

01-Oct-2020



Securing the IoT: Threats, Challenges, and Safeguards

Joseph Bugeja

Redacted Version

ABOUT ME



- ✓ Lic in Computer Science, MSc in Information Security, BSc in Computer Science and AI
- ✓ 15 years working in the software industry

- ✓ Doctoral student in Computer Science (PhD viva happening this Dec/Jan).
- ✓ Main research themes: security, privacy, and Internet of Things



TEACHING RESPONSIBILITIES AT MALMÖ UNIVERSITY

Start / Training / Computer Science: Information Security

COURSE BASIC LEVEL 7.5 CREDITS

COMPUTER SCIENCE: INFORMATION SECURITY

Summary


[Syllabus](#)

[plug](#)

[Registration](#)

Source: <https://edu.mah.se/sv/Course/DA351A>


AGENDA



Introduction



Challenges in Securing the IoT



Countermeasures



The Internet of Things



Attacks and Malicious Threat Agents



Introduction

THE LANDSCAPE AROUND US HAS EVOLVED



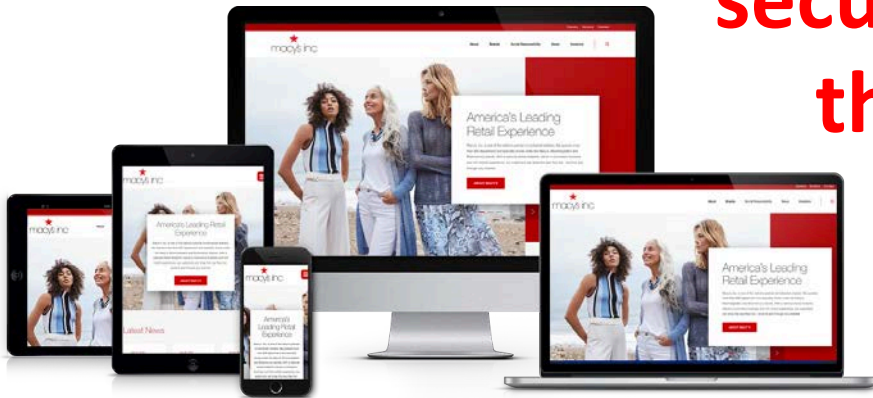
Internet



Smart speakers



Wearables



Websites

**How can we
secure these
things?**



Drones

SECURITY AND PRIVACY OF CITIZENS IS AT RISK

- ✓ 73,000 private video cameras leaking live footage (2014)



RISKS WITH POPULAR CONSUMER IOT DEVICES

- ✓ Smart devices may jeopardize your security and privacy



“Hackers could steal personal information and turn the microphone of the doll into a surveillance device”

“A hacker could crank up the temperature of a smart thermostat to a sweltering 99 degrees”

Ransomware PoC FTW!

#Defcon24 #wargames @IoTville



Hackers demonstrated first ransomware for IoT thermostats at DEF CON



“After hearing the anchor’s comment, their own devices also tried to order pricey dollhouses”

A GLIMPSE INTO SOME EMERGING TECH



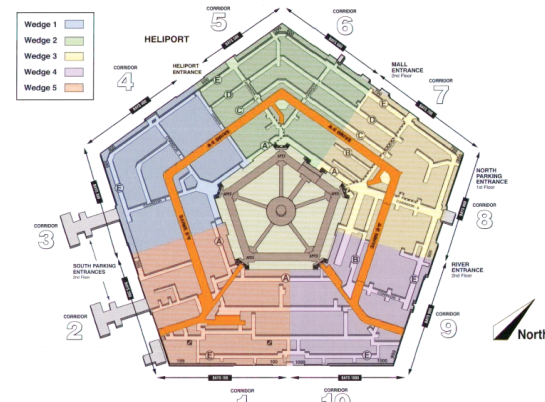
A plain-clothed police officer quickly identifies and locks in on a wanted suspect in a crowded square through the 5G glasses' facial recognition function.

