RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: HT-F01

AirGapping is Overrated: Pressing a Red Button via a Multi-Function Printer

Ben Nassi

Ph.D. Student
Ben Gurion University of the Negev & CBG Labs
@ben_nassi

Ben Nassi - About Me

- Ph.D. student 4th year.
- Investigating security and privacy in the era of IoT devices.
- Former Google employee.
- A paper based on this talk was published on ***"IEEE Transactions on Information Forensics and Security"*** on 2019 under the name ***"Xerox Day Vulnerability"***.

Paper

Research's webpage

Outline

1. Covert Channels
2. Air Gapping
3. Multi Function Printers
4. Pressing a red button via a MFP
5. Demonstration against real organization.
6. Countermeasures

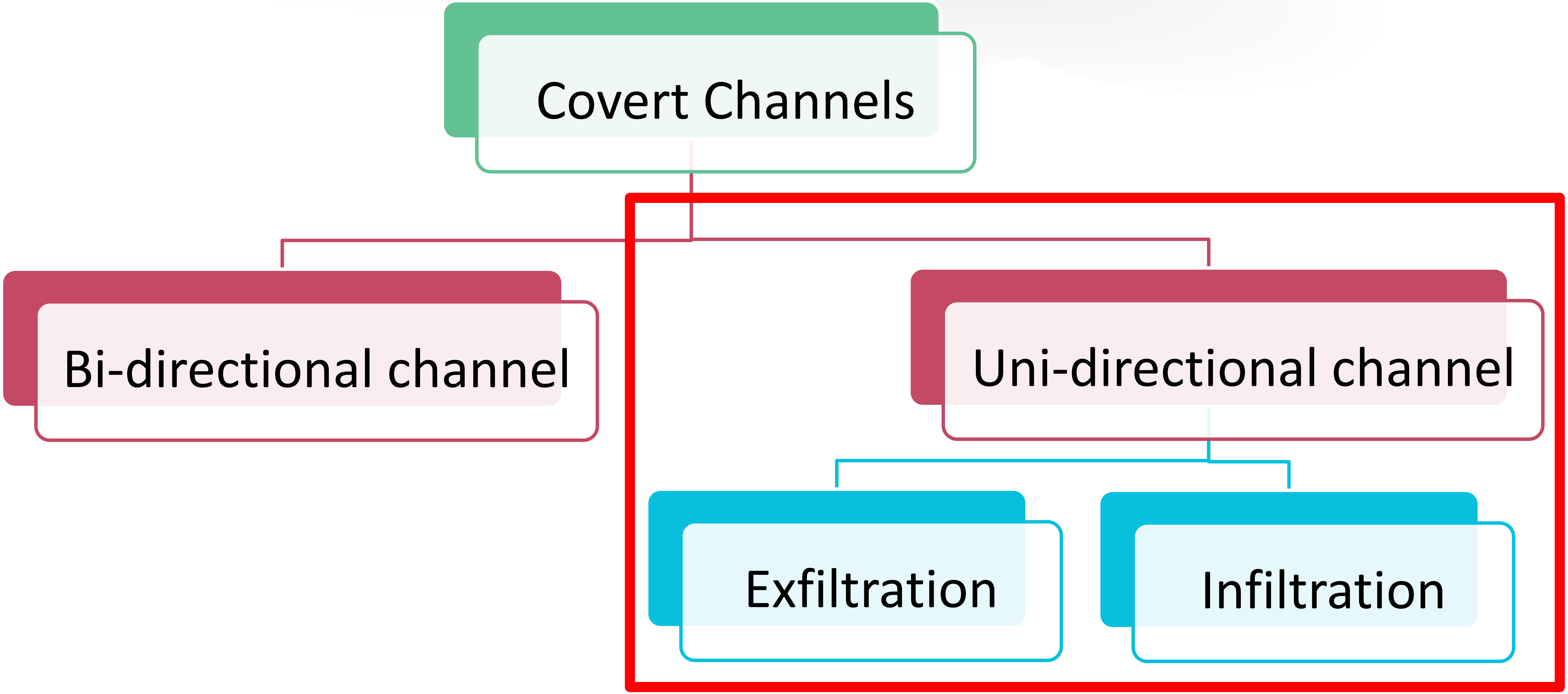
Covert Channels

Covert Channels - Definition

“Creating a capability to transfer information between parties that are not supposed to be allowed to communicate by measures that were not designed for communication.”

A Note on the Confinement Problem.
Butler Lampson, 1973

Covert Channels - Types



Covert Channels

Bi-directional channel

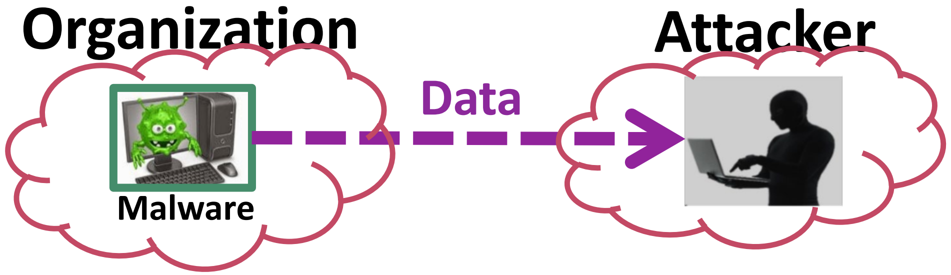
Uni-directional channel

Exfiltration

Infiltration

Unidirectional Channels

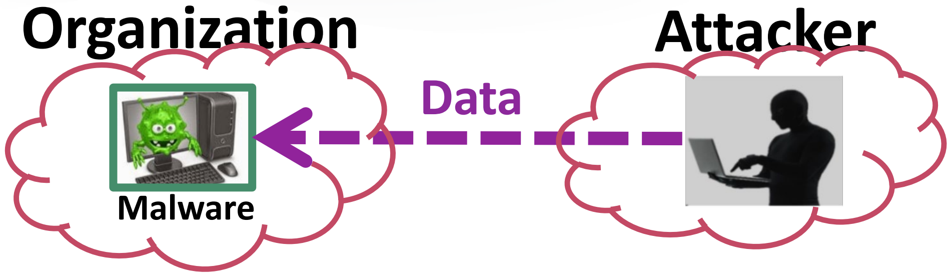
Exfiltration Covert Channel



A malware (source) modulates the data and sends it to an outside attacker (destination).

- Widely investigated
- Examples: optical/electomagnetic covert channels
- Main use case: exfiltration of assets

Infiltration Covert Channel



A malware (destination) demodulates the data that has been sent from an outside attacker (source).

- Limited amount of studies
- Examples: thermal/acoustic covert channels
- Main use cases: red button triggering

Covert Channel and Side Channel Attacks

	Covert Channels	Side Channel Attacks
Assumptions	Pre installed malware in an organization	1. Attacker within physical proximity 2. A process creates informative side-effect
Goal	Exfiltration/Infiltration any kind of message	Learning about something (asset/secret) from a process by analyzing its side-effects.

Air Gapping

Mitigating Covert Channels – Air Gapping

- Most commonly used countermeasure method against covert channels is Air Gapping: physically isolating a set of computers/network from unsecured networks (e.g., Internet or LANs)

- Air Gapping is mostly employed in:
  - Highly secret organizations (e.g., intelligence agencies).
  - Industrial control systems (e.g., gas fields).
  - Critical infrastructures (e.g., nuclear plant, medical devices).
  - Financial computer systems.

Air Gapped Networks

Air Gapping in the context of covert channels is used to prevent two actions:

1. Compromising a computer.
   Attackers use alternative methods to compromise a computer:
   - Supply Chain Attacks.
   - Social Engineering.

Air Gapped Networks

Air Gapping in the context of covert channels is used to prevent two actions:

1. Compromising a computer.
   Attackers use alternative methods to compromise a computer:
   - Supply Chain Attacks.
   - Social Engineering.

Conclusion: Motivated attackers find alternative ways to compromise an isolated network.

Air Gapped Networks

Air Gapping in the context of covert channels is used to prevent two actions:

1. Compromising a computer.
   => Not effective against motivated attackers.
2. Communicating with external attacker.
   => effective??

Pressing a Red Button via a Multi Function Printer

Objective

Establishing an **infiltration covert channel** with a malware installed on an air-gapped computer .

