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

Chaouki KASMI, José LOPES ESTEVES,

Philippe VALEMBOIS

BotConf- 04/12/2015

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

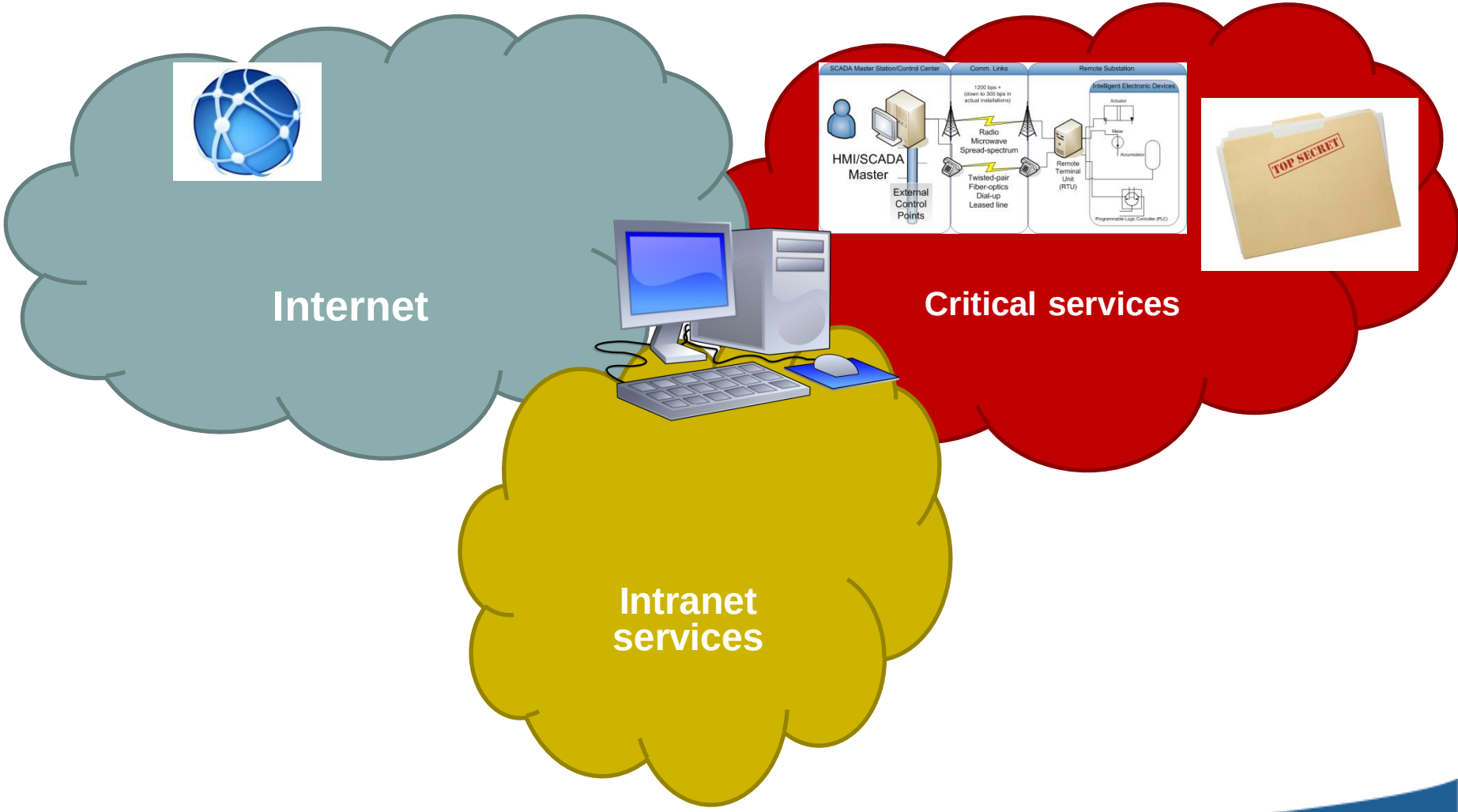
Air Gap Principles

...

