Air-gap Limitations and Bypass Techniques: “Command and Control” using Smart Electromagnetic Interferences

Chaouki Kasmi, José Lopes Esteves, Philippe Valembois
WHO WE ARE

C. Kasmi, J. Lopes Esteves, P. Valembois

- ANSSI-FNISA / Wireless Security Lab
- Electromagnetic threats on information systems
- RF communications security
- Embedded systems
- Signal processing
- Not malware/botnet analysts 😊
AGENDA

- Air Gap principles
- Air Gap bridging techniques
- IEMI
- IEMI effects exploitation: design of a covert channel
- Countermeasures
- Conclusion
Air Gap Principles
 critical infrastructures
- Heterogeneous information systems (IS)
  - Internet
  - Intranets
  - Operational/production networks
- Different information sensitivity and trust levels
- Untrusted IS compromise can spread to trusted ones
Critical services

Internet

Intranet services
Critical services

Internet
CONTEXT

Internet

Critical services
CONTEXT

Internet

Critical services

AIR GAP

ANSSI
THE AIR GAP

- Physical isolation of sensitive IS
- Removal of communication channels with machines from different IS
- Mitigates risk of sensitive information access and compromise of trusted IS from untrusted IS

![Diagram showing the concept of the air gap with a barrier between trusted and untrusted IS through a potable supply line and a non-potable mixture with an overflow rim and outlet.]
DRAWBACKS

- Implies multiplication of number of machines
  - Cost ++
  - Space occupation on desk (or server rooms) ++
  - KVM switch temptation ++
- Work process / organizational constraints ++
  - Data sometimes still has to be shared between IS
  - Diodes, sanitization devices
  - What about update process?
DRAWBACKS

We’re sending you to set up computers for our overseas partner. They have backward technology but cheap labor.

KVM Switch.

Do you guys have a KVM switch? I can set up your computers faster four at a time.

Of course! We have several.

No. 1. OK.
No. 2. OK.
No. 4.

icanbarelydraw.com CC BY-NC-ND 3.0
Air Gap Bridging Techniques

A state of the art
AIR GAP BRIDGING

- Covert channel
- Using disabled networking interfaces
- Using peripherals
- Using mechanical waves
- Using light
- Using temperature
- Using radio frequency EM waves
Covert channel:

- Information transfer (uni- or bi-directional)
- Entities not allowed to communicate
- Channel not intended for communication

Prerequisite: preliminary infection

- Both ends know the covert channel
- Both ends know the protocol
- Out of scope of this talk
Communication interfaces
Especially RF (no need for physical connection)
Software disable is not enough
Hardware kill-switch may not be enough [1]
Have to be physically removed
Peripherals used simultaneously or alternatively

Microcontrollers + memory chips = persistent storage or states (+ malicious firmware)

- e.g. USB devices: webcam, keyboard, mass storage
- e.g. Display devices: I2C channel + EEPROM (DDC, MCCS), multisource, networking capabilities (HDMI)
- e.g. KVM switches
USING SHARED PERIPHERALS

[Diagram of KVM connections with labels for EEPROM DDC, Emulation EEPROM RO, and KVM]
USING SHARED PERIPHERALS

- EEPROM DDC
- KVM
- Emulation EEPROM
- RO RW

1

2
USING MECHANICAL WAVES

Sound / vibrations:

- Google Tone [2], Ultrasound [3][4], Cross-Device Tracking
- Sender controls sound source (audio output, fan speed, *emanations from internal components* [5]…)
- Receiver controls audio input, gyroscope [6]…
Shamir, BHUSA keynote [7]:

- Sender controls light source (display, LEDs, smart light bulbs…)
- Receiver controls light sensor (video camera, scanner…)

USING LIGHT

Laser beam to scanner sensor
Blinking LED
BitWhisper [8]:
- Sender controls temperature (heating system, thermostat, CPU activity…)
- Receiver controls temperature sensor

![Thermal Images](image.png)

