Insights from Waves

Forensic Insights from IoT with Electromagnetic Side-Channel Analysis

Asanka Sayakkara, Mark Scanlon, Nhien-An Le-Khac

DFRWS EU 2020

UCD Forensics and
Security Research Group

Outline

- Electromagnetic Side-Channel Analysis for Digital Forensics - 1 hour

  coffee break - 15 mins

- Introduction to EMvidence Framework - 1 hour and 15 mins

Electromagnetic Side-Channel Analysis for Digital Forensics

(Duration: 1 hour)

Asanka Sayakkara, Mark Scanlon, Nhien-An Le-Khac

DFRWS EU 2020

UCD Forensics and
Security Research Group

Digital Forensics

- Computers have become an integral part of day-to-day life.
- We leave enough information in digital form that give away our actions.
- Hard disks, smartphones, USB sticks, SD cards, CCTV systems, cloud storage, online accounts, and many more.

Digital forensics is a branch of forensic science that uses material found in digital devices to assist investigations.

Important Trends in Digital Forensics

Data encryption:

- Important files can be encrypted.
- Data communication can be end-to-end encrypted.
- Law-enforcement requires the owners cooperation to decrypt data.

Important Trends in Digital Forensics

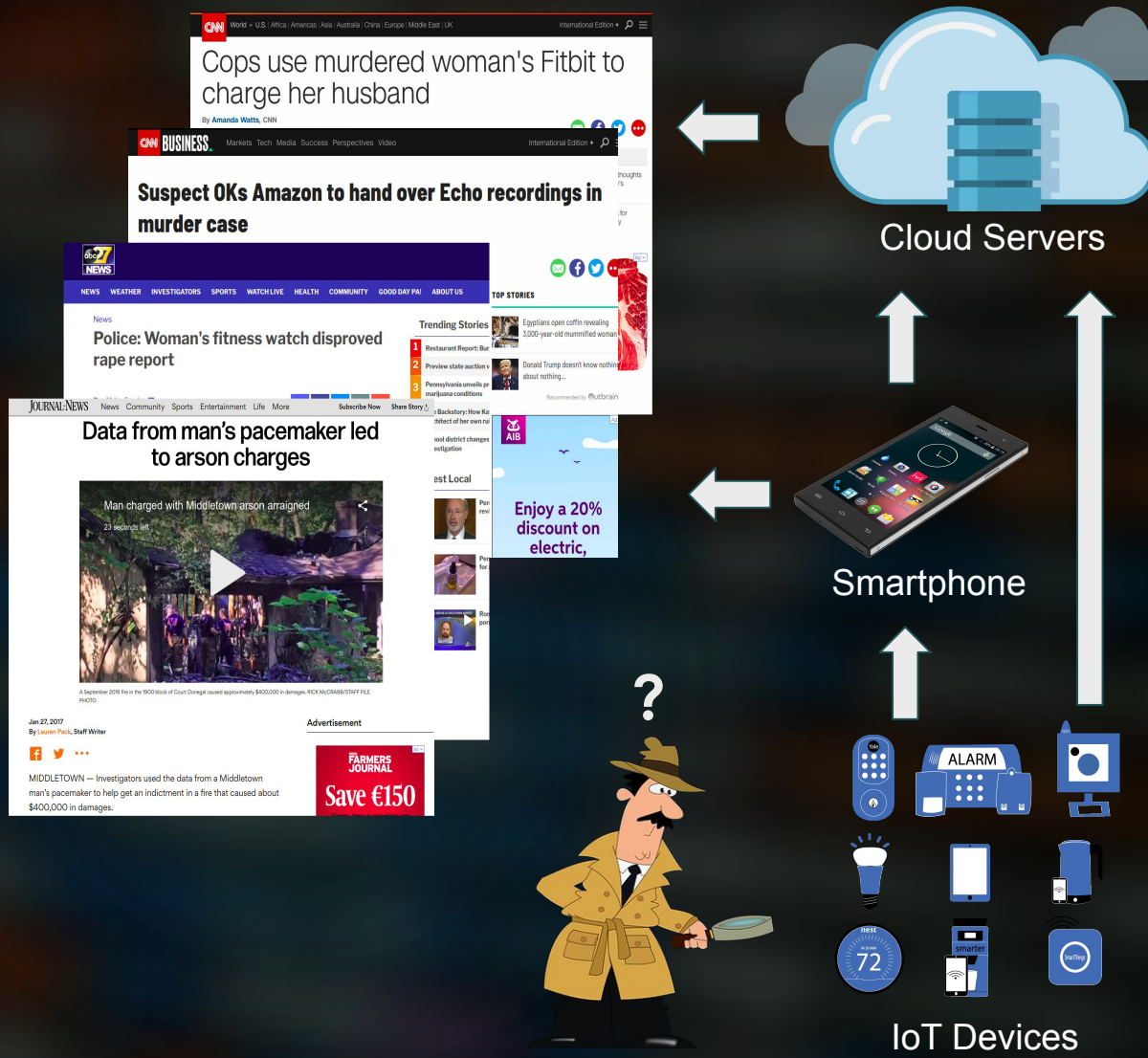
Internet of Things:

- Small battery-operated devices with Internet connectivity.
- Highly diverse makes and models for various purposes.
- ...health implants, sports wearables, smart burglar alarms, smart thermostats...

Forensics of Internet of Things

- Lightweight cryptographic algorithms, e.g., ECC, can be run on low-resourced devices.
- IoT devices can incorporate cryptography to defend internal storage and communication.
- Resulting IoT systems are even harder to forensically inspect.

Direction of IoT Forensics



- Most IoT devices connects to mobile apps and cloud servers.
- Forensic inspection of them can reveal information related to IoT
- Chip-off forensics - physically removing memory chips from the devices and inspecting them.

But there's a road less traveled…

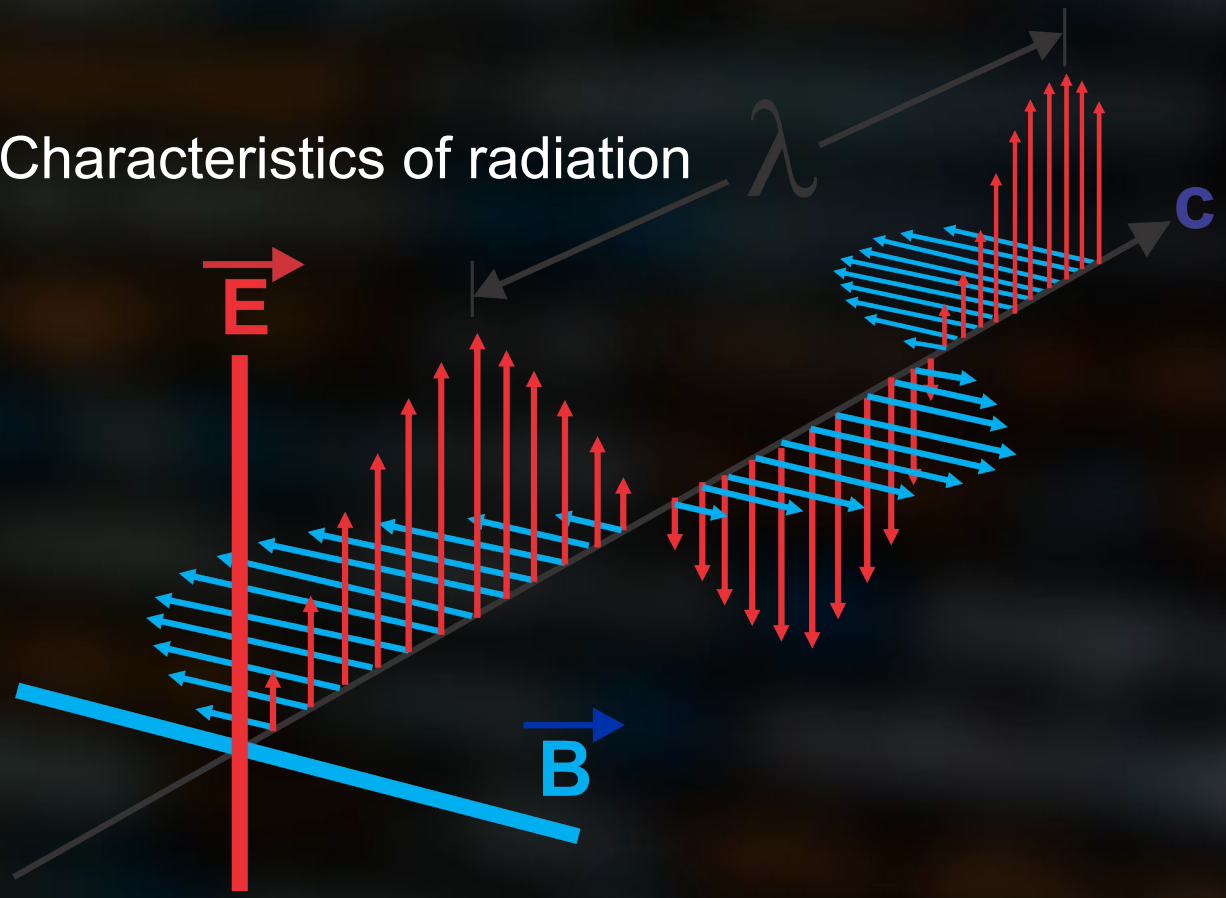
Electromagnetic Side-Channel Analysis

Time-varying electrical currents ⇒ Electromagnetic radiation

Nature of the time-varying current ⇐ Characteristics of radiation

EM radiation from computer processors leak information

EM side-channel analysis (EM-SCA)



A Gesture of Friendship...

In August 4, 1945 (few weeks before the end of WWII), US Ambassador in Moscow was gifted a carved wooden plaque by USSR as a *gesture of friendship*. It remained hung on the wall of ambassador's residence in Moscow for 7 years.

