The Air-Gap Jumpers

Mordechai Guri, PhD
The Head of R&D, Cyber-Security Research Center
Ben-Gurion University of the Negev, Israel

About Me

➢ Computer scientist (PhD)

➢ Head of R&D Cyber-Security Research Center, BGU

➢ Co-founder of Morphisec Endpoint Security

➢ Research focus
  ➢ Advance Persistent Threats (APTs), Rootkits
  ➢ Security of embedded systems
  ➢ Low-level attacks/defense
  ➢ Mobile security
  ➢ Air-gap security

➢ A profile on my research at WIRED by *Andy Greenberg*:
   https://www.wired.com/story/air-gap-researcher-mordechai-guri/

המכון לחקר ביטחון החברה והמדינה
Homeland Security Research Institute

➢ Papers and videos of this presentation can be found in my **air-gap research page** [1]

https://cyber.bgu.ac.il/advanced-cyber/airgap

Agenda

➢ Background

➢ Threats, attack-vectors

➢ Air-gap jumping techniques ('covert channels')

    ➢ Demo videos
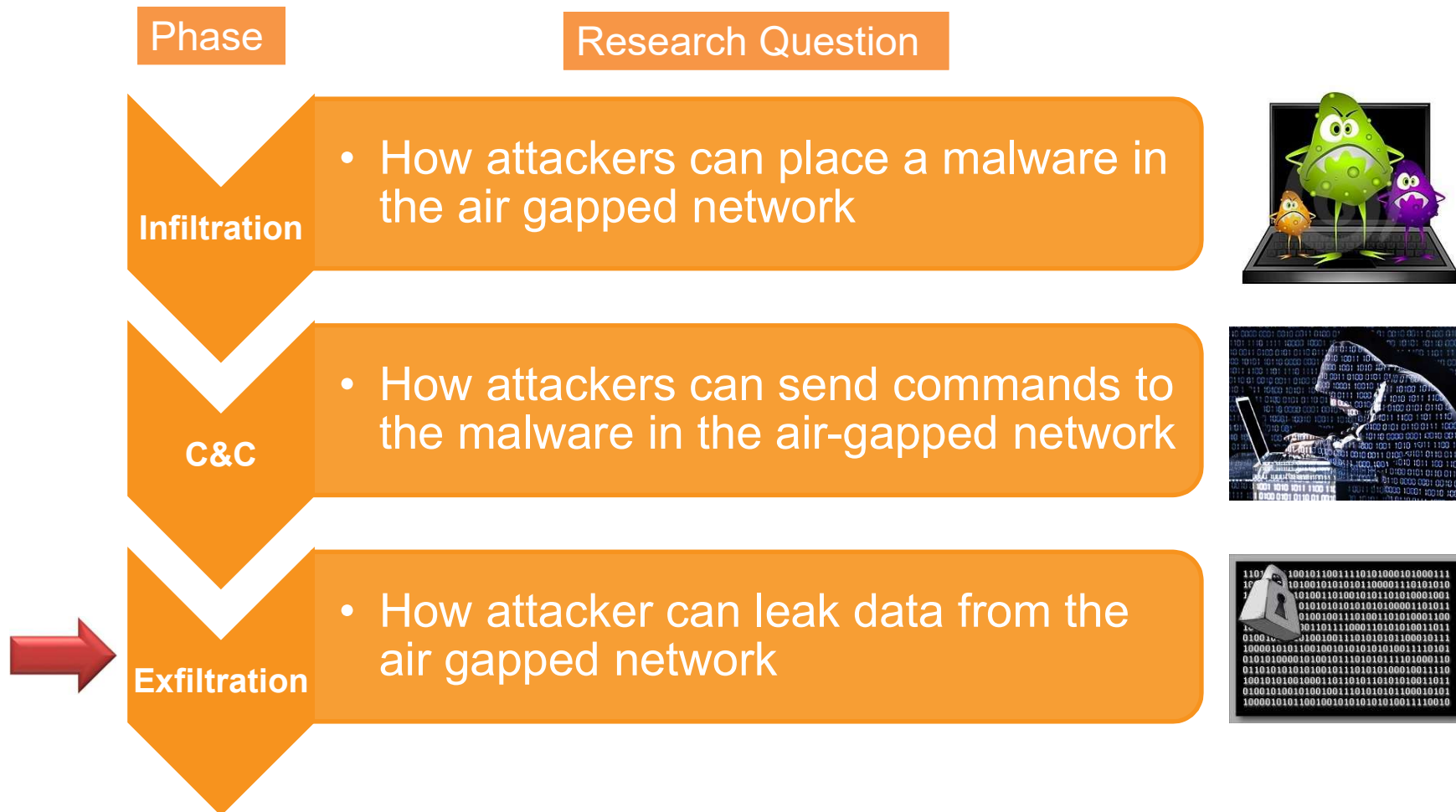
➢ Evaluation

➢ Countermeasures

Air Gap

Definition: A cyber security measure that secures computer network by *physically* isolating it from unsecured networks, such as the Internet or another unsecured local area networks.

Examples of the types of networks or systems that may be air gapped:
- ➢ Military defense system
- ➢ Critical infrastructure command and control centers
- ➢ Computerized medical equipment and healthcare
- ➢ Banking and finance sectors
- ➢ Cryptocurrencies air-gapped ('cold') wallets, blockchain

Threats – Chain of Attack

Phase	Research Question	
Infiltration	• How attackers can place a malware in the air gapped network	
C&C	• How attackers can send commands to the malware in the air-gapped network	
Exfiltration	• How attacker can leak data from the air gapped network	

Infiltration

➢ **Despite the level of isolation, air-gapped networks are not immune to breaches**

 ➢ **Supply Chain Attacks**

 ➢ **Malicious Insiders**

 ➢ **Deceived Insiders**

המכון לחקר ביטחון החברה והמדינה
Homeland Security Research Institute

Infiltration (1)

07.2018:

Ben-Gurion University of the Negev

המכון לחקר ביטחון החברה והמדינה
Homeland Security Research Institute

Infiltration (2)