*Figure 1. A “thermal ping” sent between two adjacent PCs. The snapshots were taken by using a thermal camera.*

*Picture from [8]*
USING RF

- Funtenna [9], Airhopper [10], GSMem[11]
- Exploit internal components’ RF leakage
  - Controllable wires/lines
  - Leaking video display
  - Cpu/memory activity
- Only used for data exfiltration
- Today: combining RF/IEMI and target’s temperature sensors to send data to the target
<table>
<thead>
<tr>
<th>Method</th>
<th>Transmitter</th>
<th>Receiver</th>
<th>Direction*</th>
<th>Distance (m)</th>
<th>Rate (bit/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirHopper</td>
<td>Display cable</td>
<td>FM receiver</td>
<td>Out</td>
<td>7</td>
<td>480</td>
</tr>
<tr>
<td>Ultrasonic</td>
<td>Speaker</td>
<td>Mic</td>
<td>In-Out</td>
<td>19.7</td>
<td>20</td>
</tr>
<tr>
<td>GSMem</td>
<td>RAM bus</td>
<td>GSM baseband</td>
<td>Out</td>
<td>5.5</td>
<td>2</td>
</tr>
<tr>
<td>GSMem</td>
<td>RAM bus</td>
<td>Dedicated equipment</td>
<td>Out</td>
<td>30+</td>
<td>100-1000</td>
</tr>
<tr>
<td>BitWhisper</td>
<td>CPU/GPU Heating system</td>
<td>Heat Sensor</td>
<td>In-Out</td>
<td>0.4</td>
<td>0.002 (8 bits/hour)</td>
</tr>
</tbody>
</table>

* In: Data sent to the target
Out: Data sent by the target
Intentional Electromagnetic Interference
Electromagnetic Compatibility and Info. Sec.
IEMI, definition
Classification of effects
Effects on IT systems and Experimental results
EMC AND INFO. SEC.

- **OUT covert channels**
  - Data Exfiltration

- **IN covert channels**
  - Data Infiltration

- **Information Security**
  - Confidentiality
  - Integrity
  - Availability
  - Susceptibility
  - EMC Threats

- **EMC AND INFO. SEC.**
“Intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes”

Zurich EMC Symposium, February 1999
and IEC 61000-2-13:2005
## Classification of Effects

<table>
<thead>
<tr>
<th>Level</th>
<th>Effect</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>unknown</td>
<td>Unable to determine due to effects on another component or not observed.</td>
</tr>
<tr>
<td>N</td>
<td>no effect</td>
<td>No effect occurs or the system can fulfill his mission without disturbances.</td>
</tr>
<tr>
<td>I</td>
<td>interference</td>
<td>The appearing disturbance does not influence the main mission.</td>
</tr>
<tr>
<td>II</td>
<td>degradation</td>
<td>The appearing disturbance reduces the efficiency and capability of the system.</td>
</tr>
<tr>
<td>III</td>
<td>loss of main function</td>
<td>The appearing disturbance prevents that the system is able to fulfill its main function or mission.</td>
</tr>
</tbody>
</table>

*Source: Sabath et al, URSIGASS, 2008*
CLASSIFICATION OF EFFECTS

**Benefits:** fast application, classification is simple and easily applicable to any system.

**Drawbacks:** high level methodology, does not allow analyzing the effects induced by EM perturbations on each part of the system.

**Solutions:** recursive application of the last approach combined with « log events » profile of effects when the device is exposed to different IEMI attack scenarios - « behavioral analysis ».
Experiments: radiated case
EXPERIMENTS: CONDUCTED CASE

- Experiments: conducted case

![Diagram showing an experimental setup with a Faraday Cage, Power Network, Power Amplifier, Ethernet connections, and Signal frequencies CW: 100-1,000MHz and AM: 0001101001001]
EFFECTS ON IT SYSTEMS

