03-Oct-2019

IoT Security:
Threats, Challenges, and Safeguards

Joseph Bugeja

MALMÖ UNIVERSITY
INTERNET OF THINGS AND PEOPLE RESEARCH CENTER

LUNDS UNIVERSITET

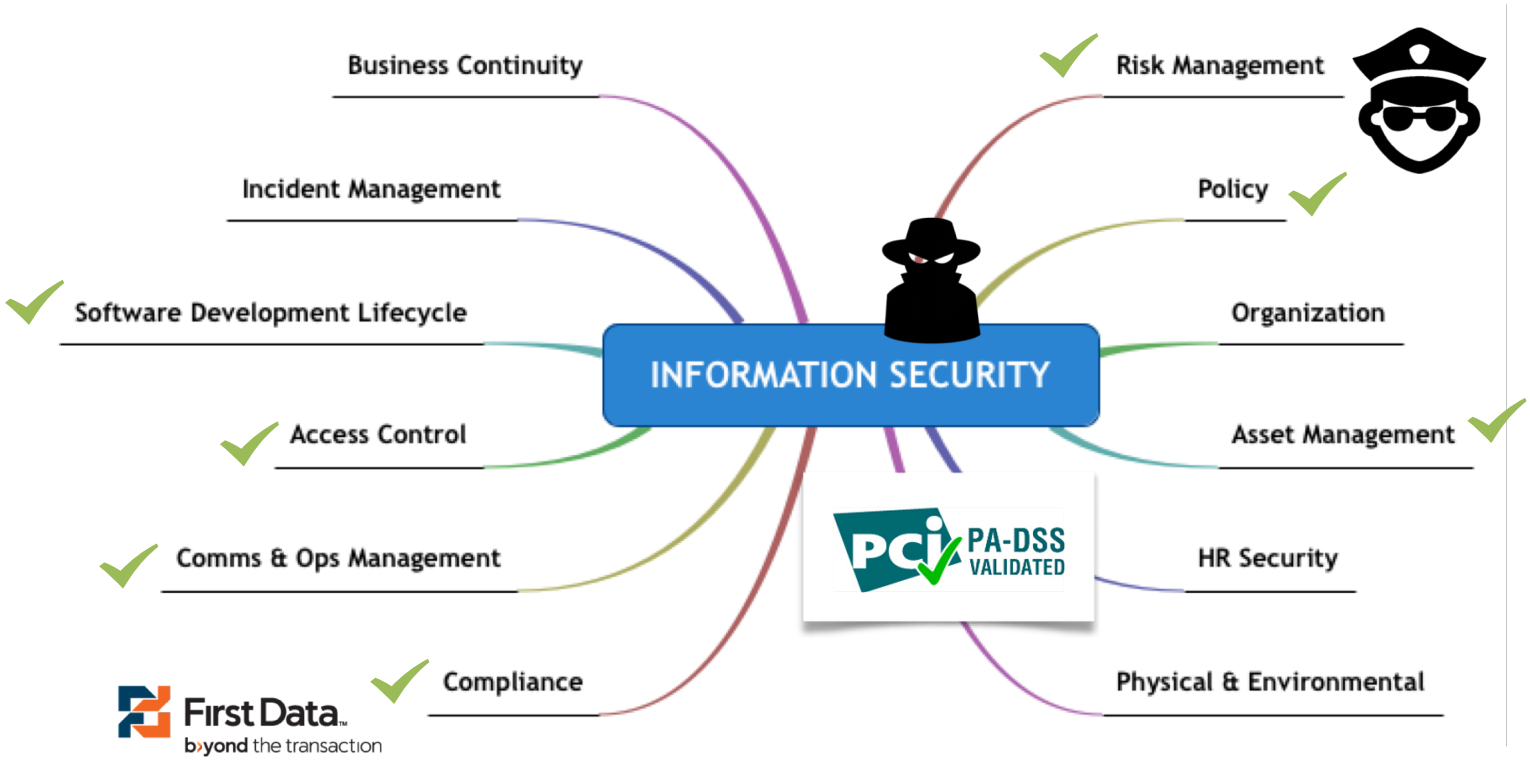
KK-stiftelsen

ABOUT ME

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

- ✓ Phd student in Computer Science
- ✓ Main research themes: security, privacy, and Internet of Things

MY PREVIOUS PROFESSIONAL INFORMATION SECURITY DUTIES



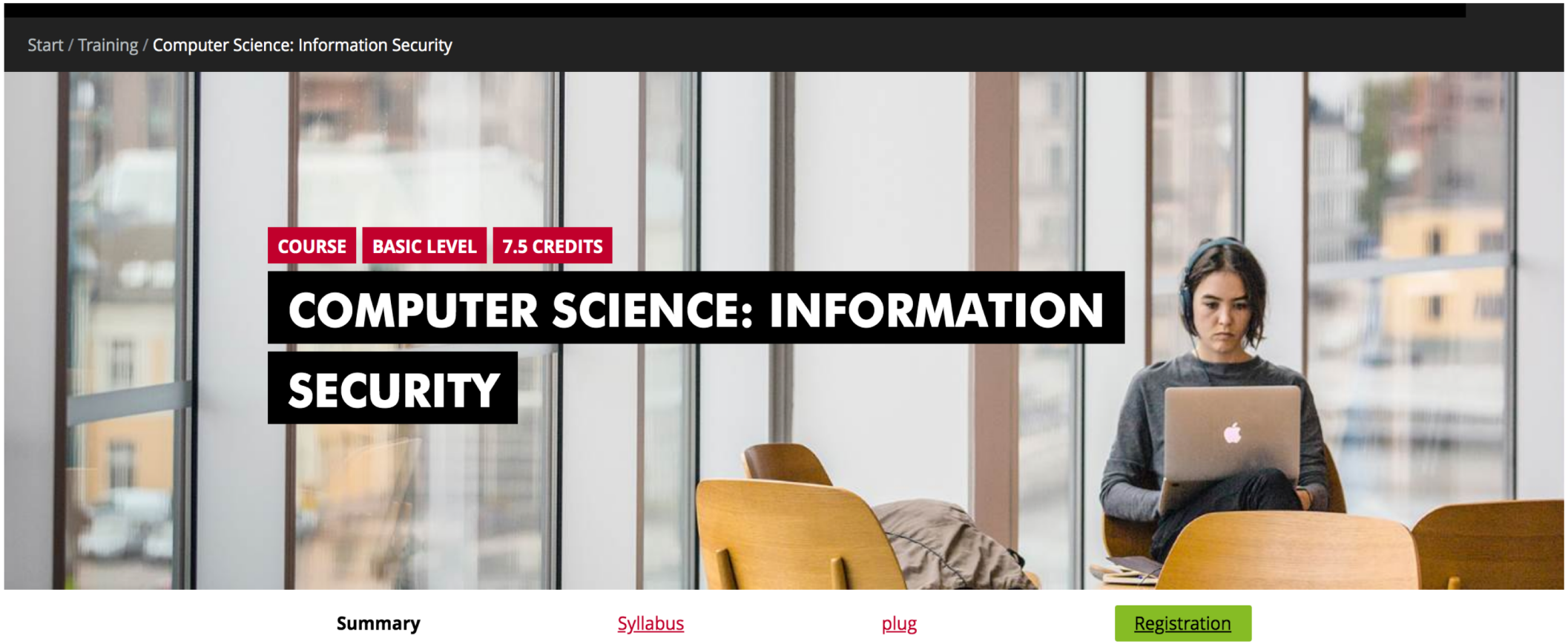
BARCLAYS worldpay

Swedbank EVRY globalcollect payments. knowledge. growth.

