Διαδίκτυο των Πραγμάτων (IoT): Το πεδίο των απειλών
The Internet of Things: A challenging threat landscape

Panayiotis Kotzanikolaou (Assist.Prof.), *Ioannis Stellios* (PhD cand.)
Department of Informatics, University of Piraeus, Greece

Presentation at CIE 2017 - University of Piraeus – October 2017

Presentation Outline

1. Introduction
2. IoT threat modeling: A generic approach
3. Analysis of real/verified IoT-enabled attacks in IoT sectors
    - *Intelligent Transportation Systems*
    - *Medical sector*
    - *Industrial SCADA*
    - *Smart Grids*
    - *Smart home*
4. Conclusions

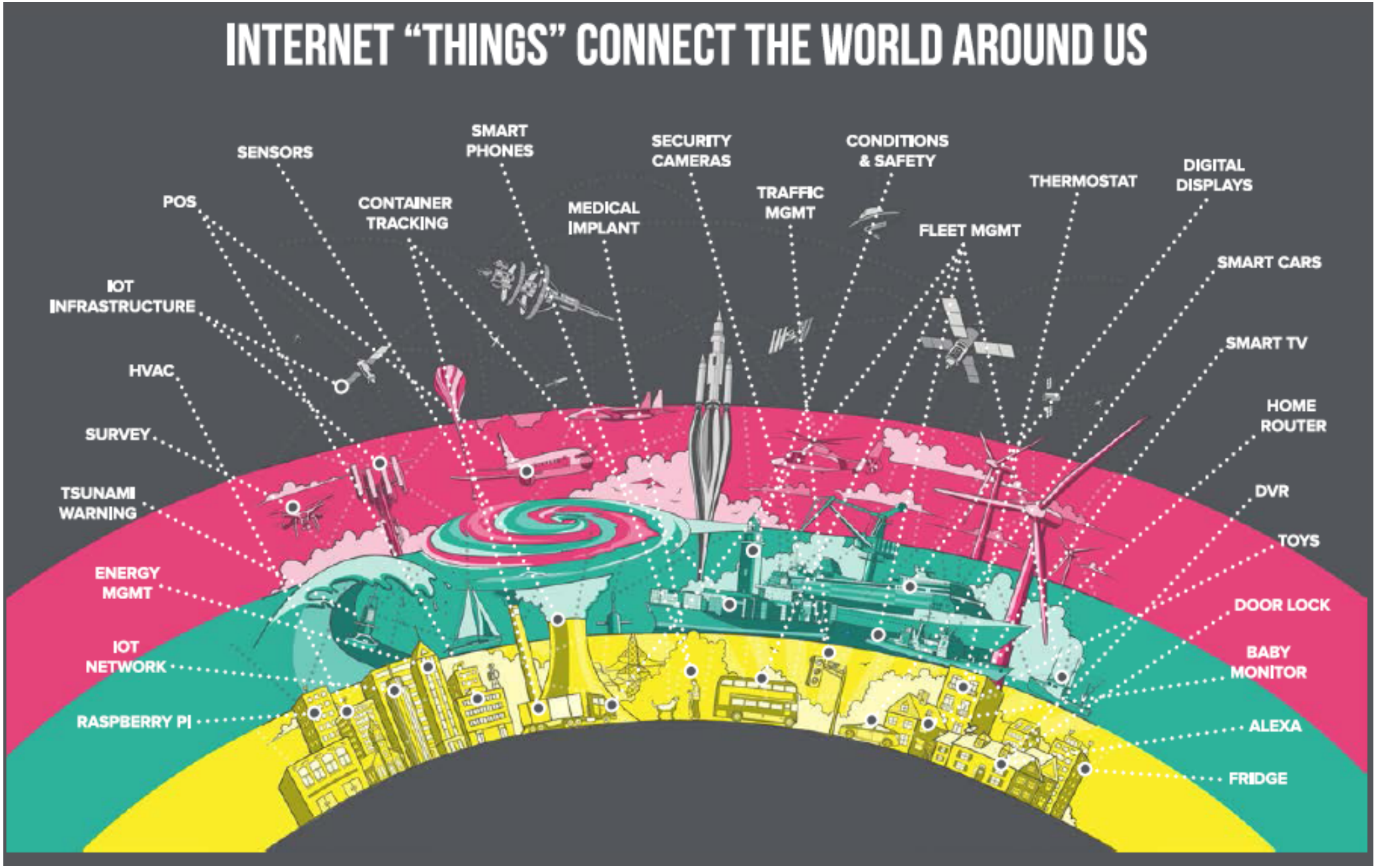
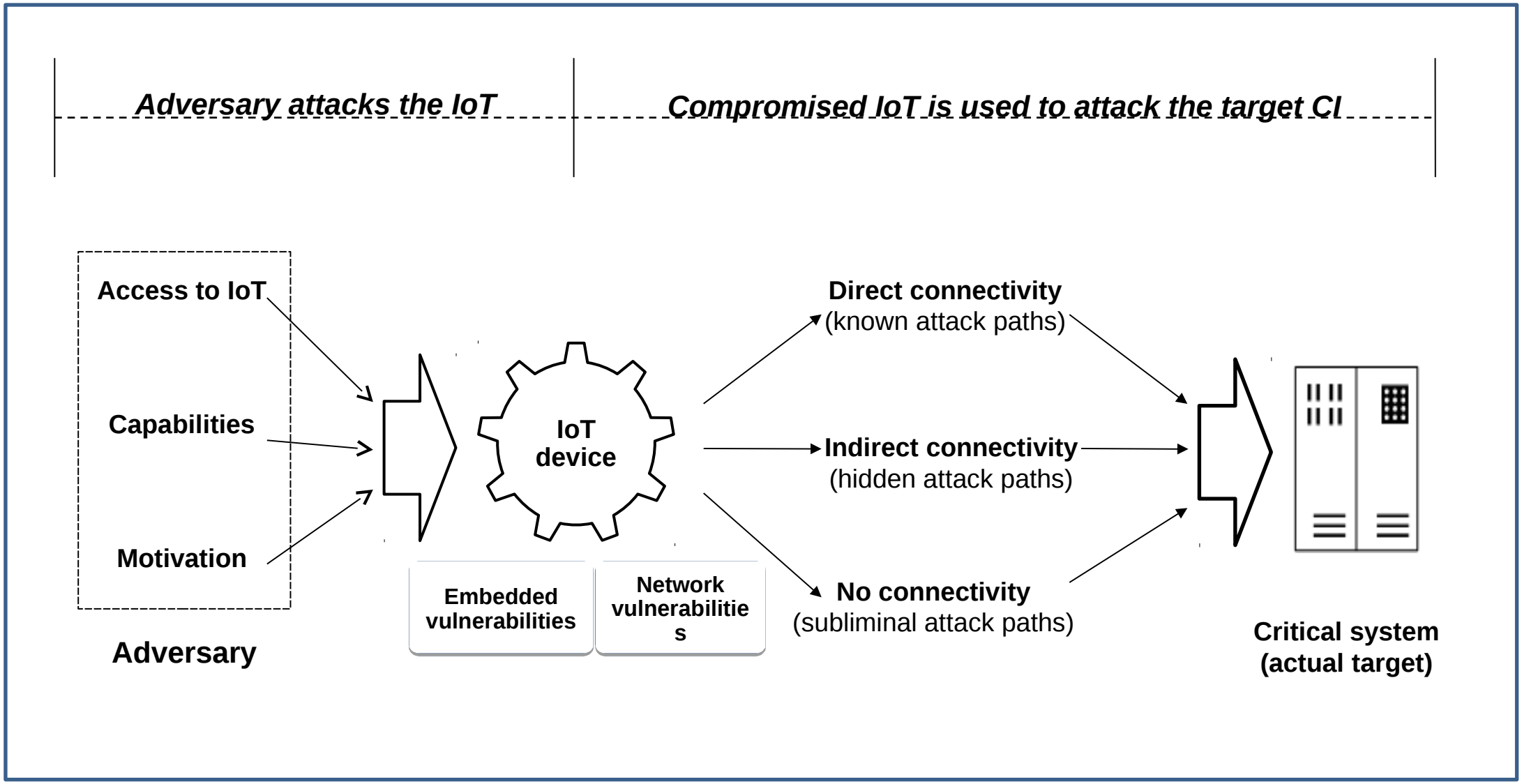