Great Seal Bug contained no active electronics or a power source. It's just a condenser microphone connected to a open ended wire.

Image Source: https://en.wikipedia.org/wiki/The_Thing_(listening_device)

Attacks on Video Displays

- In 1980's Wim van Eck showed that video displays leak EM radiation that can be used to reconstruct video content remotely.

Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?

Wim van Eck
PTT Dr. Neher Laboratories, St. Paulusstroat 4. 2264 XZ Leidschendam, The Netherlands

This paper describes the results of research into the possibility of "eavesdropping' on video display units. by picking up and decoding the electromagnetic interference produced by this type of equipment. During the research project. which started in January. 1983. it became more and more clear that this type of information theft can be committed very easily using a normal TV receiver.

1. Introduction

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

Attacks on Video Displays

- Same principles can be extended to attack modern digital video displays.
- VGA and HDMI interfaces carry video information that causes EM radiation.
- If you know the resolution and frame rate (FPS) of a computer display, you can reconstruct the content displayed on the screen.

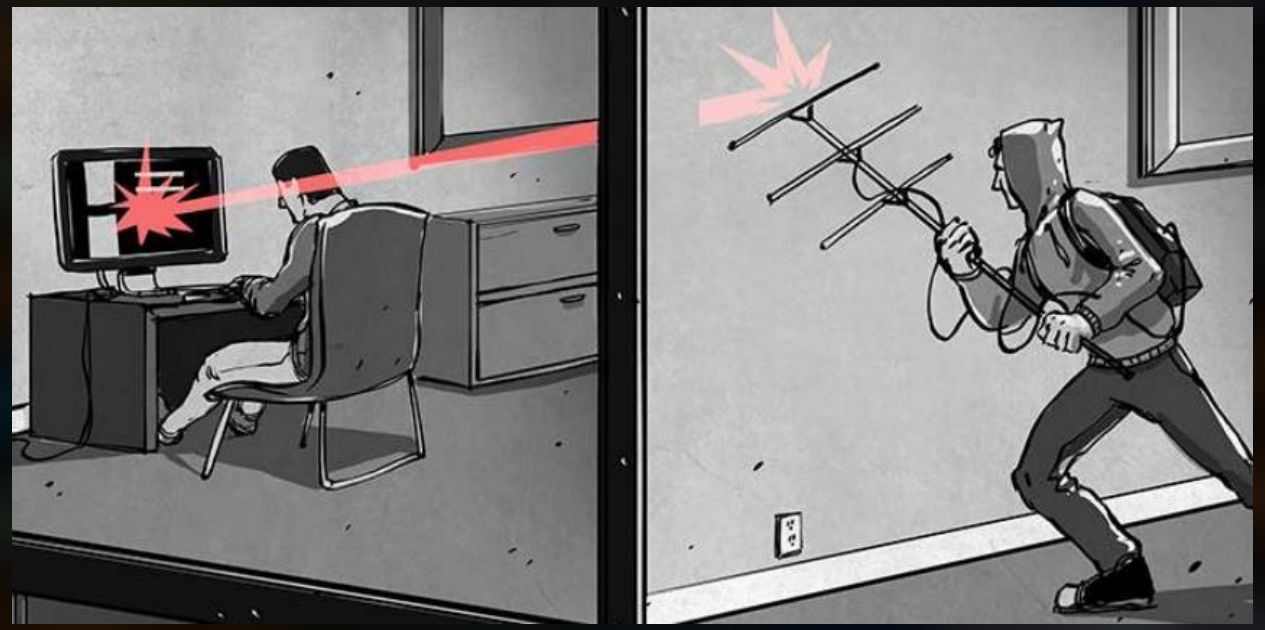
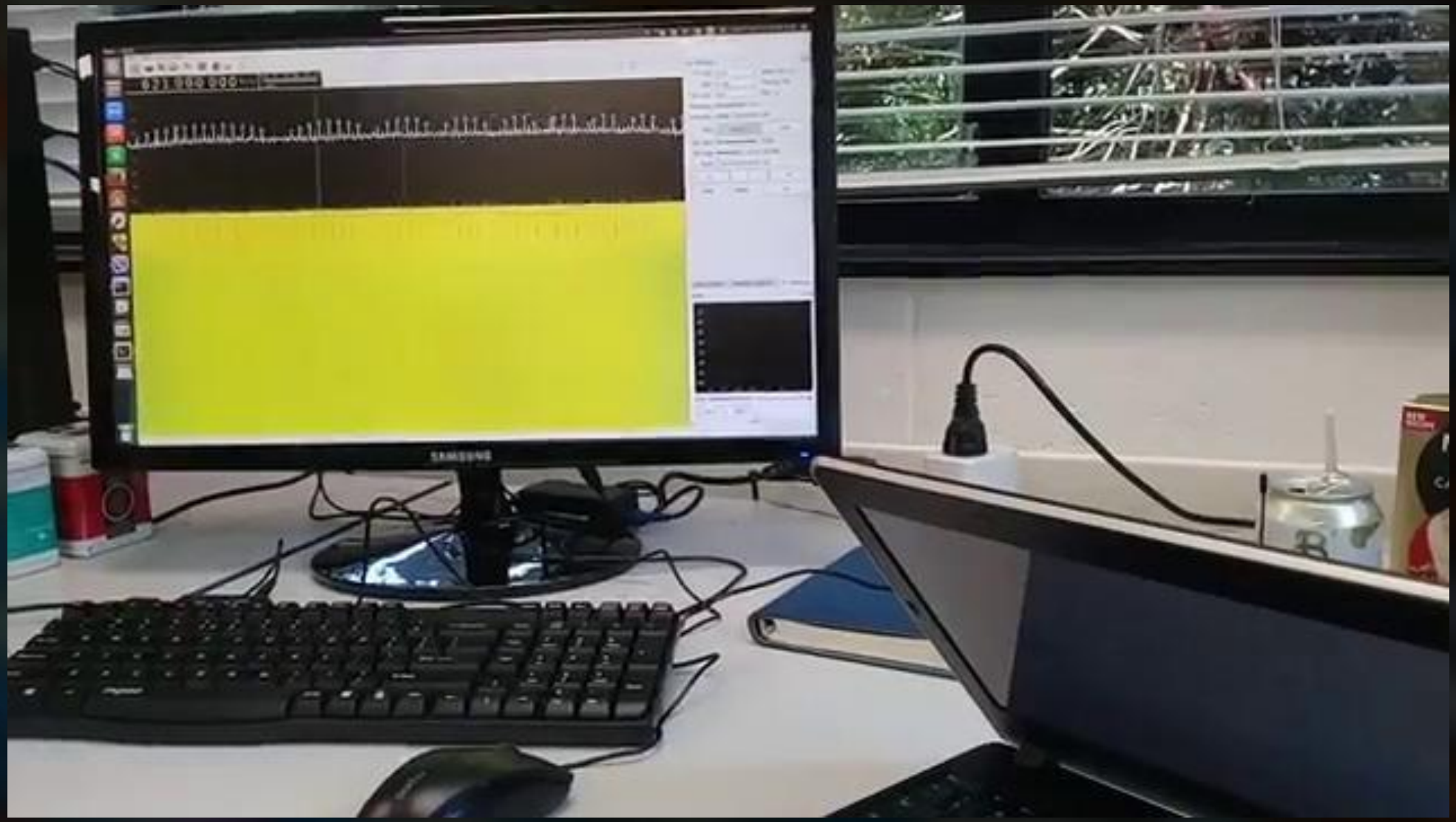
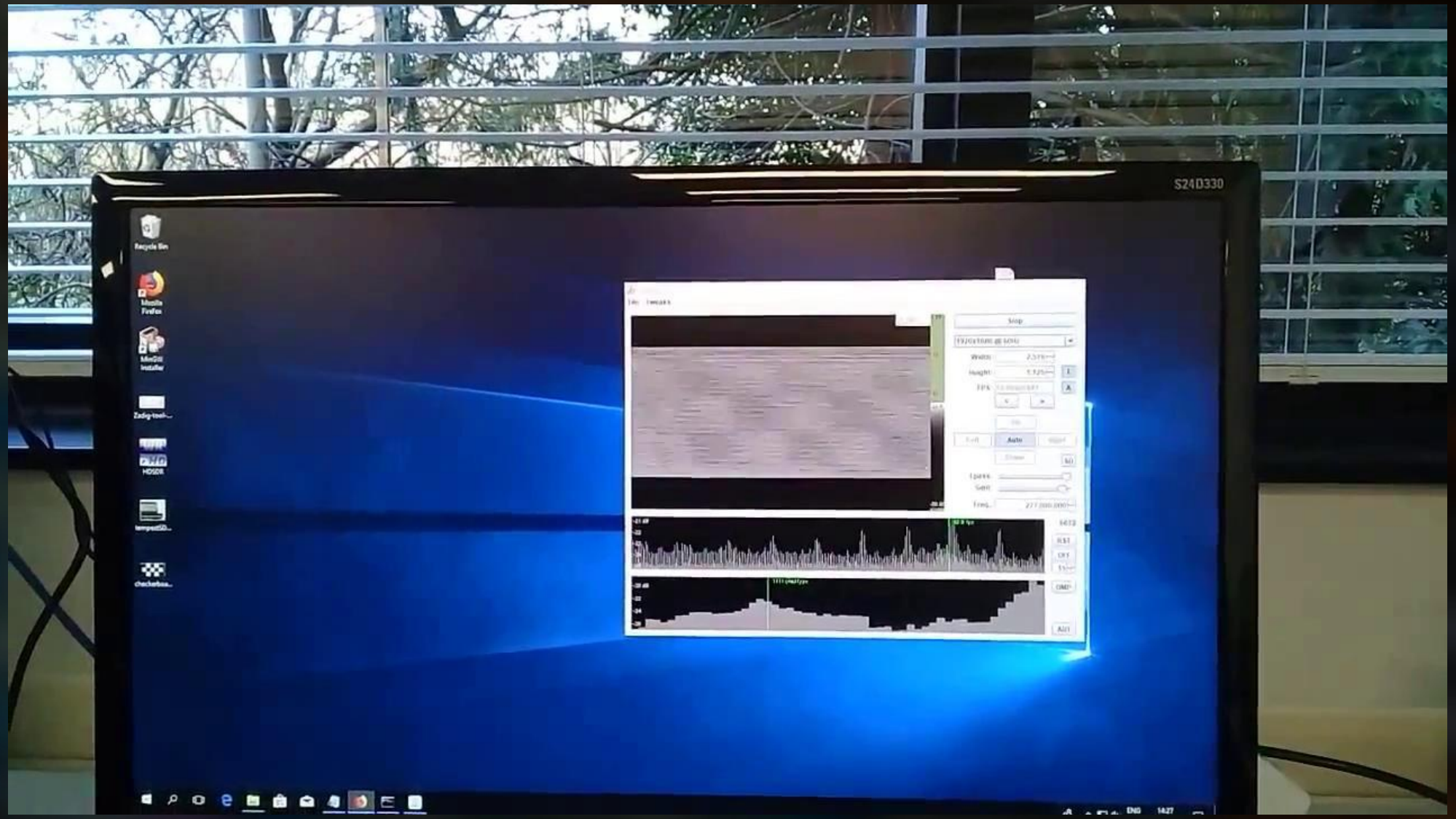