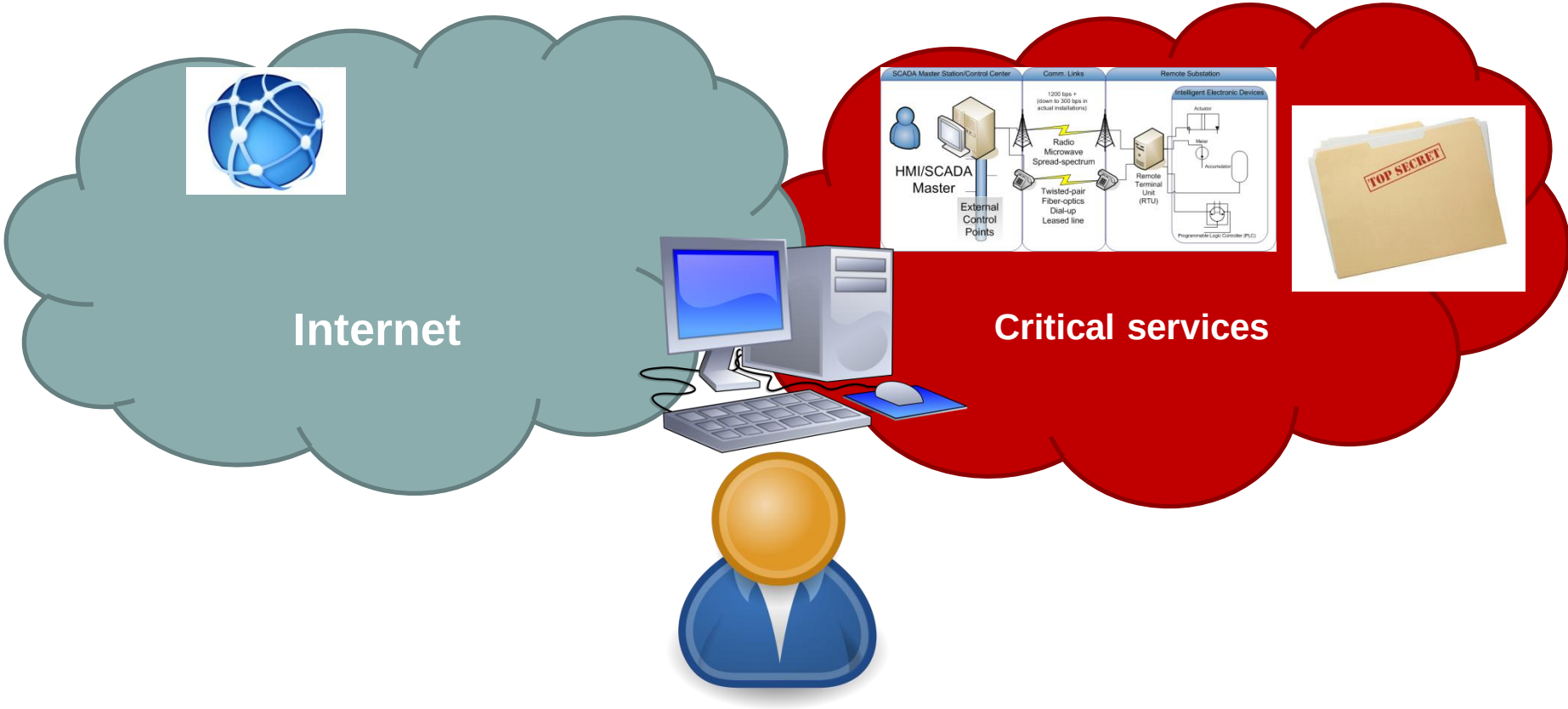
CONTEXT

- 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

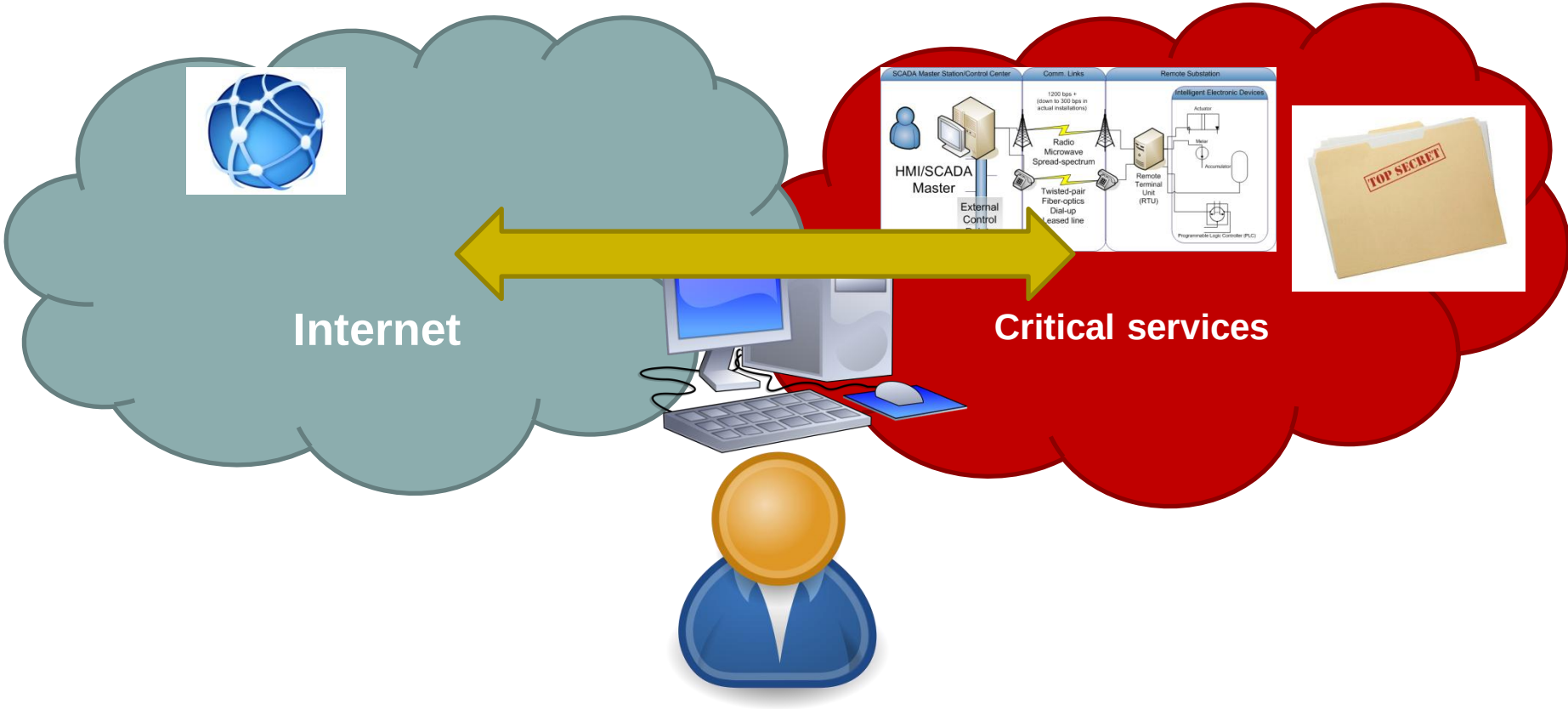
CONTEXT


Internet
SCADA Master Station/Control Center
Comm. Links
Remote Substation
Intelligent Electronic Devices
HMI/SCADA Master
External Control Points
Radio
Microwave
Spread-spectrum
Twisted-pair
Fiber-optics
Dial-up
Leased line
Remote Terminal Unit (RTU)
TOP SECRET
Critical services
Intranet services

CONTEXT


Internet
SCADA Master Station/Control Center
Comm. Links
Remote Substation
Intelligent Electronic Devices
HMI/SCADA
Master
External
Control
Points
Radio
Microwave
Spread-spectrum
Twisted-pair
Fiber-optics
Dial-up
Leased line
Remote
Terminal
Unit
(RTU)
TOP SECRET
Critical services

CONTEXT

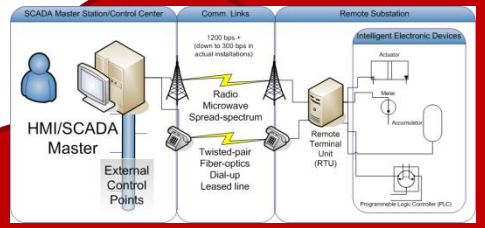

Internet
Critical services
SCADA Master Station/Control Center
Comm. Links
Remote Substation
HMI/SCADA
Master
External
Control
Radio
Microwave
Spread-spectrum
Twisted-pair
Fiber-optics
Dial-up
Leased line
Intelligent Electronic Devices
Remote
Terminal
Unit
(RTU)
TOP SECRET

CONTEXT

Internet

A
I
R

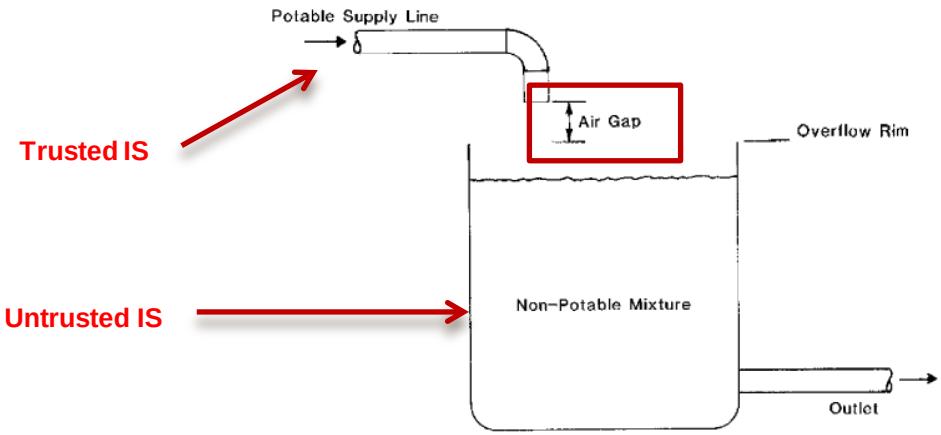
G
A
P



Critical services

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



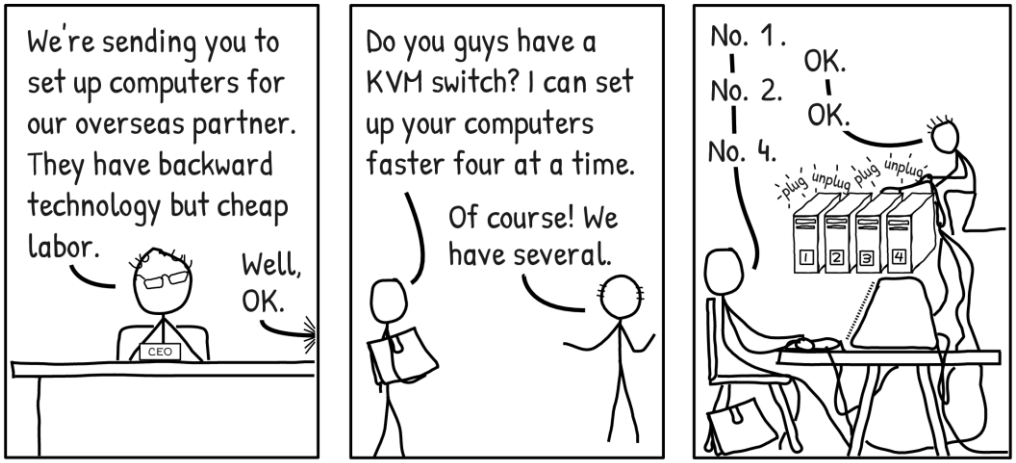
DRAWBACKS

- 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

Image: bangkokpost.com

Image: visualphotoscom



KVM Switch.