Figure source. "*The hunt for IoT: The rise of the thingbots*", *F5 Labs 2017 Report*

Security-related facts about IoT

- **Installed in Cyber-Physical systems**
  - Industrial systems, cars, smart grids, humans….
- **There are too many (and they grow very fast)**
  - **50 billion devices by 2020**
- **Technologies are not standardized**
  - Diversity in H/W (ARM, x86, x64,…)
  - Diversity in S/W (CoAP, proprietary,…)
  - Diversity in network protocols (802.15.x, 802.11.x, Ethernet, Modbus, proprietary…).
- **They create various connectivity paths (not always obvious)**
  - Local connections
  - Internet connections
- **IoT are used as attack enablers/amplifiers against other systems**
  - **Usually far more important**

Modeling IoT-enabled cyber attacks

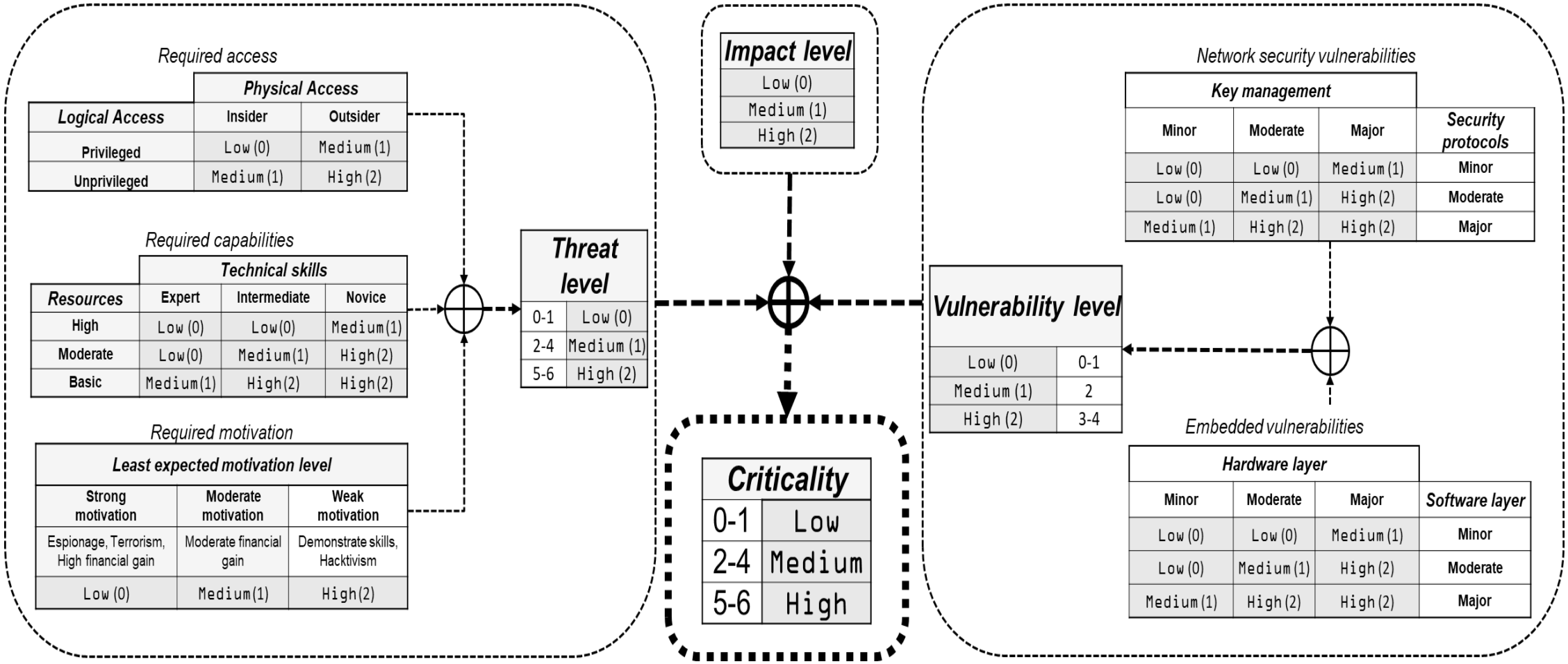


Assessing IoT-enabled Cyber Attacks: A risk-based approach

Criticality = Threat ⊗ Vulnerability ⊗ Impact

- **Threat Level:** Based on characteristics of the adversary
- **Vulnerability level:** Based on embedded and network layer vulnerabilities of the attack enablers (IoT devices)
- **Impact level:** Based on the Impact of possible targets, connected in some way with the IoT device