➢ US military base in the Middle East

➢ A USB flash drive infected with a worm (Agent.BTZ) was left in the parking lot

➢ Inserted into a laptop that attached to the United States Central Command network

➢ From there it spread undetected to other classified and unclassified networks

➢ The Pentagon spent nearly a year cleaning the worm from military networks

Air-Gap Jumping Research

➢ So, attackers *can* infect air-gapped networks

➢ We assume that an attacker already has a foothold (APT) in the air-gapped network

➢ The attacker want to *exfiltrate* data from the network
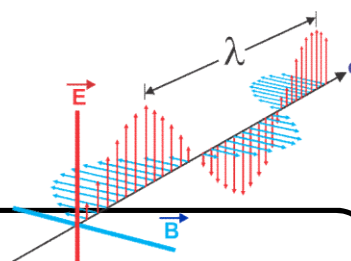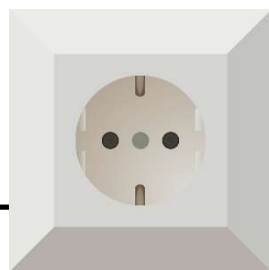 ➢ No internet

Physical Media

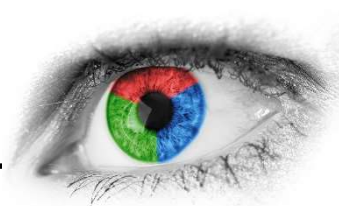➢ Many developed APTs are able to jump over air gaps via USB ([2]).
  ➢ Turla,
  ➢ MiniDuke,
  ➢ RedOctober
  ➢ Fanny
  ➢ Remsec
  ➢ …

➢ Use USB flash drives to jump into air-gapped networks

➢ Use USB flash drives to exfiltrate data from air-gapped networks

Physical Media - Countermeasures

- ➢ Physical media is forbidden (policy)

- ➢ USB I/O activities are monitored

- ➢ USB port blocks (hardware/software)

- ➢ Write protected USB
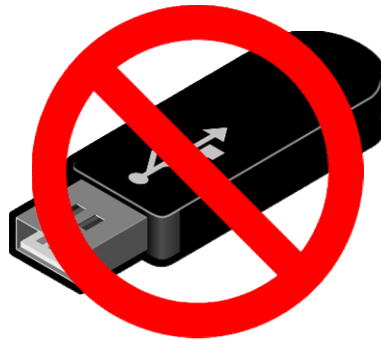
ACOUSTIC

Ultrasonic

Ultrasonic

BeatCoin demo: https://cyber.bgu.ac.il/advanced-cyber/airgap

Ultrasonic

	Range
Humans	20 Hz to ~18 kHz
Cats	55 Hz up to 79 kHz (a range of 10.5 octaves)
Dogs	40 Hz to 60 kHz
Bats	1 kHz - 200 kHz
Mice	1 kHz to 70 kHz.
Dolphins	110 kHz

Ultrasonic
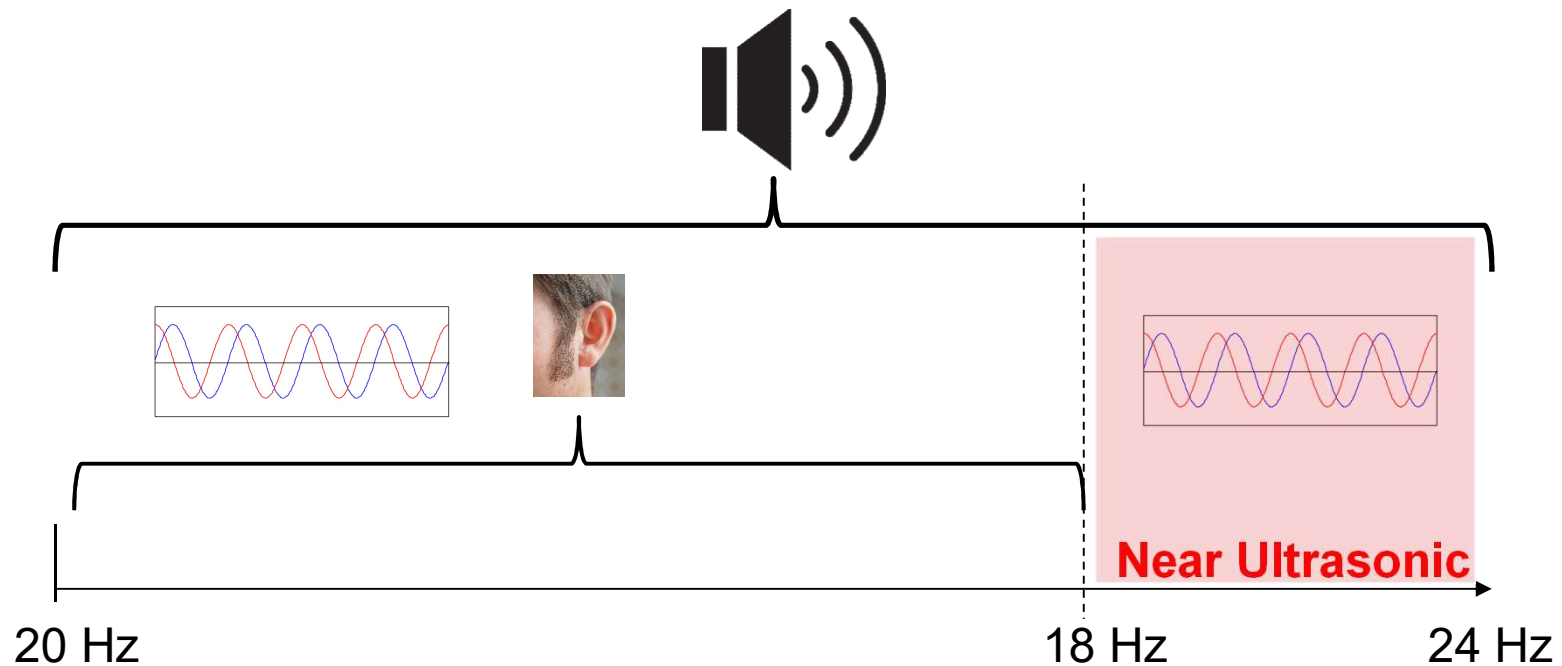
An ordinary computer can produce sound at a frequency band of 0-24kHz

