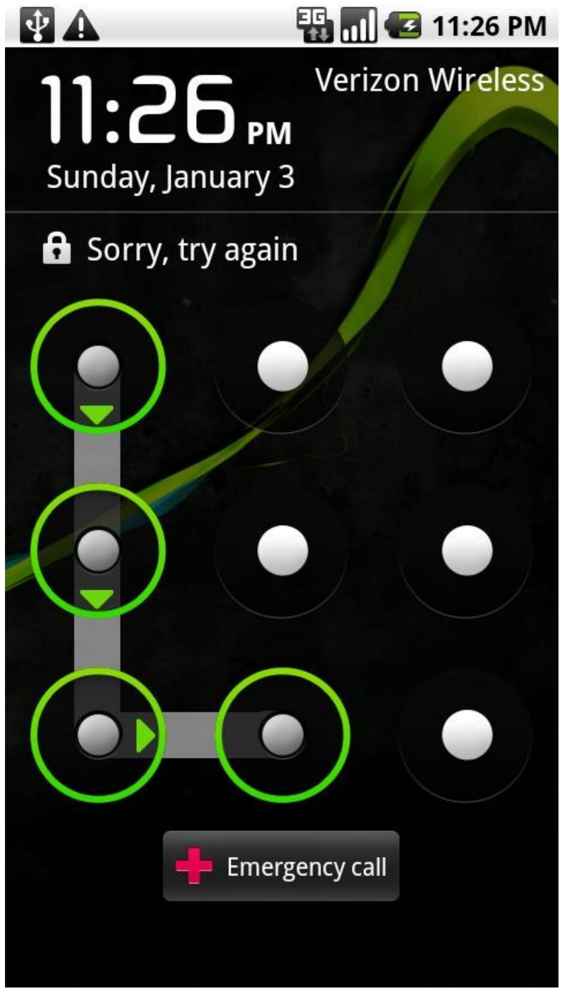
Key Extraction via Electric Potential

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



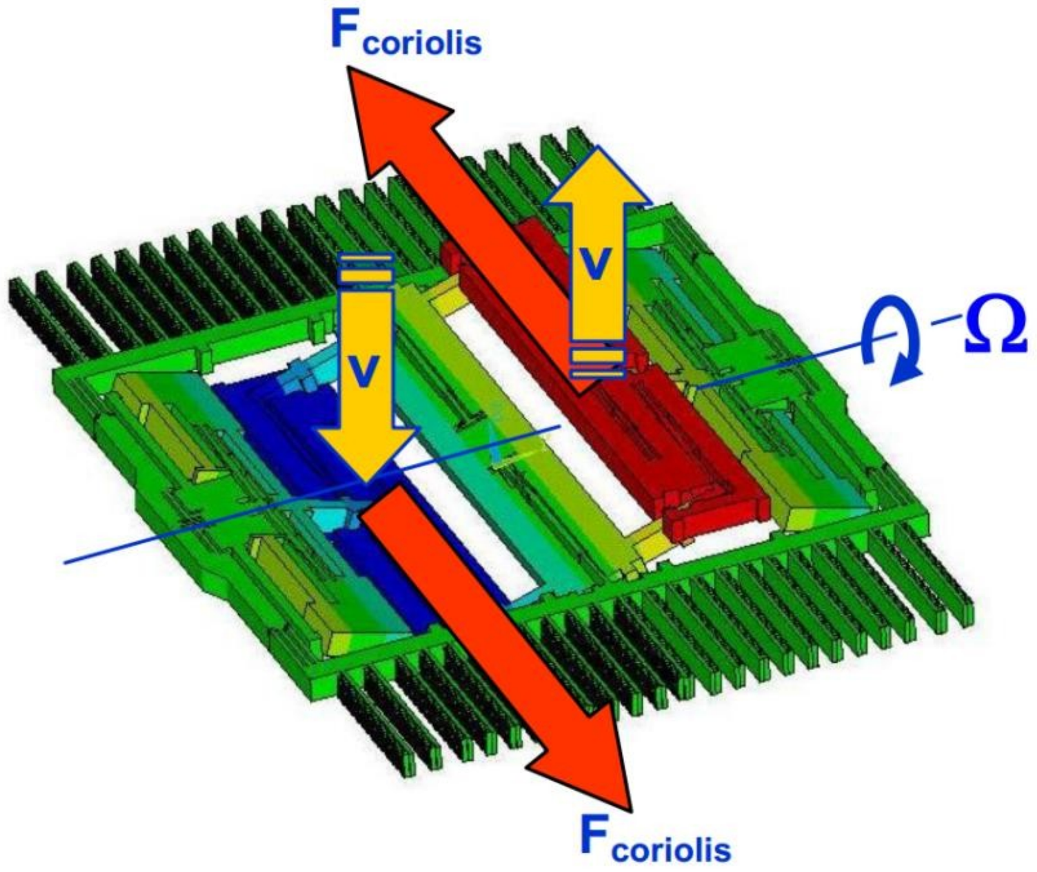
Accelerometer Eavesdropping





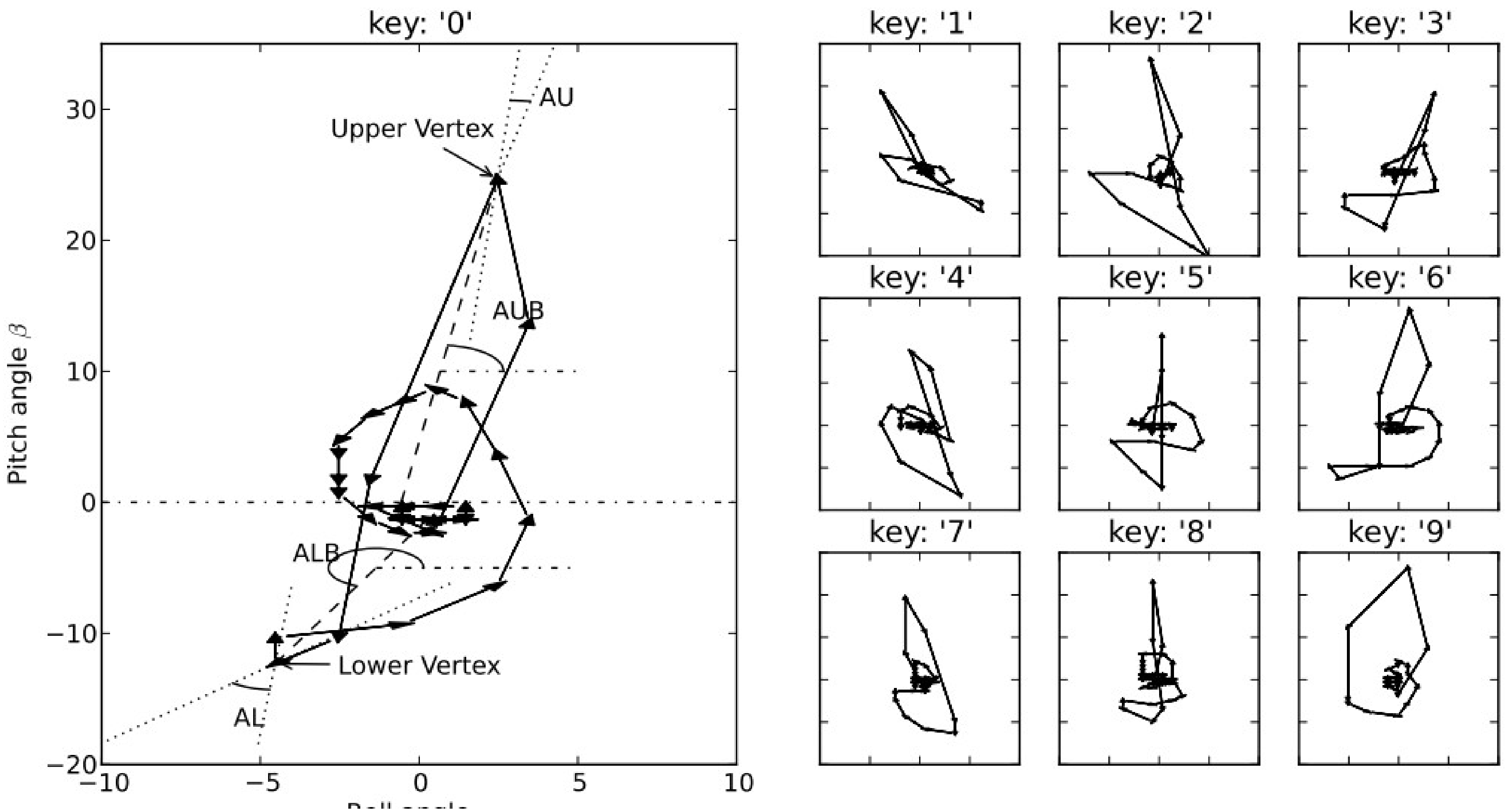
Aviv et al. “Practicality of Accelerometer Side Channels on Smartphones” ACSAC 2012

Gyroscope Eavesdropping



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

Gyroscope Eavesdropping



Chen et al. “TouchLogger: Inferring Keystrokes On Touch Screen From Smartphone Motion” HotSec 2011