Image Source: https://hackaday.com/2015/10/19/tempest-a-tin-foil-hat-for-your-electronics-and-their-secrets/

Attacks on Video Displays



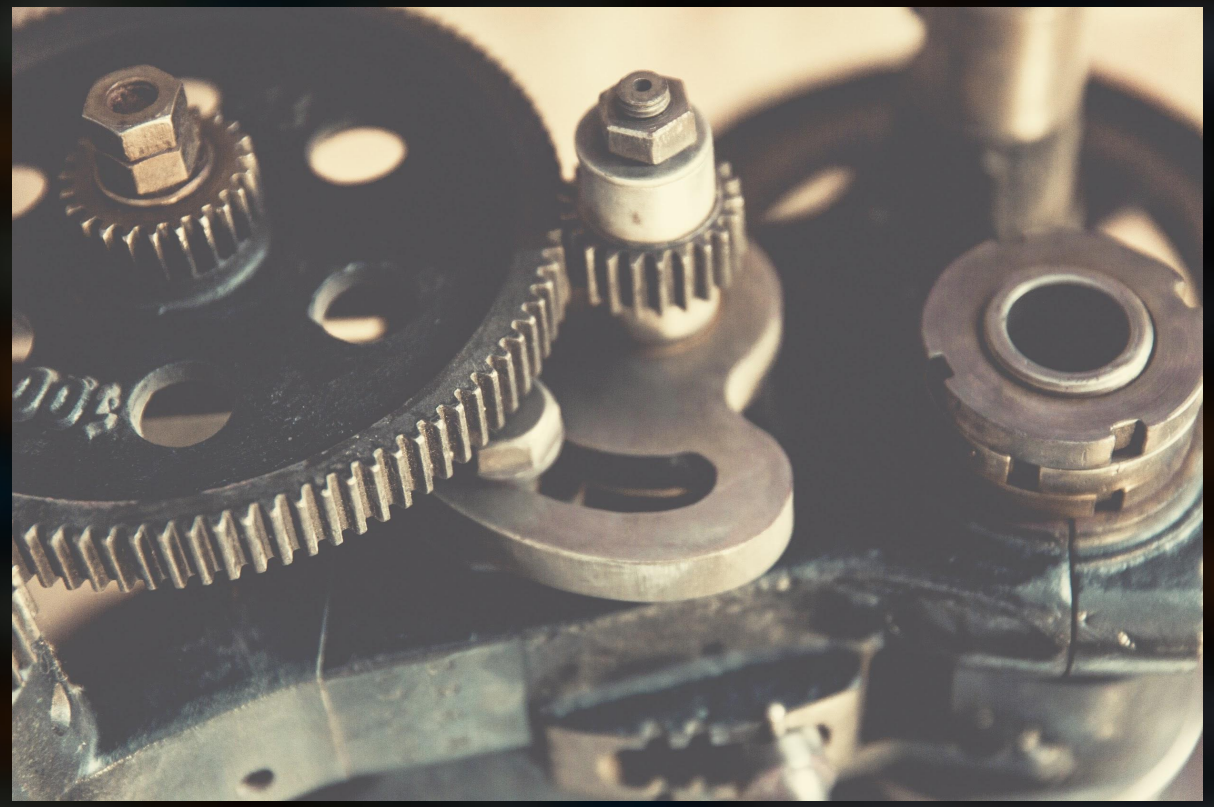
Attacks on Video Displays



Ref: https://github.com/martinmarinov/TempestSDR

Cryptographic Key Retrieval Attacks

- Cryptographic algorithms are implemented with an important assumption: Intermediate states and variables handled by the algorithms are not accessible to outsiders.
- When a cryptographic algorithm is running, intermediate variables handled on processor registers the power consumption of the device.
- Through power consumption - and consequently, EM emission - such intermediate states of the running algorithm get exposed.



Simple Electromagnetic Analysis (SEMA)

- An EM emission trace is visually observed.
- Direct observation of instructions of a program which has conditional branching leads us to identify input data which governed the execution sequence.
- Eg: Observation of Modular Exponentiation loops in a cryptographic algorithm leads to identify the Key bits involved in the operation.

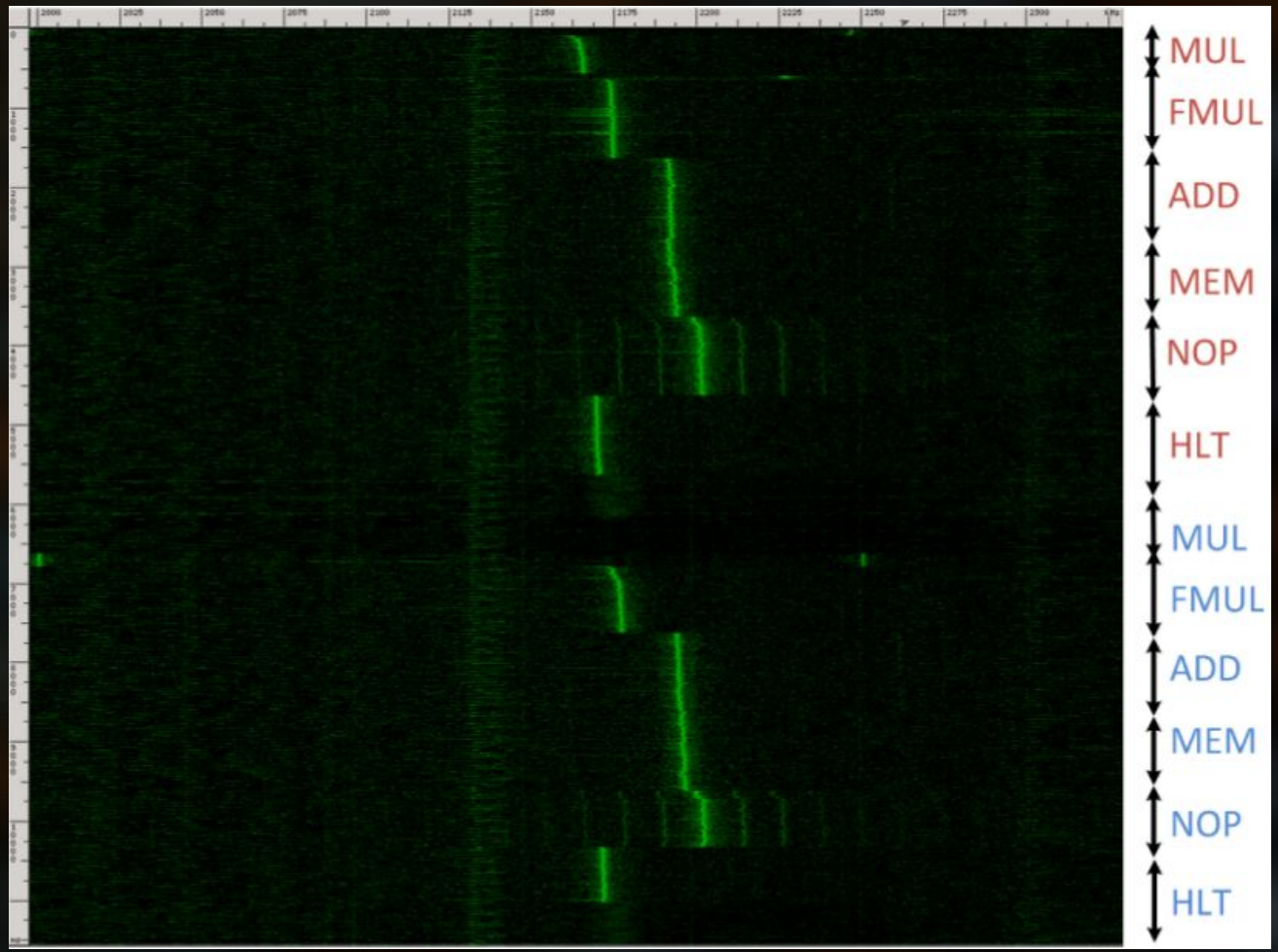
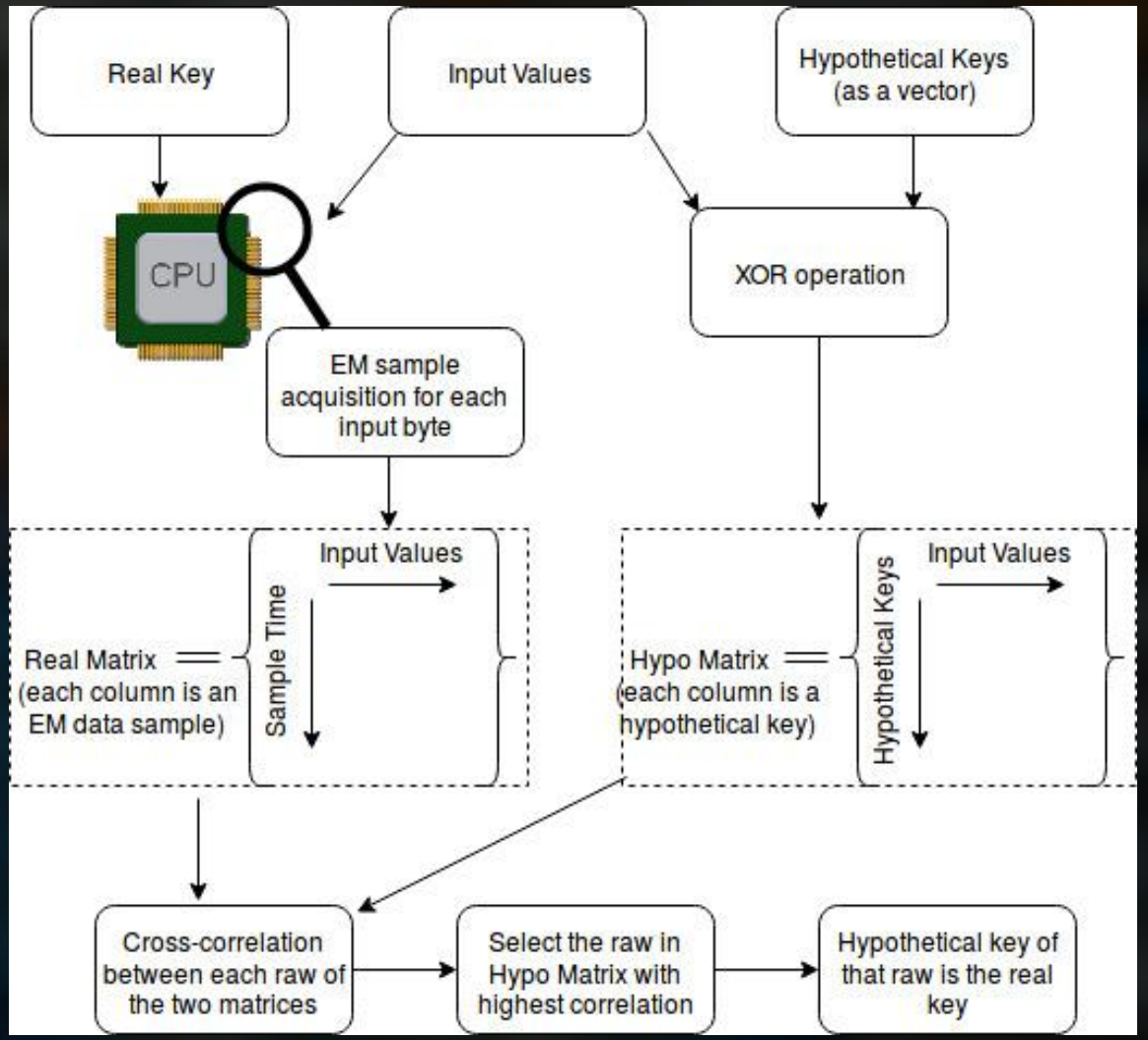