Ultrasonic

המכון לחקר ביטחון החברה והמדינה
Homeland Security Research Institute

Audio-Gap

➢ The solution to the ultrasonic covert-channels: Maintaining an 'Audio-Gap'

➢ Common practices and security policies may prohibit the use of speakers [16]

➢ Disable the audio hardware

➢ 'hermetic' solution?
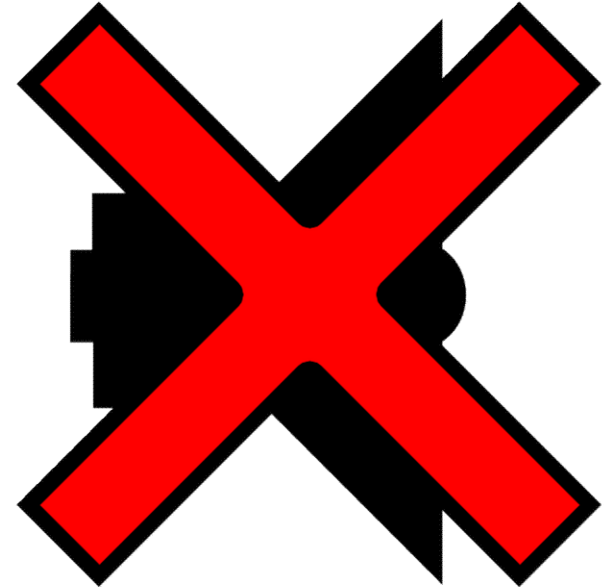
Fansmitter

- Computer fans
  - CPU cooling fans
  - Chassis fans
  - Power-supply fan
  - GPU fans

- The Blade Pass Frequency (BPF)
  - Number of blades
  - Rotation speed
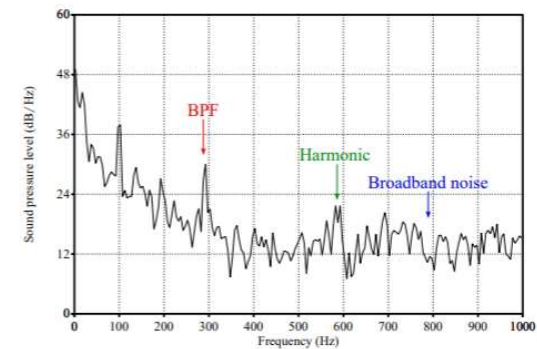
- Malware can control the fan speed (RPM)
  - Control the BPF

Fansmitter

Fansmitter demo: https://cyber.bgu.ac.il/advanced-cyber/airgap

Fansmitter

➢ Move to a "water cooling"?

Diskfiltration

➢ The *actuator arm* is controlled by a motor that moves the hard drive head arm

➢ Can be controlled by malware by performing I/O between tracks (read/write)

➢ With user level privileges (temp folder)
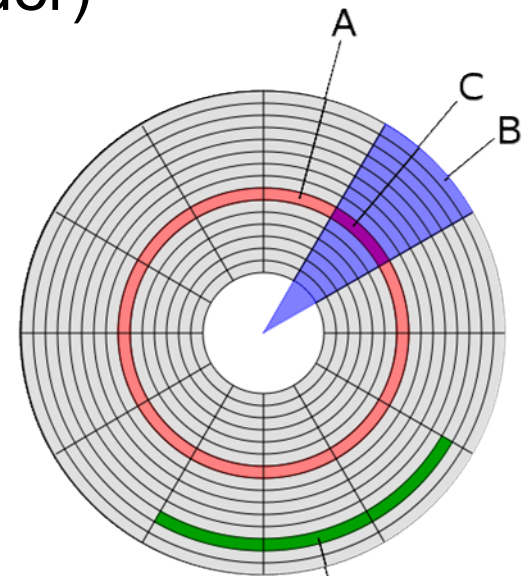
DiskFiltration

DiskFiltration demo: https://cyber.bgu.ac.il/advanced-cyber/airgap

MOSQUITO

- Ultrasonic covert channel requires
  - Speakers (transmit data)
  - Microphones (receive data)

- What if microphones are
  - Banned
  - Disconnected
  - Muted
  - Taped

- Speakers-only environment

MOSQUITO

➢ A malware that exploit a specific audio chip feature

➢ *Reverse* the connected speakers from *output* devices into *input* devices

➢ Turn speakers/headphones/earphones to microphones

➢ Speaker-to-Speaker communication

MOSQUITO

MOSQUITO demo: https://cyber.bgu.ac.il/advanced-cyber/airgap
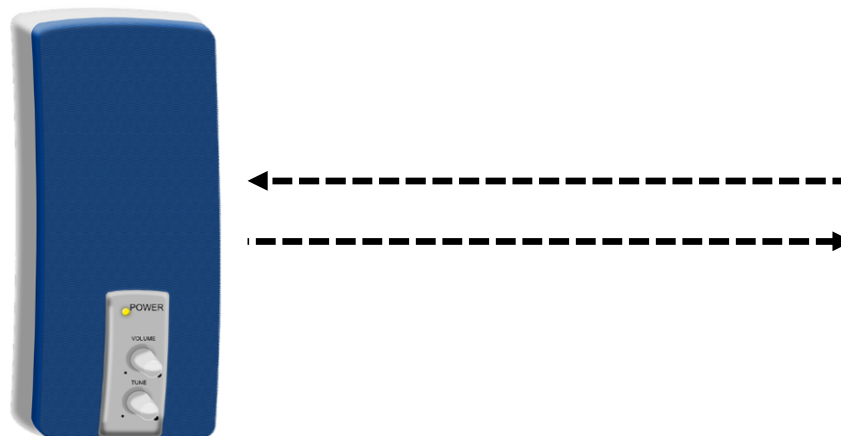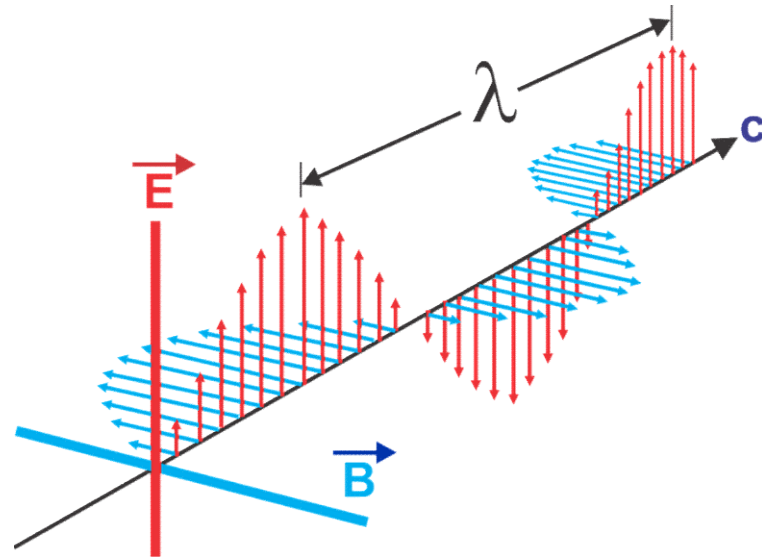
ELECTROMAGENTIC