Chinese police test gait-recognition technology from AI start-up Watrix that identifies people based on how they walk

- Known as gait recognition, the technology works by analysing thousands of metrics about a person's walk and storing them in a database
- Software can identify a person from 50 metres away – even if they have their face covered or back to camera

The Pentagon has a laser that can identify people from a distance — by their heartbeat

The Jetson prototype can pick up on a unique cardiac signature from 200 meters away, even through clothes.

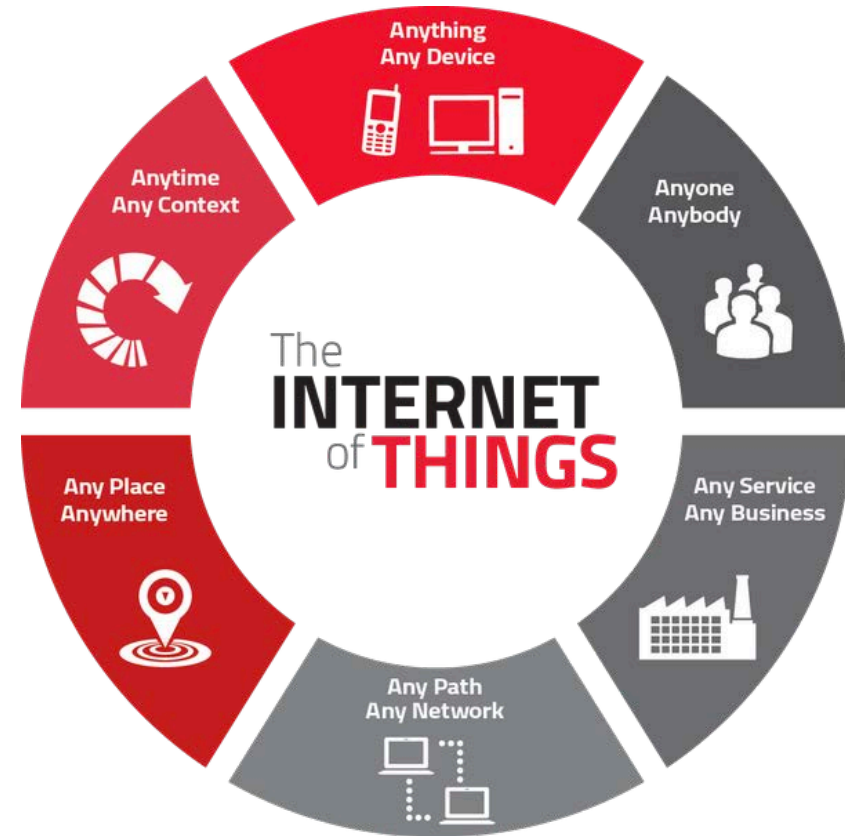




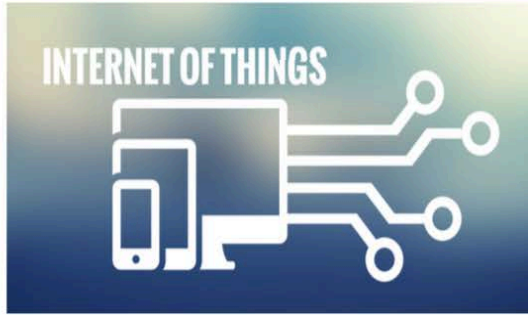
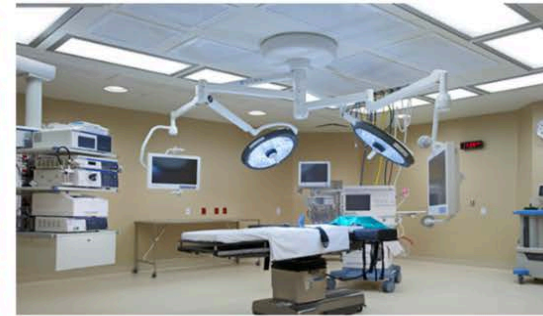
The Internet of Things