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

AIR GAP BRIDGING

- 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

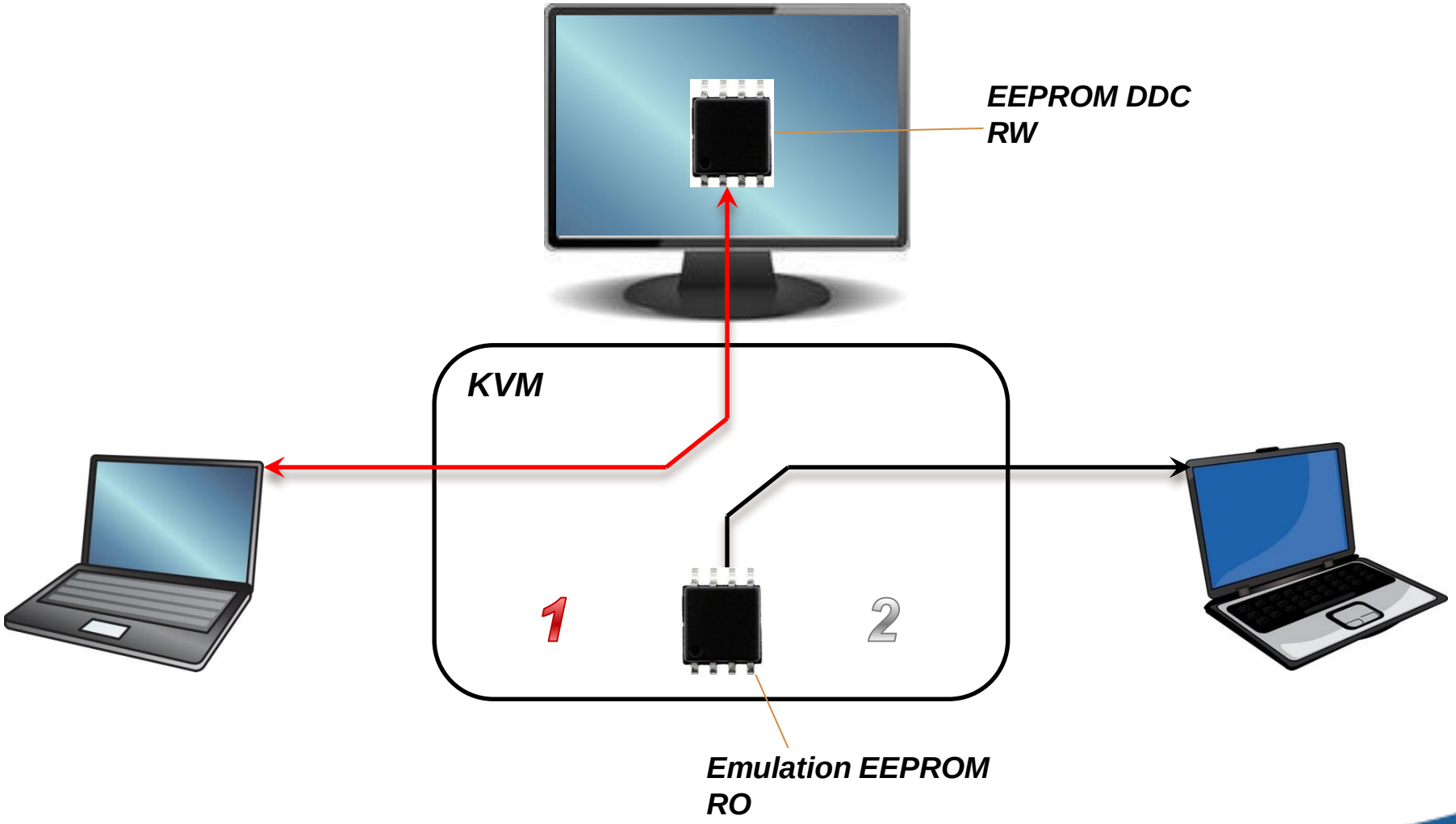
USING DISABLED INTERFACES

- 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

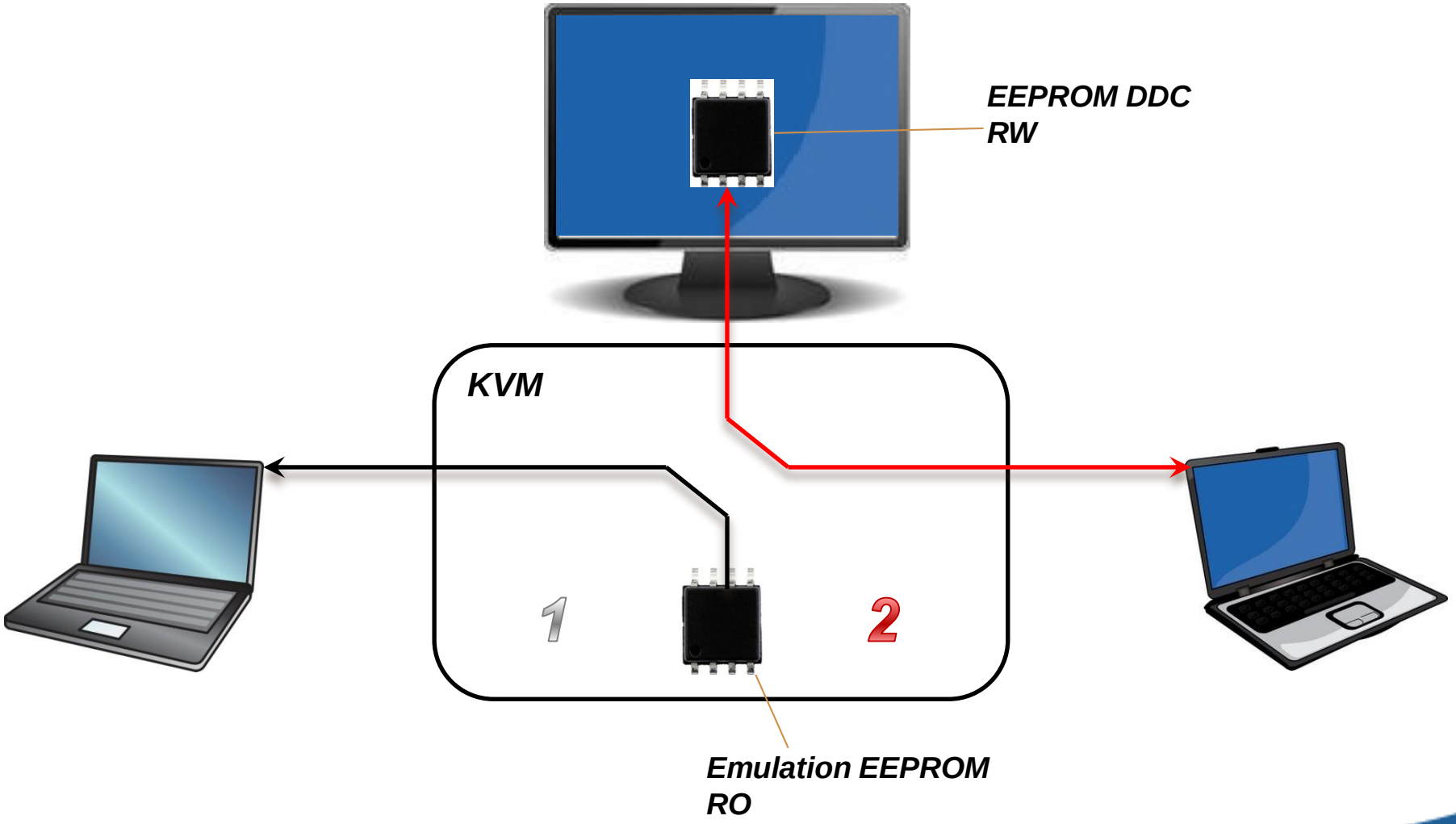
USING SHARED PERIPHERALS

- 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

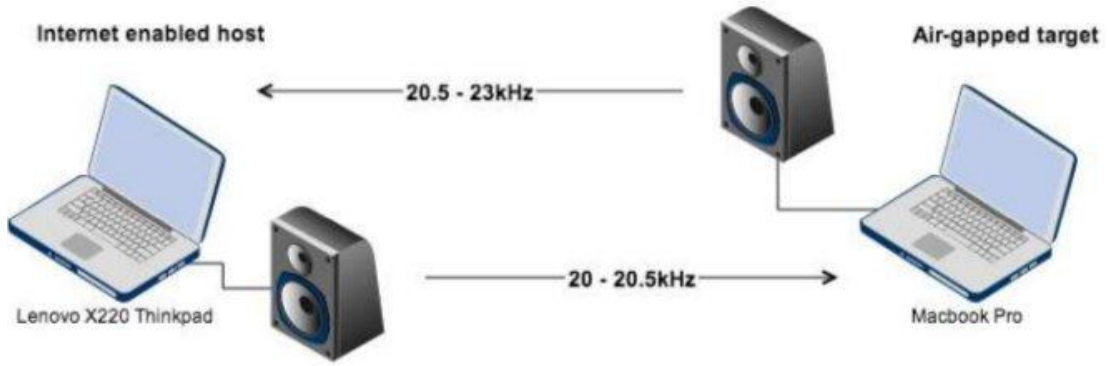


USING SHARED PERIPHERALS



USING MECHANICAL WAVES

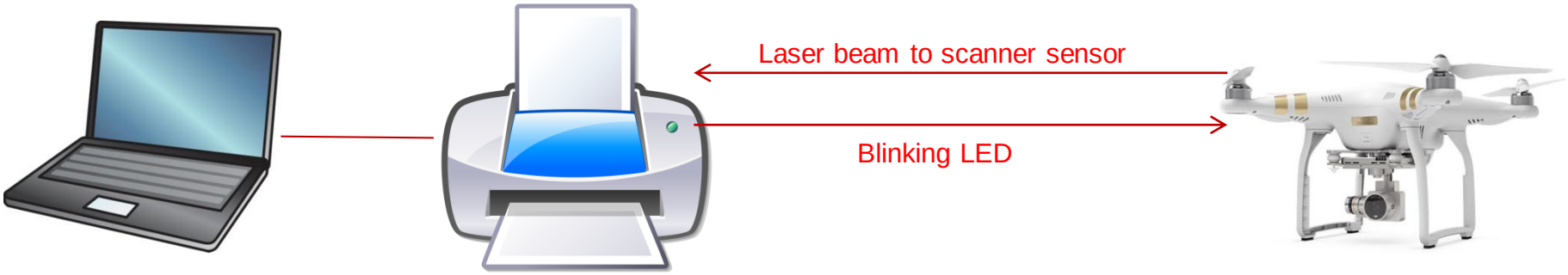
- Sound / vibrations:
  - Google Tone [2], Ultrasound [3][4], Cross-Device Tracking
  - Sender controls sound source (audio output, fan speed, *emanations from internal components* [5]…)
  - Receiver controls audio input, gyroscope [6]…



Bi-directional audio covert channel, from [3]

USING LIGHT

- Shamir, BHUSA keynote [7]:
  - Sender controls light source (display, LEDs, smart light bulbs…)