- Effects on computers

```bash
input: PS/2 Generic Mouse as /devices/platform/i8042/serio1/input/input0
psmouse serio1: bad data from KBC - timeout
atkbd serio0: Unknown key pressed (translated set 2, code 0x9e on isa0060/serio0).
atkbd serio0: Use 'setkeycodes e01e <keycode>' to make it known.
psmouse serio1: alps: Unknown ALPS touchpad: E7=10 00 64, EC=10 00 64
psmouse serio1: bad data from KBC - timeout
```
EFFECTS ON IT SYSTEMS

- Effects on computers

---

PS/2 links errors

USB links errors

---

```
input: PS/2 Generic Mouse as /devices/platform/i8042/serio1/input/input0
serio1: bad data from KBC - timeout
serio1: Unknown key pressed (translated set 2, code 0x9e on isa0060/serio0).
ps2bd serio1: Use 'setkeycodes e00 9e keyname<keycode>' to make it known.

hub 1-0:1.0: port 1 disabled by hub (EMI?), re-enabling...
usb 1-1: reset full-speed USB device number 2 using uhci_hcd
usb 1-1: USB disconnect, device number 2
usb 1-1: USB disconnect, device number 3
usb 1-1: new low-speed USB device number 4 using uhci_hcd
usb 1-1: device descriptor read/64, error -71
usb 1-1: string descriptor 0 read error: -71
usbhid 1-1:1.0: can't add hid device: -71
usbhid: probe of 1-1:1.0 failed with error -71
usb 1-1: device not accepting address 5, error -71
hub 1-0:1.0: unable to enumerate USB device on port 1
usb 1-1: unable to read config index 0 descriptor/all
usb 1-1: can't read configura
---SYSTEM CRASH
```
EFFECTS ON IT SYSTEMS

- Effects on computers
EFFECTS ON IT SYSTEMS

- Effects on computers

![Graph showing CPU temperature over time with IEMI on and off events.]
IEMI effects exploitation: design of a covert channel
DESIGN OF A COVERT CHANNEL

- Hypothesis
- Channel coding
- Frame decomposition
- Results
HYPOTHESIS

- When field amplitude rises, measured temperature rises

<table>
<thead>
<tr>
<th>CW frequency (MHz)</th>
<th>Temperature reading error (°C)</th>
<th>Mean field strength required (V/m)</th>
<th>Additional effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>+5</td>
<td>35</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>+25</td>
<td>81</td>
<td>Fan speed increases</td>
</tr>
<tr>
<td>300</td>
<td>+5</td>
<td>23</td>
<td>no</td>
</tr>
</tbody>
</table>
|                   | +15                            | 33                                | Fan speed increases
|                   |                                 |                                   | Network interface down |
|                   | +25                            | 65                                | Computer reboots |
| 600               | +5                             | 31                                | no                |
|                   | +25                            | 50                                | Fan speed increases |
We can use this to send information
 CHANNEL CODING

➢ Channel coding, need for a robust channel encoding scheme for the C&C:
   - Data encoding ?
   - With/without synchronization ?
   - Data integrity correction ?

➢ Transmission imposed by IEMI effects:
   - ASK-modulation scheme
     - ON/OFF shift keying
Needs for a robust encoding scheme

- Time needed to query sensors isn’t constant, the sampling of temperature has some jitter.
- Manchester coding makes clock recovery easier because there is a transition for each bit transmitted.
- The clock must have a frequency twice higher than the bit-rate and the bit sequence is \textit{XOR}ed with the clock sequence.
- As a consequence, the clock is included in the signal with the data.
**FRAME STRUCTURE**

- **Frame decomposition**

<table>
<thead>
<tr>
<th>Offset in bits</th>
<th>0</th>
<th>8</th>
<th>16</th>
<th>N*8+16</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Content</strong></td>
<td>Preamble</td>
<td>Size (N)</td>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>