Pressing a Red Button via a MFP

Contributions

1. Exploiting a legitimate MFP to establish a covert channel, as opposed to unauthorized hardware that is considered vulnerable (e.g., microphones).
2. The covert channel can be established far away from the target scanner (1 km away).
3. Much higher transmission rate compare to other infiltration covert channels.
4. The installed malware does not require any special permissions.
5. Can even be performed invisibly.

Multi Function Printers (MFP)

Multi Function Printers (MFP)

- Used for scanning, printing, copying, and faxing.
- Commonly used in most organizations nowadays.
- Connected to the organizational network.

Multi Function Printers (MFP)

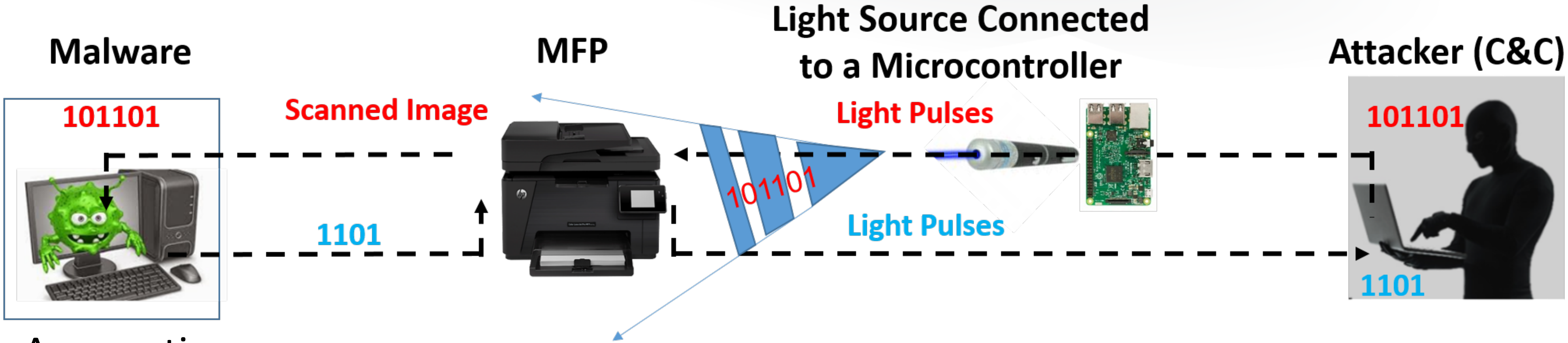
Scanning Process

1. A lamp passes over the scanner's pane (from the bottom) and illuminates the pane.
2. Using a series of lenses and mirrors, the light is bounced back to an optic sensor (e.g., CCD/CMOS sensors).
3. A lens splits the image into three colors and the associated electrical charge is measured. The brighter the light reflected, the greater the electrical charge.
4. An ADC device converts the electrical charge to a binary code that represents the document that is located on the pane.
5. The binary representation (a file in a configured format e.g., PDF, PNG, etc.) is transferred to a computer for storage using wired/wireless connection.

Multi Function Printers (MFP)

- What happen when the ambient light in the room of a MFP is changed while scanning with an open flatbed?

Threat Model

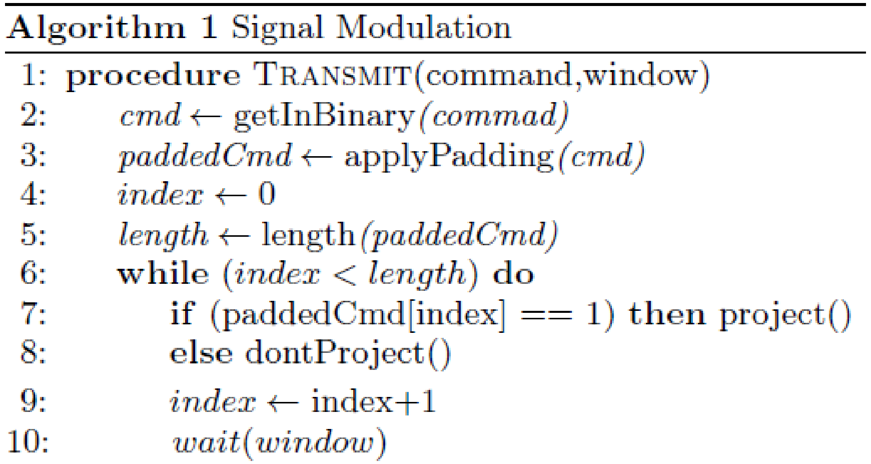


Assumptions:

- A malware was pre-installed on a computer that is connected to the isolated network.
- A MFP is connected to the isolated network.
- The malware can trigger a remote scanning of the connected MFP.
- The MFP flatbed was left partially/fully open.

Code

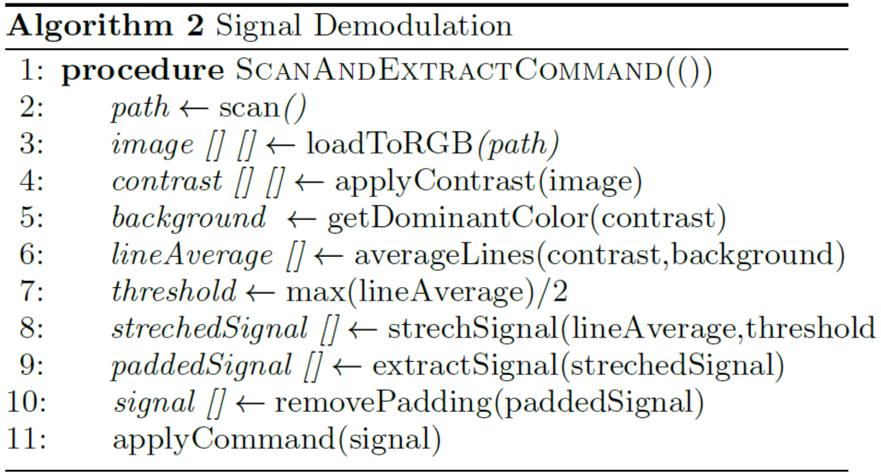
Attacker Code



Algorithm 1 Signal Modulation

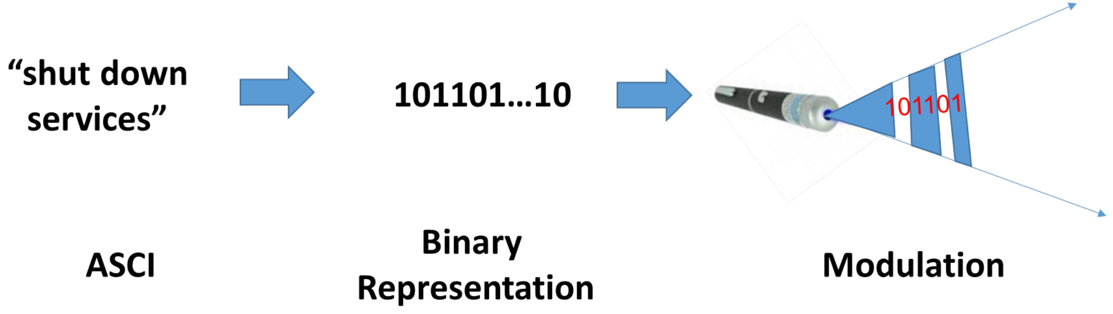
```
procedure TRANSMIT(command,window)
    cmd ← getInBinary(commad)
    paddedCmd ← applyPadding(cmd)
    index ← 0
    length ← length(paddedCmd)
    while (index < length) do
        if (paddedCmd[index] == 1) then project()
        else dontProject()
        index ← index+1
        wait(window)
```

Malware's Code



Algorithm 2 Signal Demodulation

```
procedure SCANANDEXTRACTCOMMAND(())
    path ← scan()
    image [] [] ← loadToRGB(path)
    contrast [] [] ← applyContrast(image)
    background ← getDominantColor(contrast)
    lineAverage [] ← averageLines(contrast,background)
    threshold ← max(lineAverage)/2
    strechedSignal [] ← strechSignal(lineAverage,threshold
    paddedSignal [] ← extractSignal(strechedSignal)
    signal [] ← removePadding(paddedSignal)
    applyCommand(signal)
```