Keyboard Eavesdropping

- Emit RF and audio
- Bluetooth, USB, custom protocols

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

Identifying Web Pages: Traffic Analysis

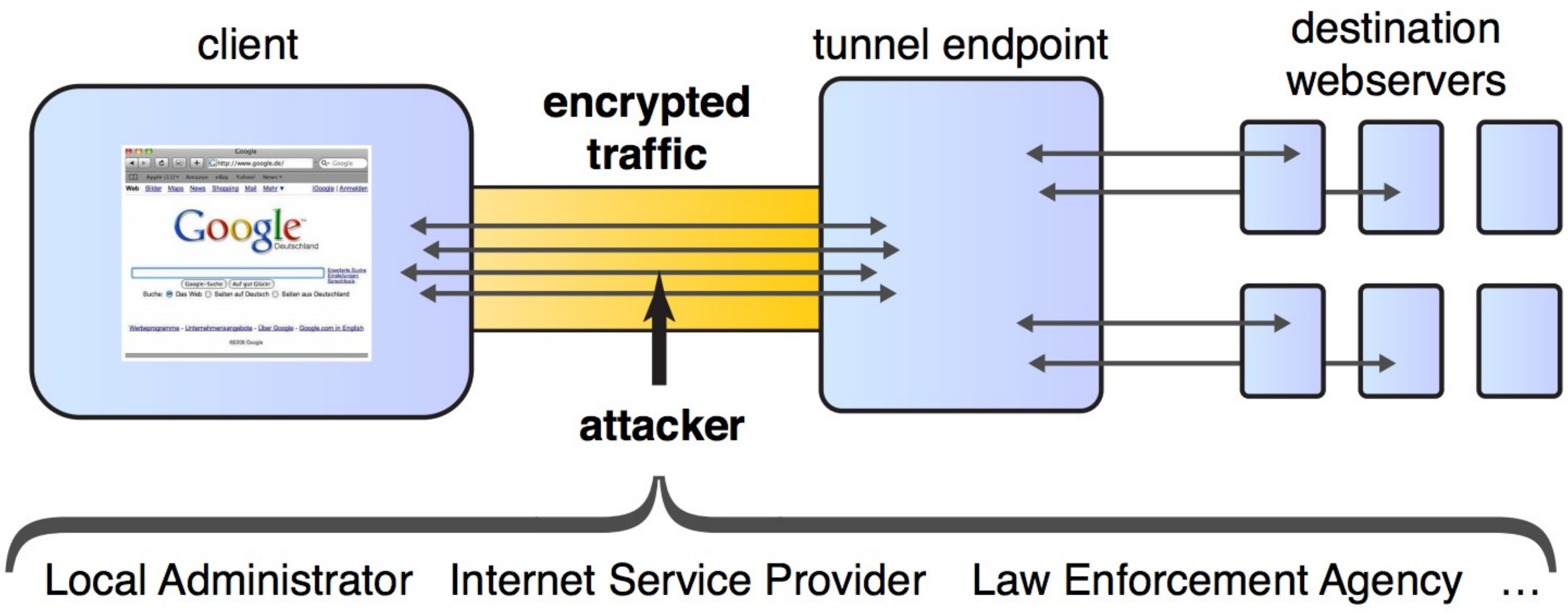
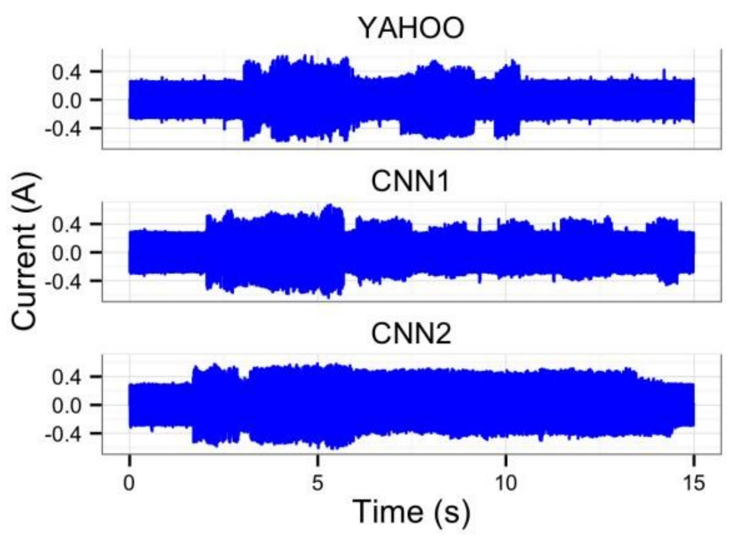


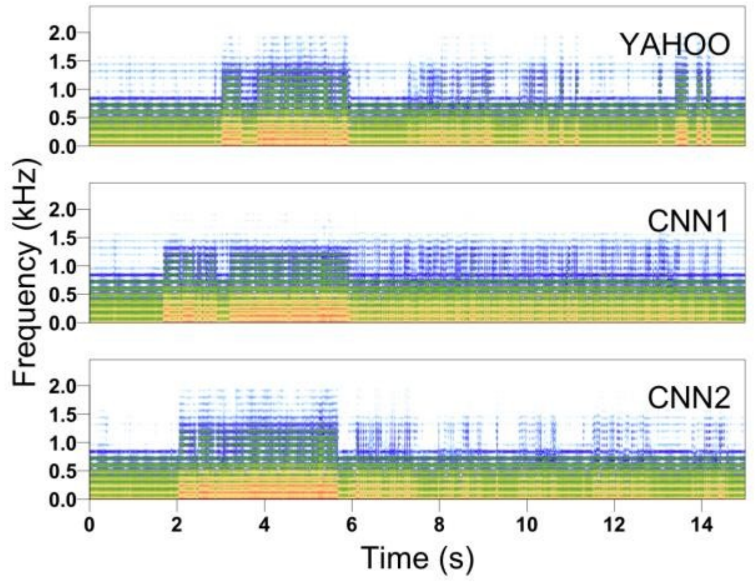
Figure 1: Website fingerprinting scenario and conceivable attackers