THE INTERNET OF THINGS

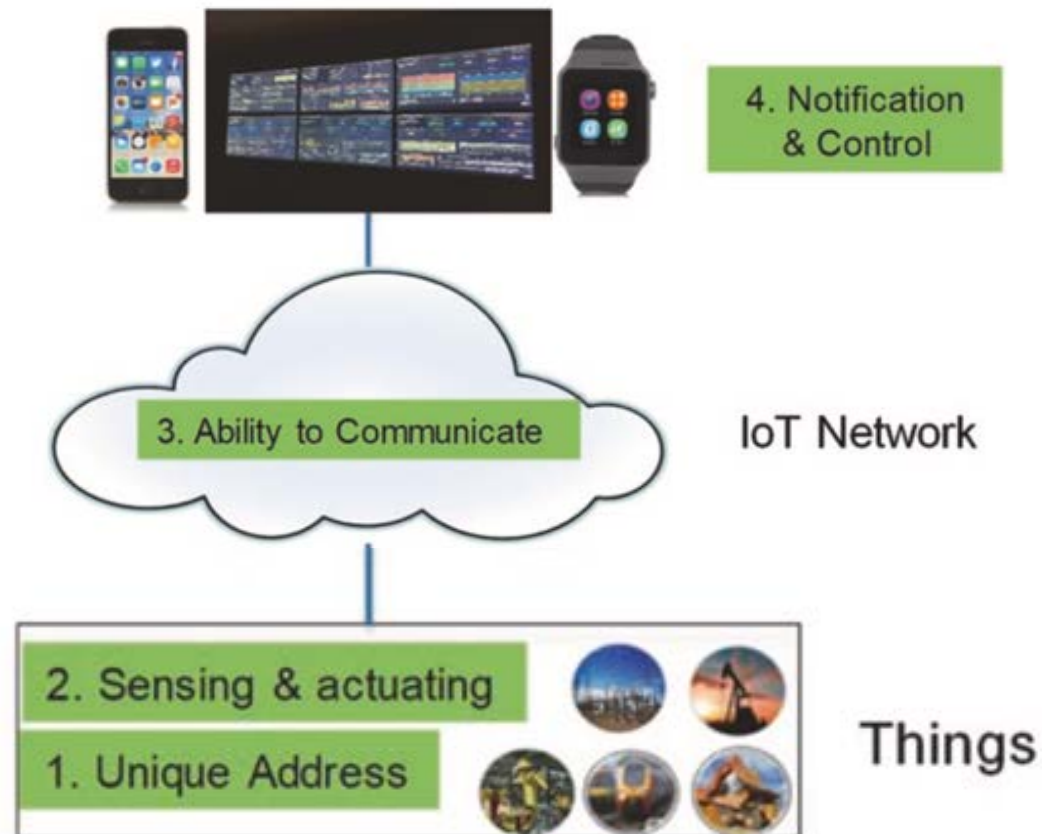
5. Internet of Things



DIFFERENT APPLICATIONS OF IOT



BASIC REQUIREMENTS FOR AN IOT SOLUTION



INTERNET-CONNECTED DEVICES

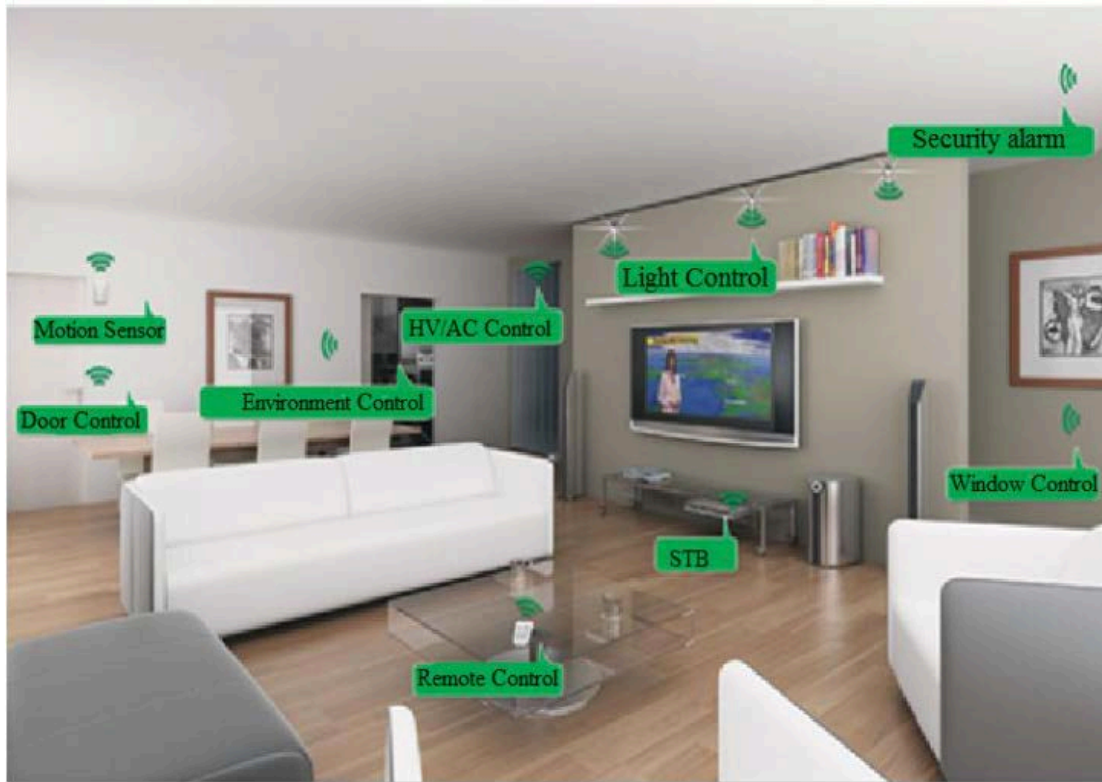


Single-purposed
IoT Devices

‘IoT-ish’
Devices

Multi-purposed
non-IoT Devices

IOT IN SMART HOMES



- ✓ Improves energy efficiency, security/safety, entertainment, and healthcare support.
- ✓ Remote management of Internet-connected devices such as doors, refrigerators, TVs, etc.
- ✓ Data related with home, power, telecoms, gas and water can be sent automatically to utility companies and to other service providers for other reasons.

THE SMART CONNECTED HOME

- ✓ A smart connected home leverages IoT technologies to improve the quality and efficiency of life to the residents