  - Receiver controls light sensor (video camera, scanner…)



USING TEMPERATURE

- BitWhisper [8]:
  - Sender controls temperature (heating system, thermostat, CPU activity…)
  - Receiver controls temperature sensor

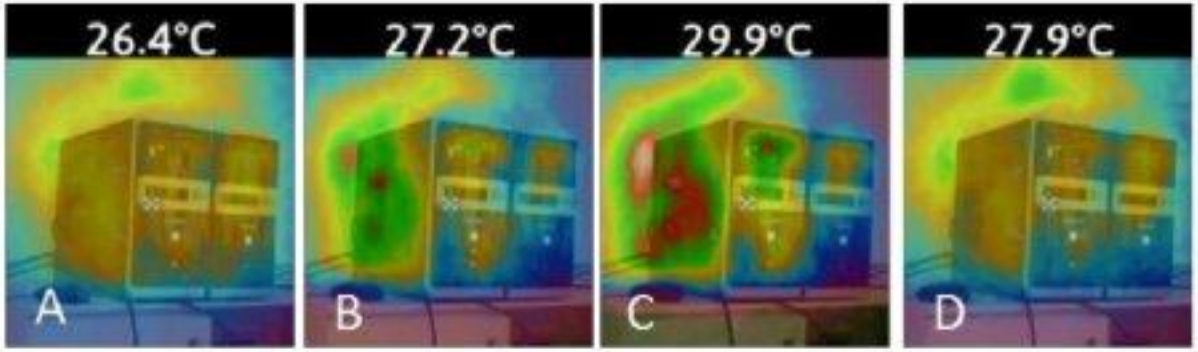


Figure 1. A "thermal ping" sent between two adjacent PCs. The snapshots were taken by using a thermal camera.

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

SUMMARY

Method	Transmitter	Receiver	Direction*	Distance (m)	Rate (bit/s)
AirHopper	Display cable	FM receiver	Out	7	480
Ultrasonic	Speaker	Mic	In-Out	19.7	20
GSMem	RAM bus	GSM baseband	Out	5.5	2
GSMem	RAM bus	Dedicated equipment	Out	30+	100-1000
BitWhisper	CPU/GPU Heating system	Heat Sensor	In-Out	0.4	0.002 (8 bits/hour)

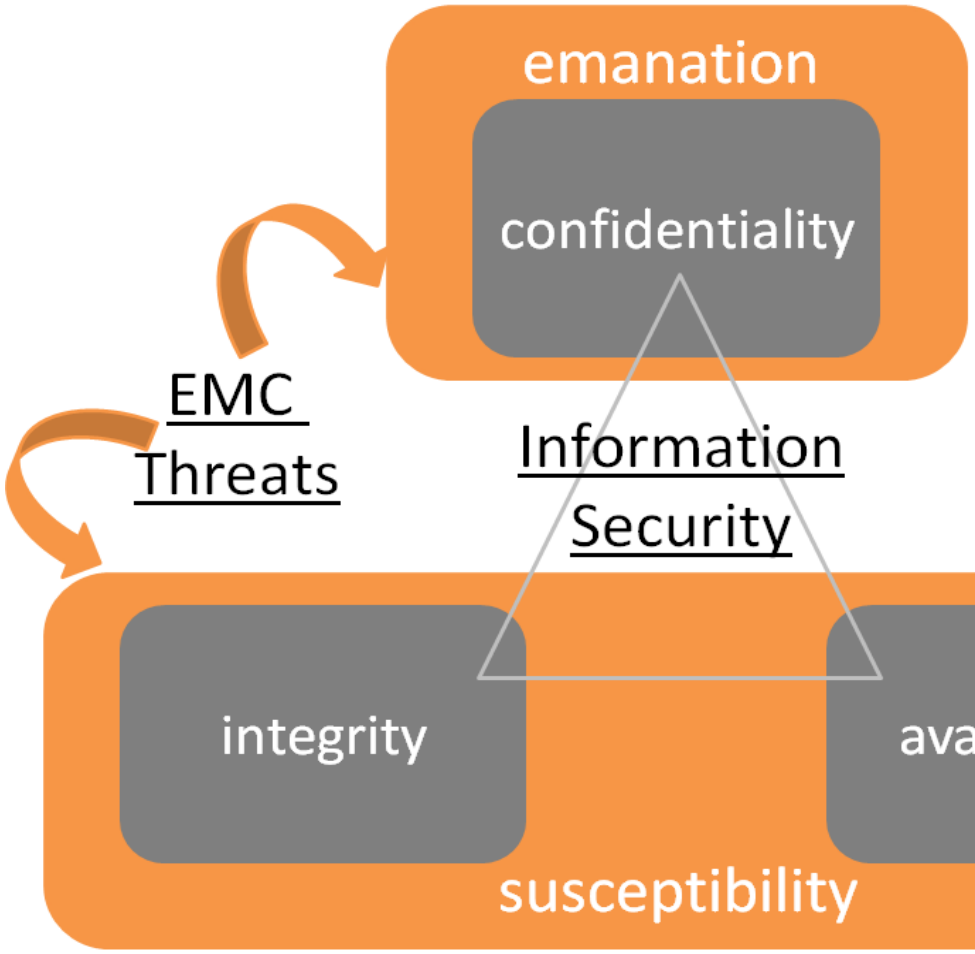
*** In: Data sent to the target**
Out : Data sent by the target