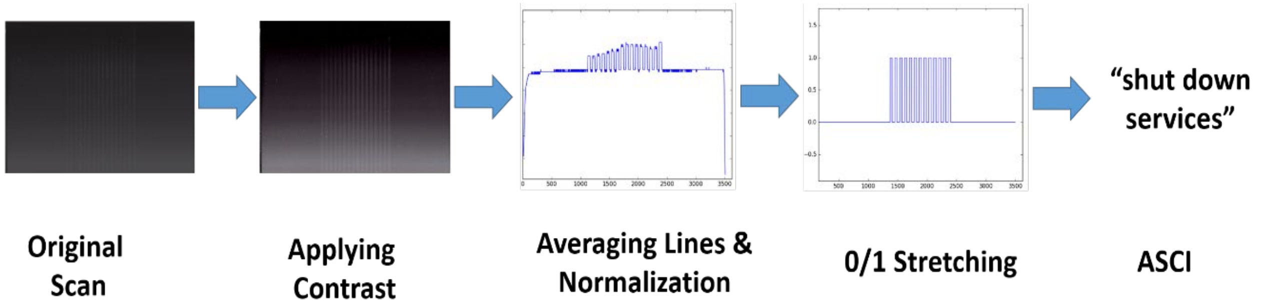


“shut down services” → 101101…10 → Modulation

ASCI

Binary Representation

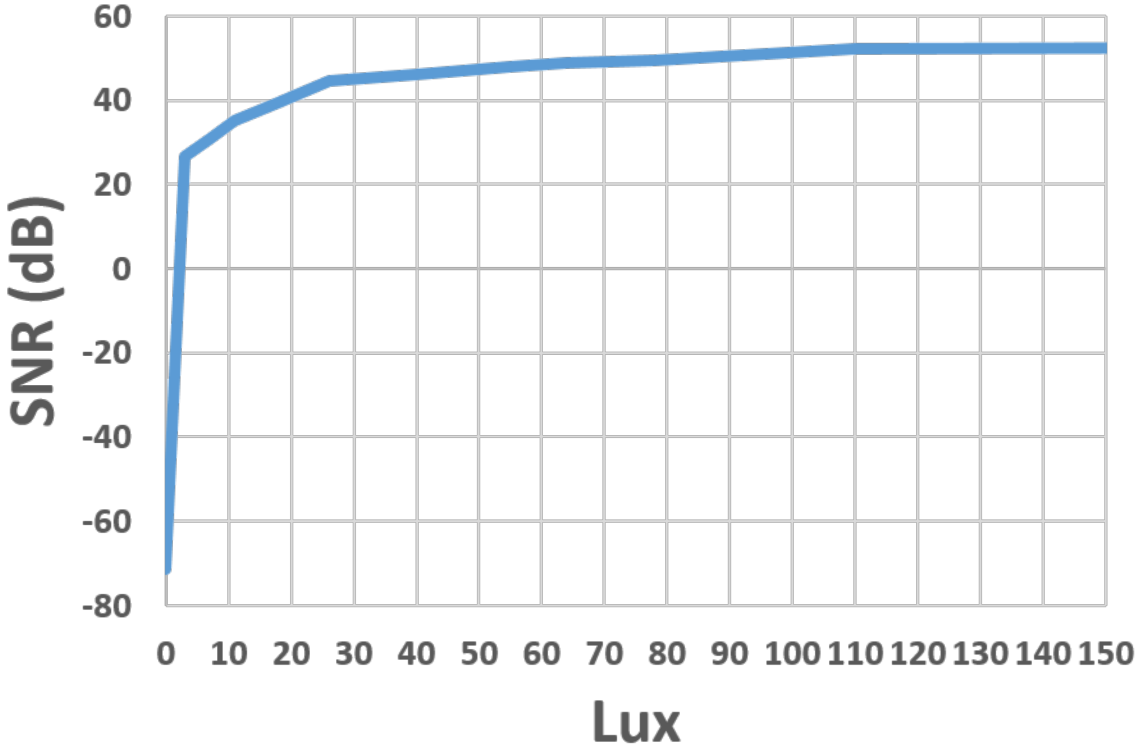
Modulation



Original Scan → Applying Contrast → Averaging Lines & Normalization → 0/1 Stretching → “shut down services”