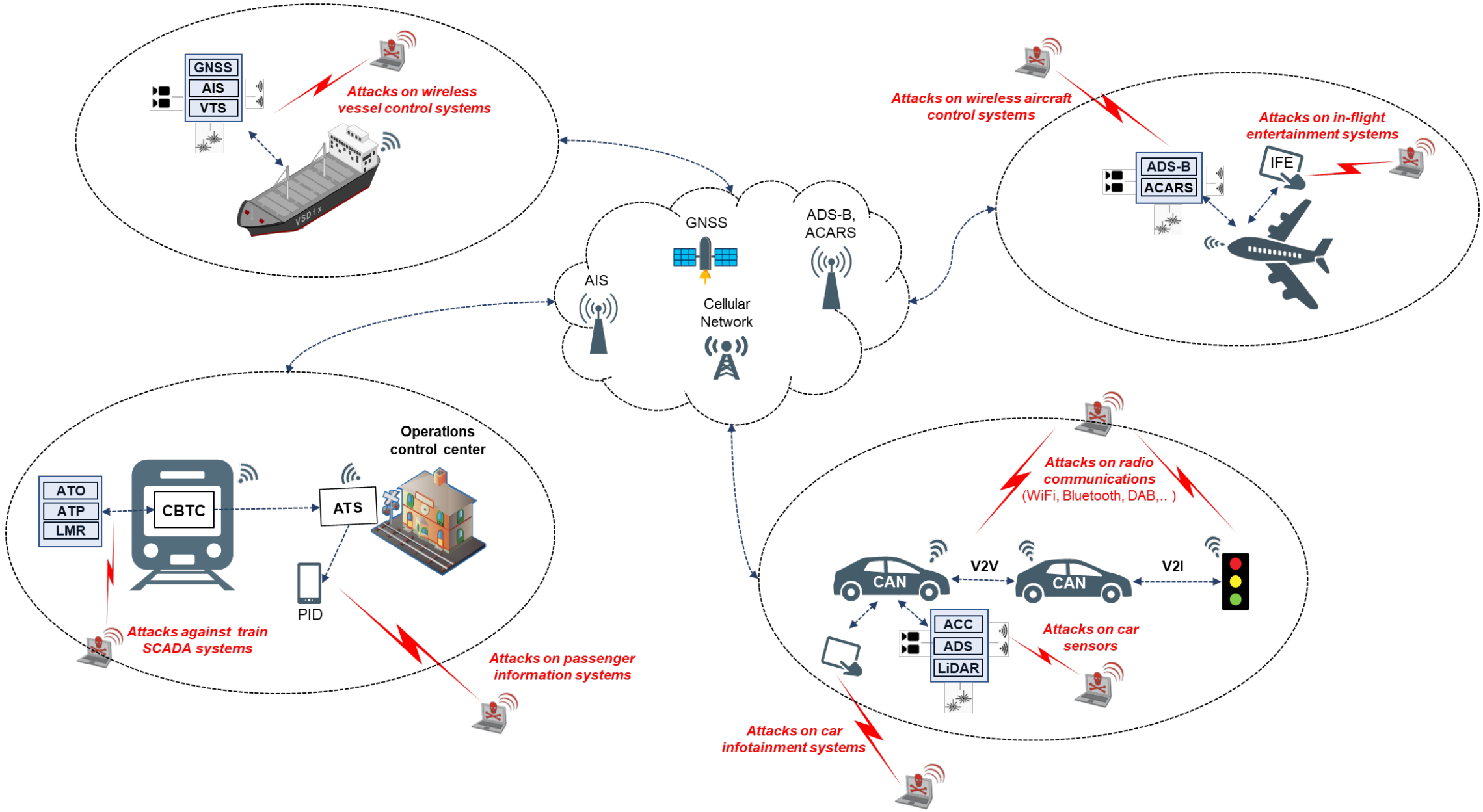
Assessing IoT-enabled Cyber Attacks



Analysis of IoT enabled attacks

- Use the risk-based methodology to assess real incidents or verified proof of concept (PoC) attacks
- We examine more than 50 recent attacks in various IoT sectors
- For each attack we describe the attack vectors and we assess their criticality level based on real/realistic data

ITS infrastructure and relative IoT-enabled attacks



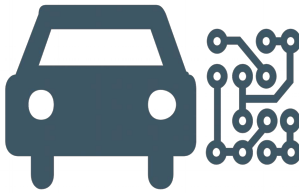
Control of a car from the Internet

Attack example [1]: *Take control of cars through the Internet, by **abusing the car Infotainment system** (PoC by security researchers on Cherokee Jeep, 2015)*

Attack vector

1. Connect to the Infotainment through an **open port** (discovered in a certain provider)
2. Remotely exploit the head unit **to install SSH and Command Line Interface to the Infotainment system**
3. Use SSH/CLI to **flash modified firmware** through the Infotainment system
4. Using the **indirect connectivity** of the IFE system (through the CAN Bus) with critical car control systems to remotely control cars.