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



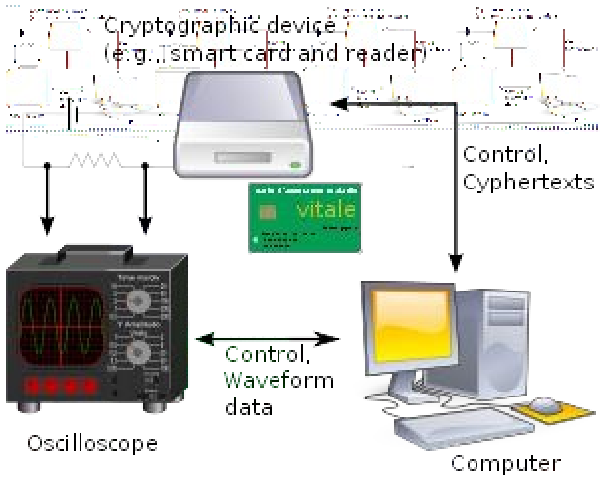
(b) Spectrogram plots

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.

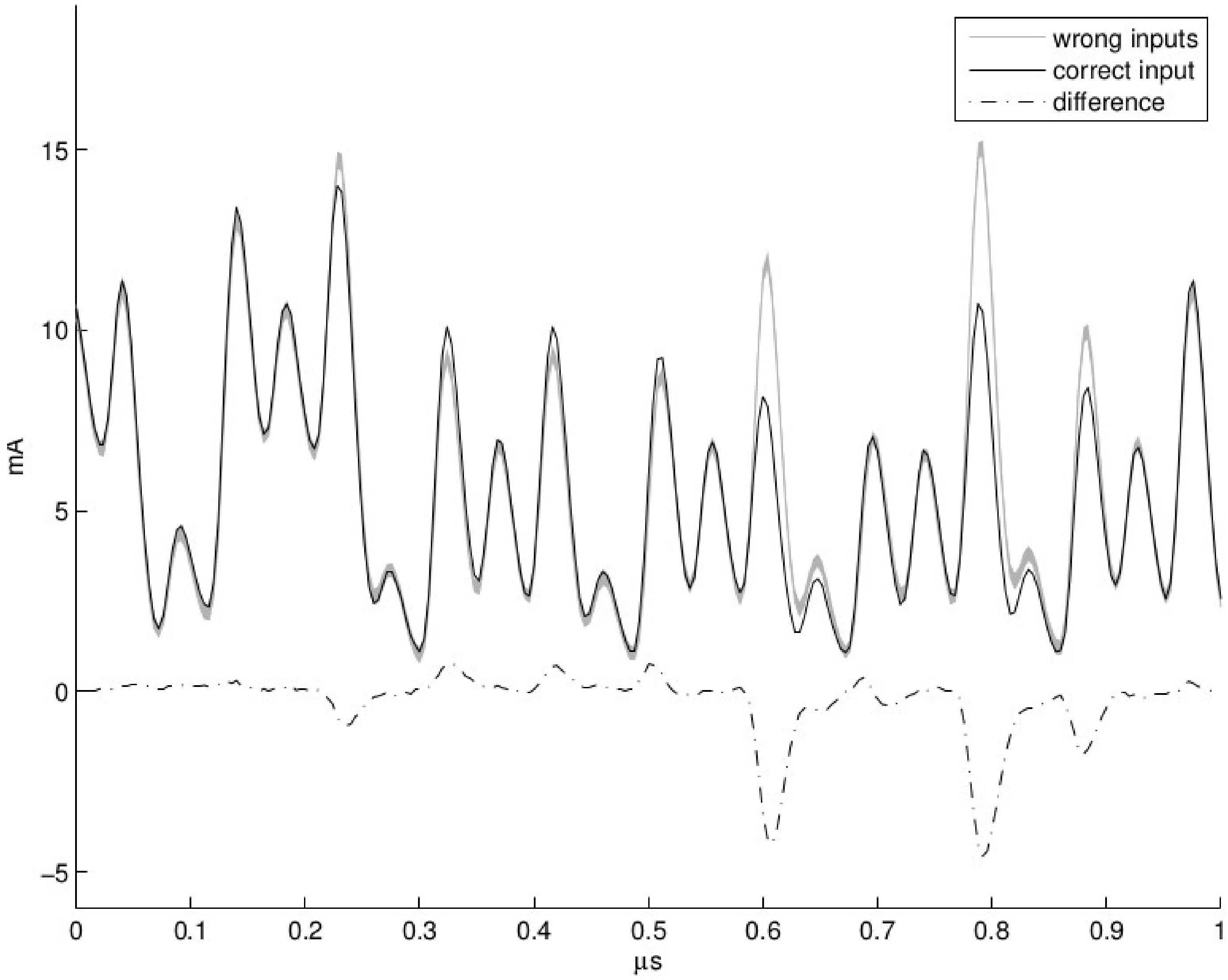
Clark et al. "Current Events: Identifying Webpages by Tapping the Electrical Outlet" ESORICS 2013