Image source: Genkin et al. ECDSA key extraction from mobile devices via nonintrusive physical side channels, 2016.

Correlation Electromagnetic Analysis (CEMA)

- When a bit in a CPU register is flipped from 0 to 1 or 1 to 0, it consumes some amount of energy which is reflected in the EM emission.
- When a register updates it's values, the hamming distance of the old and new values is reflected in the emitted EM signal. Higher the hamming distance, higher the EM emission difference.
- The goal of CEMA is to identify Possible Keys which can generate similar EM emission amplitude patterns as the Real Key would do, for the same input plaintexts.
- For this, we need large number of EM traces with large number of input plaintexts to attack a key.
- A computationally costly work, but better than brute forcing for the key.

Correlation Electromagnetic Analysis (CEMA)



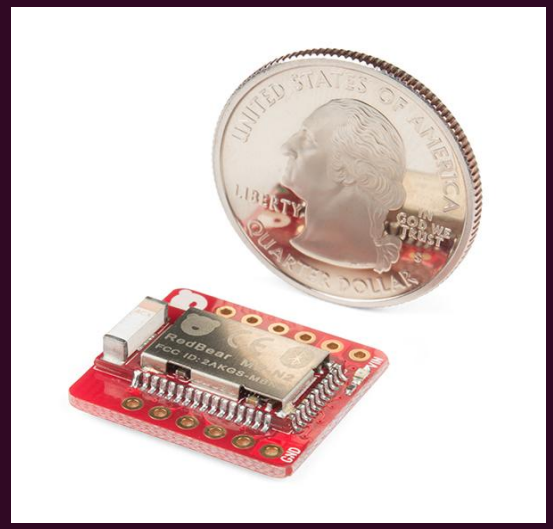
Screaming Channels

- EM-SCA has been applied to recover cryptographic keys,

  e.g., Camurati et al. (2018)
- Target device: BLE-Nano running AES-128 encryptions.
- ~ 8000 EM trace samples.
- Correlation electromagnetic

  analysis (CEMA)
- 18 minutes to recover the key

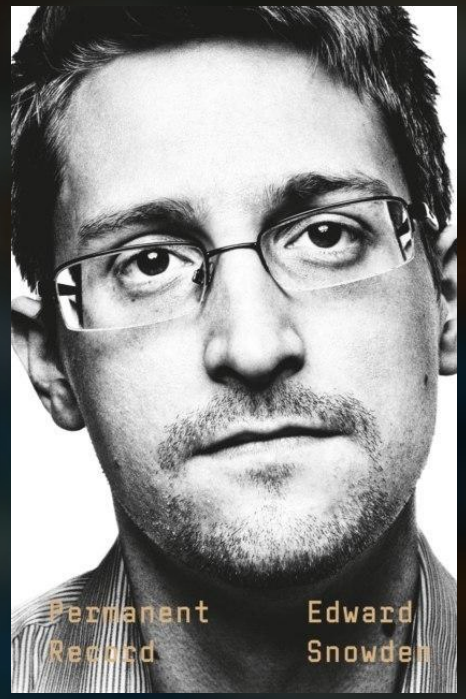
```
Subkey 15, hyp = ed:  0.012530354407226786
Subkey 15, hyp = ee:  0.017266581888572823
Subkey 15, hyp = ef:  0.010556395126552152
Subkey 15, hyp = f0:  0.02396490987572155
Subkey 15, hyp = f1:  0.012949217484922705
Subkey 15, hyp = f2:  0.014502574032304778
Subkey 15, hyp = f3:  0.014963314285949247
Subkey 15, hyp = f4:  0.012954752080796888
Subkey 15, hyp = f5:  0.01303155617835003
Subkey 15, hyp = f6:  0.013772034631913068
Subkey 15, hyp = f7:  0.019364248397445407
Subkey 15, hyp = f8:  0.010932180008903168
Subkey 15, hyp = f9:  0.013027691526298332
Subkey 15, hyp = fa:  0.01665869128411864
Subkey 15, hyp = fb:  0.015427833690631214
Subkey 15, hyp = fc:  0.011935004419024819
Subkey 15, hyp = fd:  0.014665594979696694
Subkey 15, hyp = fe:  0.018540794601137632
Subkey 15, hyp = ff:  0.018274501184871804
Best Key Guess:   56   89   ed   be   4c   65   db   f2   aa   2c   bd   c9   26   42   e6   e1
Known Key:        56   89   ed   be   4c   65   db   f2   aa   2c   bd   c9   26   42   e6   e1
PGE:             000  000  000  000  000  000  000  000  000  000  000  000  000  000  000  000
SUCCESS:           1    1    1    1    1    1    1    1    1    1    1    1    1    1    1    1
NUMBER OF CORRECT BYTES: 16
```

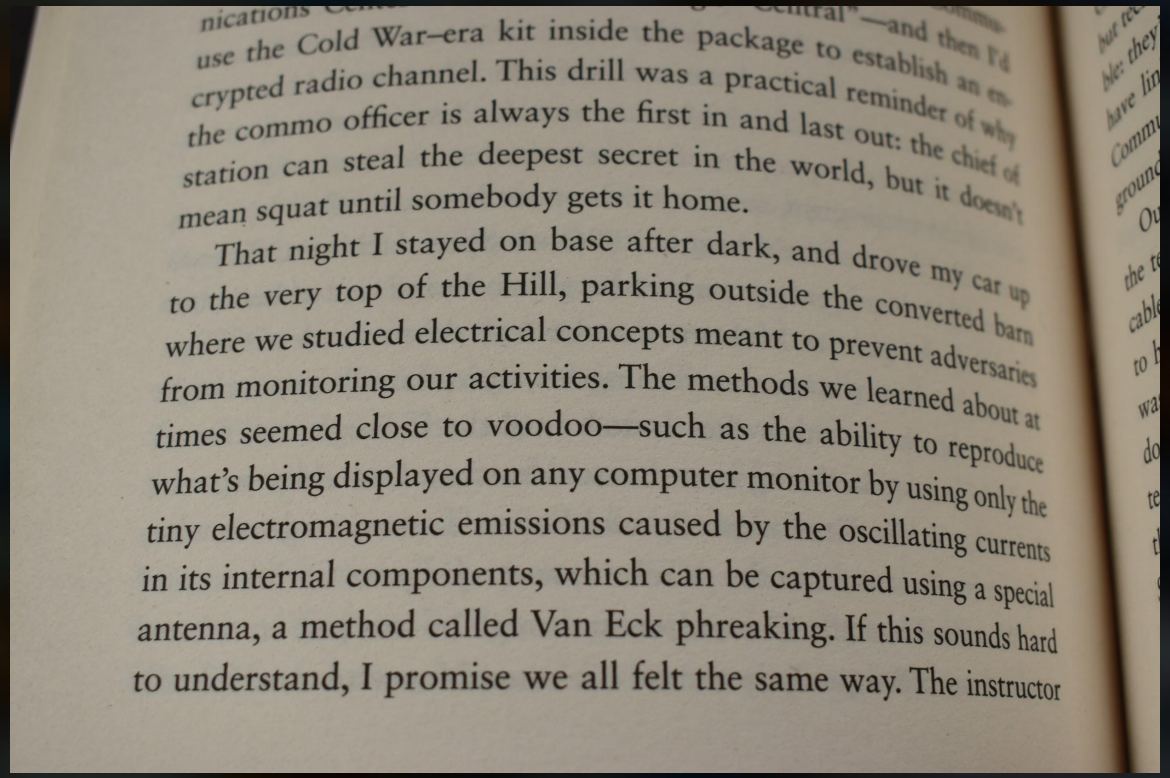


Ref: http://s3.eurecom.fr/tools/screaming_channels/

EM-SCA in the real world...