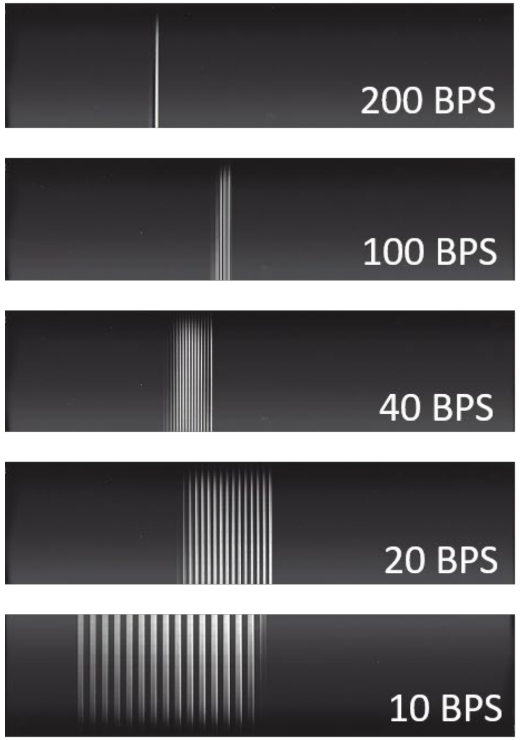
ASCI

Influence of Projection Intensity

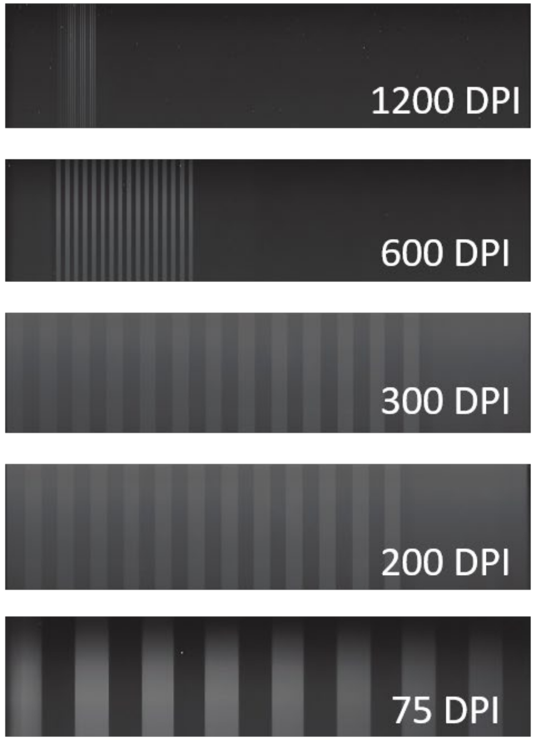


Influence of Transmission Rate & Resolution

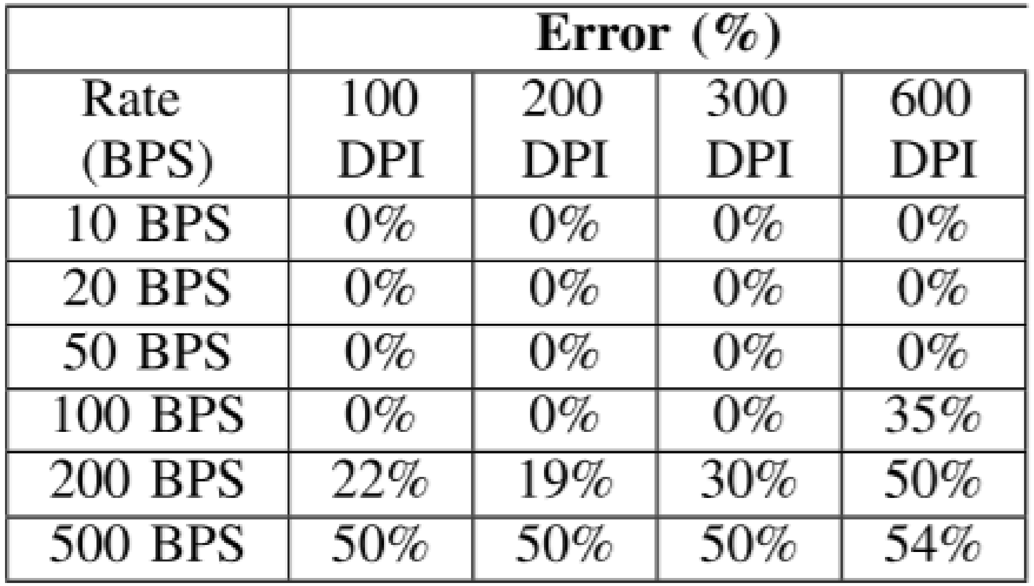
Fixed Resolution



Fixed Transmission Rate

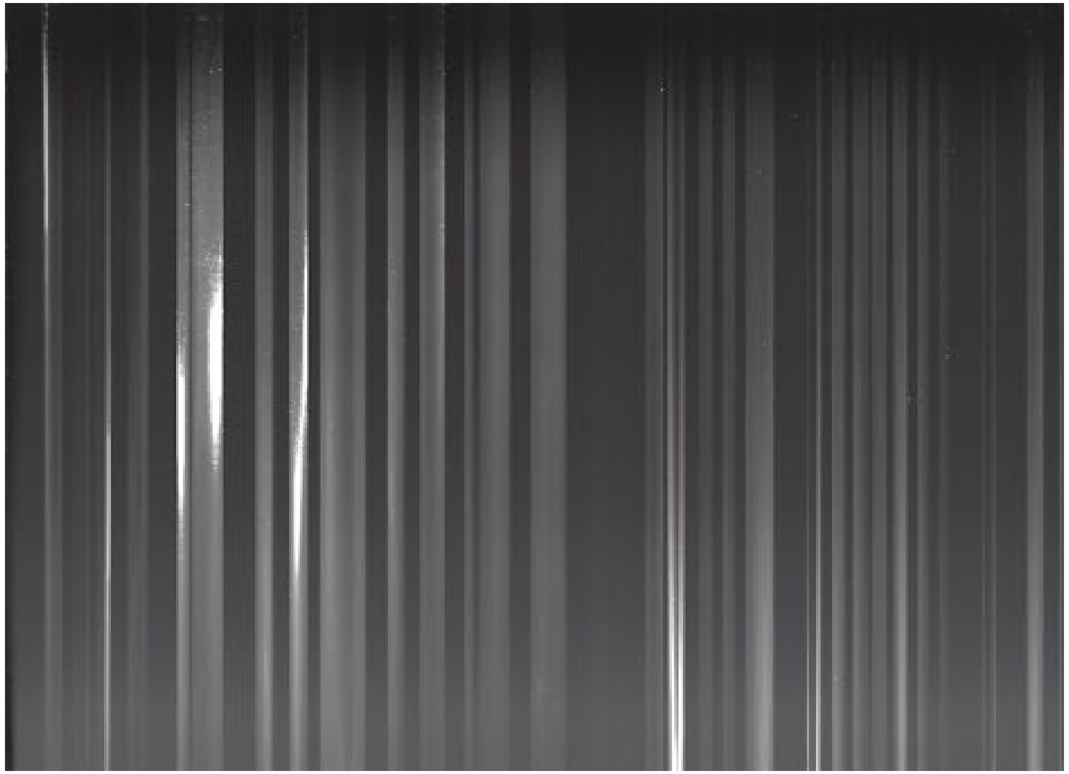


BIT ERROR RATE OF DIFFERENT TRANSMISSION RATES AND RESOLUTIONS

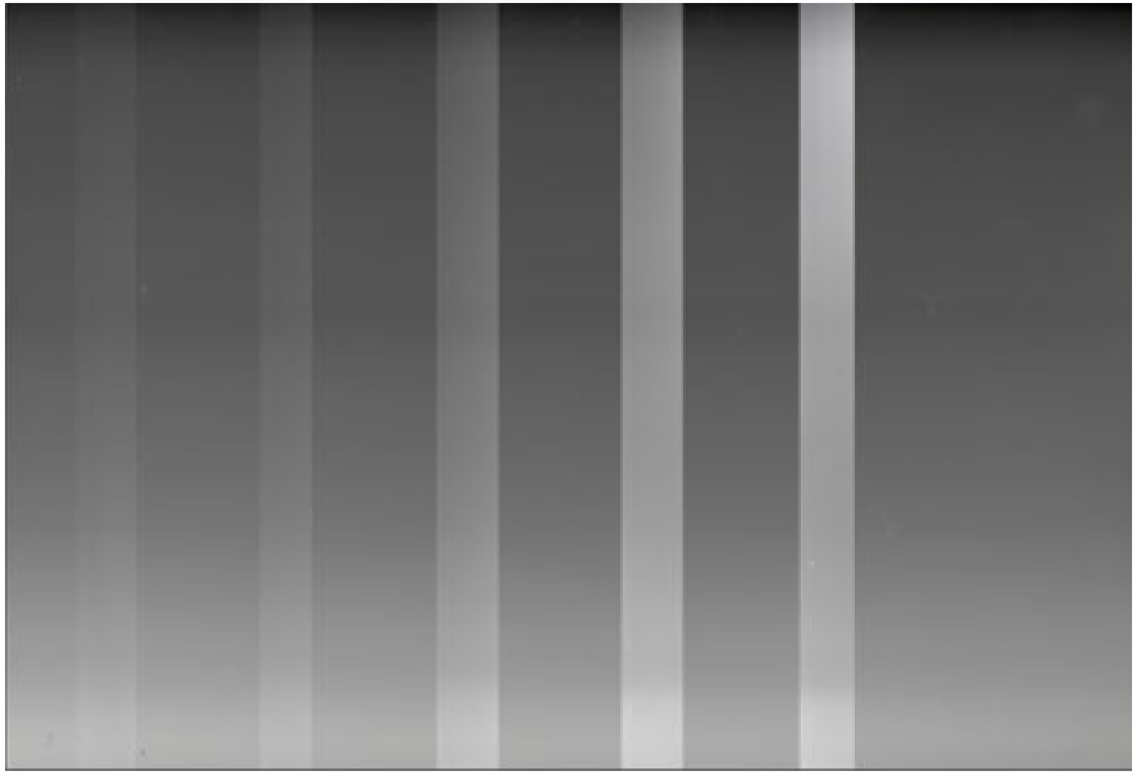