Power Analysis

- **Simple power analysis**
  - Directly read off bits from power-line traces
- **Differential power analysis**
  - Look for statistical differences in power traces, based on guesses of a key bit



Differential Power Consumption



Differential Power Consumption

- **Why does this work?**
  - ISA is not-uniform, instructions have different power-profiles
  - Different data inputs (bytes) may affect instructions used
  - Writing to memory is a power-spike (e.g. EEPROM)
- **Allows attackers to see bit-level or byte-level differences in processing**
- **Can inform correct/incorrect guesses**

Powerline Eavesdropping

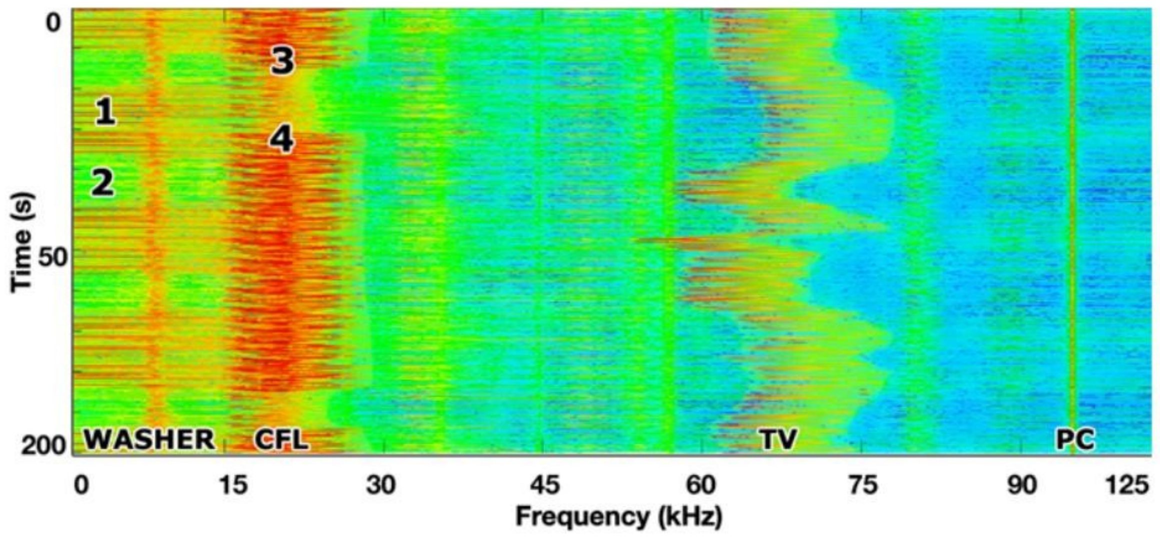


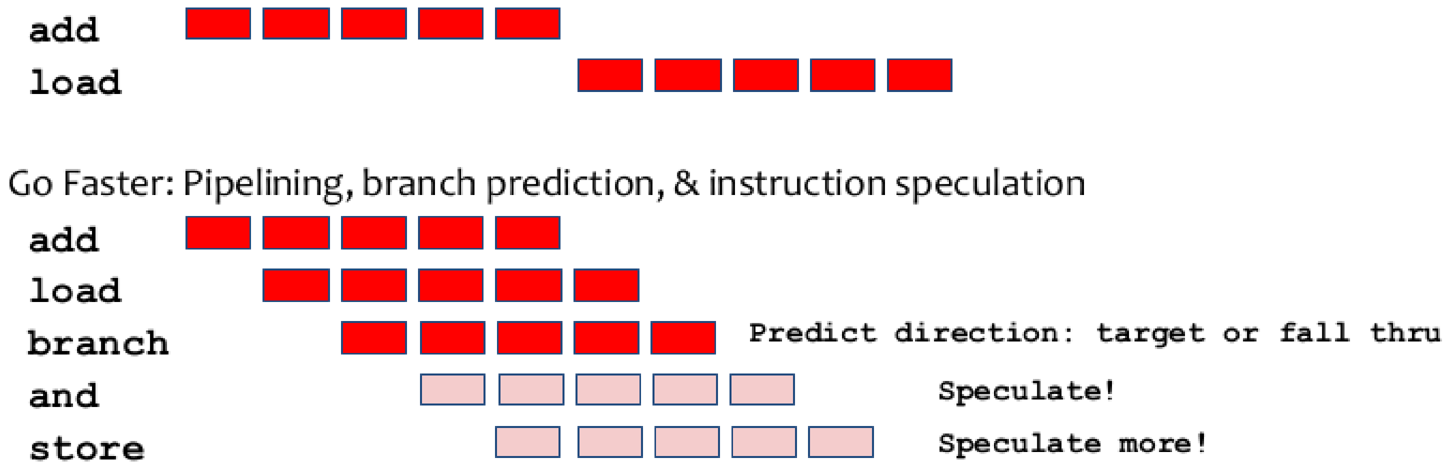
Figure 1: Frequency spectrogram showing various electrical appliances in the home. Washer cycle on (1) and off (2). CFL lamp turning off briefly (3) and then on (4). Note that the TV's (Sharp 42" LCD) EMI shifts in frequency, which happens as screen content changes.