Electromagnetic - Basics

➢ Electric current in a wire produces an electromagnetic field

➢ The electromagnetic field depend the current pass through the wire

➢ If we control the current in a wire, we control the electromagnetic emission
  ➢ Frequency
  ➢ Amplitude
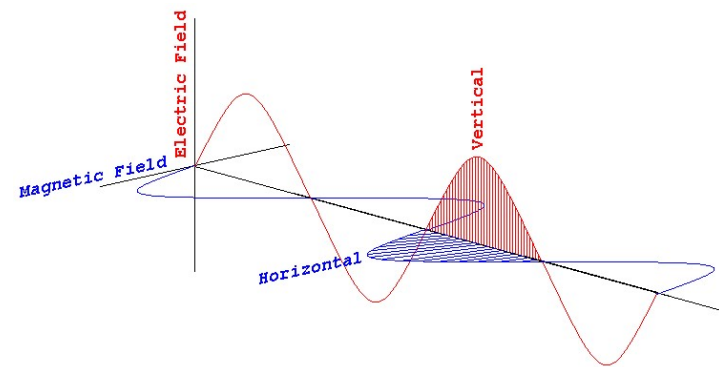
AirHopper

- ➢ Screen cables are emanating electromagnetic radiation – depend on the 'image' transmitted in the cable

- ➢ We can control the electromagnetic radiation by transmitting specially crafted images

- ➢ We can adjust the electromagnetic radiation to the FM radio band! (88 Mhz-108 MHz)

- ➢ Malware uses the video display as a FM transmitter to leak data
  - ➢ Screen cable function as an antenna

AirHopper

AirHopper

AirHopper demo: https://cyber.bgu.ac.il/advanced-cyber/airgap
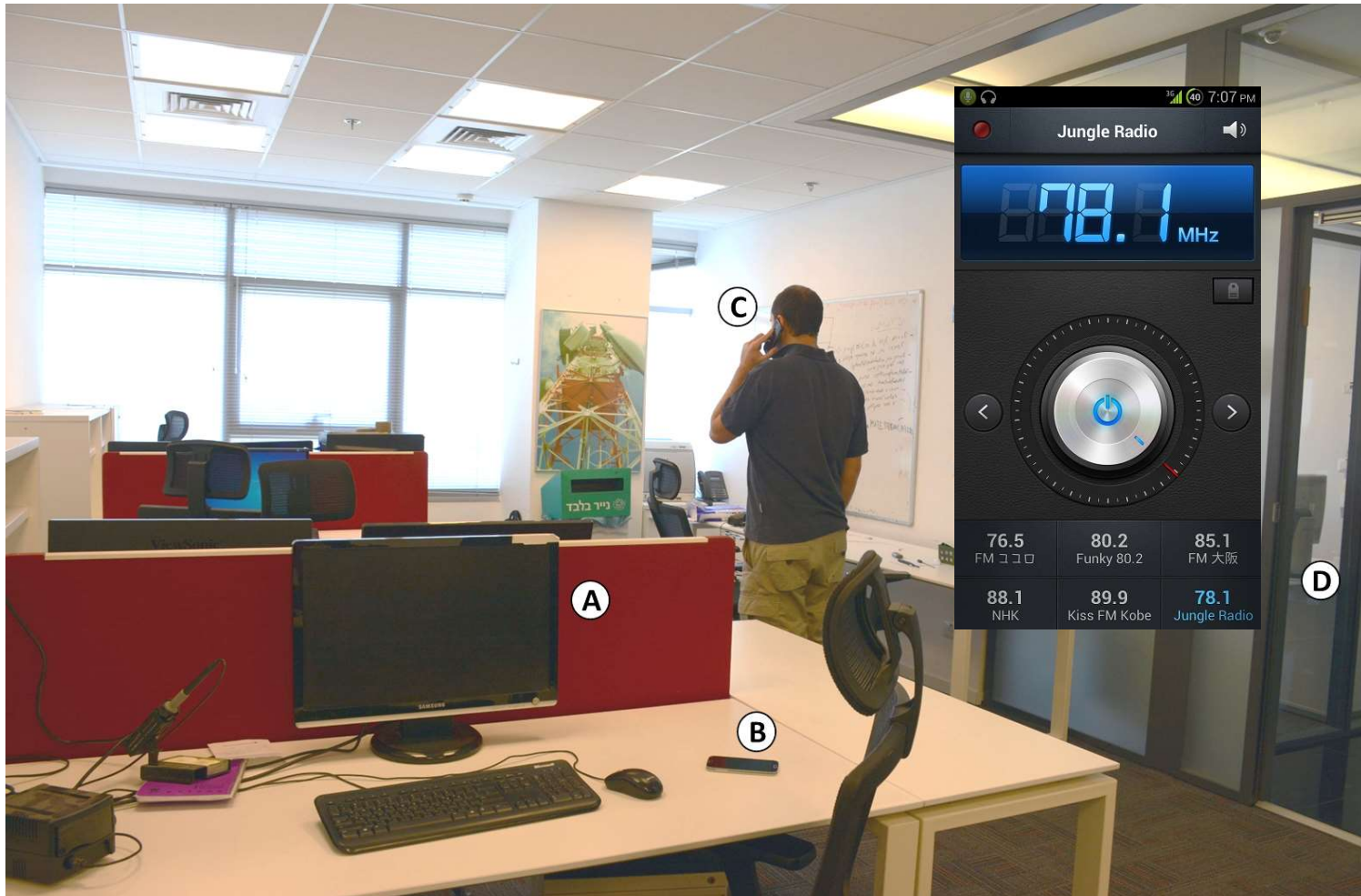
GSMem

➤ "feature-phones" might be allowed in some facilities

➤ No camera, Bluetooth, Wi-Fi, FM, etc.