	Error (%)			
Rate (BPS)	100 DPI	200 DPI	300 DPI	600 DPI
10 BPS	0%	0%	0%	0%
20 BPS	0%	0%	0%	0%
50 BPS	0%	0%	0%	0%
100 BPS	0%	0%	0%	35%
200 BPS	22%	19%	30%	50%
500 BPS	50%	50%	50%	54%

Influence of Transmitted Wavelength



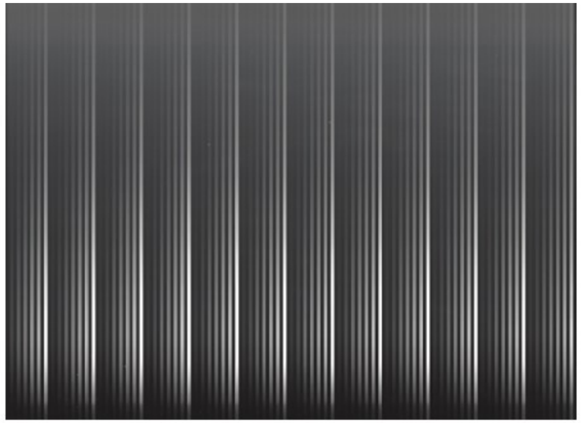
infrared (980nm) laser pointer



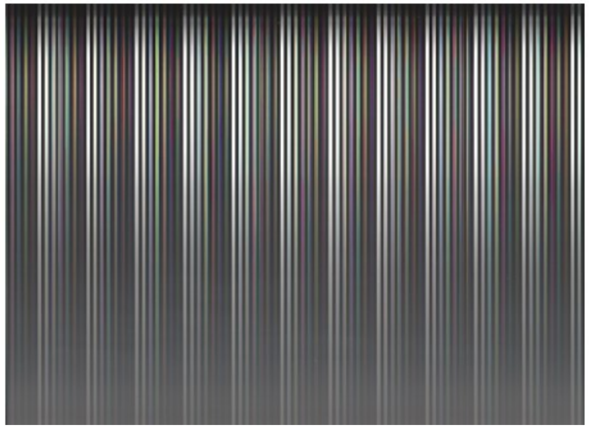
ultraviolet flashlight (365 nm)