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

Spectre

- **Exploit speculative execution and cache timing information to extract private information from the same process**
  - Example: JavaScript from web page trying to extract information from Browser
- **Architecture Background:**
  - Hardware architecture provides “promises” to software
  - Those proposes focus on the functional properties of the software, not performance properties
  - Architectures do a lot to try to increase performance

Instruction Speculation Tutorial

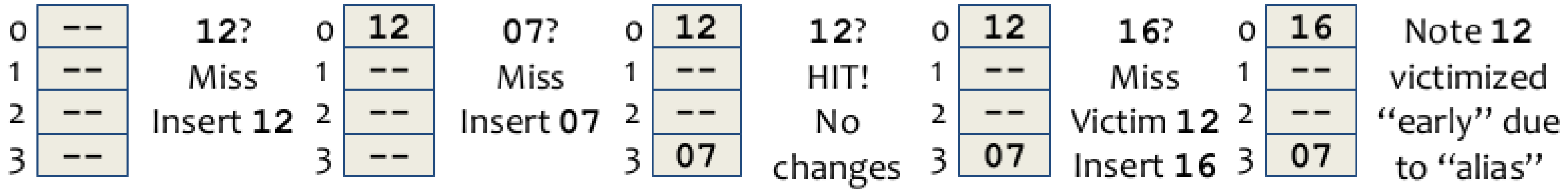

add
load
Go Faster: Pipelining, branch prediction, & instruction speculation
add
load
branch
and
store
Predict direction: target or fall thru
Speculate!
Speculate more!

- **Speculation correct (fast!):**
  - Commit architectural changes of AND (register) & STORE (memory)
- **Mis-speculate (oops…):**
  - Abort architectural changes (registers, memory); go in other branch direction

Hardware Caching Tutorial

- **Main Memory (DRAM) 1000x too slow**
- **Add Hardware Cache(s): small, transparent hardware memory**
  - Like a software cache: speculate near-term reuse (locality) is common
  - Like a hash table: an item (block or line) can go in one or few slots

E.g., 4-entry cache w/ slot picked with address (key) modulo 4



Spectre (Worksheet)

- **Consider this code, running as a kernel system call or as part of a cryptographic library.**

  if (x < array1_size)

  y = array2[array1[x] * 256];

- **Suppose:**
  - That an adversary can run code, in the same process.
  - That an adversary can control the value x.
  - That an adversary has access to array2.
  - That the adversary's code cannot just read arbitrary memory in the process.
  - That there is some secret value, elsewhere in the process, that the adversary would like to learn.
- **Can you envision a way that an adversary could use their own code, to call a vulnerable function with the above code, to learn the secret information?**
- **Leverage branch prediction and cache structure / timing.**

Spectre: Key Insights

1) Train branch predictor to follow one branch of a conditional
2) Make the followed branch access information that the code should not be allowed to access
3) That access information will be loaded into the cache
4) After the hardware determines that the branch was incorrectly executed, the logic of the program will be rolled back but the cache will still be impacted
5) Time reads to cache, to see which cache lines are read more efficiently