Image: Shutterstock



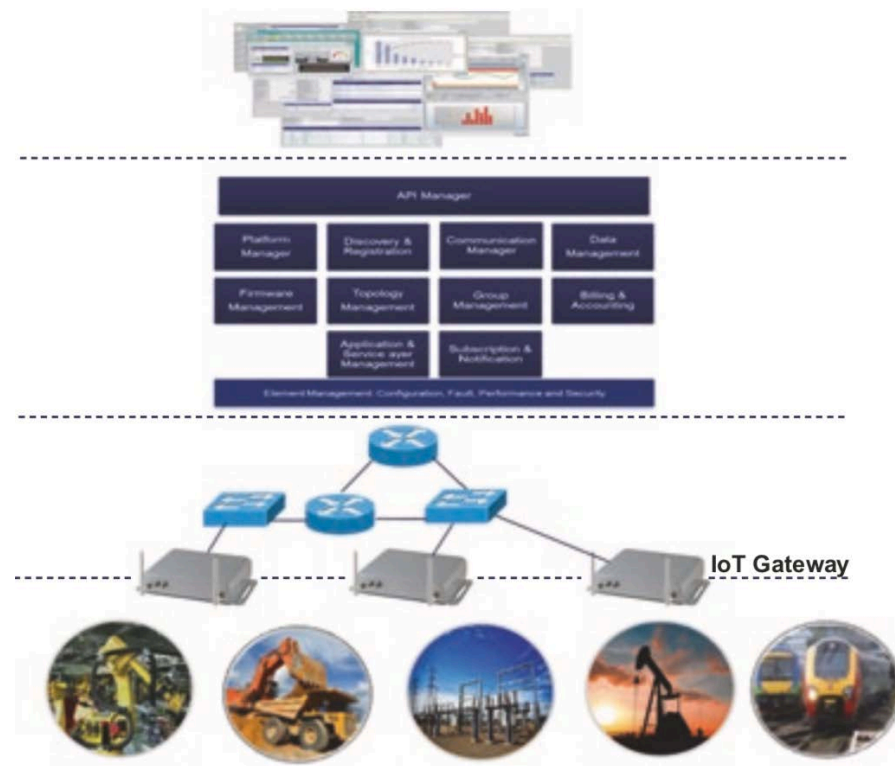
Challenges in Securing the IoT

IOT REFERENCE FRAMEWORK

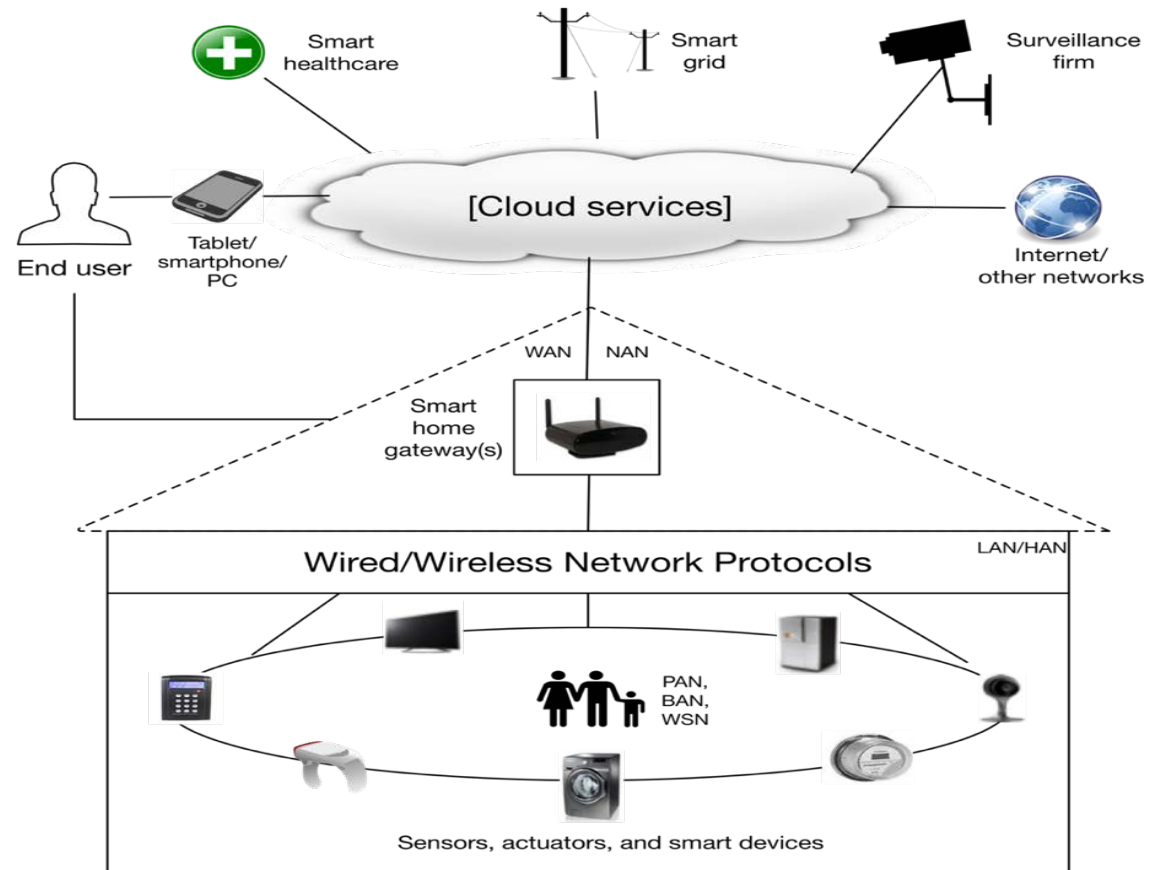
Software apps.
IoT Services

Network channels and infrastructure
IoT Network

Sensors
IoT Devices
Actuators
Connected objects



THE SMART CONNECTED HOME ARCHITECTURE



Note: WAN, LAN, NAN, HAN, PAN, BAN, and WSN correspond to wide area, local area, neighbourhood area, home area, personal area, body area, and wireless sensor networks respectively