HSBC

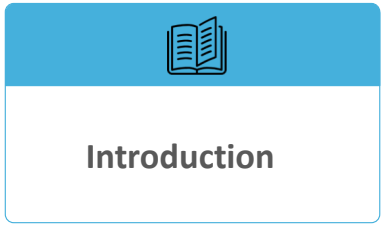
PCI DSS COMPLIANT

TEACHING RESPONSIBILITIES AT MALMÖ UNIVERSITY



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

AGENDA



Introduction

Challenges in Securing IoT

Countermeasures

The Internet of Things

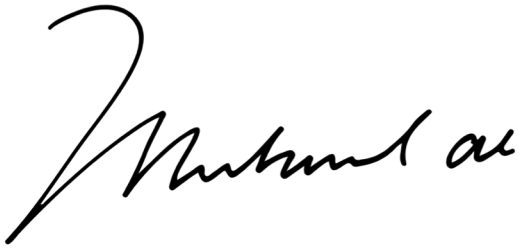
Attacks and Malicious Threat Agents

Introduction

A WHILE AGO AND STILL

Fences

Seals



Signatures

Locks

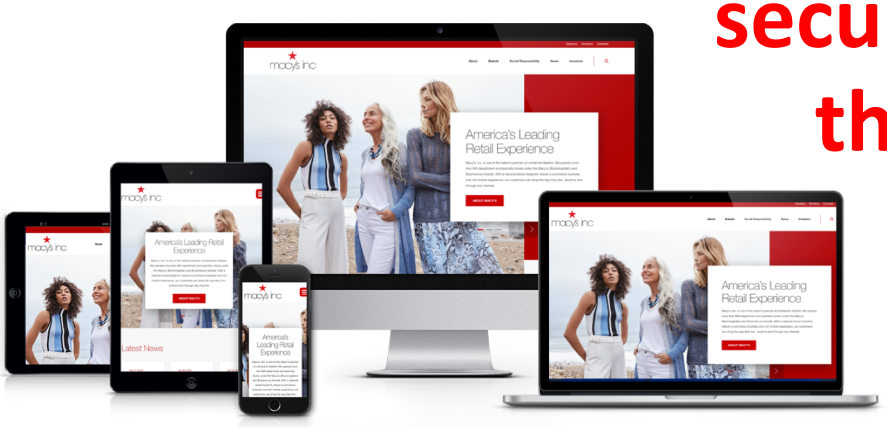
THE LANDSCAPE AROUND US HAS EVOLVED

Internet

Smart speakers

Wearables

How can we secure these things?

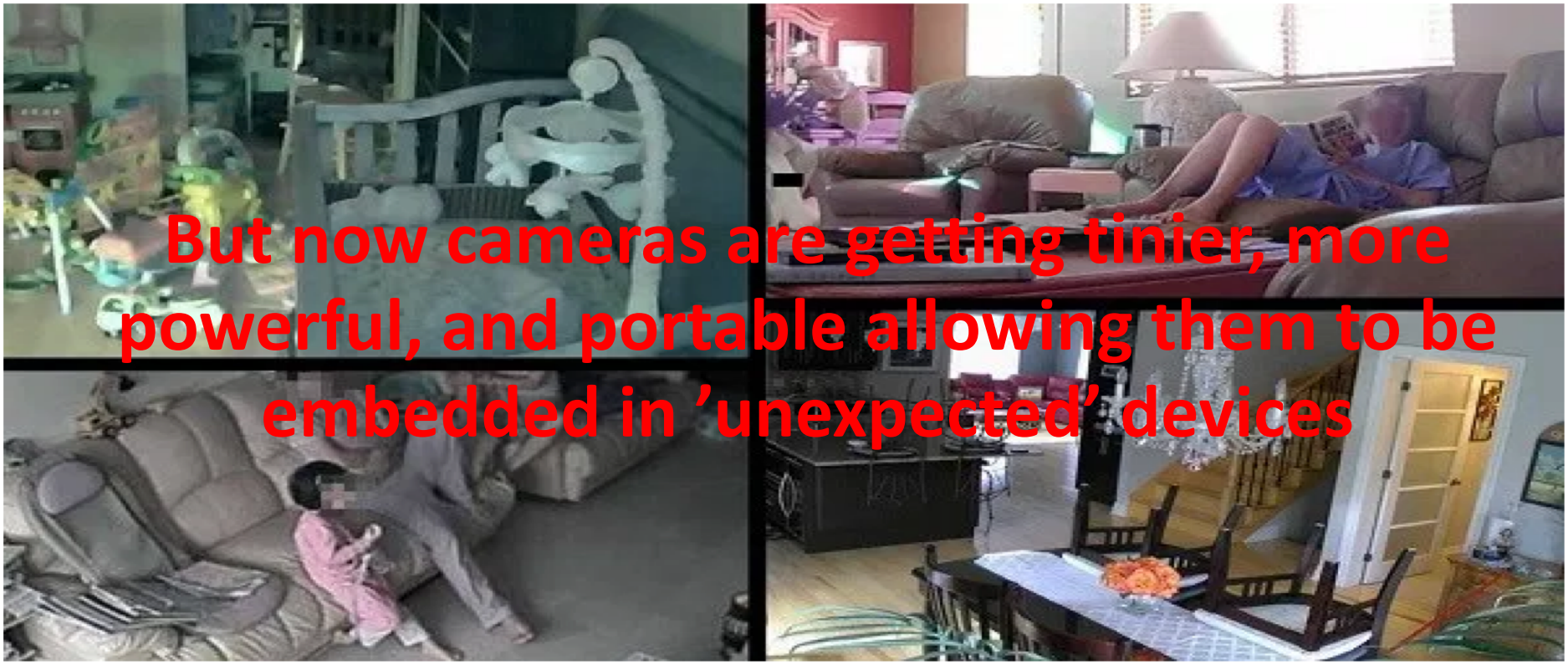


Websites

Drones

SECURITY AND PRIVACY OF CITIZENS IS AT RISK

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



SECURITY AND PRIVACY OF CITIZENS IS AT RISK

✓ 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 @IoTvillage

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"

SECURITY AND PRIVACY OF CITIZENS IS AT RISK

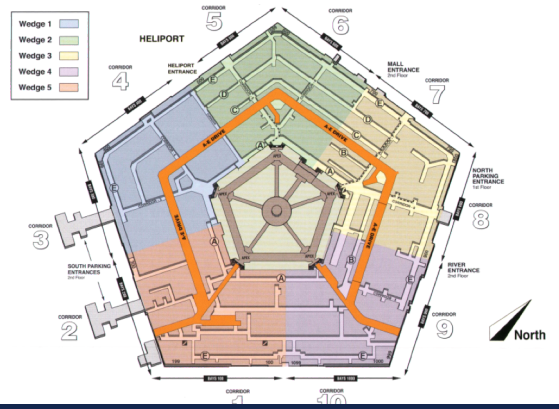
A plain-clothed police officer quickly identifies and locks in on a wanted suspect in a crowded square through the 5G glasses' facial recognition function.

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

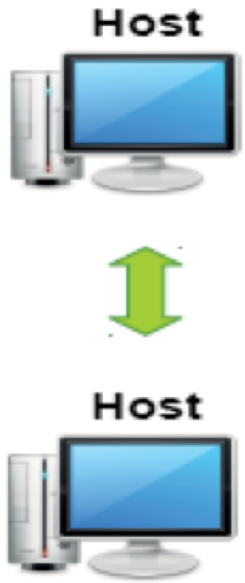
The Jetson prototype can pick up on a unique cardiac signature from 200 meters away, even through clothes.