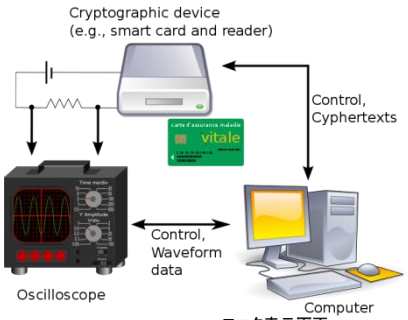
Intentional Electromagnetic Interference

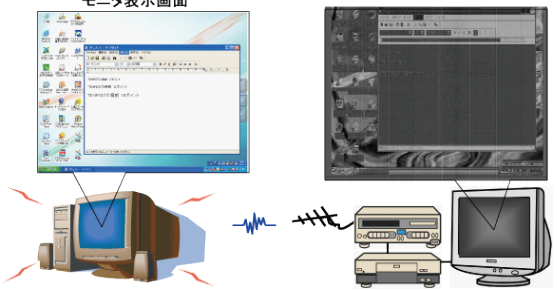
INTENTIONAL EM INTERFERENCE

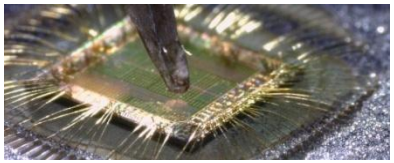
- Electromagnetic Compatibility and Info. Sec.
- IEMI, definition
- Classification of effects
- Effects on IT systems and Experimental results

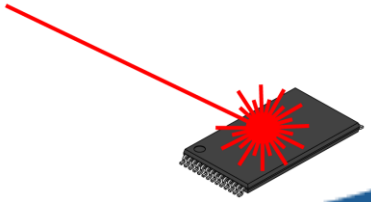
EMC AND INFO. SEC.





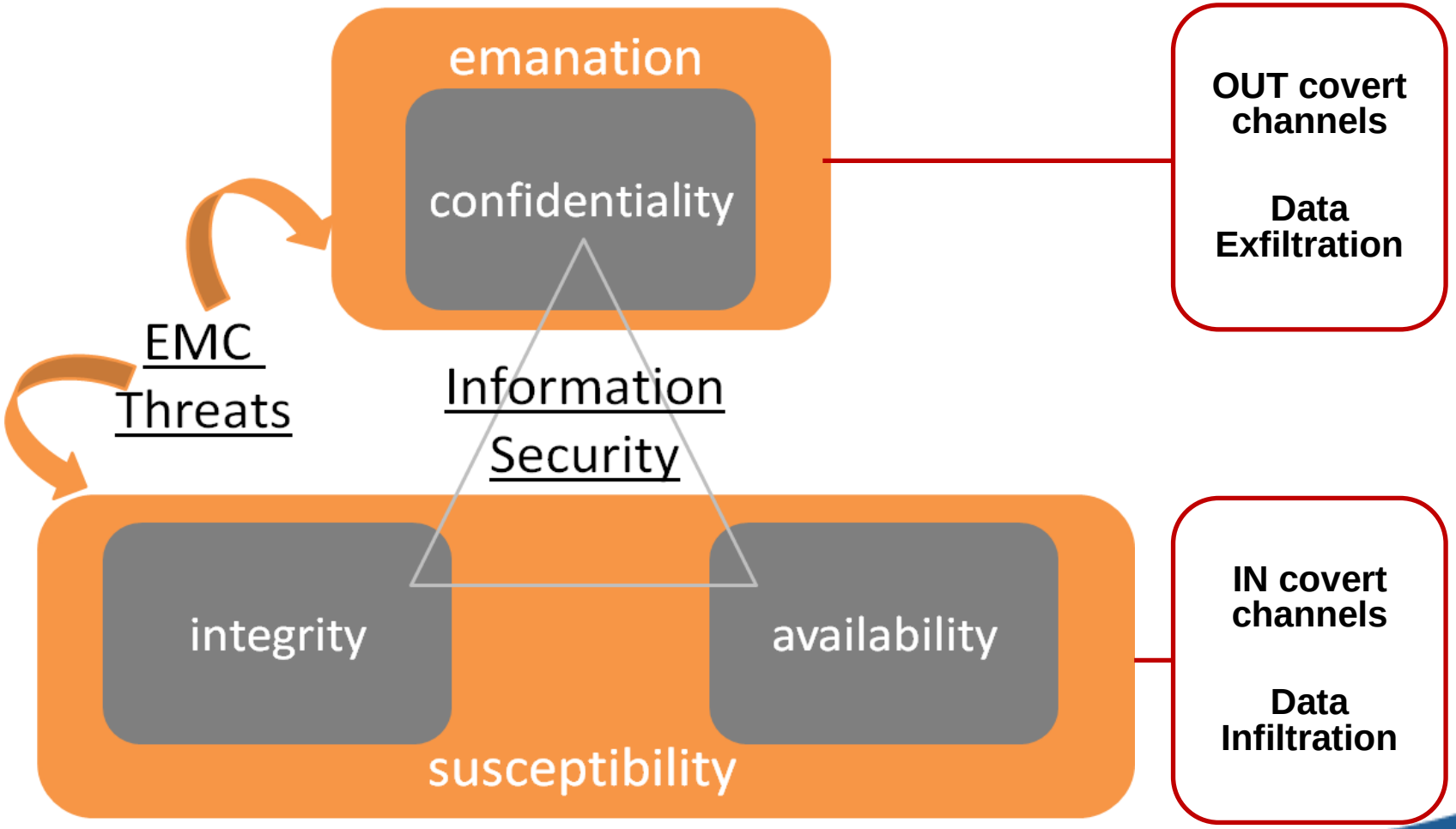






Pictures from aisec.fraunhofer.de, emsec.rub.de, climateviewer.com, wikipedia.com

EMC AND INFO. SEC.