Real damage: The manufacturer was forced to recall and patch 1.400.000 vehicles
Potential damage: harm people safety, disrupt traffic
Criticality level: High



Take control of traffic control lights

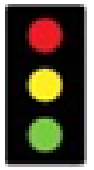
Attack example [2]: *Exploit* ***radio communication of traffic control systems*** *to control them (Real by security researchers, 2014)*

Attack vector

1. Use off-the-shelf radio equipment to communicate with traffic control systems
2. **Passively eavesdrop** communications (900 MHz and 5.8GHz)
3. Messages are **not authenticated/encrypted.** Manipulate old messages to create fake messages
4. Introduce **fake/replay messages** to control traffic control systems

Potential damage: A malicious adversary may brick traffic lights to cause traffic jams, or even cause multiple car accidents

Criticality level: High



Take control of plane systems via IFE

Attack example [3, 4]: *Exploit* ***In Flight Entertainment (IFE) system*** *to control of various systems (by two security researchers, while in flight, 2015, 2016)*

Attack vector

1. **Reverse engineer firmware** of an IFE system (found on the Internet)
2. Extract **hardcoded credentials** and use them to access a real IFE
3. Perform **SQL injection** attacks to control the displays of other passengers

Potential damage: A malicious adversary may use such attacks to take control of critical systems of a plane

Criticality level: High

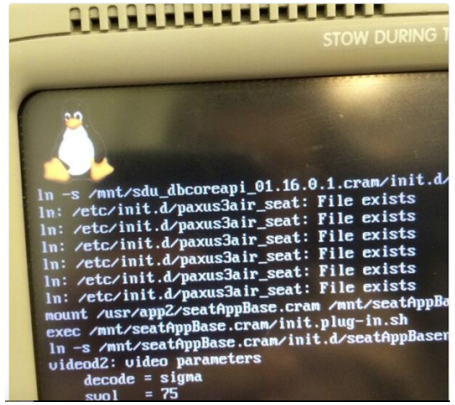
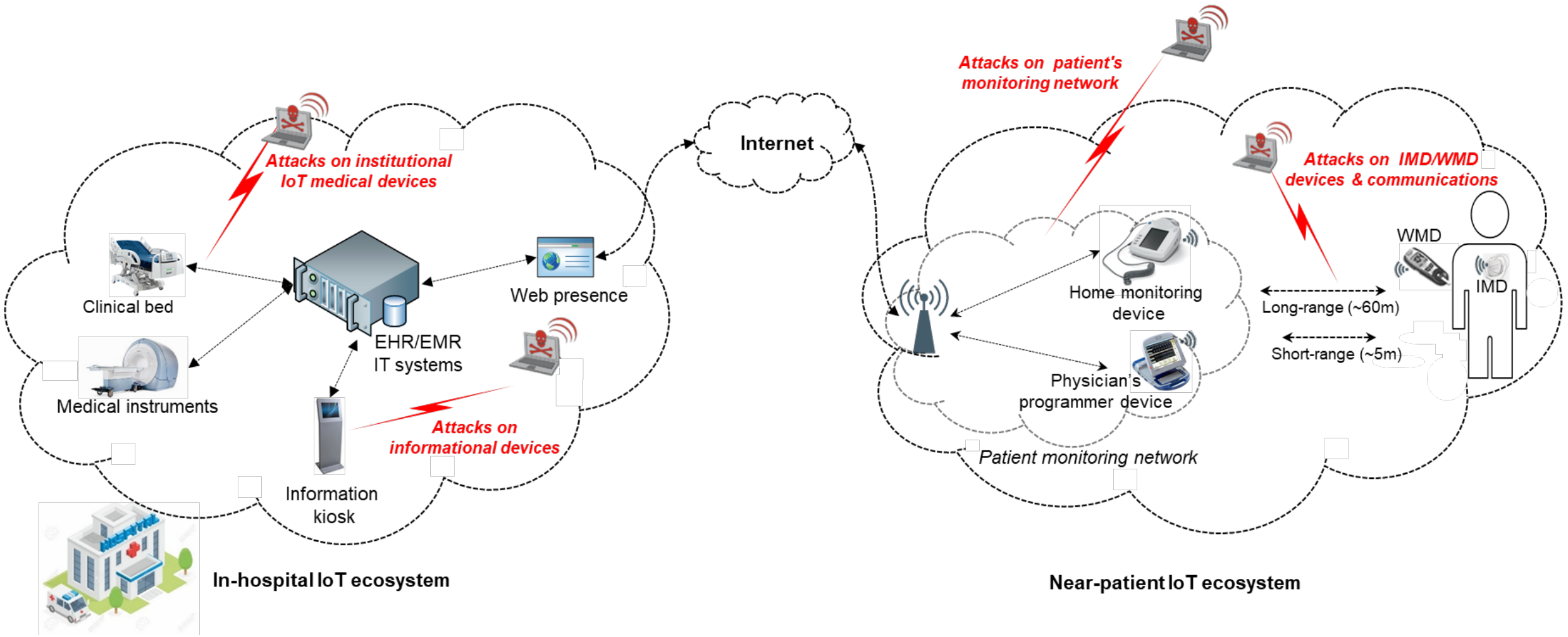


Figure from **[3]**

Healthcare infrastructure and relative IoT-enabled attacks



Manipulating implantable pacemakers

Attack example [5]: *Exploit **proprietary network protocols** to control a pacemaker (security researchers, 2017)*

Attack vector

1. **Reverse engineer proprietary network protocols** of implantable medical devices (peacemakers)
2. Use off-the-shelf equipment to bypass security controls and **remotely induce small amounts of electricity** that could potentially harm patients

Real damage: ICS-CERT issued an advisory that forced 65.000 patients to visit their doctors in order to have their devices updated

Potential damage: A malicious adversary may harm people from a distance (up to 60m)

Criticality level: High

Take control of in hospital devices

Attack example [6]: *A real security analysis of three hospitals revealed **compromised in-hospital medical IoT systems** (security researchers, 2017)*