The Internet of Things

THE EVOLUTION OF NETWORKING

1. Network



2. The Internet

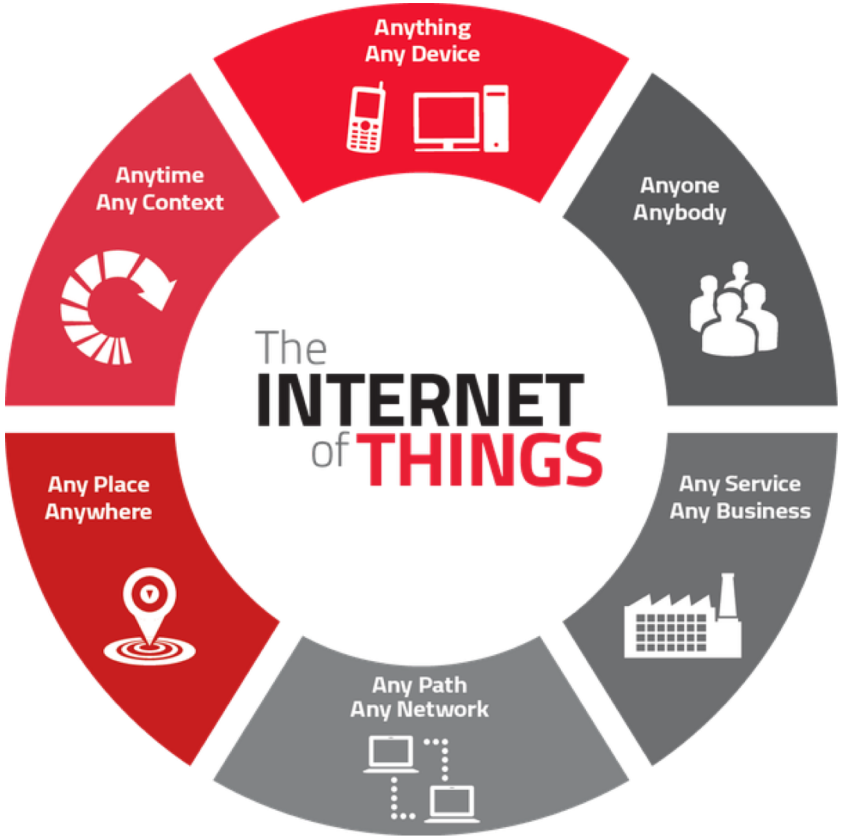
THE EVOLUTION OF NETWORKING

3. Mobile-Internet

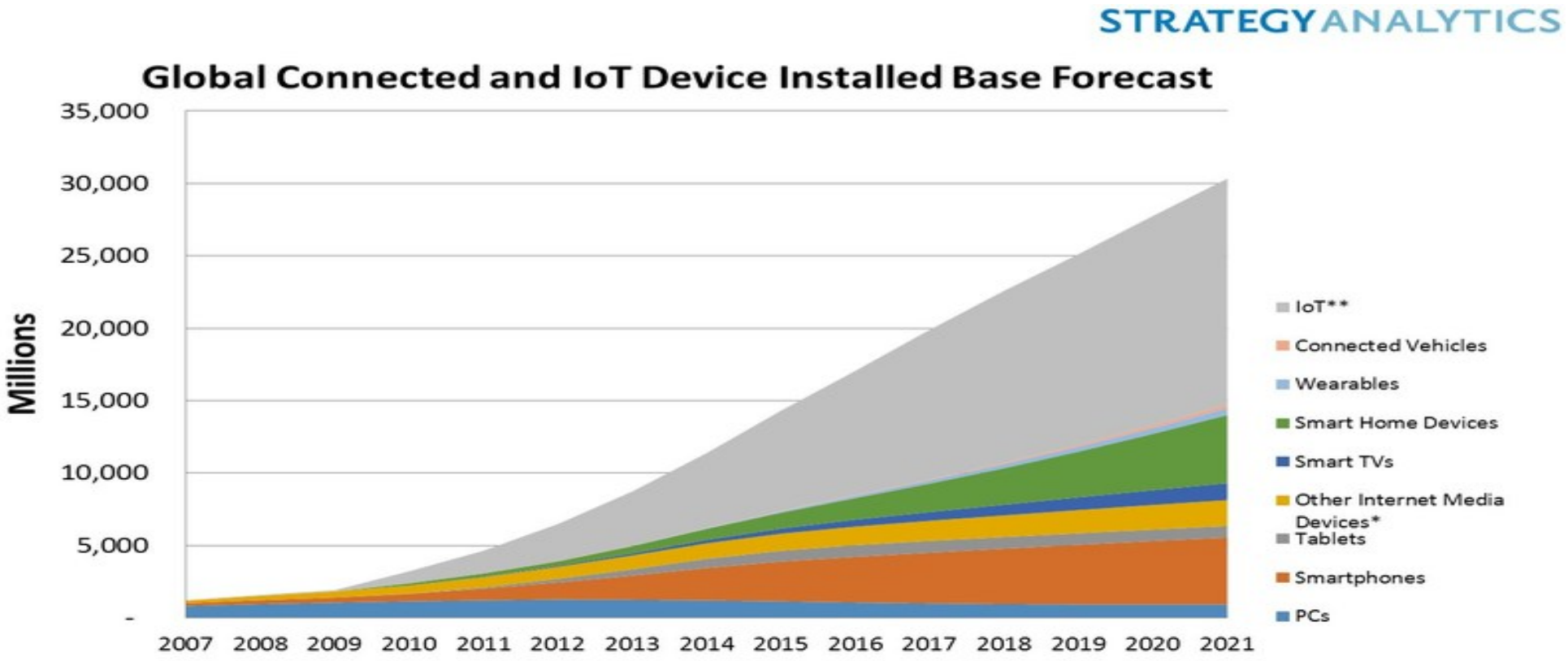
4. Mobiles + People + PCs

THE INTERNET OF THINGS

5. Internet of Things



THE INCREASE IN THE DEPLOYMENT OF IOT DEVICES

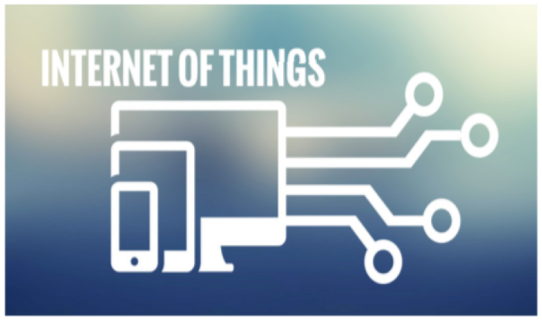


Source – Strategy Analytics research services ,October 2017: IoT Strategies , Connected Home Devices, Tablet and Touchscreen Strategies, Wireless Smartphone Strategies, Wearable Device Ecosystem, Smart Home Strategies