- **Preamble with good auto-correlation properties**
  - Barker sequence (Bluetooth): 7 bits ‘1110010’ + prepended ‘0’
- **‘0’ vs ‘1’ reading**
  - $T_c > 1.05 \times \text{mean}(\text{Temp}) \Rightarrow \text{‘1’}$
- **1 bit is obtained with 4 measures** (sampling theorem)
RESULTS

Results
RESULTS

- Low power required for the conducted case
- Extension of the communication range thanks to the good propagation medium at HF;
- Bit-rate expected: 2.5 bits/s
## RESULTS

<table>
<thead>
<tr>
<th>Method</th>
<th>Transmitter</th>
<th>Receiver</th>
<th>Direction*</th>
<th>Distance (m)</th>
<th>Rate (bit/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirHopper</td>
<td>Display cable</td>
<td>FM receiver</td>
<td>Out</td>
<td>7</td>
<td>480</td>
</tr>
<tr>
<td>Ultrasonic</td>
<td>Speaker</td>
<td>Mic</td>
<td>In-Out</td>
<td>19.7</td>
<td>20</td>
</tr>
<tr>
<td>GSMem</td>
<td>RAM bus</td>
<td>GSM baseband</td>
<td>Out</td>
<td>5.5</td>
<td>2</td>
</tr>
<tr>
<td>GSMem</td>
<td>RAM bus</td>
<td>Dedicated equipment</td>
<td>Out</td>
<td>30+</td>
<td>100-1000</td>
</tr>
<tr>
<td>BitWhisper</td>
<td>CPU/GPU Heating system</td>
<td>Heat Sensor</td>
<td>In-Out</td>
<td>0.4</td>
<td>0.002 (8 bits/hour)</td>
</tr>
<tr>
<td>Our method</td>
<td>SDR + amplifier</td>
<td>Heat Sensor</td>
<td>In</td>
<td>5+ /30+</td>
<td>2.5</td>
</tr>
</tbody>
</table>

* In: Data sent to the target  
  Out: Data sent by the target
Recommandations
ADMINISTRATORS

- Remove any unneeded analog or digital IO interface
- Monitor the remaining ones
- Isolate the critical machines accordingly to risk analysis
  - Co localization with untrusted devices admissible?
  - Dedicated room, blind, faradized, filtered power network, anechoic
- Educate the users
Follow the rules, even if constraining

The Air Gap robustness relies on your behavior

- Avoid preliminary infection
- Don’t change/add peripherals without permission

Should not be a reason to deceive

« oh whatever, it’s disconnected from the network… so I can charge my phone/plug my USB drive/share my display/add a KVM switch… »
Send / Receive capabilities discovery:
- Hardware identification
- Interfaces / Sensors enumeration and instrumentation

PHY communication protocol:
- Modulation/Demodulation
- Preamble detection
- Encoding/Decoding
- Error correction
- Packet/Frame parsing
Results presented are related to specific conditions (PoC + tests)

- Physical medium choices
- Transmission choices (modulation…)
- Target capabilities (sensors sensitivity…)
- Scenario topology (line of sight…)

Lack of common metrics to compare techniques (range and bitrate insufficient)

Hard to evaluate in risk analyses
Conclusion
CONCLUSION

➢ New technique for command channel for air gapped computer malware
  ❑ Improved range and bitrate regarding state of the art

➢ Smart IEMI can be an efficient attack vector against information systems
  ❑ Not limited to DoS
  ❑ More and more affordable (SDR…)

➢ Take it into account for risk analysis
CONCLUSION

- Air Gap can be really efficient, but
- It is very constraining
  - Money, security policy, work processes
- It is very fragile
  - Relies on good security policy enforcement
  - Security overestimated
  - Constraints lead to deception
- And still can be bypassed
  - Active research topic
  - But high attacker profile
References
REFERENCES

QUESTIONS ?

- Chaouki Kasmi, chaouki.kasmi@ssi.gouv.fr
- Jose Lopes Esteves, jose.lopes-esteves@ssi.gouv.fr
- Philippe Valembois, philippe.valembois@ssi.gouv.fr