- “Permanent Record” by Edward Snowden





nications ... Central"—and then I'd use the Cold War–era kit inside the package to establish an encrypted radio channel. This drill was a practical reminder of why the commo officer is always the first in and last out: the chief of station can steal the deepest secret in the world, but it doesn't mean squat until somebody gets it home.

That night I stayed on base after dark, and drove my car up to the very top of the Hill, parking outside the converted barn where we studied electrical concepts meant to prevent adversaries from monitoring our activities. The methods we learned about at times seemed close to voodoo—such as the ability to reproduce what's being displayed on any computer monitor by using only the tiny electromagnetic emissions caused by the oscillating currents in its internal components, which can be captured using a special antenna, a method called Van Eck phreaking. If this sounds hard to understand, I promise we all felt the same way. The instructor

- NSA Playset - http://www.nsaplayset.org/

Hardware for EM-SCA

Oscilloscopes / spectrum analyzers / traditional radio receivers

Difficult to handle in in digital forensic investigation settings.

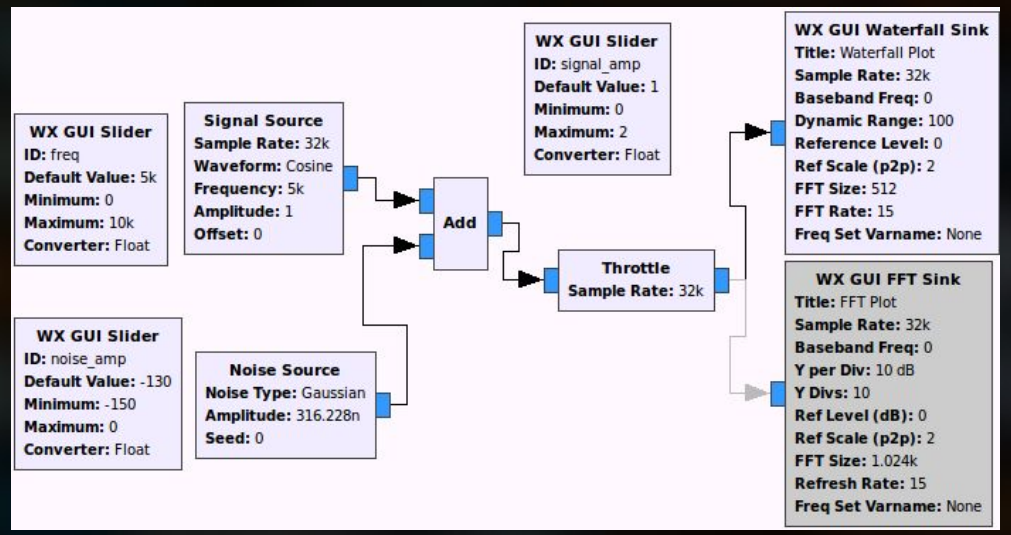
Software-defined radios (SDR)

Easily configurable with software.

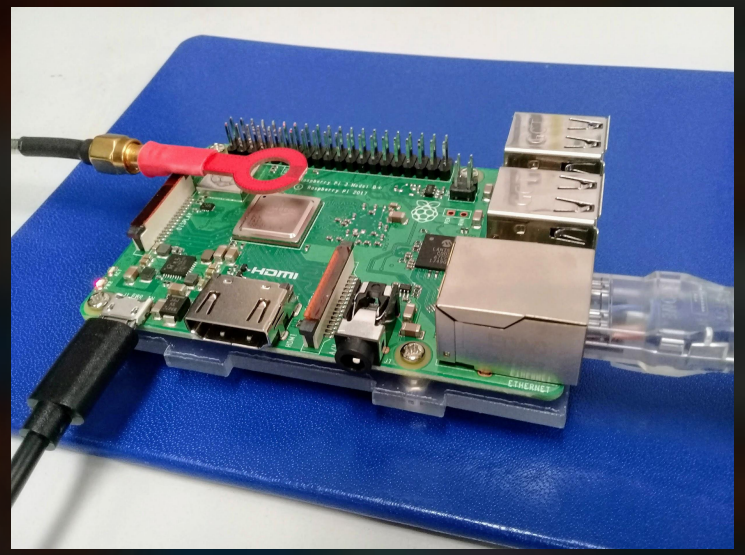
Software Defined Radio (SDR)

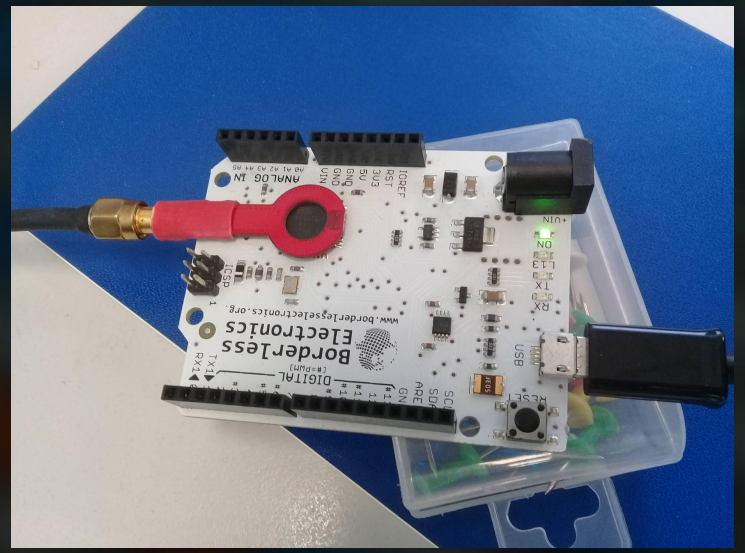
- A fast analog-to-digital converter (ADC).
- RTL-SDR, HackRF, USRP
- Generates digitized samples in Inphase-Quadrature (I-Q) format.
- Open source libraries to process streams of I-Q data samples.
- Can program for a task using Python or using a visual flowgraph editor, GRC.