Attacker Steps

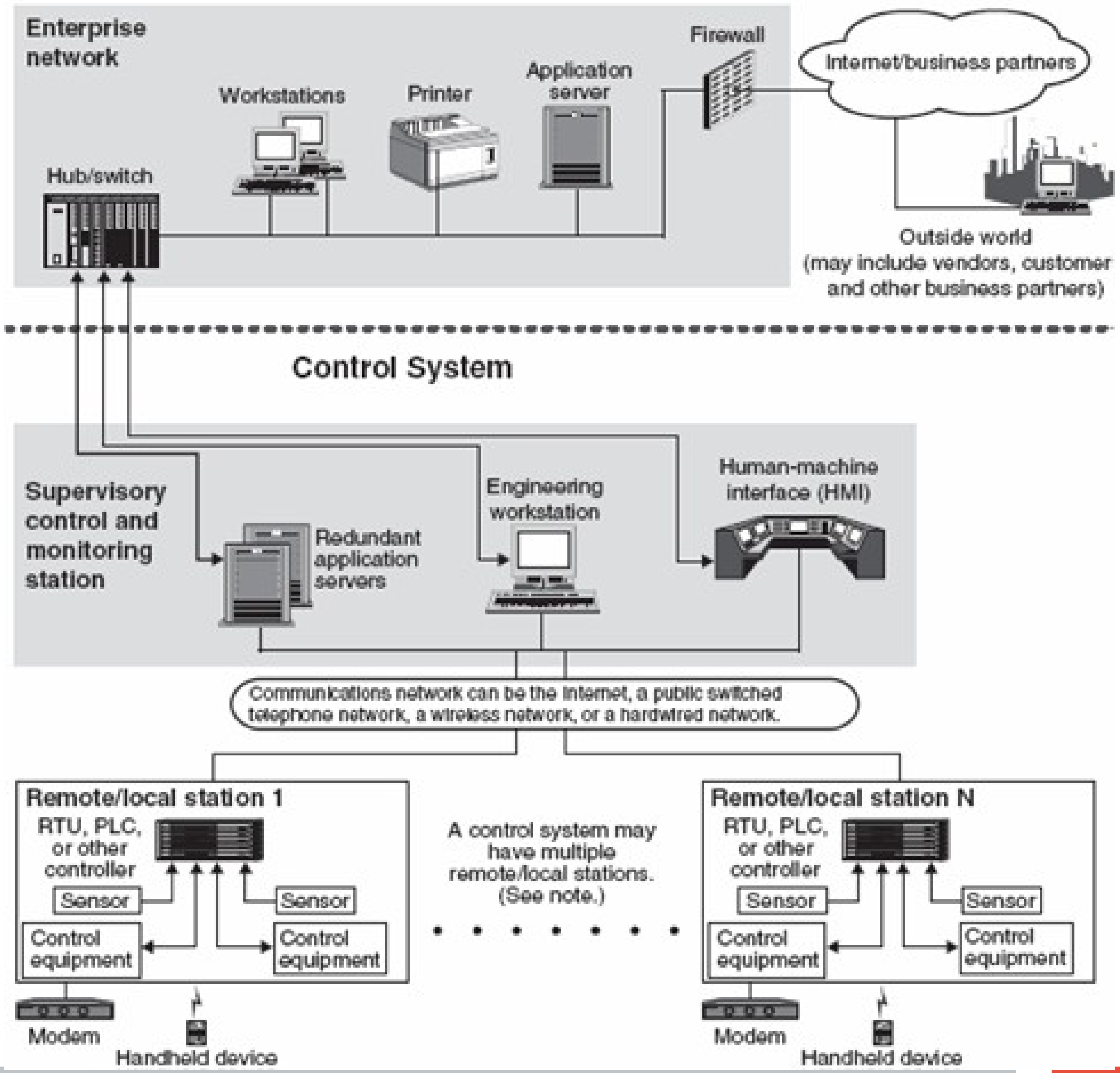
- **Attacker: Execute code with valid inputs, train branch predictor to assume conditional is true**
- **Attacker: Invoke code with x outside of array1 , array1_size and array2 not cached, but value at array1+x cached // Attacker goal: read secret memory at address array1+x**
- **CPU: CPU guesses bounds check is true, speculatively reads from array2[array1[x]*256] using malicious x**
- **CPU: Read from array2 loads data into cache at an address that depends on array1[x] using malicious x**
- **CPU: Change in cache state not reverted when processor realizes that speculative execution erroneous**
- **Attacker: Measure cache timings for array2; read of array2[n*256] will be fast for secret byte n (at array1+x)**
- **Attacker: Repeat for other values of x**

SCADA AND CONTROL SYSTEM SECURITY

SCADA (Supervisory Control and Data Acquisition)

- **Facilities management and real-time:**
  - Remote access
  - Monitoring
  - Command and control
- **Originally proprietary systems and protocols**
  - Now TCP/IP and much more exposed
  - Protocols have standardized