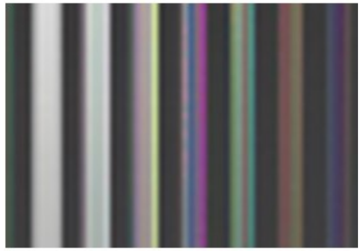
Different Modulation Techniques

Analog

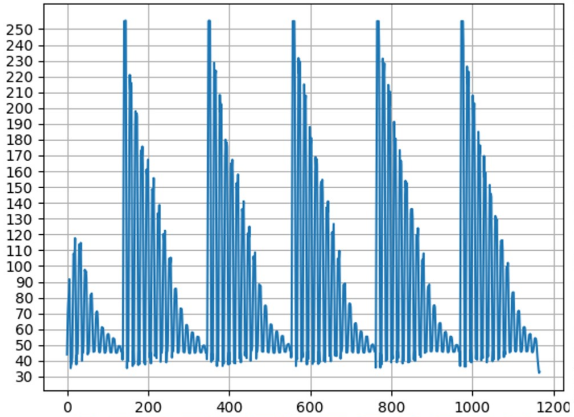


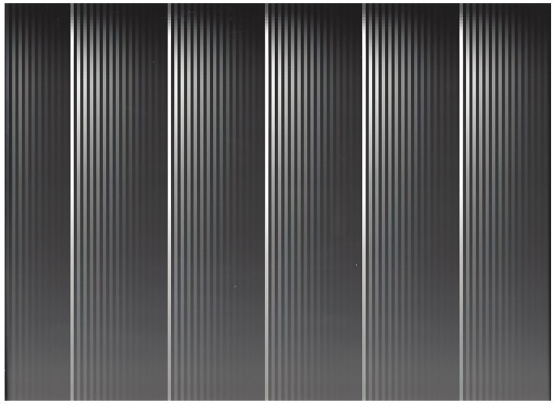
PWM



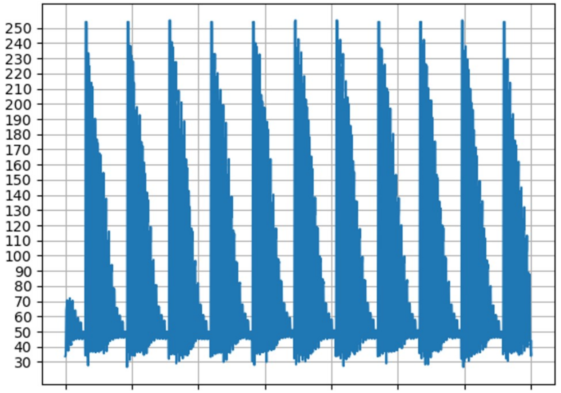


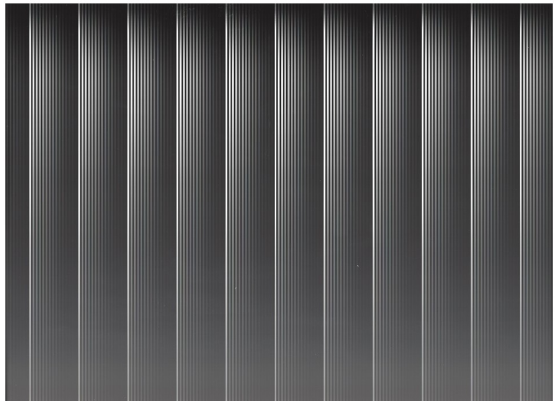
100 DPI



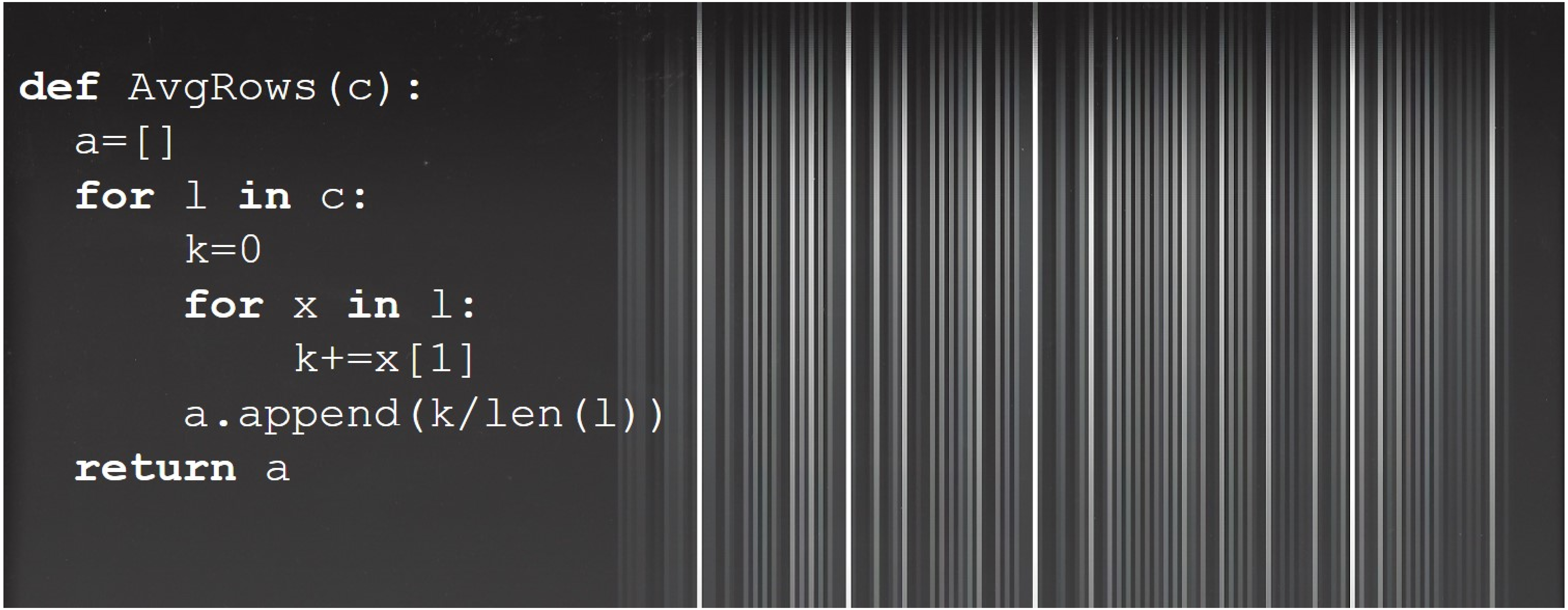


300 DPI





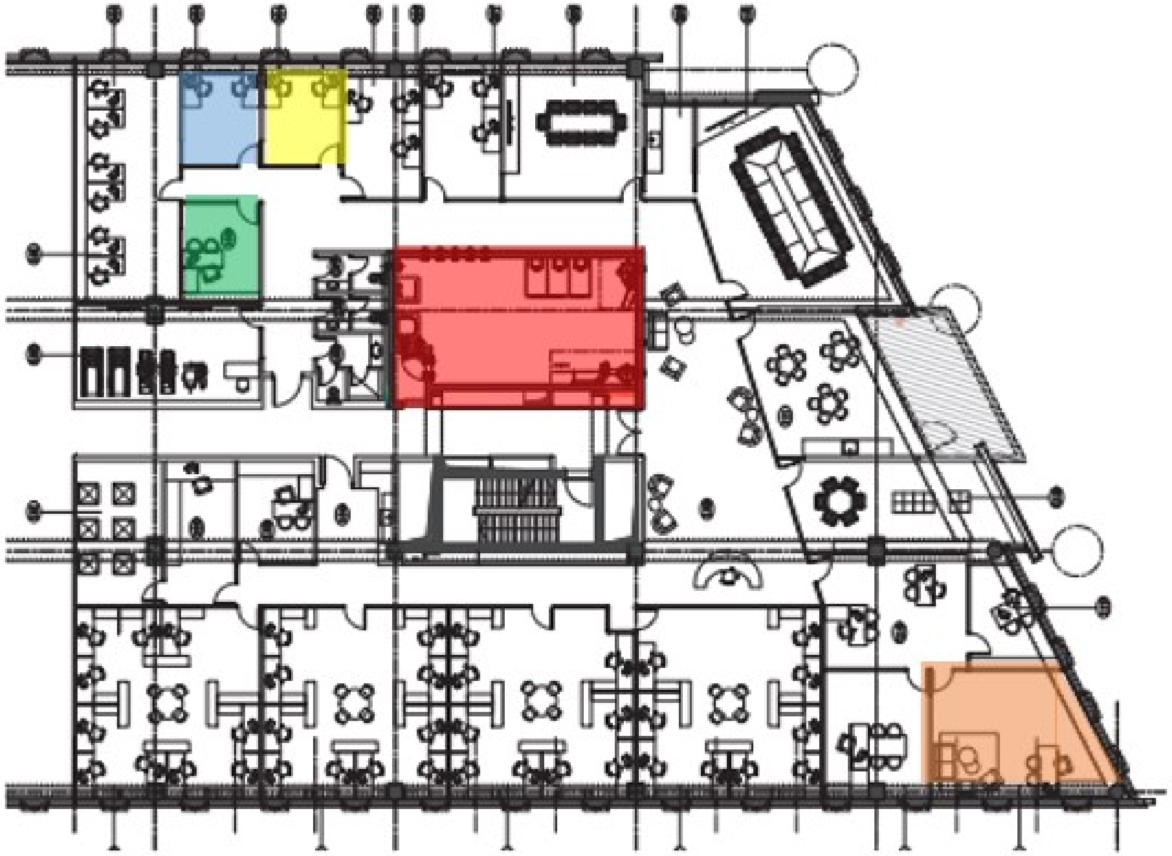
Scans



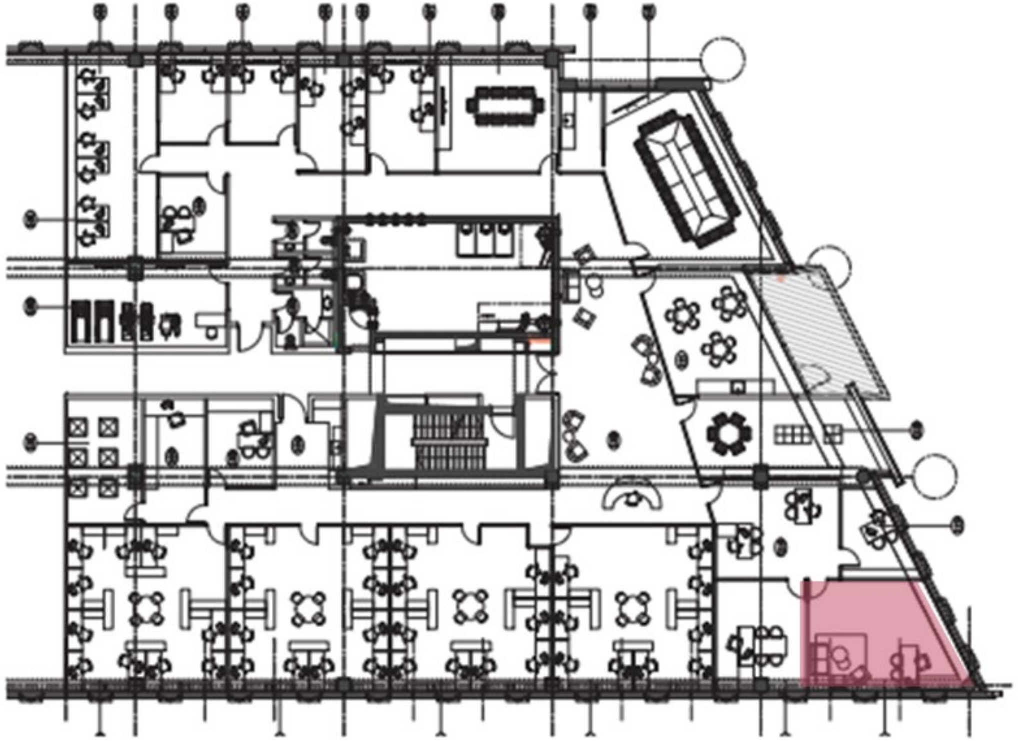
```
def AvgRows(c):
  a=[]
  for l in c:
      k=0
      for x in l:
          k+=x[1]
      a.append(k/len(l))
  return a
```