GNU Radio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

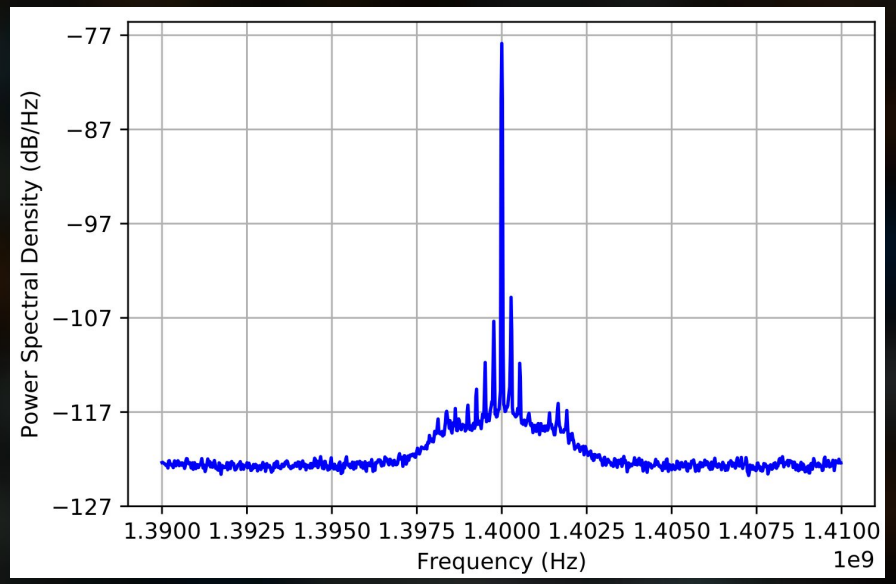


Observation of EM Side-channel





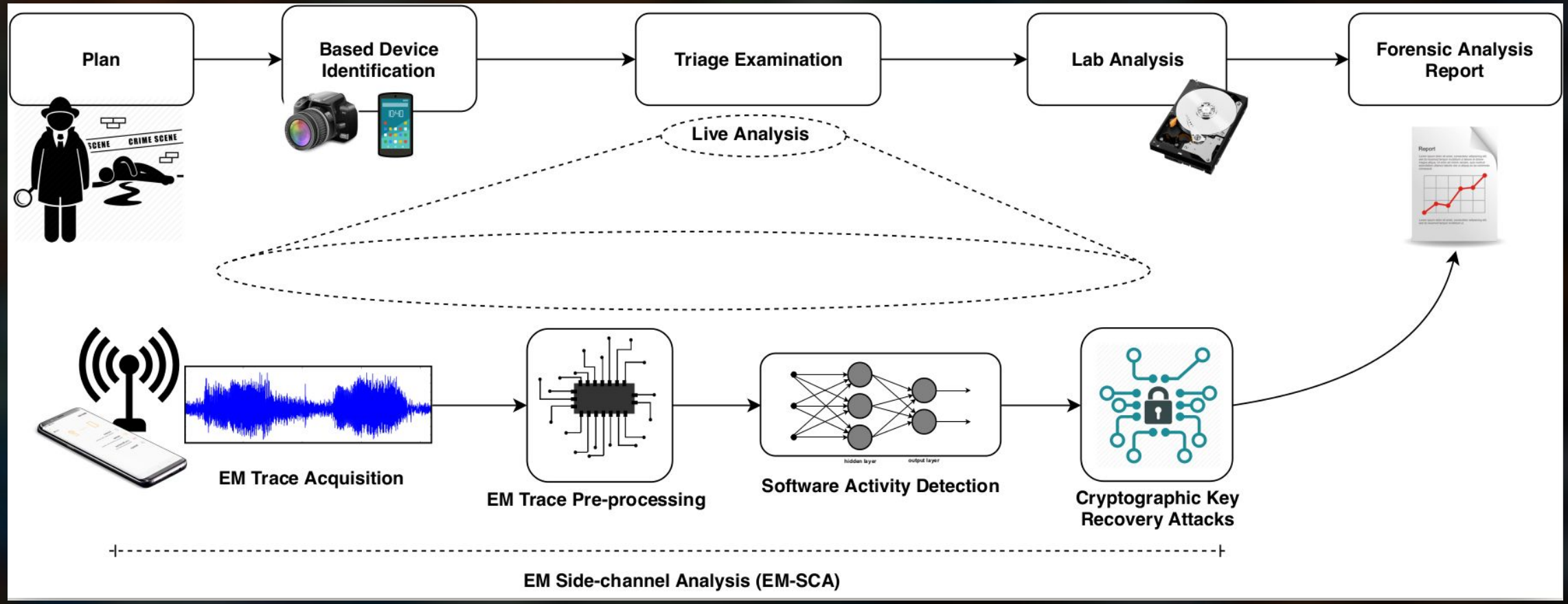
- CPU clock/oscillator is the main source of EM noise.
- EM emissions can be observed at clock frequency and its harmonics.
- Signal attenuates rapidly with distance from the CPU.
- H-loop antennas placed closer to the CPU can pick up strong signals.
- When the fundamental frequency is noisy due to external sources, harmonics can be used.



Hardware Demonstration

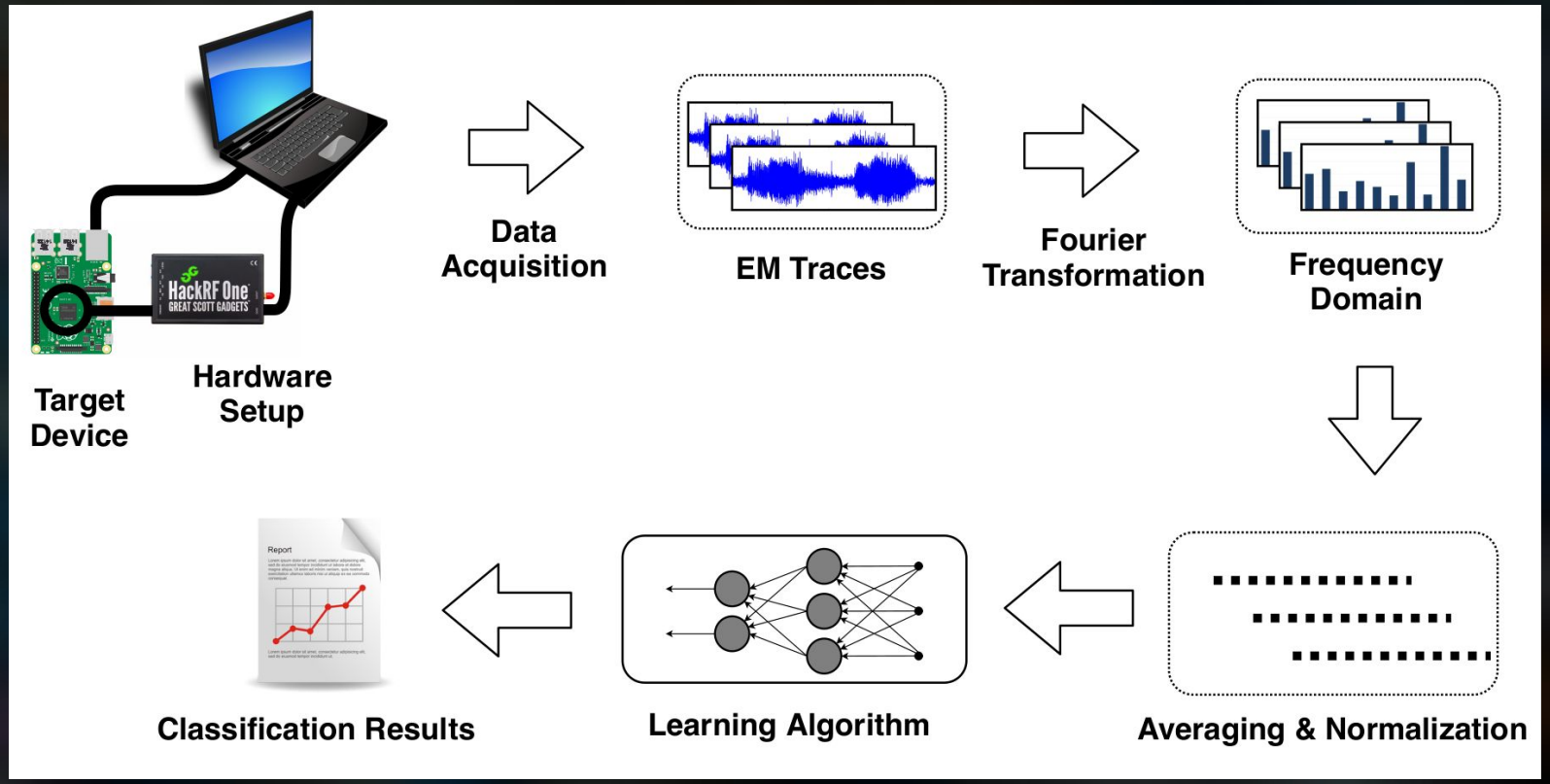
- Following video introduces,
  - RTL-SDR dongle
  - HackRF device
  - Usage of GQRX software tool with RTL-SDR and HackRF
  - Observing EM side-channel emissions of an Arduino device