DIFFERENT APPLICATIONS OF IOT

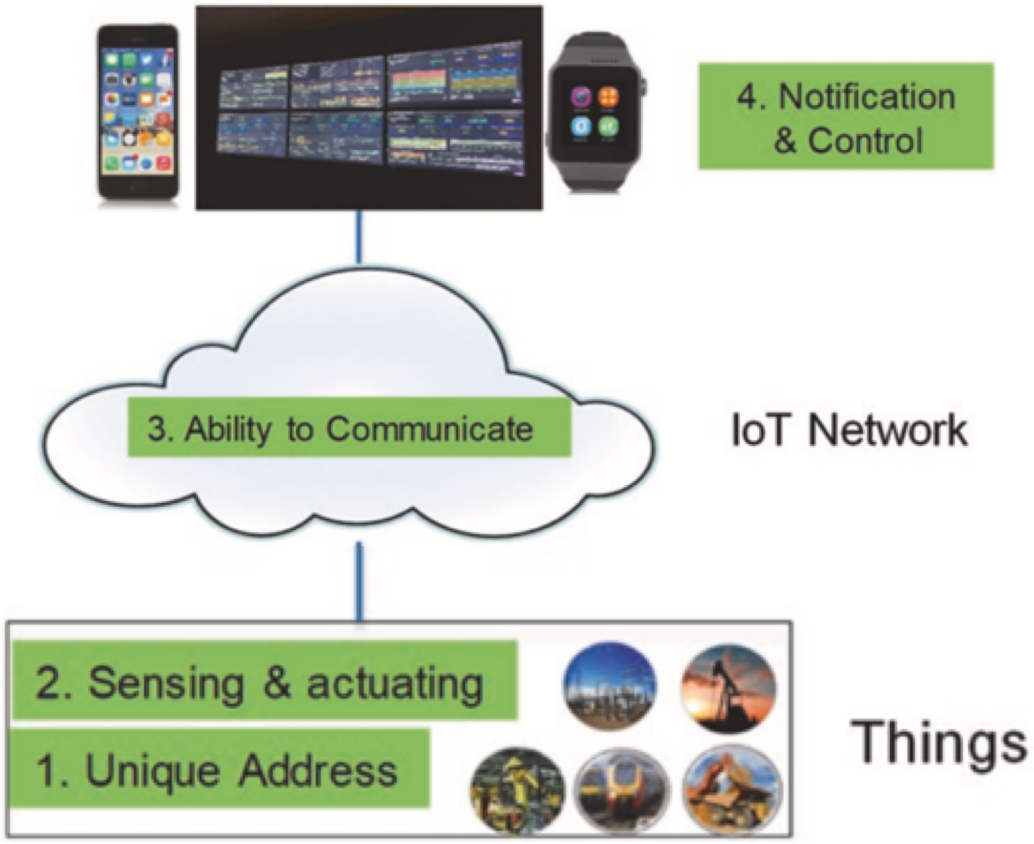









BASIC REQUIREMENTS FOR AN IOT SOLUTION



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.