GSMem

> The CPU-memory bus emit electromagnetic radiation

> We can control the radiation by building special patterns memory transfers

> The radiation can be adjusted to the GSM, UMTS and LTE frequency bands (2G, 3G and 4G)

> We use multi-channels to amplify the transmission

GSMem

Ben-Gurion University
of the Negev

המכון לחקר ביטחון החברה והמדינה
Homeland Security Research Institute

GSMem

GSMem demo: https://cyber.bgu.ac.il/advanced-cyber/airgap
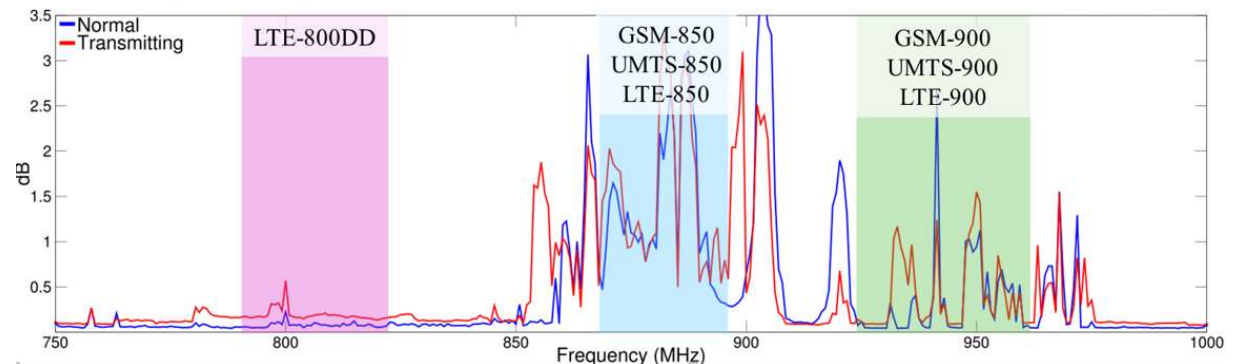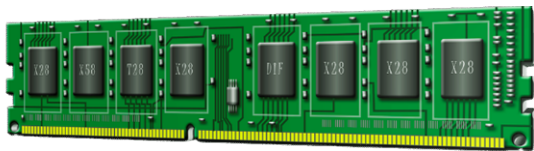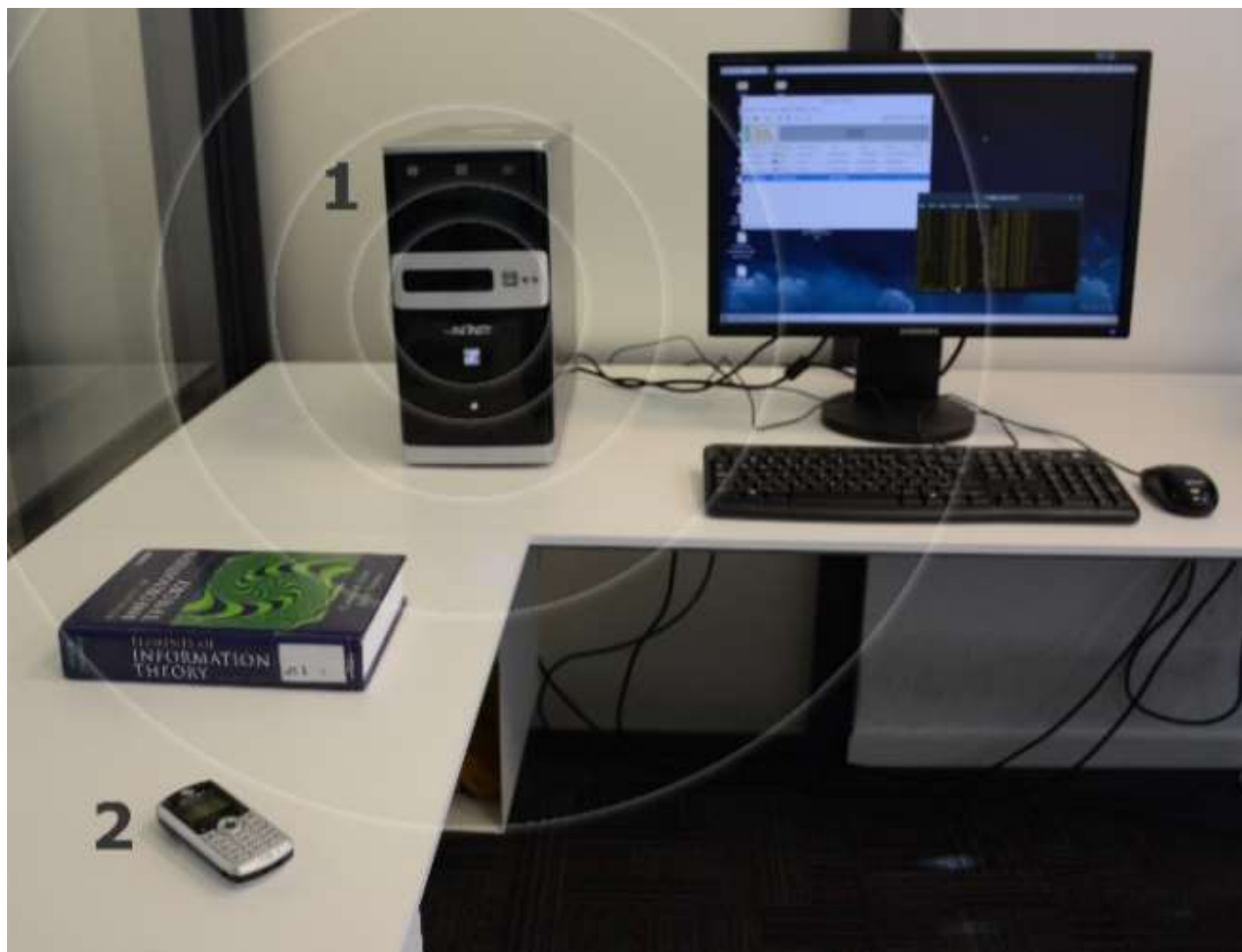
USBee