EM-SCA for Digital Forensics

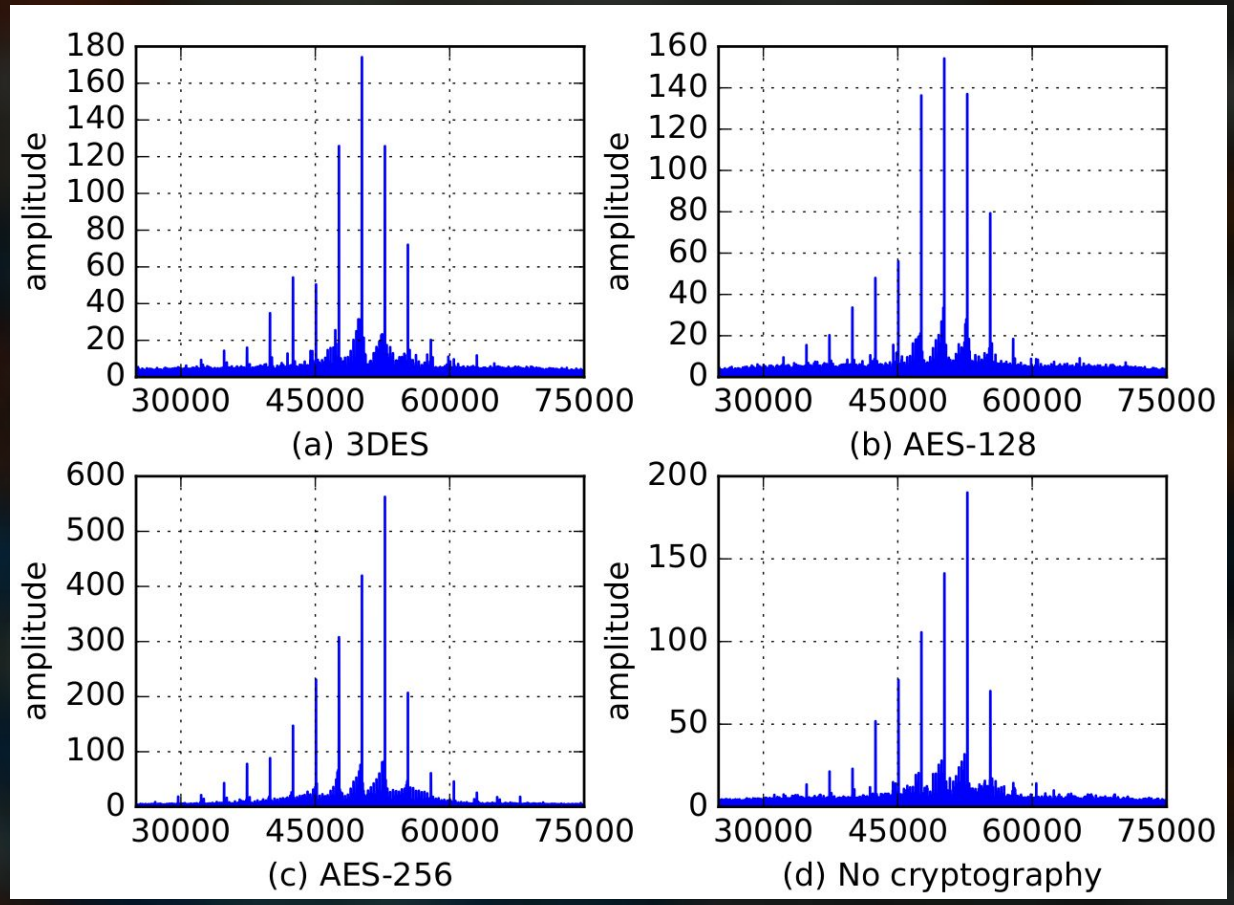


Some Experimental Results

1. Discriminating cryptographic activities
2. Detection of software behaviour
3. Detecting modifications to firmware



Discriminating Cryptographic Activities

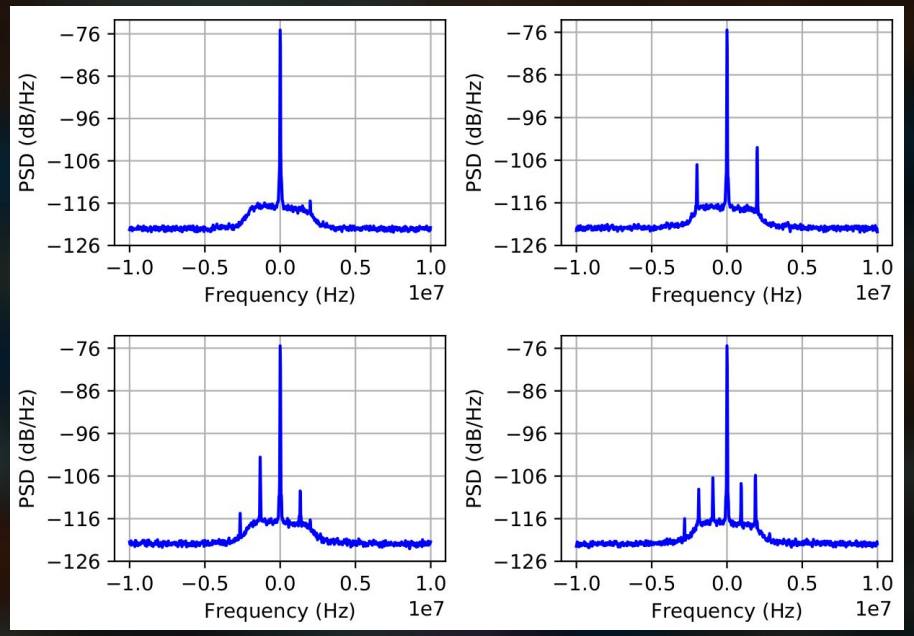


- Raspberry Pi as the target device.
- Three cryptographic classes and a ``no cryptography" class.
- From FFT to 500 features by averaging.
- 4 layer NN (2 hidden - 10x5)
- 600 samples per class.

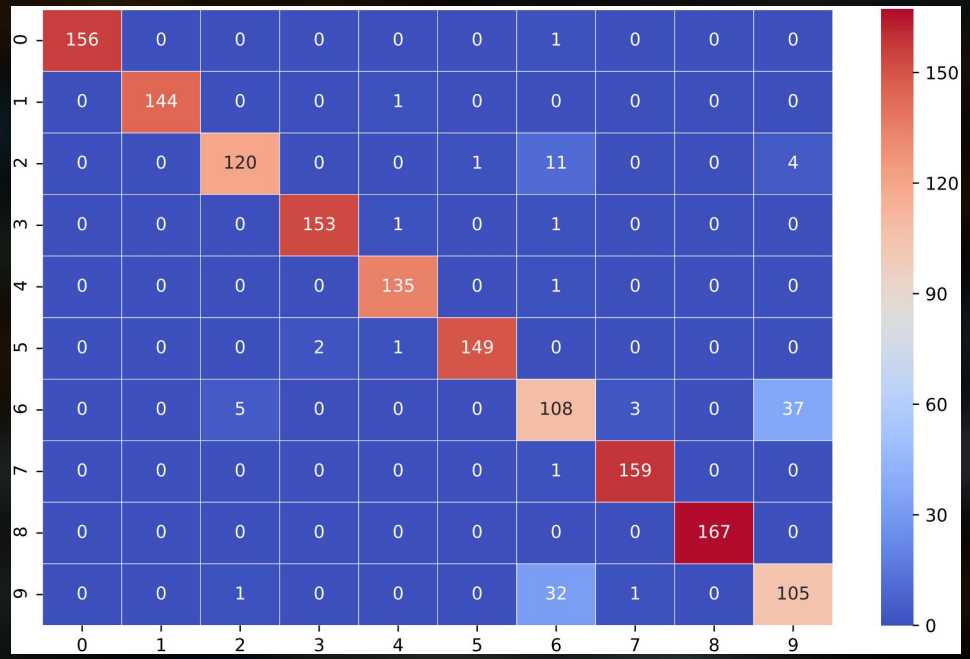
Activity	Precision	Recall	F1-Score
Other	0.93	0.85	0.89
AES-256	0.78	0.86	0.82
AES-128	0.99	0.92	0.95
3DES	0.81	0.85	0.83

Detection of Software Behaviour


```
/* Arduino test program */
void setup(){
}
void loop(){
    for(int i=0, i<20, i++) { delay(10); }
    for(int i=0, i<20, i++) { delay(10); }
    /* further loops */
}
```

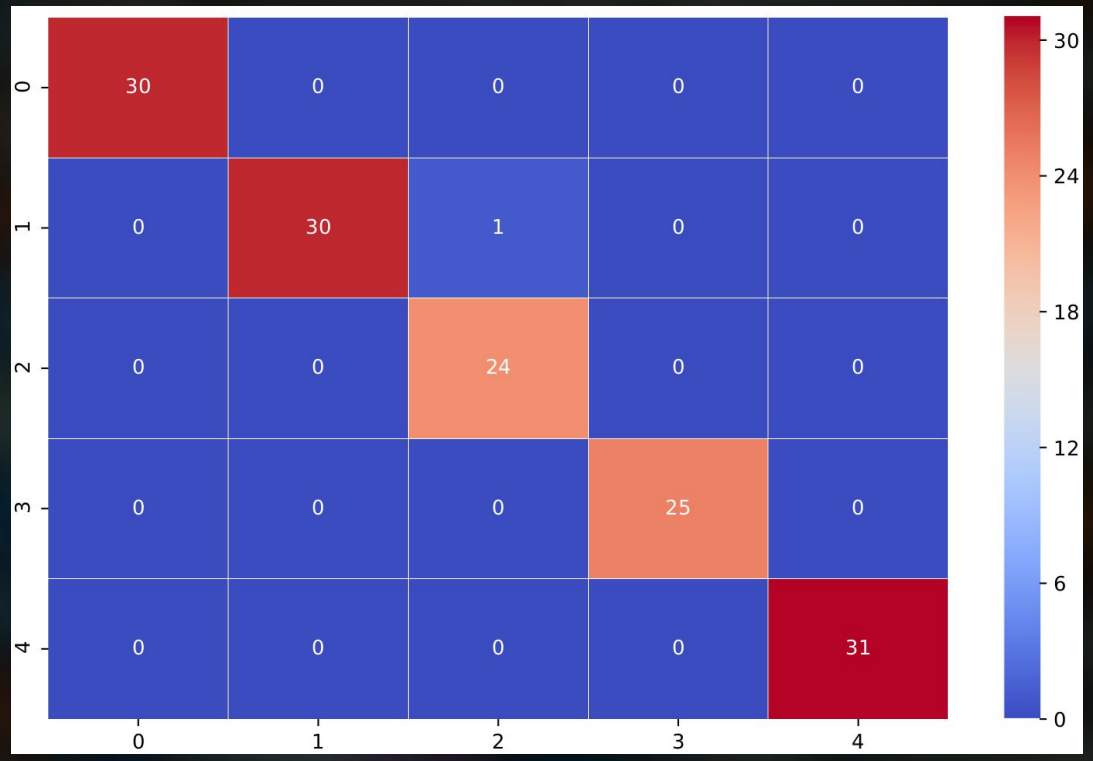


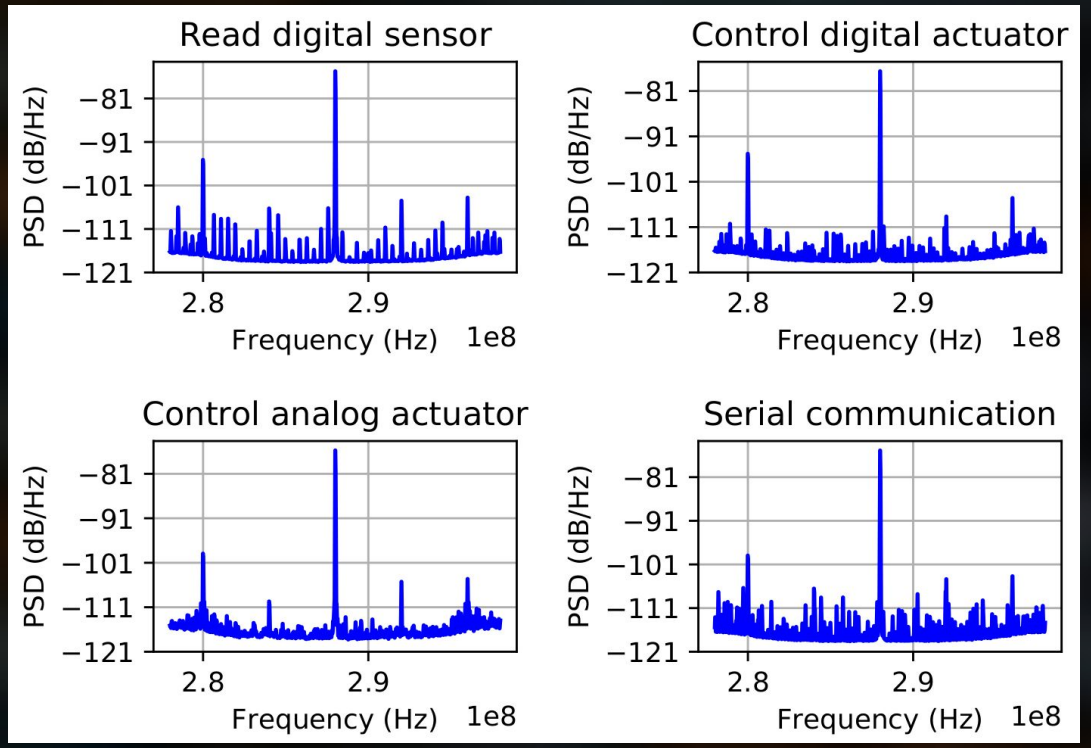
- Arduino Leonardo running 10 programs
- FFT (20,000,000) to a vector of 1000 features.
- 1000 buckets with max values.
- Over 90% classification accuracy