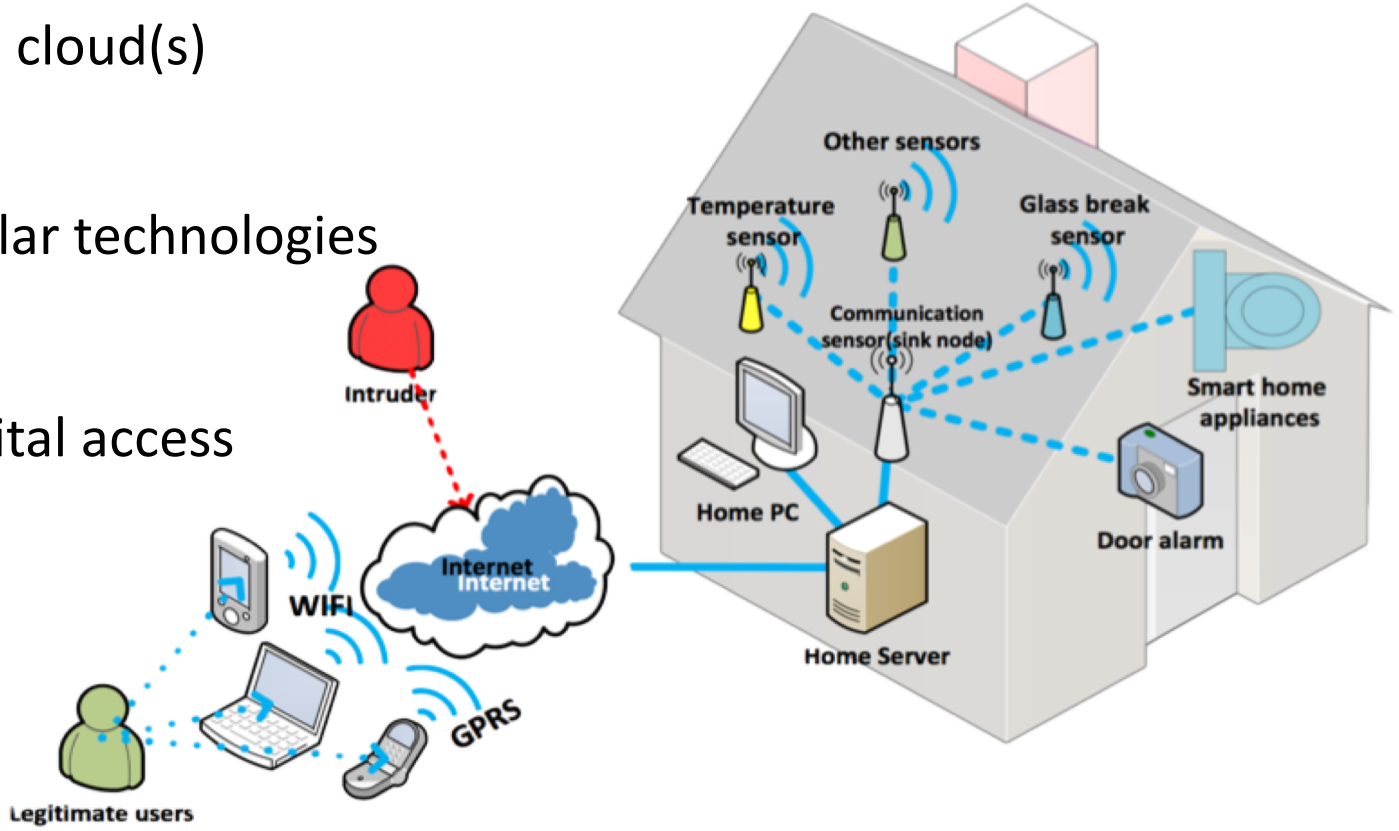
THE SMART CONNECTED HOME

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

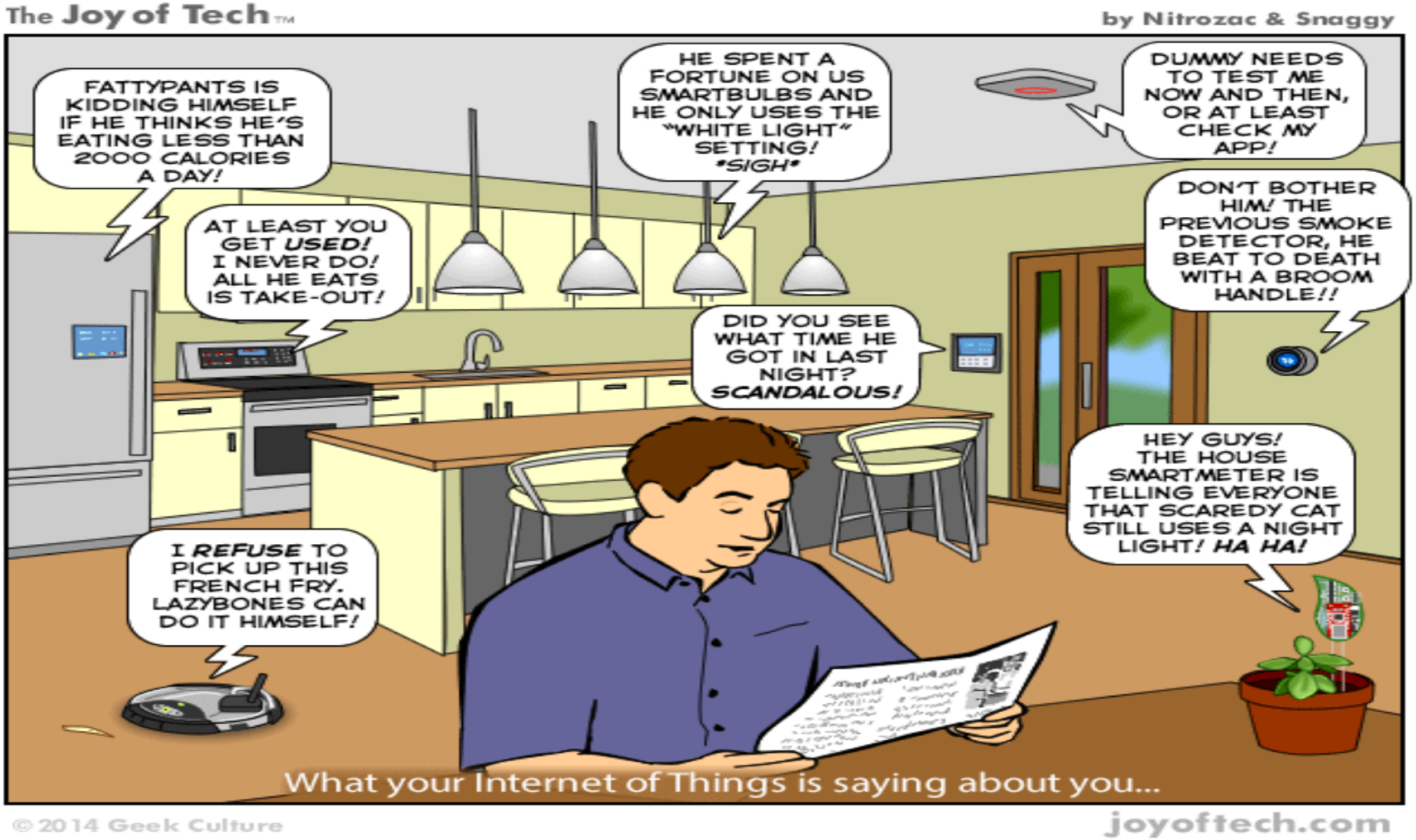
Image: Shutterstock

THE SMART CONNECTED HOME CHARACTERISTICS

- Perimeter in the cloud(s)
- Wireless & cellular technologies
- Physical and digital access



DIGITAL CHATTER INSIDE THE HOME



Challenges in Securing IoT

IOT REFERENCE FRAMEWORK

Software apps.

IoT Services

Network channels and infrastructure

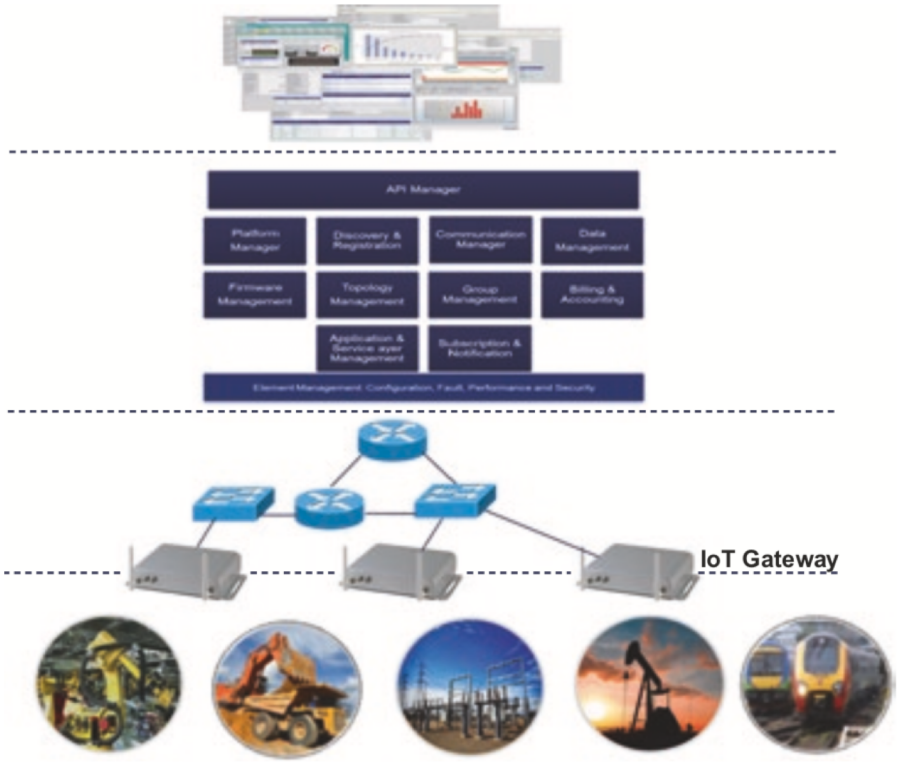
IoT Network

Sensors

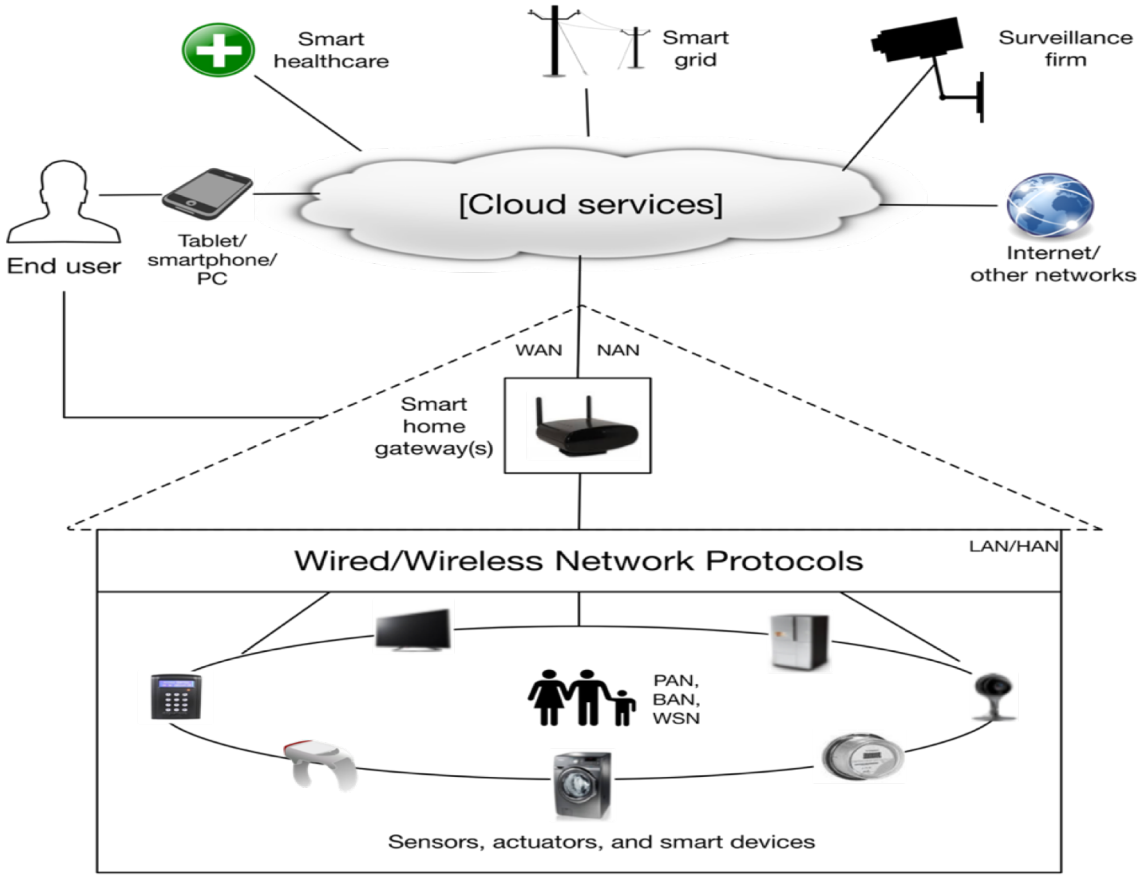
IoT Devices

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

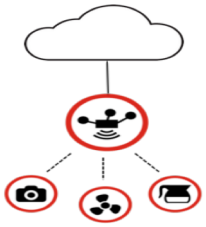
SOME DEVICE LEVEL CHALLENGES

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

- Lack of keyboard, mouse, and tactile screen

- Easily accessible devices are prone to physical attacks

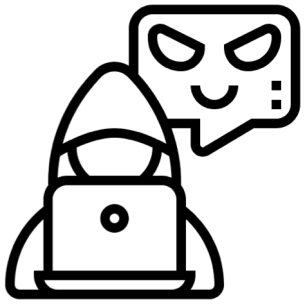
SOME NETWORK AND SERVICE-LEVEL CHALLENGES