Attack vector

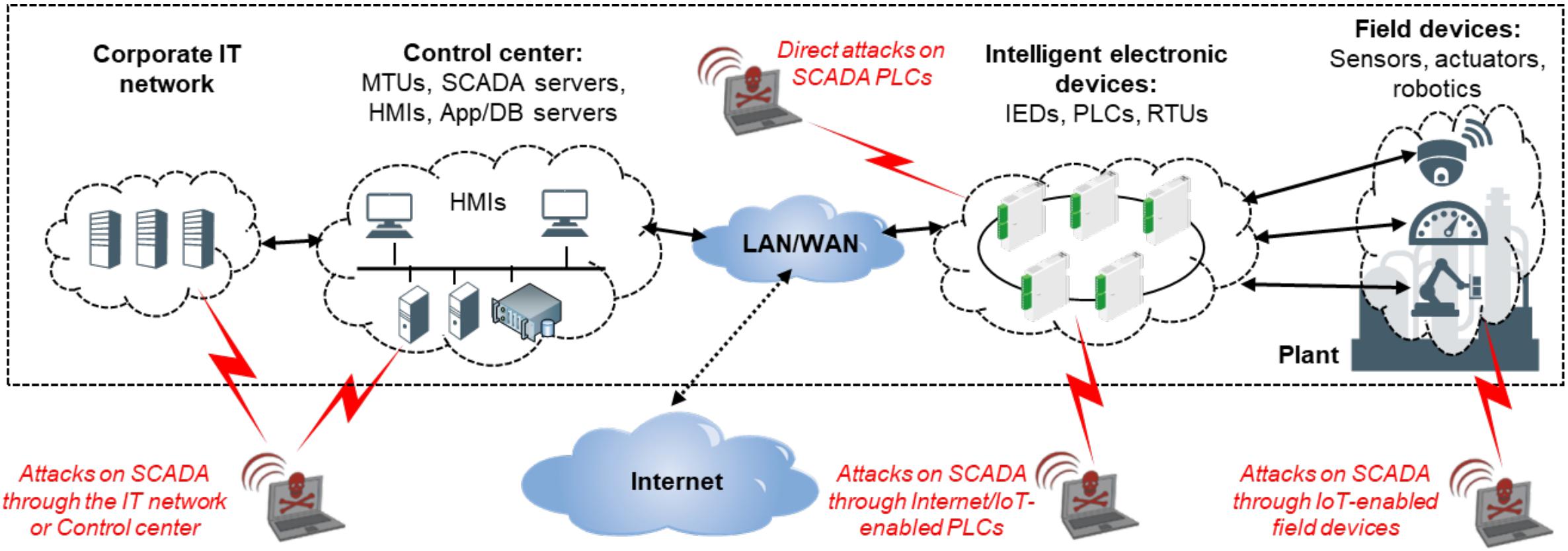
1. TrapX Research Labs in 2017 **introduce emulated IoT-enabled medical devices** inside hospitals
2. **Monitor for attacks against the emulated devices**, using special software
3. In a few days they discovered attacks against the emulated devices, that were **originating form real medical devices** within the hospital
4. Most of the malicious code found was never detected by hospital's IT stuff or the installed security systems and firewalls.

Real damage: The remediation took several weeks since the infected devices hat to be replaced

Potential (real?) damage: Use infected medical systems to gain access to medical records

Criticality level: High

Industrial SCADA infrastructure and relative IoT-enabled attacks



Simulated water treatment plant attack

Attack example [7]: *Take control of Internet facing PLCs, by* ***creating a self-spreading cross-ventor ransomware worm (LogicLocker) -*** *(PoC attack by security researchers of Georgia Institute of Technology, 2017)*

Attack vector

1. Locate vulnerable internet-facing PLCs **through Shodan** search engine susceptible to ransomware attack (discovered 1.500 of the model under attack)
2. Using **brute force** techniques recover the password.
3. Remotely infect PLCs with ransomware
4. **Locks the PLCs and send a ransom note** to the authorities.

Potential damage: Harm people safety, public confidence and trust.

Criticality level: High

Take control of internet connected industrial robots

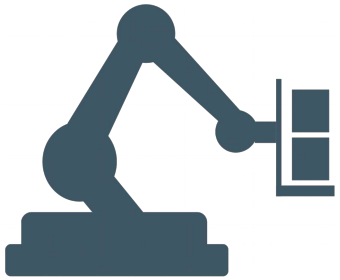
Attack example [8] : *By **exploiting multiple vulnerabilites such as WAN access to unfirewalled LAN ports, poor or no authentication schemes, insecure web interfaces etc-** (PoC attack by security researchers of Politecnico di Milano and TRENDMICRO, 2017)*

Five classes of robot-specific attacks that violates the basic operational requirements of industrial robots (accuracy, safety, integrity)

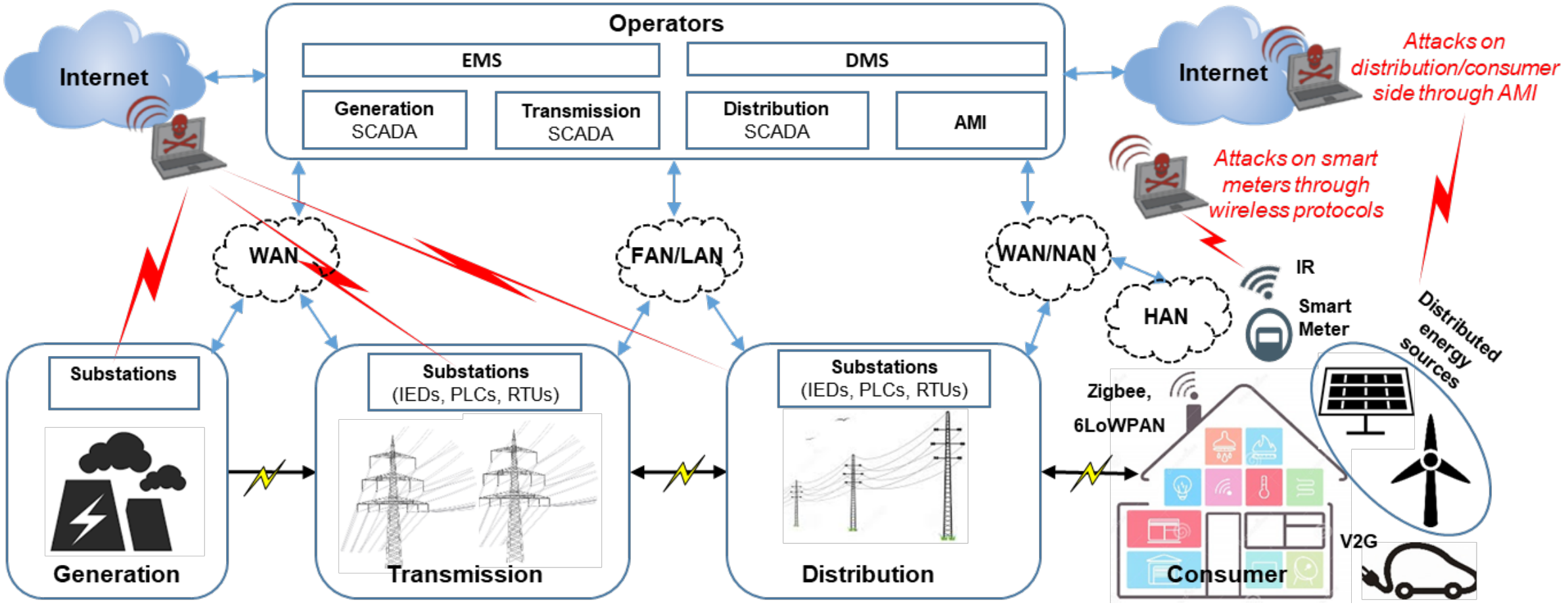
1. Control-loop parameters alteration
2. User-perceived robot state alteration.
3. Actual robot state alteration
4. Calibration parameters tampering.
5. Production logic tampering

Potential damage: Harm people safety, public confidence and trust, significant economic loss.