➢ Use the USB data bus to transmit RF signals

➢ D+/D- as small antennas

➢ Simple I/O operations (read/write)

➢ No special permission is required

USBee

USBee demo: https://cyber.bgu.ac.il/advanced-cyber/airgap

Ben-Gurion University
of the Negev

המכון לחקר ביטחון החברה והמדינה
Homeland Security Research Institute
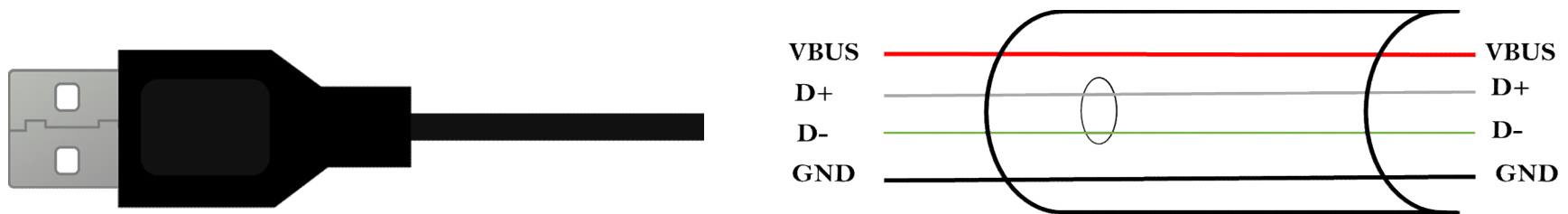
MAGNETIC

ODINI

➢ Jump air-gaps and bypass Faraday cages

➢ The ODINI method is based on an exploitation of the *low-frequency magnetic fields* generated by the computer's CPU

➢ Low frequency magnetic radiation propagates through the air, penetrating metal shielding such as Faraday cages

➢ E.g., compass still works inside Faraday cages

ODINI

ODINI demo: https://cyber.bgu.ac.il/advanced-cyber/airgap

MAGNETO

MAGNETO demo: https://cyber.bgu.ac.il/advanced-cyber/airgap

Ben-Gurion University
of the Negev

המכון לחקר ביטחון החברה והמדינה
Homeland Security Research Institute
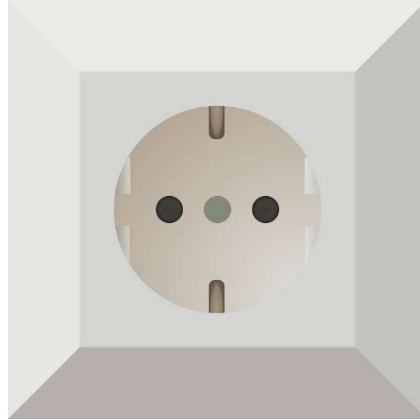
ELECTRIC

PowerHammer

- ➤ A malicious code running on a compromised computer can control the power consumption of the system by intentionally regulating the CPU utilization

- ➤ Data is modulated, encoded, and transmitted on top of the current flow fluctuations

- ➤ This it is conducted and propagated through the power lines

- ➤ This phenomena is known as a 'conducted emission'

PowerHammer

Main electrical service panel

Floor electrical service panel
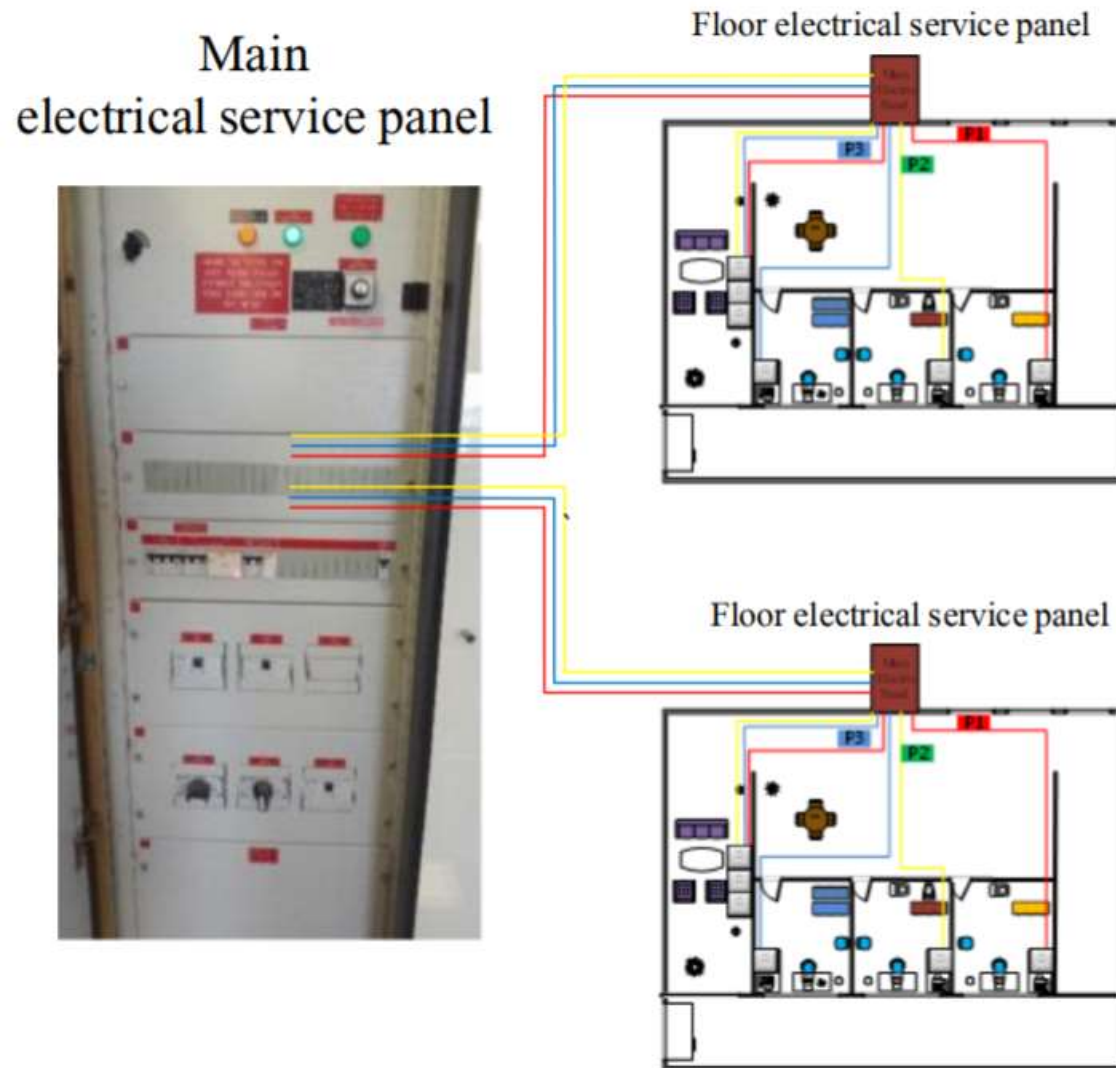
Floor electrical service panel