Typical SCADA Components

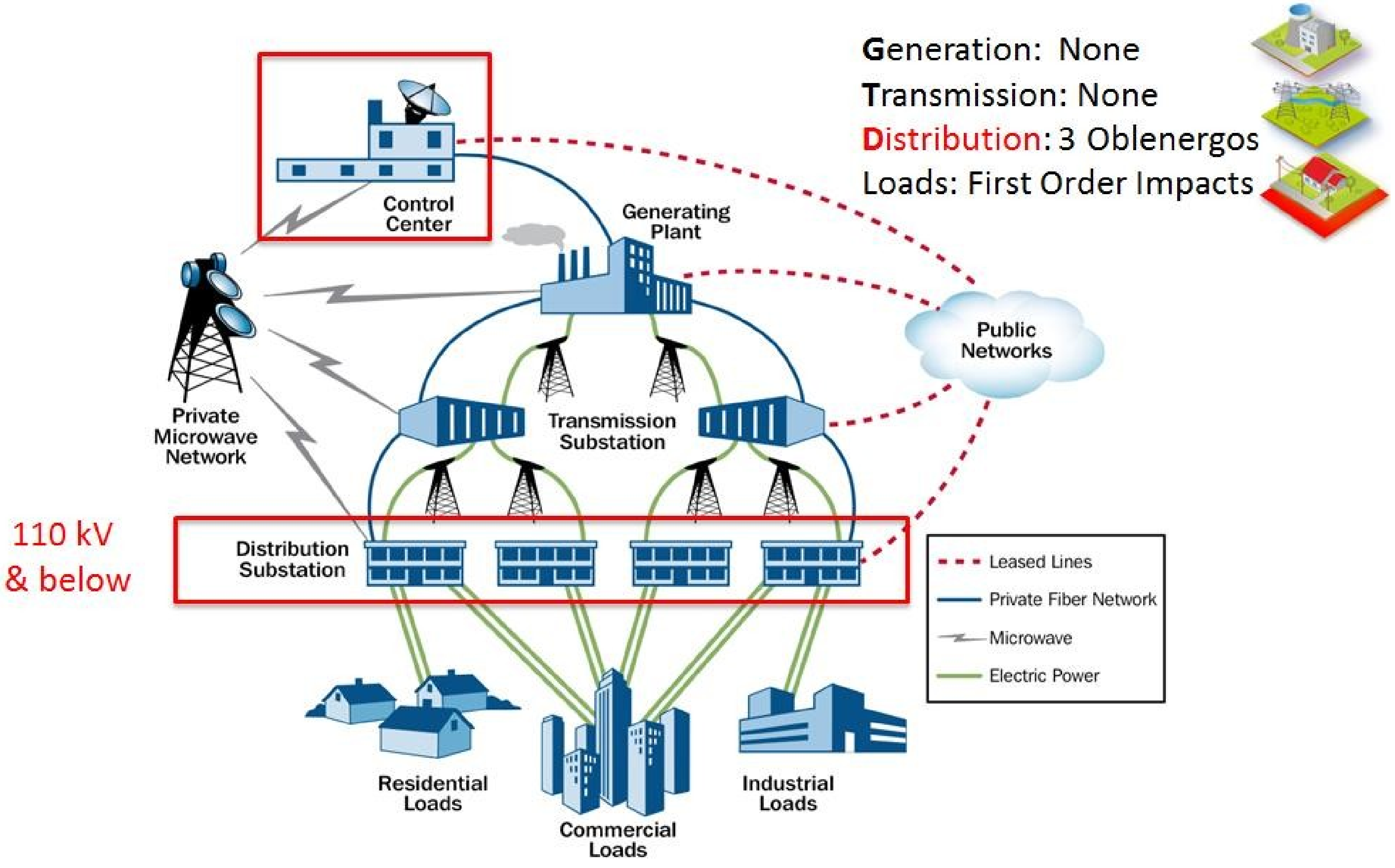


Enterprise network
Firewall
Internet/business partners
Application server
Workstations
Printer
Hub/switch
Outside world (may include vendors, customer and other business partners)
Control System
Supervisory control and monitoring station
Redundant application servers
Engineering workstation
Human-machine interface (HMI)
Communications network can be the Internet, a public switched telephone network, a wireless network, or a hardwired network.
Remote/local station 1
RTU, PLC, or other controller
Sensor
Sensor
Control equipment
Control equipment
Modem
Handheld device
A control system may have multiple remote/local stations. (See note.)
Remote/local station N
RTU, PLC, or other controller
Sensor
Sensor
Control equipment
Control equipment
Modem
Handheld device

Differences from IT systems

- **Human-machine interface**
- **Critical, real-time operation**
  - Constrained resources
  - Cascading failures
- **Industry specific-processes**
  - Physical material handling (liquids, gases, bulk material)
  - Timing and scheduling (traffic, reactions)

Ukrainian Power Grid Attack (oblenergos)



Source: Modification to the DHS Energy Sector-Specific Plan 2010

Sophisticated Multi-part Attack

- Spear phishing: gain access to the business networks
- Theft of credentials from the business networks
- VPNs to enter the ICS network
- Using existing remote access or issuing commands directly from a remote station
- Serial-to-ethernet communications devices impacted at a firmware level
- Modified KillDisk to erase the master boot record of impacted organization systems
- Targeted deletion of log files
- Using UPS systems to impact connected load with a scheduled service outage
- Telephone denial-of-service attack on the call center