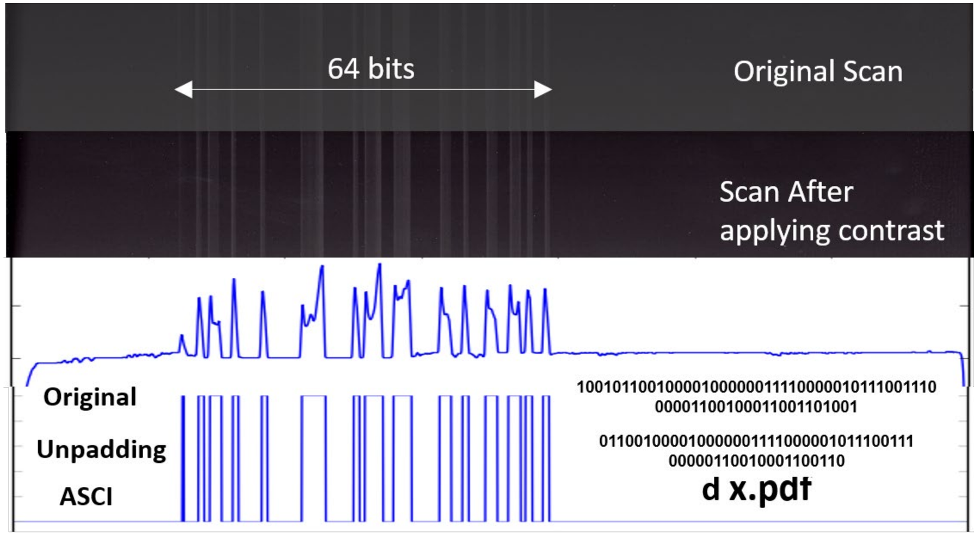
Demonstrations

Attacking a Real Organization



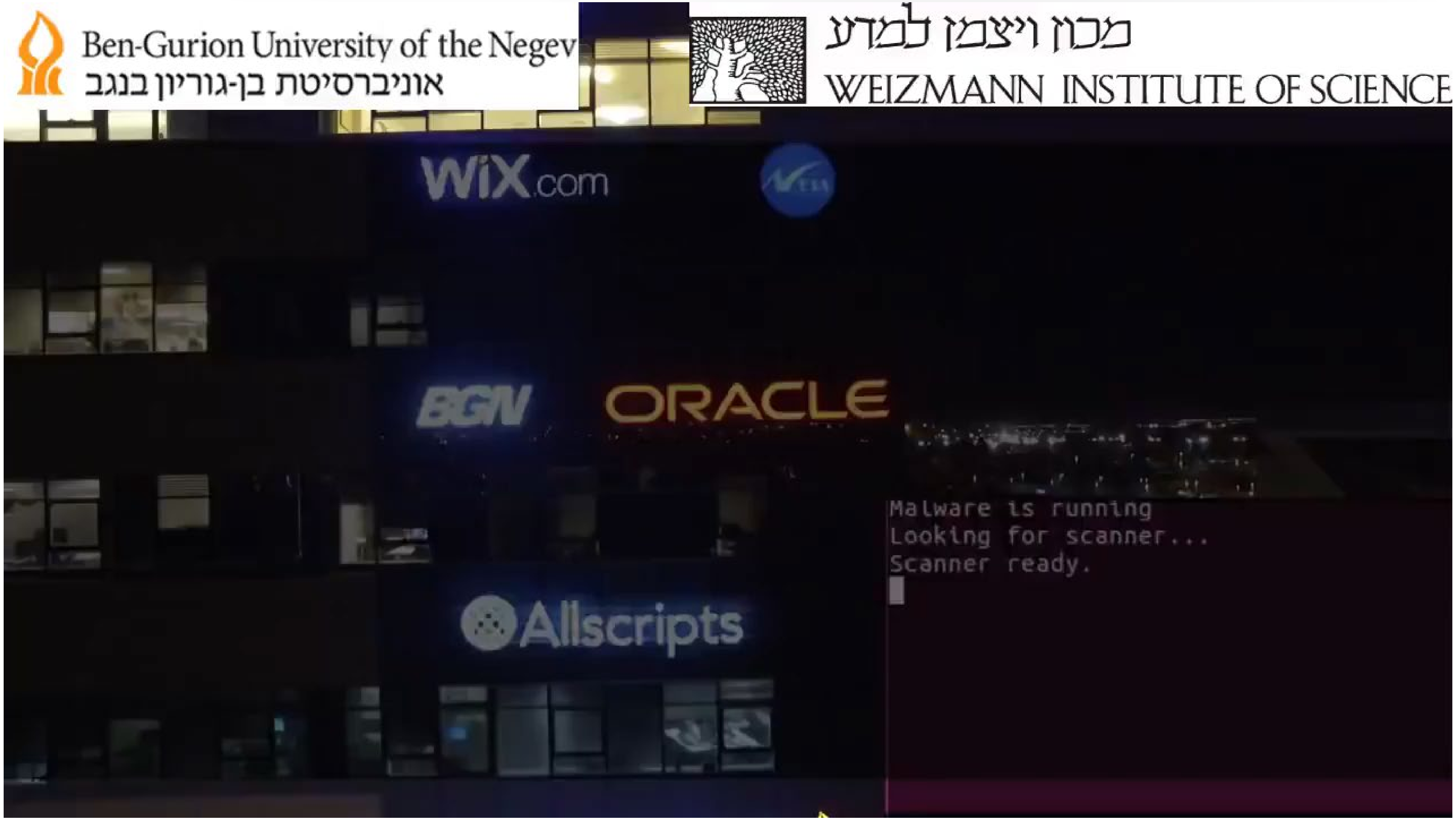
Attacking a Real Organization





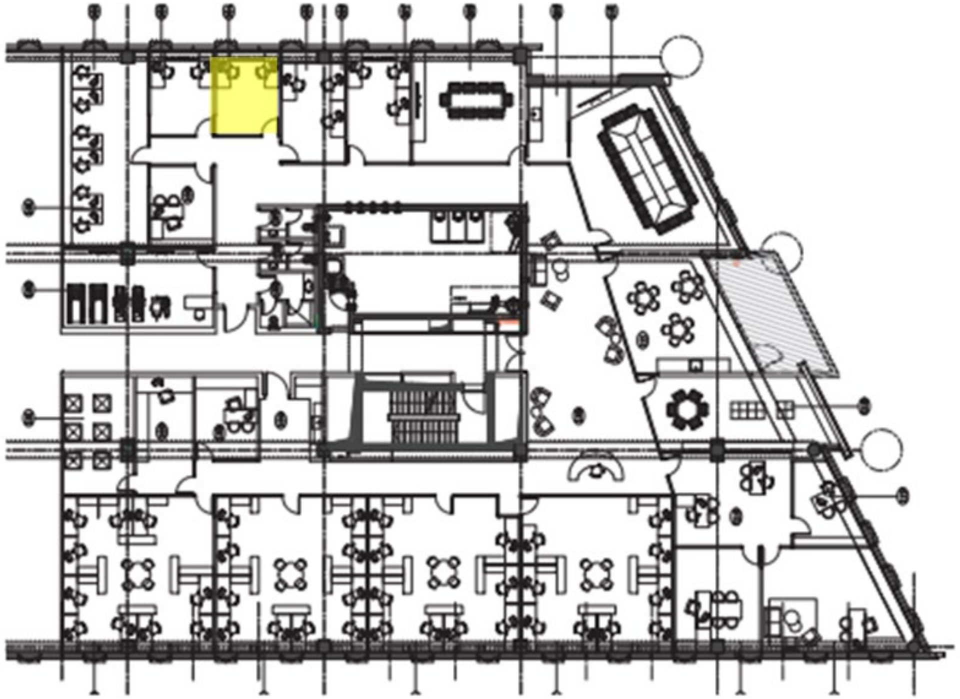
```
1001011001000010000000111100000010111001110
000011001000110011101001

0110010000100000001111000000101110011
00000110010001100110
d x.pdf
```

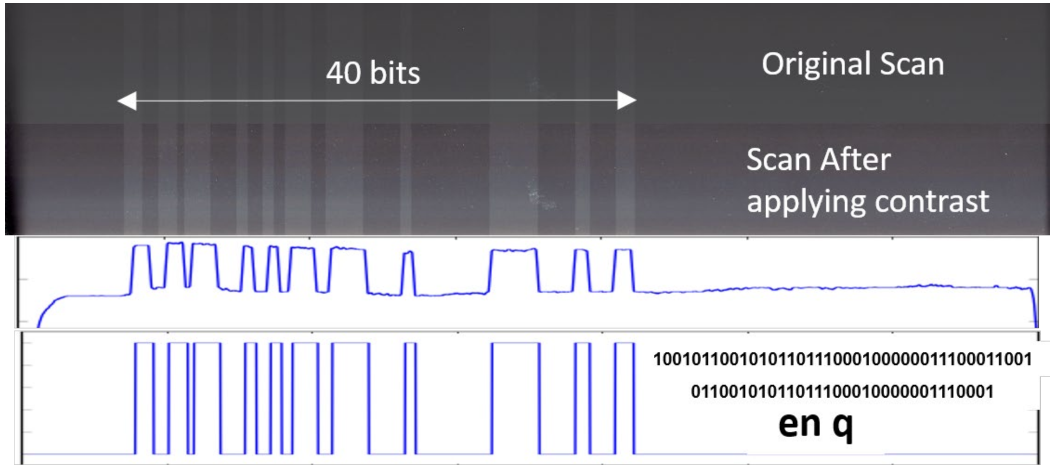
Attacking a Real Organization


Ben-Gurion University of the Negev
אוניברסיטת בן-גוריון בנגב
מכון ויצמן למדע
WEIZMANN INSTITUTE OF SCIENCE
WiX.com
BGN
ORACLE
Allscripts

```
Malware is running
Looking for scanner...
Scanner ready.
```