IEMI, DEFINITION

“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

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

Source: Sabath et al, URSIGASS, 2008

CLASSIFICATION OF EFFECTS

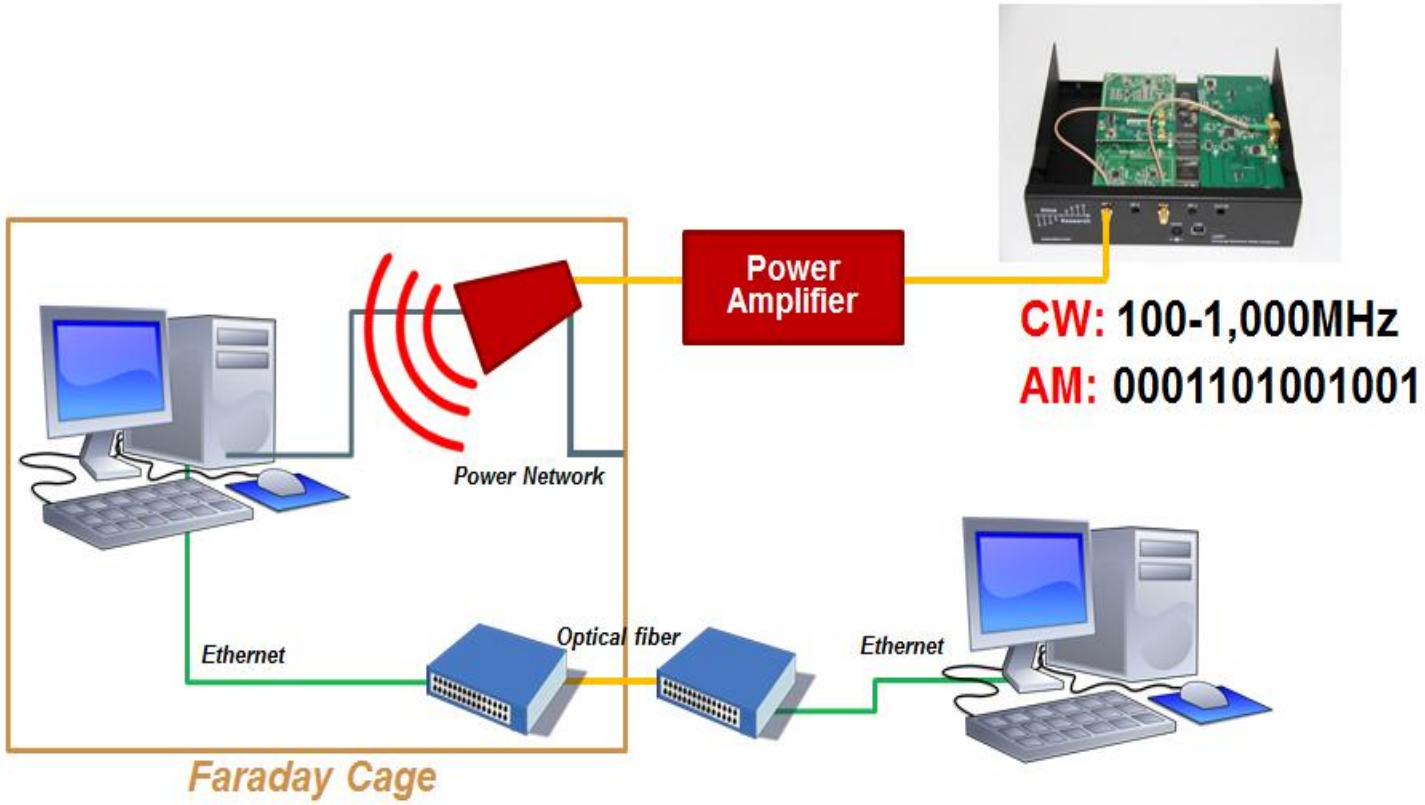
Benefits: fast application, classification is simple and easily applicable to any system.

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 ».

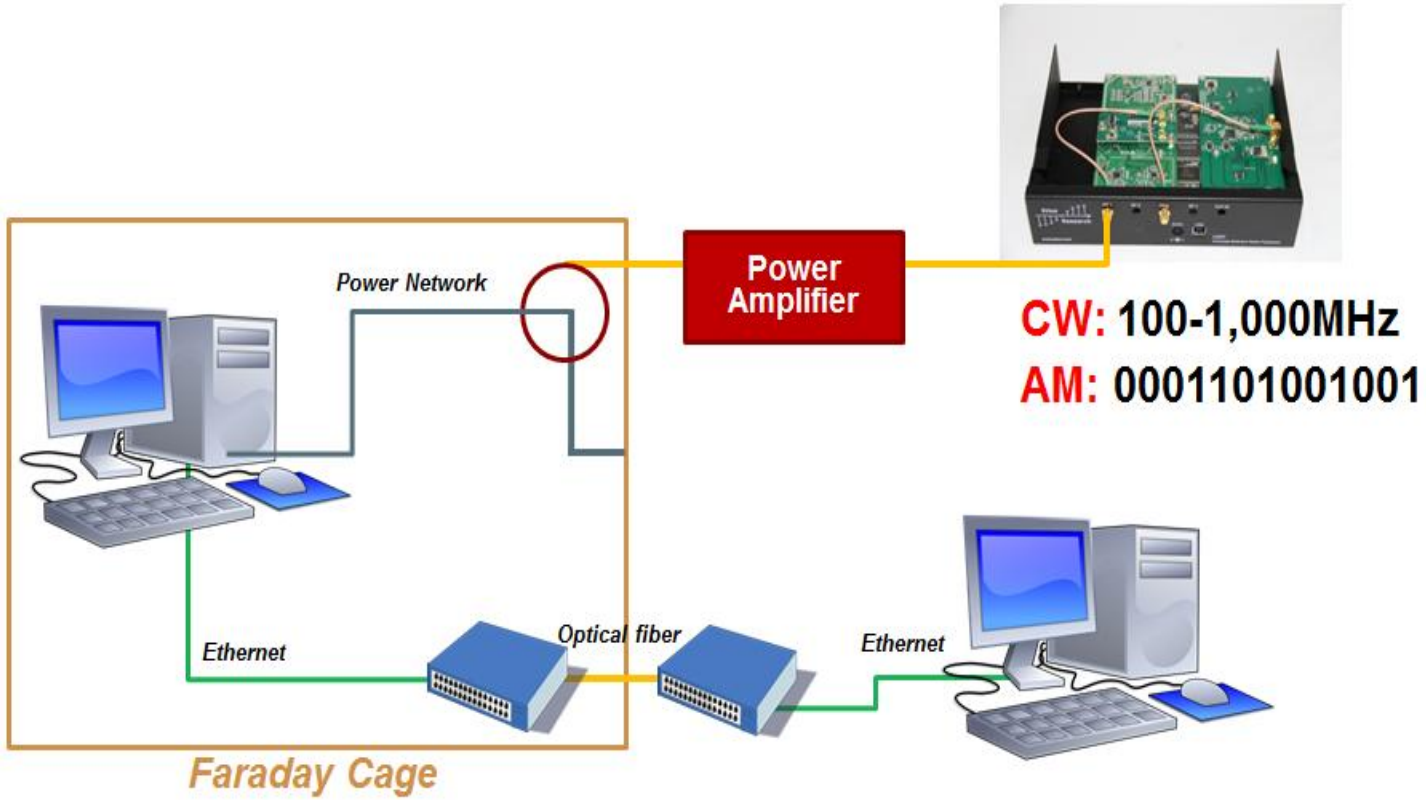
EXPERIMENTS: RADIATED CASE

- Experiments: radiated case



EXPERIMENTS: CONDUCTED CASE

- Experiments: conducted case



EFFECTS ON IT SYSTEMS

- Effects on computers

PS/2 links errors

```
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

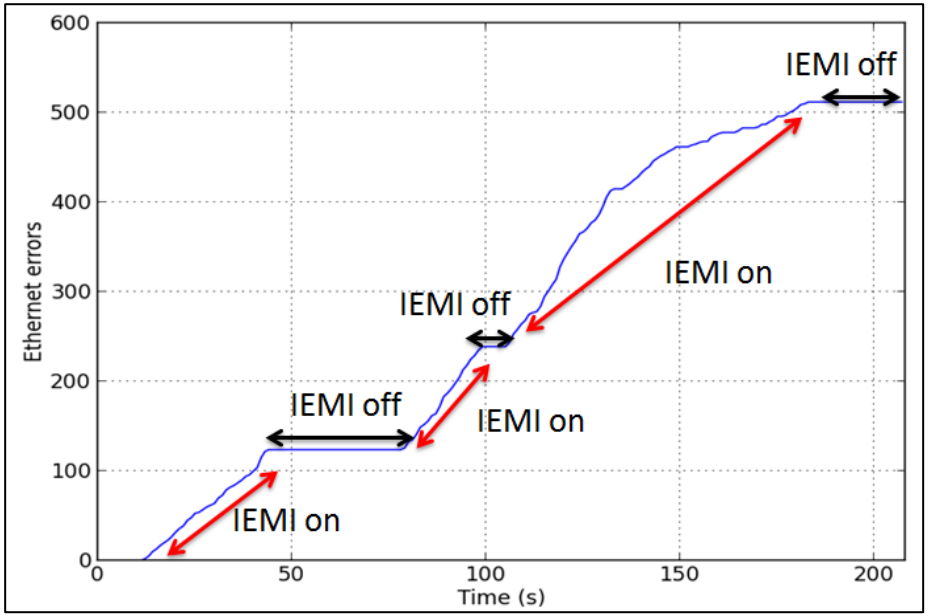
```
input: PS/2 Generic Mouse as /devices/platform/i8042/serio1/input/input0
erio1: bad data from KBC - timeout
io0: Unknown key pressed (translated set 2, code 0x9e on isa0060/serio0).
atkbd serio0: Use 'setkeycodes e01e <keycode>' to make it known.
ad: E7=10 00 64, EC=10 00 64
ut
```

USB links errors