SOME DEVICE LEVEL CHALLENGES



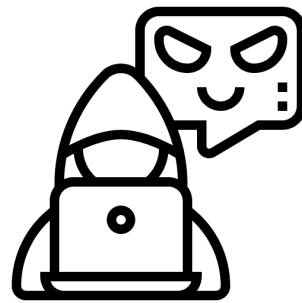
- Memory, computing, energy, storage, and throughput constraints



- Lack of keyboard, mouse, and tactile screen



- Easily accessible devices are prone to physical attacks



Attacks and Malicious Threat Agents

INFORMATION SECURITY REQUIREMENTS

- ✓ Security requirements in the Information Assurance & Security (IAS) octave

Requirement	Definition	Abbreviations
Confidentiality	Ensuring that only authorized users access the information	C
Integrity	Ensuring completeness, accuracy, and absence of unauthorized data manipulation	I
Availability	Ensuring that all system services are available, when requested by an authorized user	A
Accountability	An ability of a system to hold users responsible for their actions	AC
Auditability	An ability of a system to conduct persistent monitoring of all actions	AU
Trustworthiness	An ability of a system to verify identity and establish trust in a third party	TW
Non-repudiation	An ability of a system to confirm occurrence/non-occurrence of an action	NR
Privacy	Ensuring that the system obeys privacy policies and enabling individuals to control their personal information	P

SUMMARY OF IOT SECURITY THREATS

IoT Services

IoT Network

IoT Devices

Threat	Against
Hardware Trojans	All
Side-channel attacks	C,AU,NR,P
DoS	A,AC,AU,NR,P
Physical attacks	All
Node replication attacks	All
Camouflage	All
Corrupted node	All
Tracking	P, NR
Inventorying	P, NR
Tag cloning	All
Counterfeiting	All
Eavesdropping	C,NR,P
Injecting fraudulent packets	P,I,AU,TW,NR
Routing attacks	C,I,AC,NR,P
Unauthorized conversation	All
Malicious injection	All
Integrity attacks against learning	C,I
Non-standard frameworks and inadequate testing	All
Insufficient/Inessential logging	C,AC,NR,P