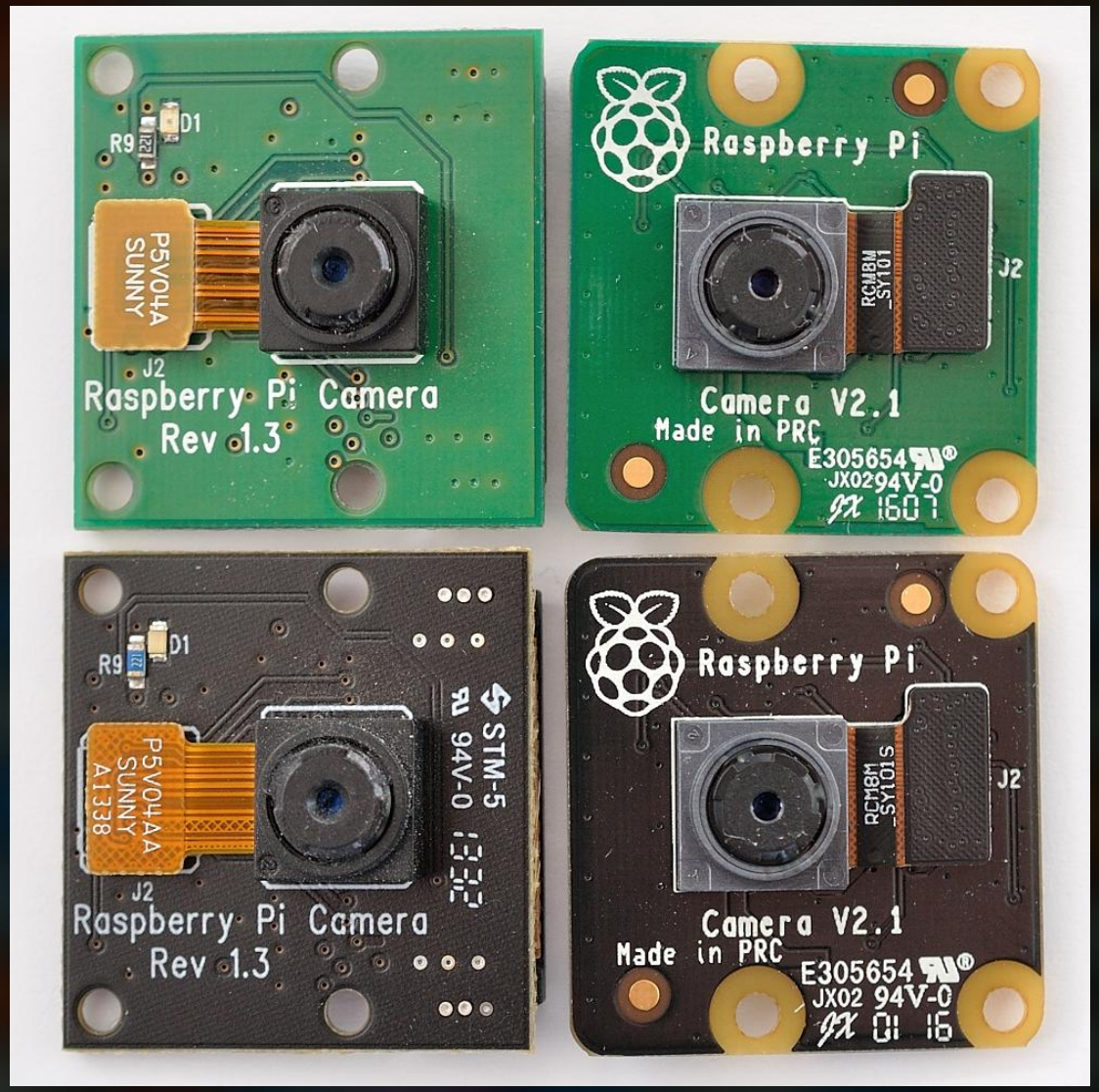
Detection of Software Behaviour (cont.)

- An IoT device with 5 internal states emulated using an Arduino.
- Similar neural network classifier like the previous case.
- Detection accuracy of over 99%





Detecting Modifications to Firmware

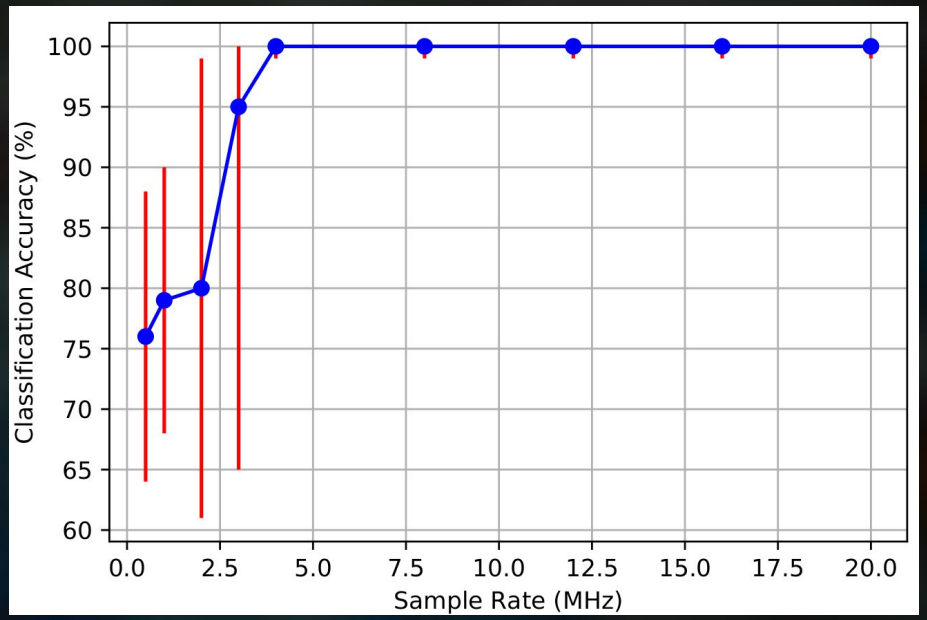


- Arduino Leonardo as the target device.
- FFT to 1000 features using max values.
- One-class SVM with a non-linear kernel (RBF).
- 1 legitimate program and 20 slightly modified programs for testing.
- 100% detection accuracy for all the tested programs.

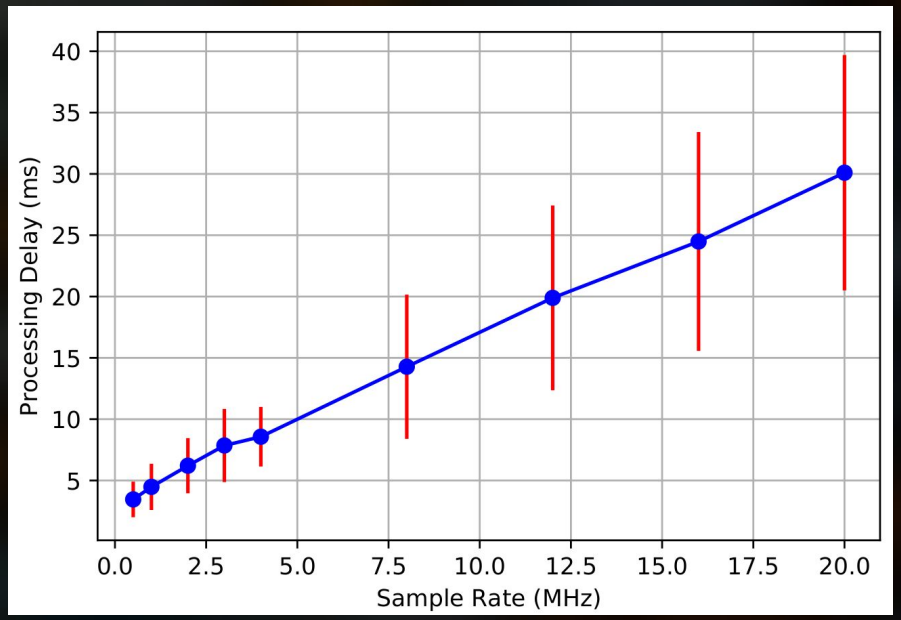
Storage and Real-time Requirements

- Each I-Q sample = 8 bytes
- Highest sampling rate = 20 MHz
- Size of the 1 minute signal capture ≈ 9 GB

  (8 bytes × 20 MHz × 60 seconds = 8.94 GB).



It's OK to have lower sampling rates to cope with storage requirements.



Even the highest sample rate does not exceed our capability to process data in real-time

Hence, live forensic analysis is possible!

What we've learned so far...

- We can identify known behaviors of software running on IoT devices.
- We can identify when known cryptographic algorithm implementations are running on an IoT device.
- Such insights can help inspecting an IoT device in a forensic investigative scenario.

- Ongoing work:
  - Cryptographic key retrieval attacks in investigative scenarios
  - Development of software tools to assist in apply EM-SCA in digital forensics easily.

ASANKA.SAYAKKARA@UCDCONNECT.IE

HTTPS://ASAYAKKARA.ORG/

WWW.FORENSICSANDSECURITY.COM

@ASAYAKKARA

@FORSECRESEARCH

UCD Forensics and
Security Research Group