- Use of bridges, hubs or gateways make the design of end-to-end security challenging

- Devices can join/leave the home networks anytime from anywhere

- Some devices are expected to operate for a long time without requiring maintenance



Attacks and Malicious Threat Agents

INFORMATION SECURITY DEFINITION

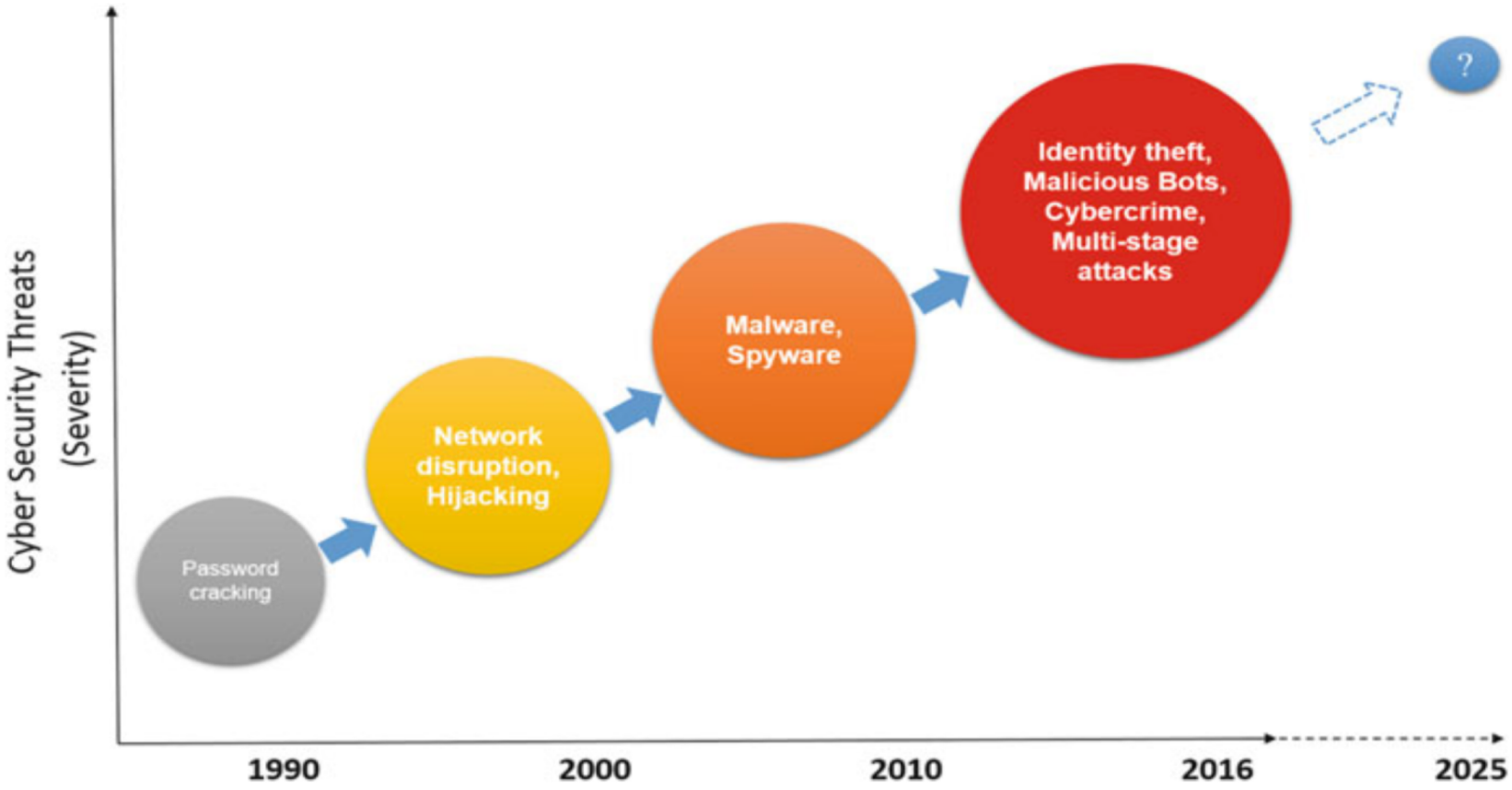
Information security is generally defined as the preservation of *confidentiality*, *integrity* and *availability* of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved (ISO27001)

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

EVOLUTION OF SECURITY THREATS OVER TIME



Source: Varadharajan, V., & Bansal, S. (2016). Data security and privacy in the internet of things (iot) environment. In *Connectivity Frameworks for Smart Devices* (pp. 261-281).

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

DOS AS AN EXAMPLE OF AN ATTACK ON DEVICES

IoT Devices

Example of an attack:

> *Denial-of-service*

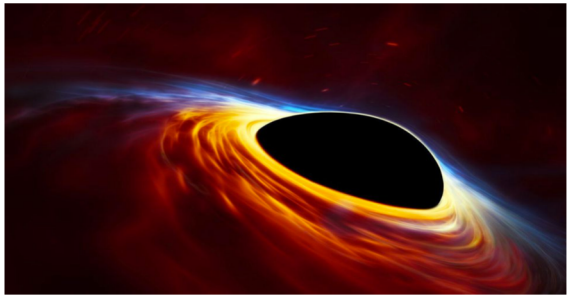
- ✓ ***Battery draining*:** By depleting the battery of a connected device, e.g., a smoke detector, an attacker will be able to disable a fire detection system
- ✓ ***Sleep deprivation*:** An attacker may attempt to send an undesired set of requests that seem to be legitimate but are not
- ✓ ***Outage attacks*:** Devices may stop functioning as a result of an unintended error in the manufacturing process, battery draining, sleep deprivation, etc.

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.