ROUTING AS AN EXAMPLE OF AN ATTACK ON THE NETWORK

IoT Network

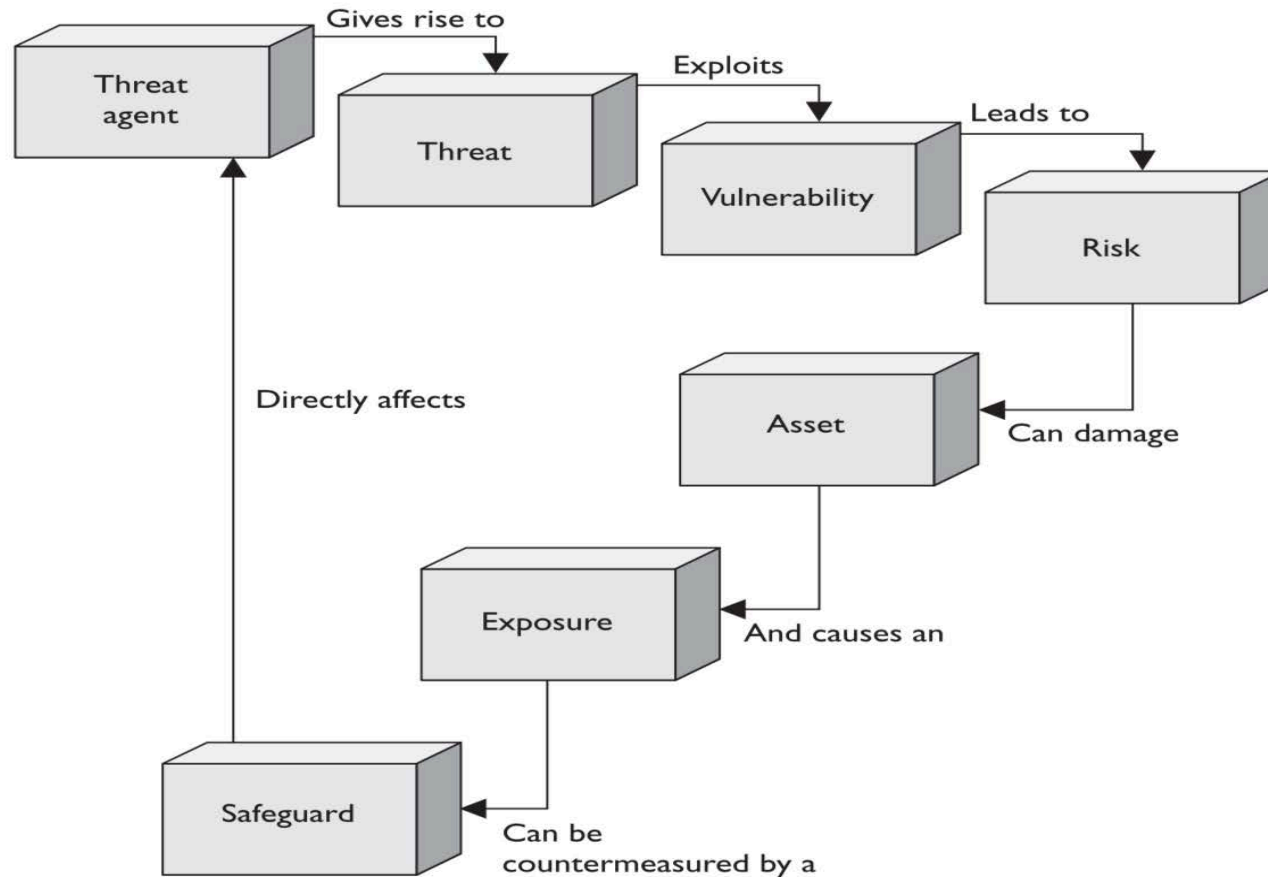
Example of an attack:

> *Routing*



- ✓ **Black hole:** This attack is launched by using a malicious node, which attracts all the traffic in the network by advertising that it has the shortest path to the destination in the network
- ✓ **Gray hole:** This attack is a variation of Black Hole attack in which the nodes selectively drop some packets
- ✓ **Worm hole:** In this attack, the attacker first records packets at one location in the network and then tunnels them to a different location
- ✓ **Others:** HELLO floods, Sybil, bogus routing information, etc.