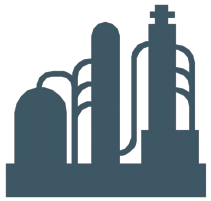
Criticality level: **High**



Smart Grid infrastructure and relative IoT-enabled attacks



Attack Ukraine’s smart Grid (part 1)



Attack example [9]: Attacks on Ukraine's smart grid transmission network.

Take control of multiple internet connected (through corporate network) circuit breakers, ***through spear-phishing campaigns*** *(2015)*

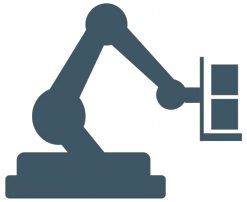
Attack vector:

1. Malware (*BlackEnergy - KillDisk*) was sent wrapped up in a word document that was attached in a phishing email impersonating a message from the Ukrainian parliament.
2. By opening the malicious word document a script run on the victims’ machines, thus planting the *BlackEnergy* infection. Then the worm
3. The malware compromise a VPN that service companies used to access remotely IoT-enabled equipment, and use it to gain control in multiple circuit breakers that controlled power flow in **distribution** network.

Real Damage: *230.000 people were affected*

Potential Damage: Harm public confidence,significant economic loss

Criticality level: **High**



Attack Ukraine’s smart Grid (part 2)

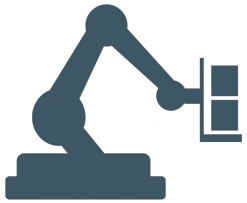
Attack example [10]: Attacks on Ukraine's smart grid distribution network (2016)

Attack vector:

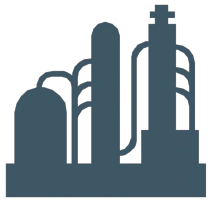
1. The infection spread through spear phishing attacks.
2. The malware (CrashOverride - Win32/Industroyer) remained hidden until it was triggered.
3. The worm could be programmed to scan the victim's network, to discover potential targets, open circuits without any intervention from the attackers.
4. It included ICS protocol stacks including IEC 101, IEC 104, IEC 61850, and OPC, a wiper to delete files and processes, modules to open circuit breakers on RTUs and force them into an infinite loop thus keeping the circuit breakers open even if grid operators attempt to shut them down.

Damage: Harm people safety, public confidence and trust, significant economic loss, user discomfort.

Criticality level: **High**



Smart Grid (PoC attack on smart grid)



Attack example [11]: Vulnerabilities on smart meters

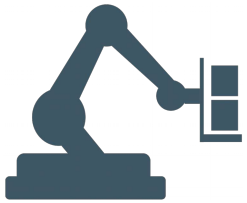
Take control of multiple interconnected (through ZigBee, Cellular network) smart meters, ***by exploiting embedded and network vulnerabilities*** *and attack the smart grid services*

Attack vector (vulnerabilities found):

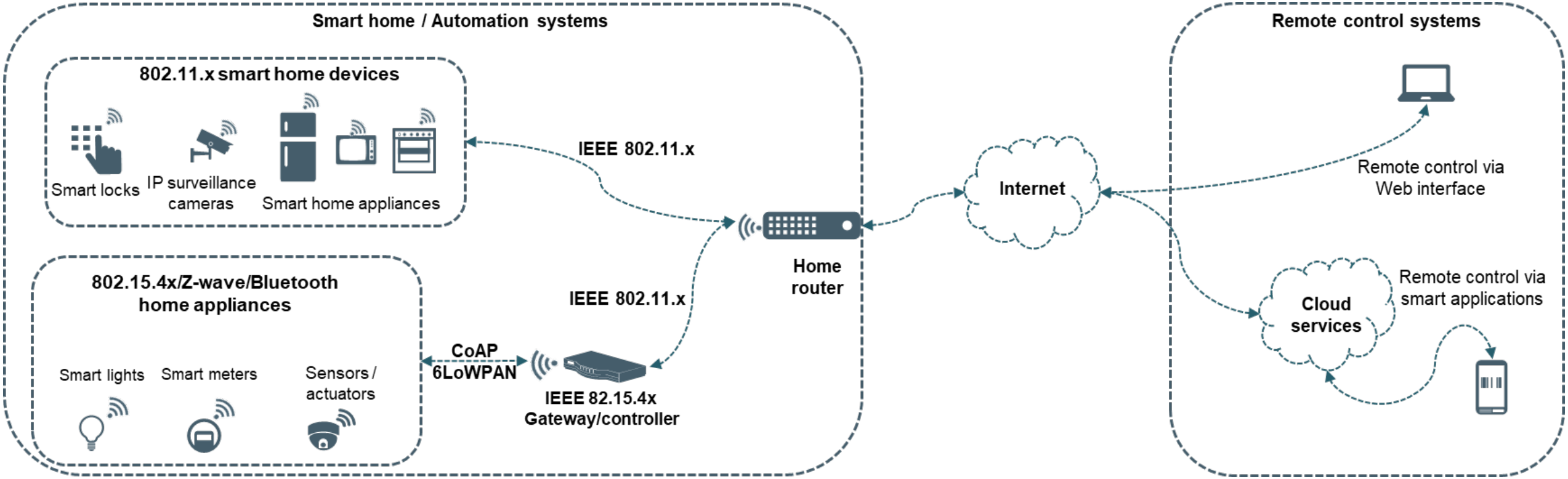
1. Encryption keys derived from short (often just six-character) device names.
2. Pairing process requires with no authentication, allowing an attacker to simply ask the smart meter to join the network and receive keys
3. Hardcoded credentials, allowing administrator access with passwords as simple and guessable as the vendor's name.
4. Code simplified to work on low-power devices skipping important checks, allowing nothing more than a long communication to crash the device.