```
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
```

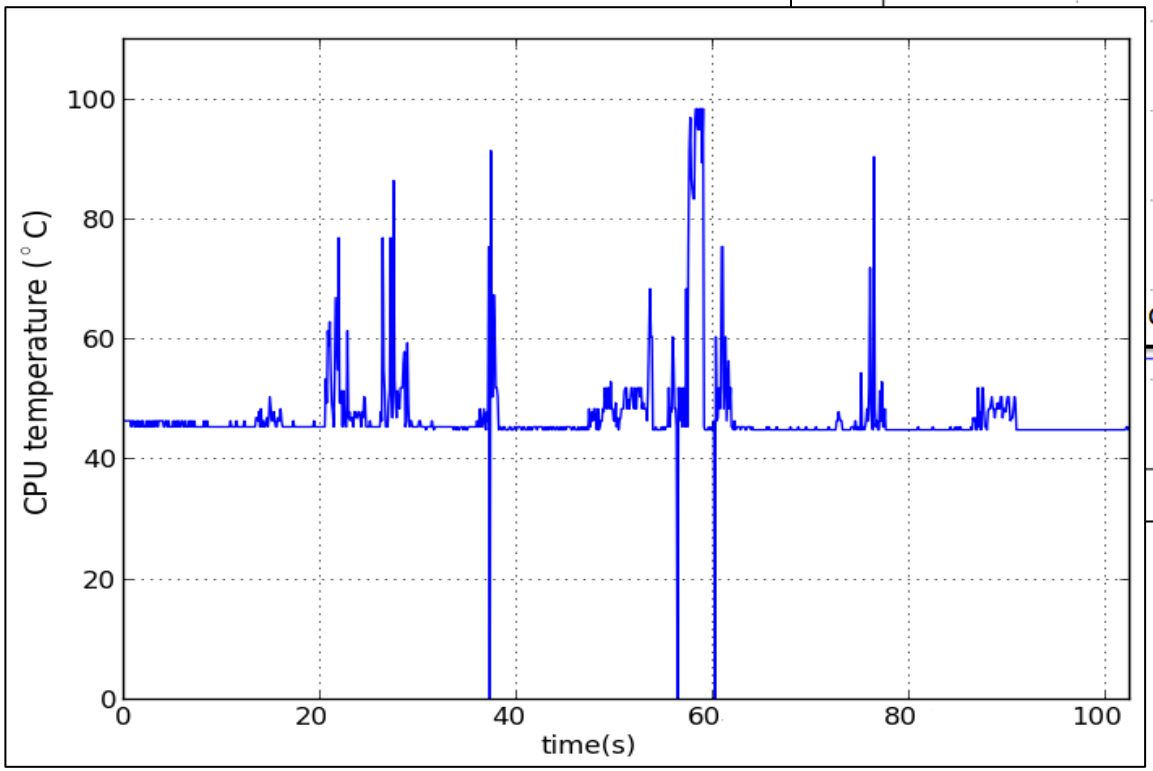
EFFECTS ON IT SYSTEMS

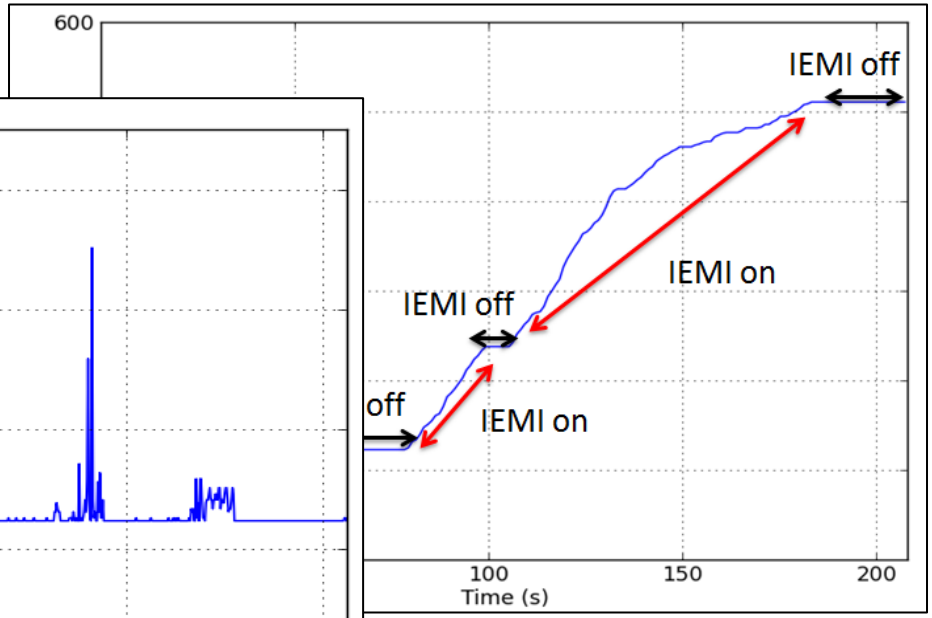
- Effects on computers



EFFECTS ON IT SYSTEMS

- Effects on computers





IEMI effects exploitation: design of a covert channel

DESIGN OF A COVERT CHANNEL

- Hypothesis
- Channel coding
- Frame decomposition
- Results

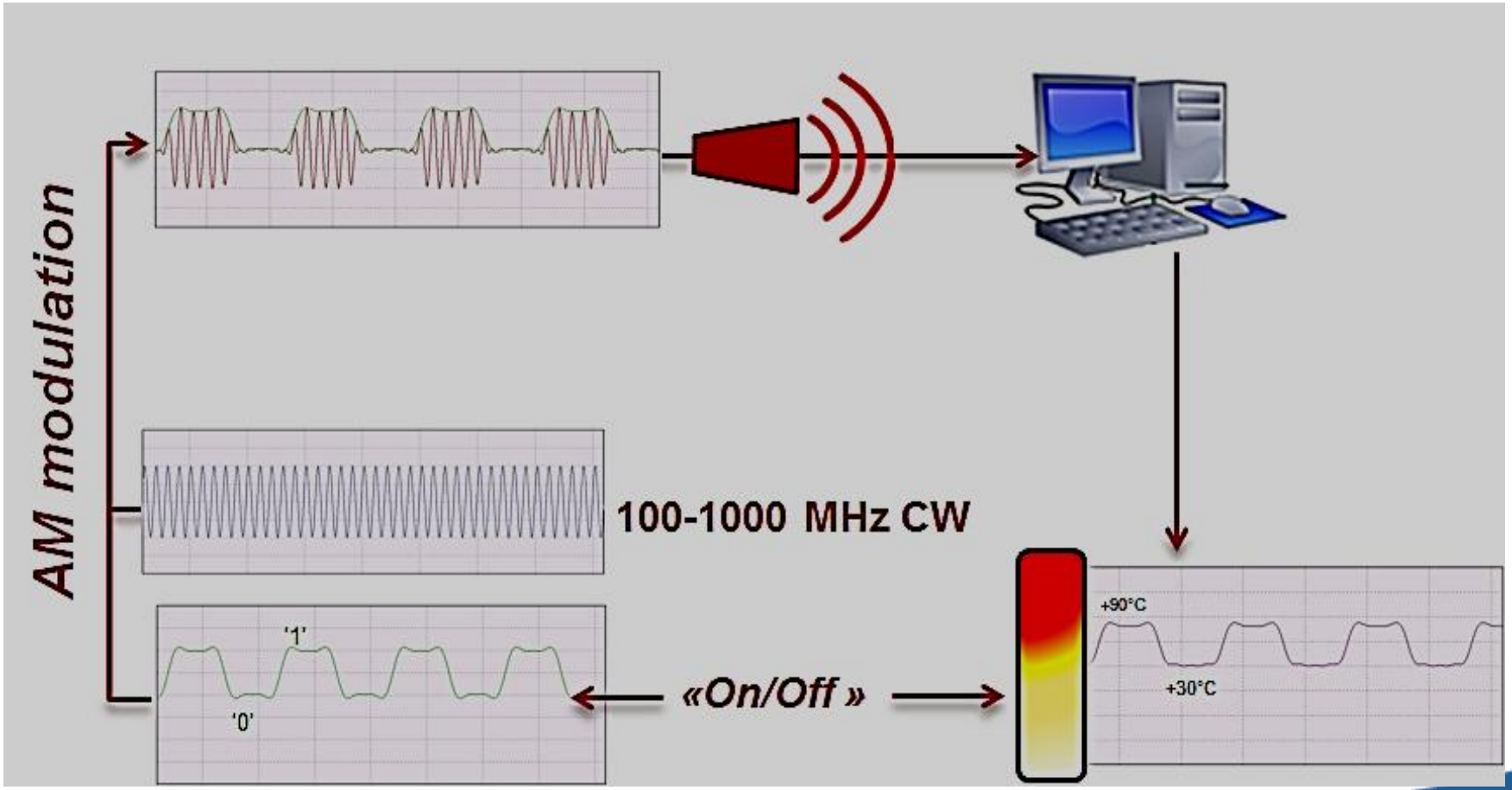
HYPOTHESIS

- When field amplitude rises, measured temperature rises

CW frequency (MHz)	Temperature reading error (°C)	Mean field strength required (V/m)	Additional effects
200	+5	35	no
	+25	81	Fan speed increases
300	+5	23	no
	+15	33	Fan speed increases Network interface down
	+25	65	Computer reboots
600	+5	31	no
	+25	50	Fan speed increases

HYPOTHESIS

- 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

MANCHESTER ENCODING

- 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 *XORed* with the clock sequence.
  - As a consequence, the clock is included in the signal with the data.

FRAME STRUCTURE

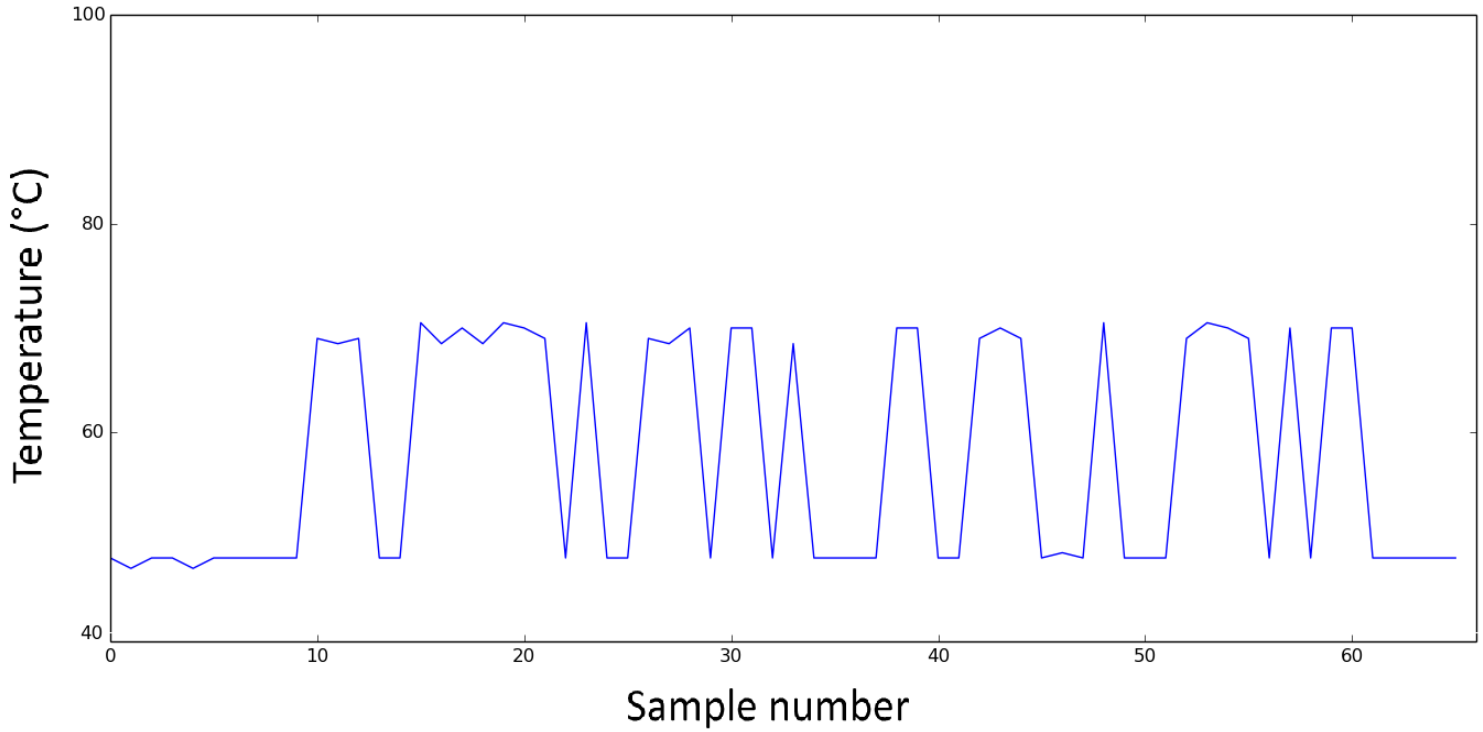
- Frame decomposition

Offset in bits	0	8	16	N*8+16
Content	Preamble	Size (N)	Data	

- Preamble with good auto-correlation properties
  - Barker sequence (Bluetooth): 7 bits ‘1110010’ + prepended ‘0’
- ‘0’ vs ‘1’ reading
  - Tc > 1.05*mean(Temp) → ‘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

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

*** 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

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… »