OPTICAL

Optical

➢ Computer and peripherals are equipped with LEDs indicators

➢ The LEDs are controllable from software/firmeware level

➢ Malware can encode data on 'blinks'

➢ Can be intercepted by local cameras or remotely (e.g., drones)

LED-it-GO

LED-it-GO demo: https://cyber.bgu.ac.il/advanced-cyber/airgap

xLED

xLED demo: https://cyber.bgu.ac.il/advanced-cyber/airgap

aIR-Jumper

➢ Security camera are equipped with IR LEDs

➢ Security cameras can 'see' IR

➢ Can not seen by humans

aIR-Jumper

aIR-Jumper demo: https://cyber.bgu.ac.il/advanced-cyber/airgap

THERMAL

BitWhisper

Motivation
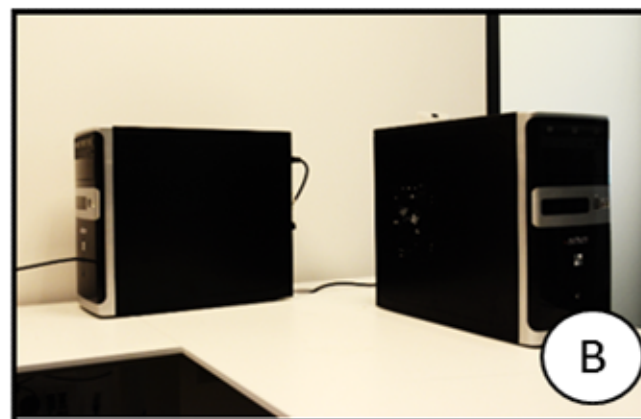
BitWhisper

➢ Computer are emitting heat from
- ➢ CPU
- ➢ GPU
- ➢ HDD
- ➢ Peripherals

➢ Computer are equipped with built-in thermals sensor
- ➢ CPU/GPU
- ➢ Motherboard
- ➢ HDDs

➢ Bi-Directional communication based on heat

BitWhisper

- A computer can detect temperature change created by the adjacent computer
- Data is encoded via temperature changes
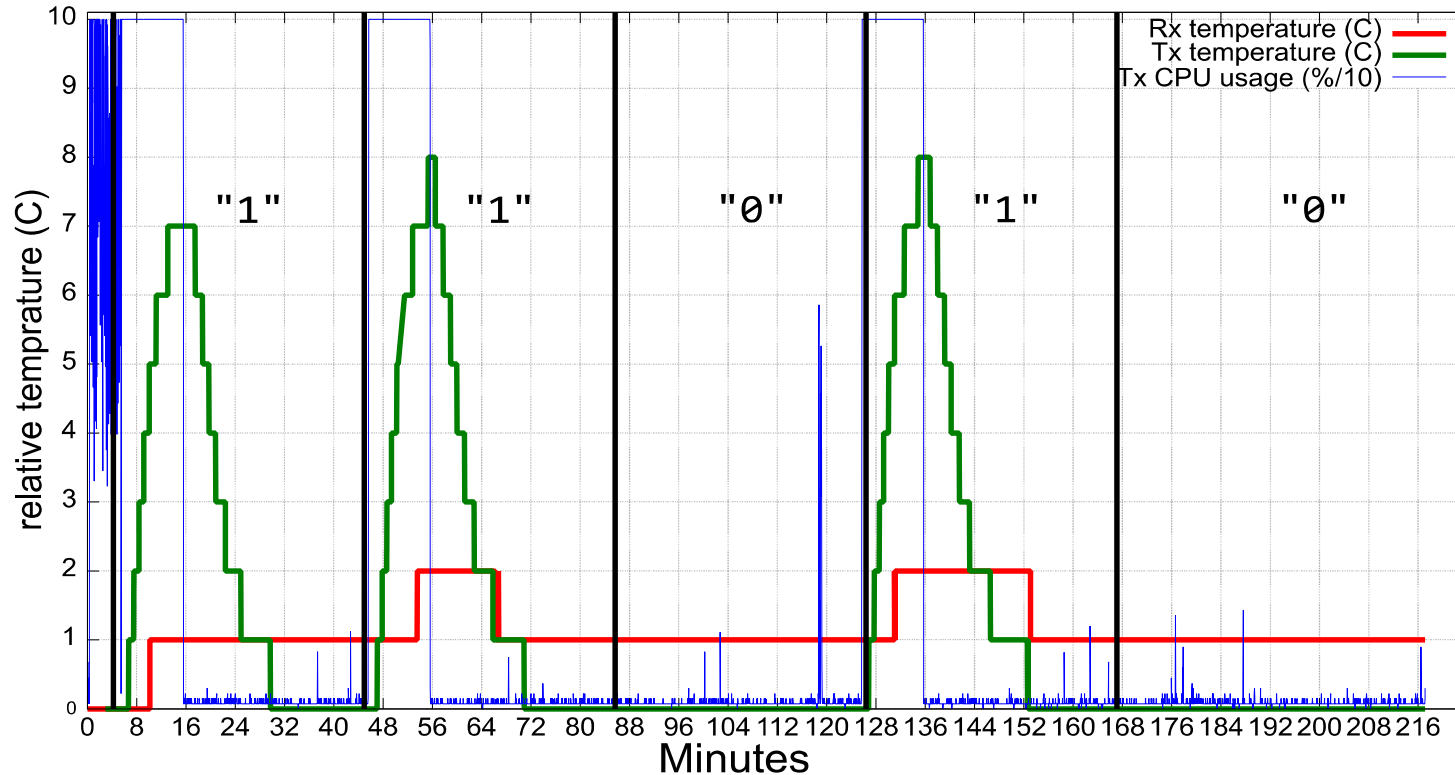
BitWhisper