Damage: Harm people safety, public confidence and trust, significant economic loss, user discomfort.

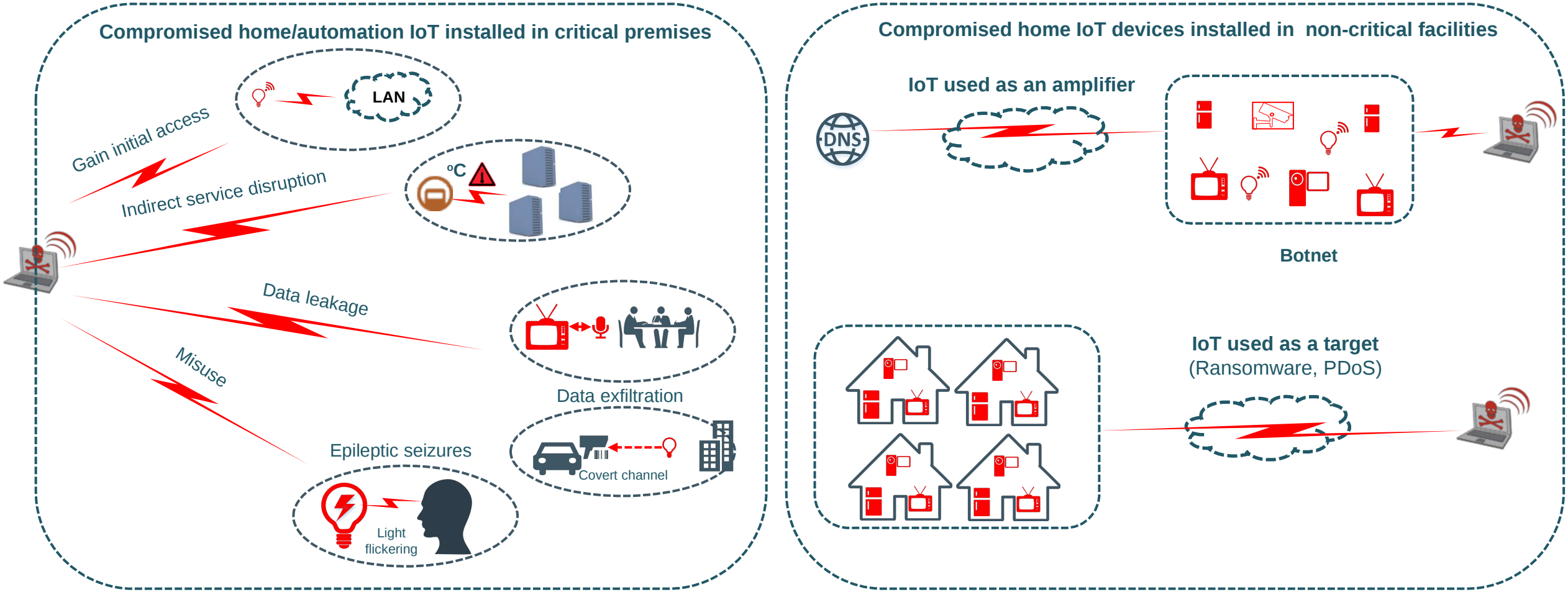
Criticality level: **High**



Smart home infrastructure



Smart home infrastructure and relative IoT enabled attacks



Smart Lights: PoC IoT enabled attacks (IoT as a target)

Create a self-spreading worm [12,13] (PoC) :

- Researchers reversed engineered several models of smart lighting systems and recovered embedded sensitive information (hard-coded encryption and signing keys).
- Using off-the-shelf equipment they managed to bypass security controls and remotely control the lamps.
- Using the recovered keys the managed to create a self propagated worm that spreads autonomously to all similar smart lighting systems. All these were possible from distances of aprox. 350 meters.
- The same group or researchers were able to create covert channels by making the smart lamps flicker in brightness levels unnoticeable to human eye. Furthermore they were able to manipulate flickering in such a way that they could cause epileptic seizures to people.