REVERSERS/ANALYSTS

- 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

RESEARCHERS

- 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

[1] M.Shkatov, J.Michael, *The hidden dangers inside the platform*, HackitoErgoSum, 2015

[2] A. Kaufmann, B. Smus, *Tone: An experimental Chrome extension for instant sharing over audio*, Google Research Blog, 2015

[3] S. J. O'Malley, K. K. R. Choo, *Bridging the Air Gap: Inaudible Data Exfiltration by Insiders*, 20th Americas Conference on Information Systems, 2014

[4] M. Hanspach et al., *On Covert Acoustical Mesh Networks in Air*. Journal of Communications, vol. 8, no. 11, 2013

[5] D. Genkin, A. Shamir, E. Tromer, *RSA Key Extraction via Low-Bandwith Acoustic Cryptanalysis*, Advances in Cryptology – CRYPTO 2014.

[6] Y. Michalevsky, G. Nakibly, D. Boneh, *Gyrophone: Recognizing Speech from Gyroscope Signals*, RSA Conference 2015, 2015

[7] A. Shamir, *Side Channel Attacks - Past, Present and Future*, BlackHat Europe, 2014

[8] M. Guri et al.: *BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations*, 2015

[9] A. Cui, M. Costello, *Hacking Cisco Phones*, CCC conference 29C3, Hamburg, Germany, 2012.

[10] M. Guri et al., *AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies*, 9th IEEE International Conference on Malicious and Unwanted Software, 2014.

[11] M. Guri et al., GSMem: Data Exfiltration fromAir-Gapped Computers over GSM Frequencies, USENIX Security 15, 2015

Thank You

QUESTIONS ?

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