RELATIONSHIP AMONG THE DIFFERENT SECURITY CONCEPTS



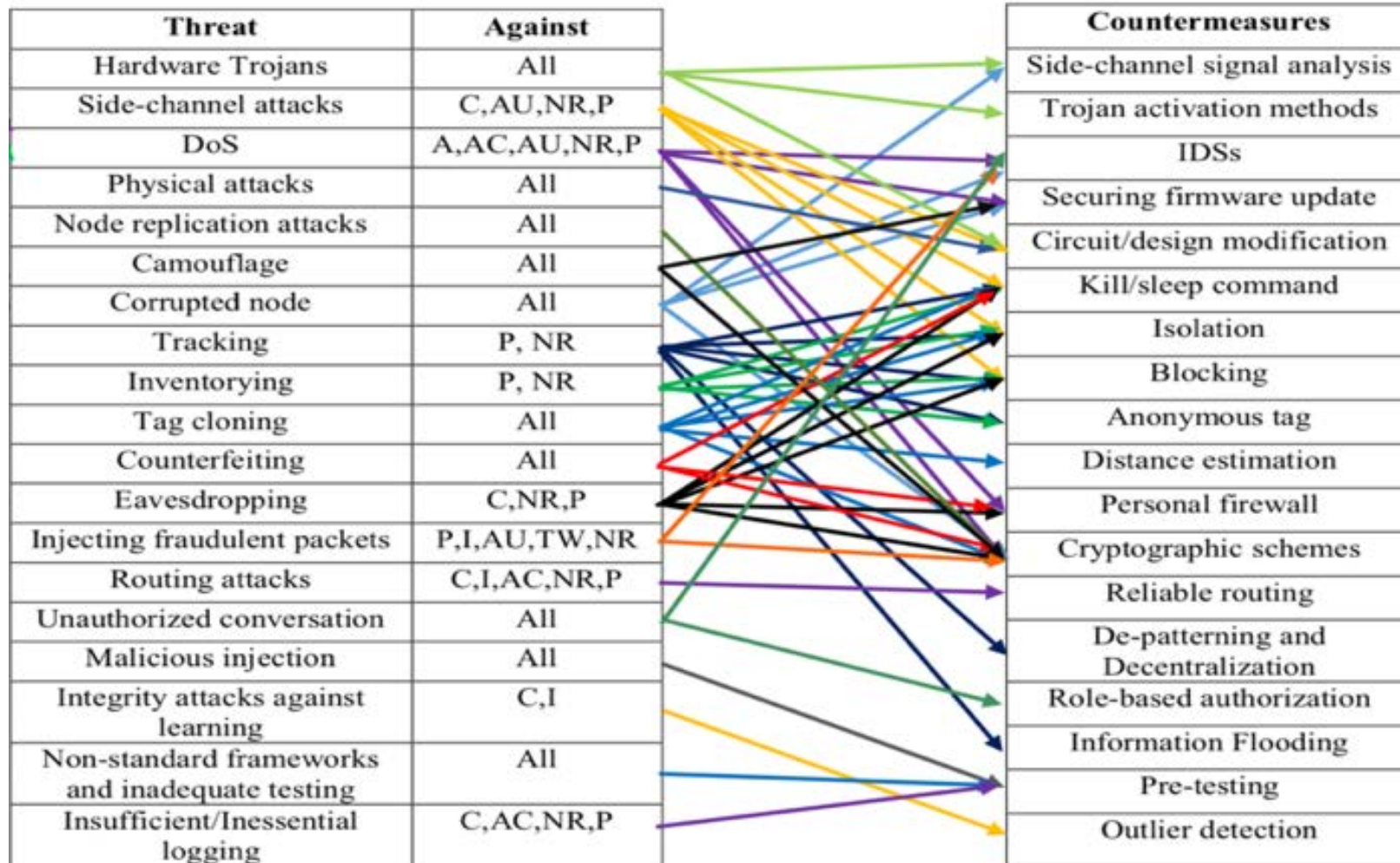
MALICIOUS THREAT AGENTS





Countermeasures

SUMMARY OF IOT SECURITY THREATS AND COUNTERMEASURES



DEFENDING AGAINST ROUTING ATTACKS

IoT Network

Secure Routing



- ✓ Secure routing is vital to the acceptance and use of sensor networks for many applications
- ✓ Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against the majority of outsider attacks
- ✓ Careful protocol design is needed for different threats, e.g., to prevent against insiders and ‘laptop-class’ adversaries

OTHER STATE-OF-THE-ART MITIGATIONS FOR IOT-BASED SYSTEMS

IoT Devices

- H/W enc, fail-secure design, and device authZ
- Enhanced algorithms, e.g. DTLS and ECSDA
- Platforms such as RERUM
- CC and EMVCo IC SE

IoT Network

- VPNs, firewalls, IDS, and IPS
- TOR-based systems
- Devices such as Cujo, Dojo, and Keezel
- ENISA, CSA, etc.

IoT Services

- Security testing, secure design, and data masking
- Cryptographic schemes
- OWASP, Builditsecure.ly, I Am the Cavalry
- Sites such as BugCrowd



FINAL REMARKS

- ✓ IoT influences many application areas of our society
- ✓ Despite its benefits, several security concerns exist at different layers in an IoT system
- ✓ We explored different IoT security attacks, countermeasures, and threat agents
- ✓ Nonetheless, several open issues need to be addressed by industrial/academic research communities as well as manufacturers

**THANK YOU
FOR *YOUR*
ATTENTION!**

FULLCIRCLE SECURITY

Expertise. Knowledge. Success.

bugejajoseph.com

[HOME](#) / [ACADEMIC](#) / [PRESENTATIONS](#) / [SERVICES](#) / [ABOUT](#) / [CONTACT](#)