Smart home: Real IoT enabled attacks

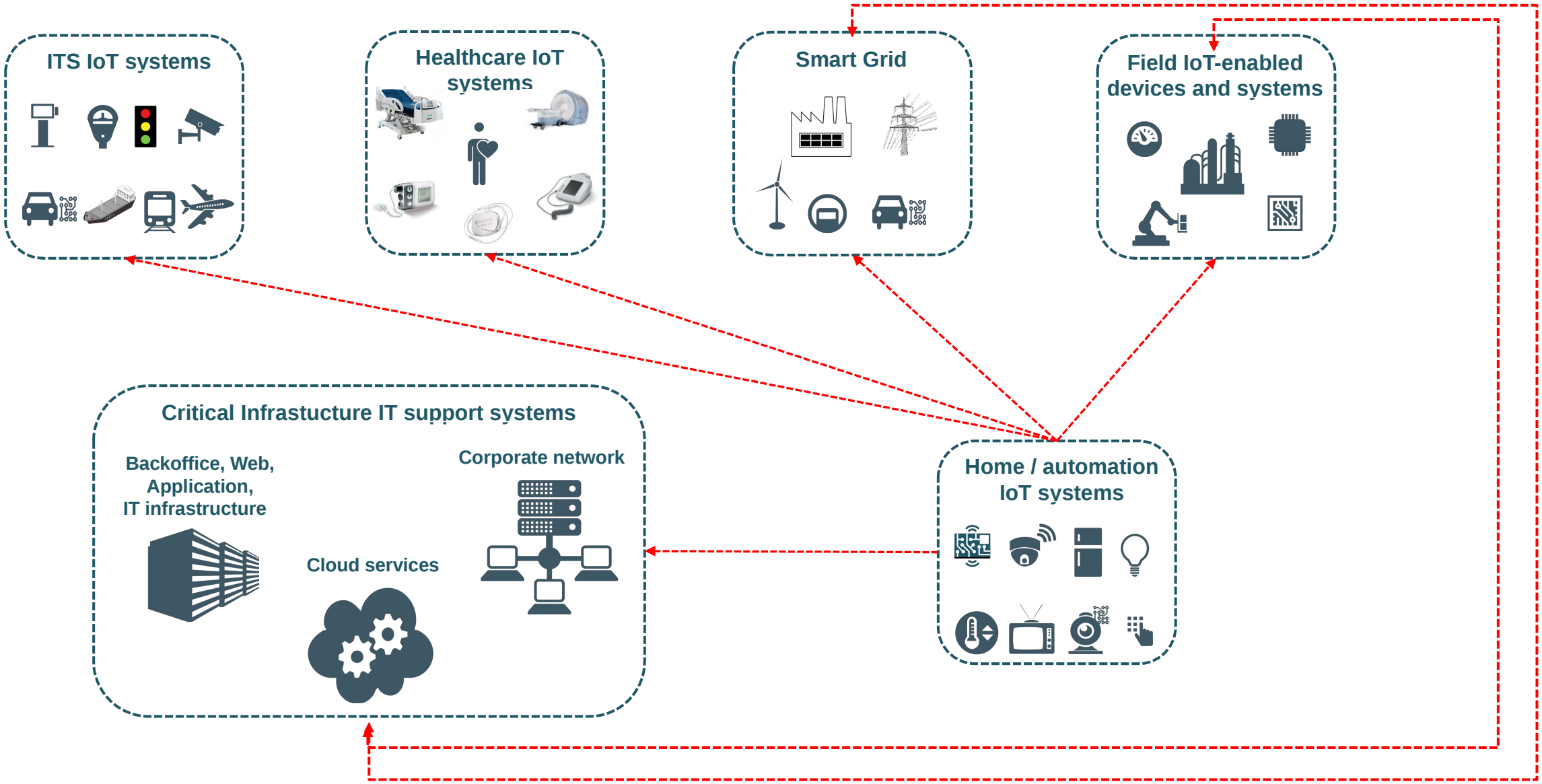
DDoS attacks on DYN DNS services [14] (October 2016 – Real – As an amplifier):

- Thousands of unsecured IoT devices, part of a BOTNET called **Mirai**, launched a coordinated DDoS attack against DYS DNS services at a rate of 600 Gbps thus preventing customers from reaching over 1.200 domains including Amazon, Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal, Verizon, and Comcast for several hours.
- The infected home IoT-enabled devices had default/weak passwords and/or vulnerable OS installed.

Attacks on smart TVs [15] (January 2017 – Real – exfiltrate data – spy on people):

- On March 2017 Wiki-Leaks published documents that revealed a CIA project named Weeping Angel. By placing the target TV in a *fake-off* mode they were able to record conversations in a room and then send them over the Internet to a covert server.

IoT enabled attack paths to and from Critical Infrastructures



Mitigation controls

- **For the operators**
  - Avoid installing IoT near critical systems
  - Properly segment/isolate networks (mission critical systems should always be isolated)
  - Consider all attack paths (not only the obvious ones)
  - Security test of IoT devices before installation
  - Control physical access to IoT devices
  - Control Internet access to/from IoT
  - Re-examine BYOD, BYOP policies
  - Favor technology diversity

- **For the manufacturers**
  - Use tamper resistant H/W
  - Protect F/W update procedure
  - Avoid to hardcode credentials
  - Use tested APIs to develop IoT S/W
  - Authenticate network communications
  - Provide encryption and integrity protection of network protocols (at least optionally)
  - Implement secure key management/key exchange procedures

- **For the regulators**
  - Enforce proper security controls for IoT devices
  - Enforce use of security IoT in critical infrastructures

References (1/2)

[1] C. Miller and C. Valasek, “Remote exploitation of an unaltered passenger vehicle,” Black Hat USA, vol. 2015, 2015.
[2] C. Cerrudo, “Hacking US traffic control systems,” 2014
[3] R. Santamarta. (2016) In flight hacking system. http://blog.ioactive.com/2016/12/in-flight-hacking-system.html
[4] E. Weise. (2015) Computer expert hacked into plane and made it briefly fly sideways, according to FBI (Independent). http://www.independent.co.uk/news/world/americas/computer-expert-hacks-into-plane-and-makes-it-fly-sideways-according-to-fbi-10256145.html

[5] B. Rios and J. Butts. (2017) Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies. https://www.a51.nl/sites/default/files/pdf/Pacemaker%20Ecosystem%20Evaluation.pdf
[6] TrapX Research, Labs, “Anatomy of Attack: MEDJACK.2 – Hospitals Under Siege,” TrapX Investigative Report, 2016.
[7] D. Formby, S. Durbha, and R. Beyah, “Out of control: Ransomware for industrial control systems,” 2017.
[8] F. Maggi, D. Quarta, M. Pogliani, M. Polino, A. M. Zanchettin, and S. Zanero, “Rogue robots: Testing the limits of an industrial robots security,” Trend Micro, Politecnico di Milano, Tech. Rep.
[9] D. U. Case, “Analysis of the cyber attack on the ukrainian power grid,” 2016
[10] G. Andy. (2017) How an entire nation became russia’s test lab for cyberwar. www.wired.com. [Online]. Available: https://www.wired.com/story/russian-hackers-attack-ukraine/
[11] H. Alex. (2016). [Online]. Available:https://www.theguardian.com/technology/2016/dec/29/smart-electricity-meters-dangerously-insecure-hackers
[12] E. Ronen, C. O’Flynn, A. Shamir, and A.-O. Weingarten, “Iot goes nuclear: Creating a zigbee chain reaction,” IACR Cryptology ePrint Archive, vol. 2016, p. 1047, 2016
[13] E. Ronen and A. Shamir, “Extended functionality attacks on iot devices: The case of smart lights,” in 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016, pp. 3–12

References (2/2)

[14] T. Greene. (2016) How the Dyn DDoS attack unfolded. [Online]. Available:http://www.networkworld.com/article/3134057/security/how-the-dyn-ddos-attack-unfolded.html.
[15] Wikileaks. (2017) Vault 7: CIA Hacking Tools Revealed – CIA malware targets iPhone, Android, smart TVs. [Online]. Available: https://wikileaks.org/αciav7p1/