MALICIOUS INJECTION AS AN EXAMPLE OF AN ATTACK ON SERVICES

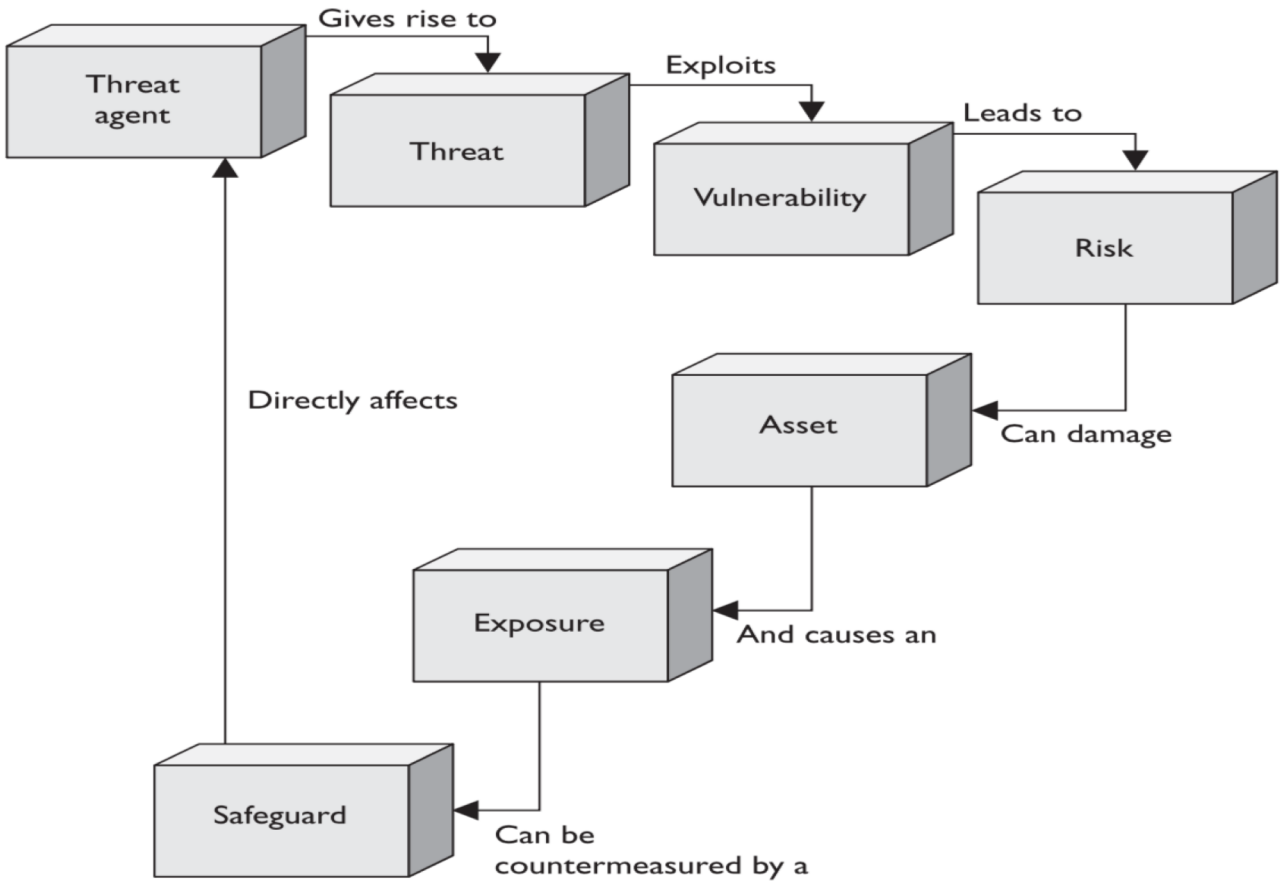
IoT Services

Example of an attack:

> Malicious injection

- ✓ Insufficient validation of the input may enable malicious input injection
- ✓ An attacker could inject a malicious input that causes the service providers to perform operations on behalf of the attacker
- ✓ For example, an attacker may add an unauthorized component that is capable of injecting malicious inputs into the servers. Afterwards, the attacker might be able to steal data, compromise database integrity, or bypass authentication
- ✓ Standard database error messages returned by a database may also assist the attacker

RELATIONSHIP AMONG THE DIFFERENT SECURITY CONCEPTS



MALICIOUS THREAT AGENTS

LICENTIATE THESIS

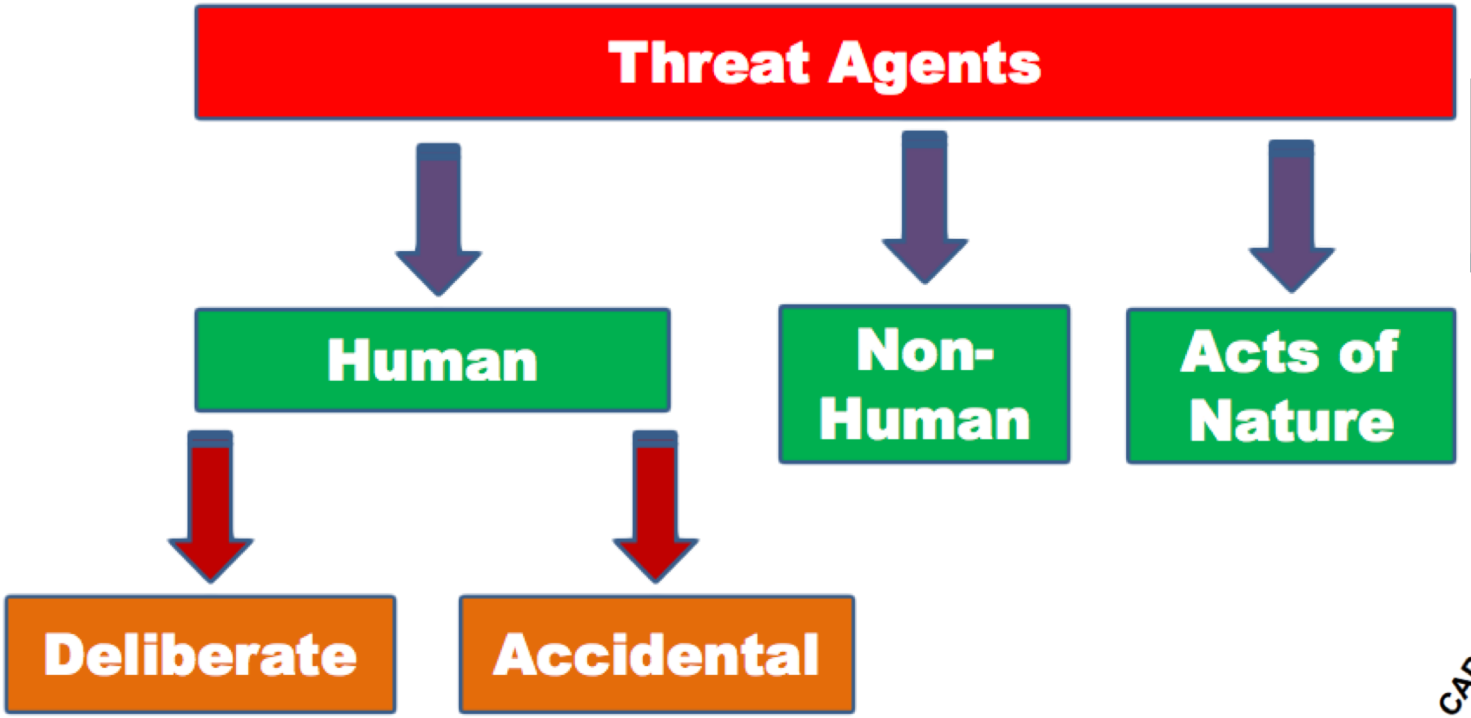
FOCUS ON THE ENEMIES

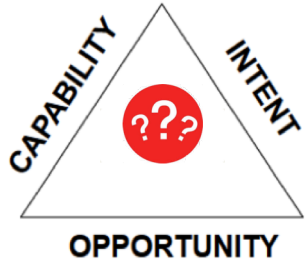
"*Know your enemy* and know yourself and you can fight a thousand battles without disaster"