BitWhisper demo: https://cyber.bgu.ac.il/advanced-cyber/airgap

Evaluation

	Channel Type			
Channel Characteristic	Acoustic	Electro magnetic /magnetic/electric	Thermal	Optical
Stealth	High	High	Medium (sensible)	Low / High
Channel Availability	High	High	Low (overnight attack)	Low (user absence)
Feasibility in Virtualization	Medium	Medium	Medium	Medium
Hardware Availability	Medium-low	High	High	High
Quality	Medium	Medium/low	Low	Medium
Required Privileges	Regular	Regular/Root	Regular/Root	Regular

Countermeasures

Method	Type	Relevancy to bridgeware types	Cost
Physical insulation/ Zoning/ Red/Black separation	Physical countermeasures	Acoustic, Electromagnetic, Thermal, Optical	High
Wires and equipment shielding	Hardware countermeasures	Electromagnetic (partial)	Low-Medium
Signal filtering	Hardware countermeasures	Acoustic, Electromagnetic (partial)	Medium
Signal jamming	Hardware countermeasures	Electromagnetic	Medium
Activity detection	Software countermeasures	Acoustic, Electromagnetic, Thermal, Optical	Low-Medium
Soft tempest	Software countermeasures	Electromagnetic	Low

Air-Gap Jumping

- **Electromagnetic**
  - AirHopper [3], GSMem [4], USBee [5]

- **Magnetic**
  - ODINI [6], MAGNETO [7]

- **Electric**
  - POWERHAMMER [8]

- **Acoustic**
  - MOSQUITO [9], Fansmitter [10], Diskfiltration [11]

- **Optical**
  - LED-it-GO [12], xLED [13], aIR-Jumper [14]

- **Thermal**
  - BitWhisper [15]

References

[1] Air-Gap Research Page, Mordechai Guri,
https://cyber.bgu.ac.il/advanced-cyber/airgap

[2] Industrial Defence In-Depth, Kaspersky Lab, Andrey Nikishin

[3] AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies."
In Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on, pp. 58-67. IEEE, 2014.

[4] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici. "GSMem: Data exfiltration from air-gapped computers over gsm frequencies." In 24th USENIX Security Symposium (USENIX Security 15), pp. 849-864. 2015.

[5] Mordechai Guri, Matan Monitz, and Yuval Elovici. "USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB." Privacy, Security and Trust (PST), 2016 14th Annual Conference on

[6] ODINI : Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via
Magnetic Fields, Mordechai Guri, Boris Zadov, Andrey Daidakulov, Yuval Elovici, https://arxiv.org/abs/1802.02700

[7] MAGNETO: Covert Channel between Air-Gapped Systems and Nearby Smartphones via CPU-Generated Magnetic Fields, Mordechai Guri, Andrey Daidakulov, Yuval Elovici https://arxiv.org/abs/1802.02317

[8] PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines", Mordechai Guri, Boris Zadov, Dima Bykhovsky, Yuval Elovici https://arxiv.org/abs/1804.04014

Ben-Gurion University
of the Negev

המכון לחקר ביטחון החברה והמדינה
Homeland Security Research Institute

References

[9] MOSQUITO: Covert Ultrasonic Transmissions between Two Air-Gapped Computers using Speaker-to-Speaker Communication ", Mordechai Guri,Yosef Solewicz, Andrey Daidakulov, Yuval Elovici, https://arxiv.org/abs/1803.03422

[10] Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, and Yuval Elovici. "Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers." *arXiv preprint arXiv:1606.05915* (2016).

[11] Mordechai Guri,Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. "Acoustic Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard-Drive Noise ('DiskFiltration')". European Symposium on Research in Computer Security (ESORICS 2017) pp 98-115

[12] Mordechai Guri, Boris Zadov, Yuval Elovici. "LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED". Detection of Intrusions and Malware, and Vulnerability Assessment - 14th International Conference, DIMVA 2017: 161-184

[13] Mordechai Guri, Boris Zadov, Andrey Daidakulov, Yuval Elovici. "xLED: Covert Data Exfiltration from Air-Gapped Networks via Router LEDs", https://arxiv.org/abs/1706.01140

[14] aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR)" Mordechai Guri, Dima Bykhovsky, Yuval Elovici, http://arxiv.org/abs/1709.05742

[15] Mordechai Guri, Matan Monitz, Yisroel Mirski, and Yuval Elovici. "Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations." In Computer Security Foundations Symposium (CSF), 2015 IEEE 28th, pp. 276-289. IEEE, 2015.

[16] https://abclegaldocs.com/blog-Colorado-Notary/air-gap-computer-network-security/

Ben-Gurion University
of the Negev

המכון לחקר ביטחון החברה והמדינה
Homeland Security Research Institute

Thank you