Attacking a Real Organization





10010110010101101110001000000011100011001

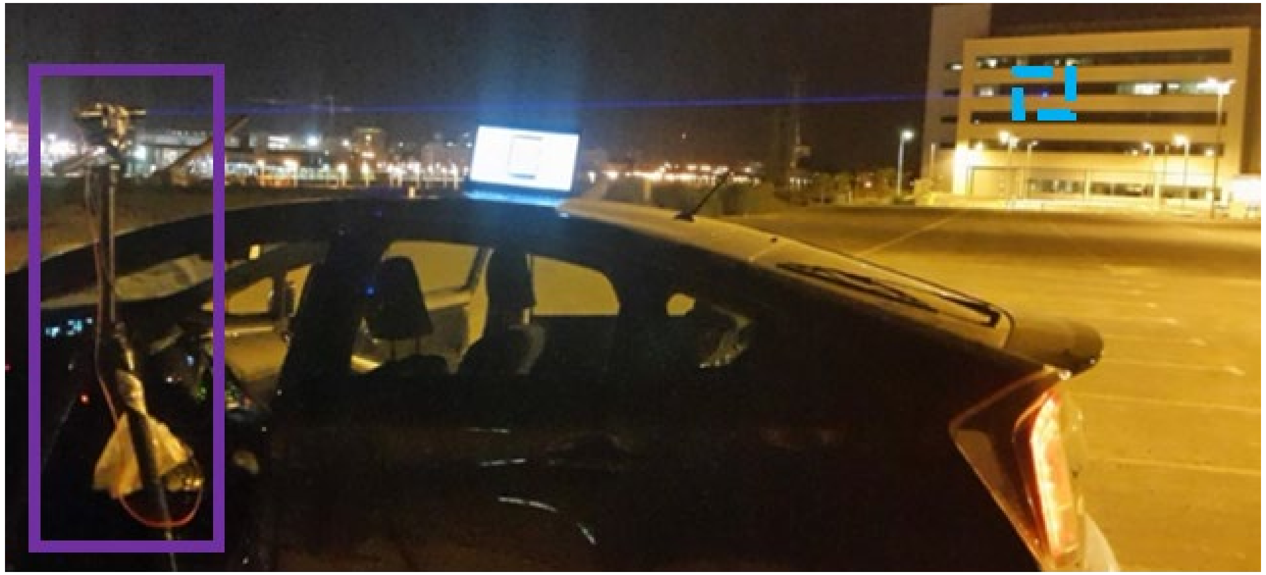
01100101010110111000100000001110001

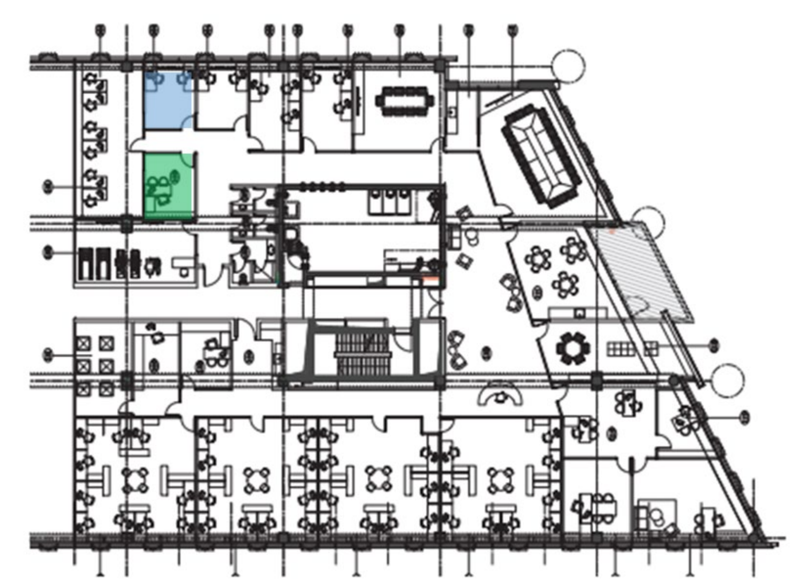
en q

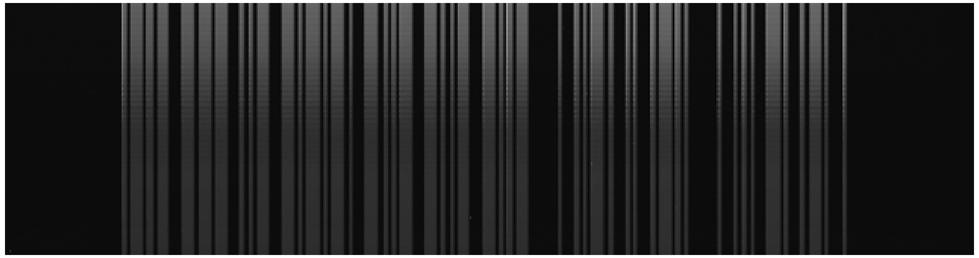
Attacking a Real Organization

Ben-Gurion University of the Negev
אוניברסיטת בן-גוריון בנגב
מכון ויצמן למדע
WEIZMANN INSTITUTE OF SCIENCE

Attacking a Real Organization





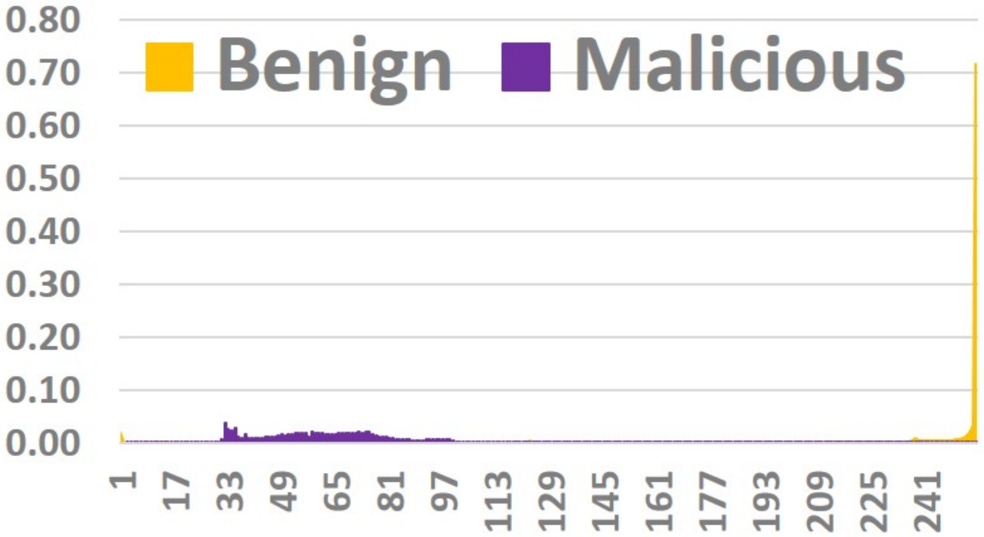


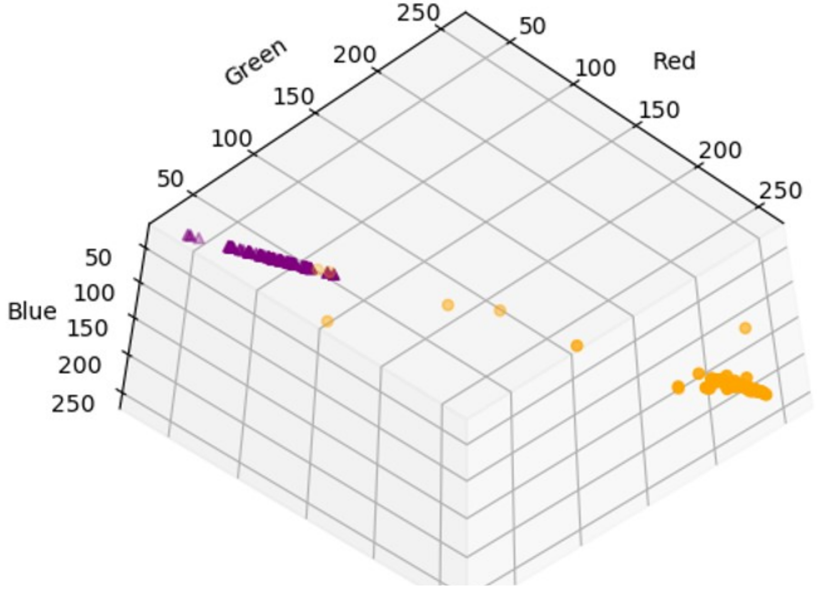
Countermeasures

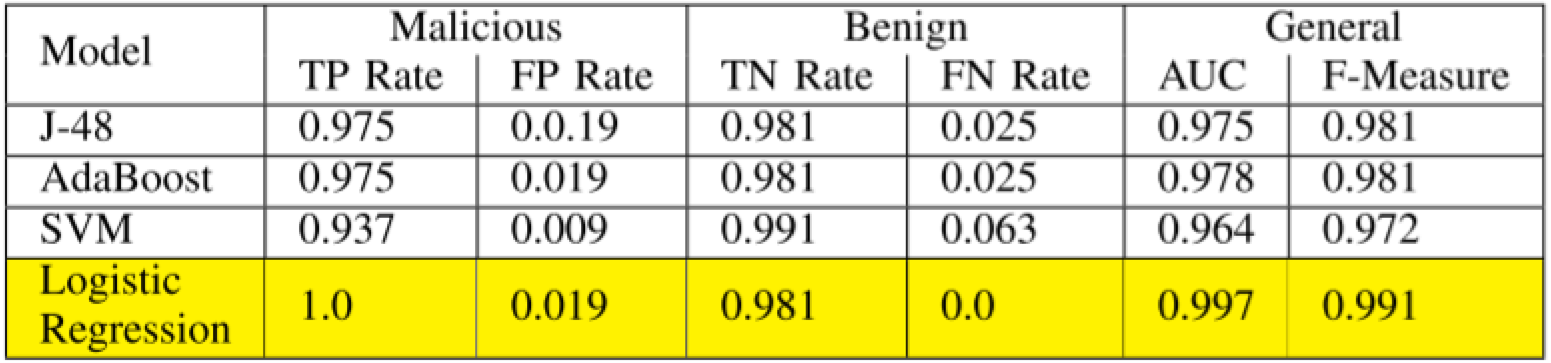
Takeaways

- Disconnect the MFP from any critical network.
- Apply an organizational policy for closing the flatbed of any connected MFP.
- Deploy a dedicated countermeasure method for detecting malicious scans.

Countermeasure Method – Firewall for Scans







Model	Malicious		Benign		General	
	TP Rate	FP Rate	TN Rate	FN Rate	AUC	F-Measure
J-48	0.975	0.0.19	0.981	0.025	0.975	0.981
AdaBoost	0.975	0.019	0.981	0.025	0.978	0.981
SVM	0.937	0.009	0.991	0.063	0.964	0.972
Logistic Regression	1.0	0.019	0.981	0.0	0.997	0.991

Questions?