- Sun Tzu

MALICIOUS THREAT AGENTS

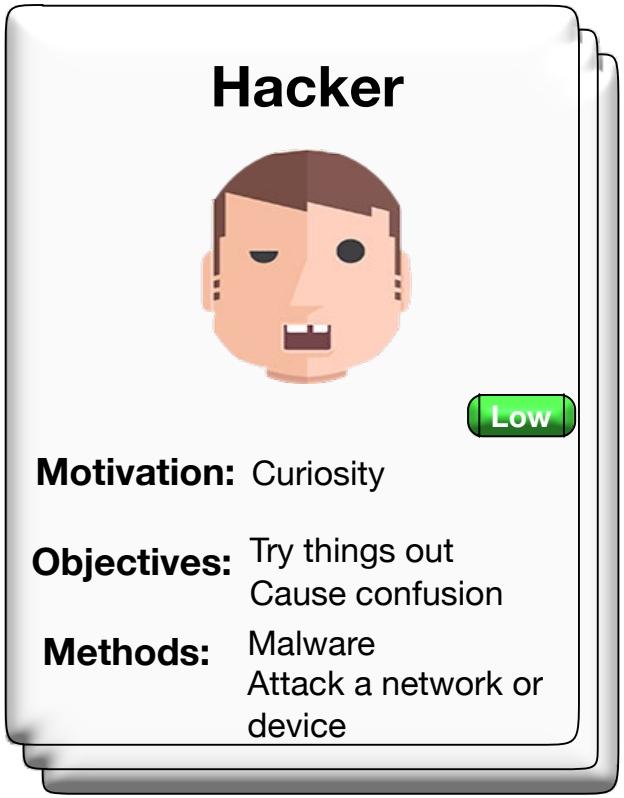
Threats can come from anywhere, but generally fall under three categories Human, Non-human, and Nature. Threats can also be deliberate or accidental.





MALICIOUS THREAT AGENTS

- ✓ *Threat agent archetypes* are collective descriptions of attacks, representing similar risk profiles
- ✓ Intelligent attackers whose motivations drive their objectives
- ✓ Attributes such as skills, access, and resources define their most likely methods



MALICIOUS THREAT AGENTS

HACKERS

- ✓ Individuals (“hobby hackers”) that include malicious persons, script kiddies, and nosy employees of an organization

SHODAN
Computer Search Engine

- ✓ Viruses, worms, phishing
- ✓ Primarily motivated by curiosity
- ✓ Skill-level: Apprentice

Low

THIEVES

- ✓ Opportunistic individuals that are associated with stealing mostly for personal financial gain

- ✓ System/physical intrusion, DoS, spoofing
- ✓ Main motive is monetary gain
- ✓ Skill-level: Apprentice

Low

HACKTIVISTS

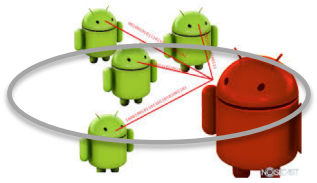
- ✓ Individuals or members of a larger group that pursue a political or social agenda

- ✓ DoS, fraud, and identity theft
- ✓ Primarily aim to promote and publicize their cause
- ✓ Skill-level: Apprentice

Low

COMPETITORS AND ORGANIZED CRIME

- ✓ Commercial competitors that compete for revenues or resources, and private criminal organizations



- ✓ Botnets, ransomware, and inside information

- ✓ Competitive advantage, CI, and monetization

- ✓ Skill-level: Journeyman

TERRORISTS

- ✓ Individuals that rely on violence or fear-related behavior to support personal socio-political agenda

- ✓ Damage/loss, outages, and physical attacks
- ✓ Terrorism
- ✓ Skill-level: Master

High

NATION STATES

- ✓ Highly sophisticated individuals that are funded by governments and associated with a military unit

ADVANCED PERSISTENT THREAT

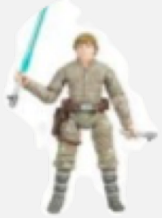
- ✓ Customized malware, spear phishing attacks, and zero-day attacks

- ✓ Cyber warfare, (counter-)intelligence

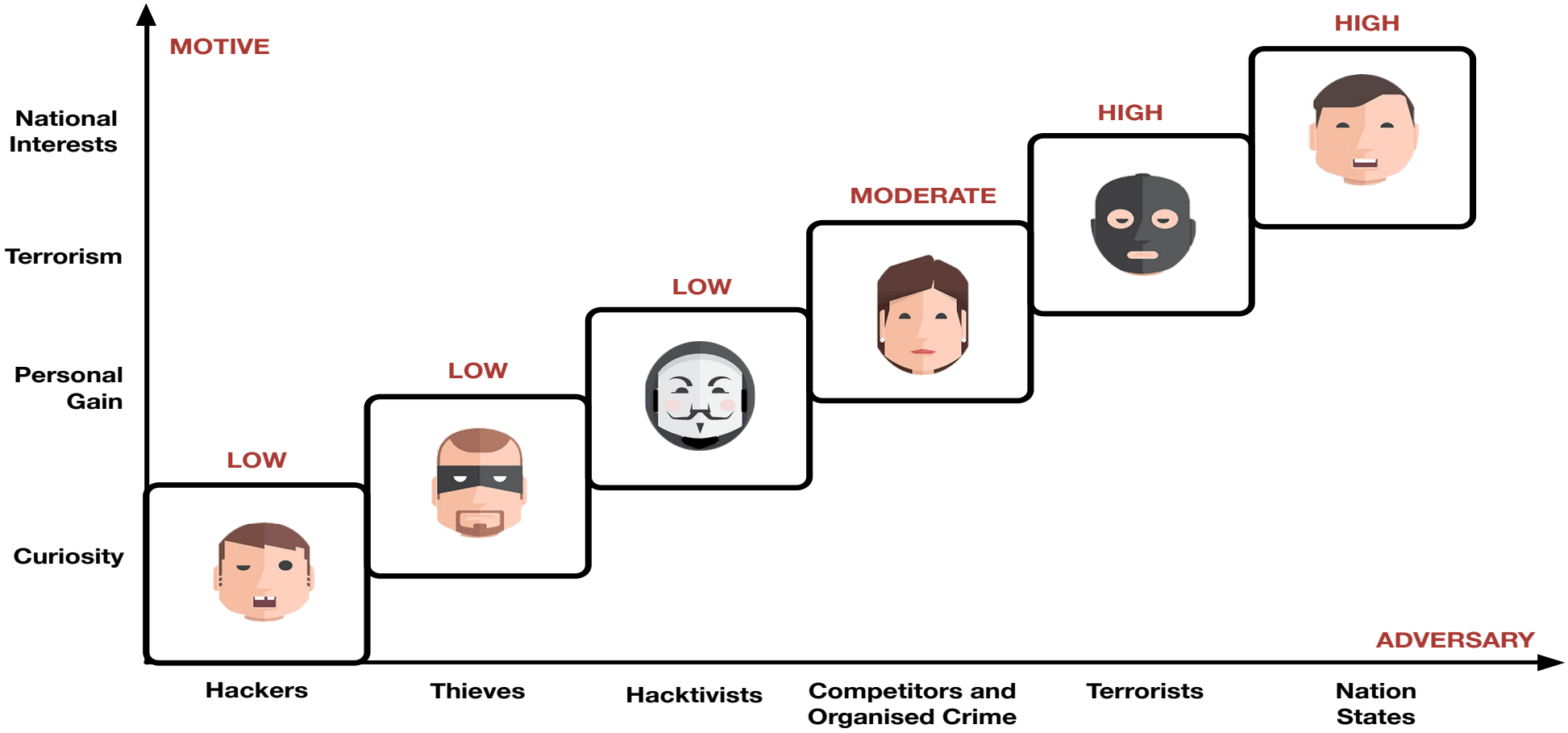
- ✓ Skill-level: Master

High

THREAT AGENT SKILLS

Low	Medium	High
Minimal technical skills 	Sufficient technical skills 	High-level technical skills 
Largest number of attackers	Locate new vulnerabilities	Write new powerful attack toolkits
Easiest to defend against	Threat agents with such skills are likely found in all classes	Hardest to defend against

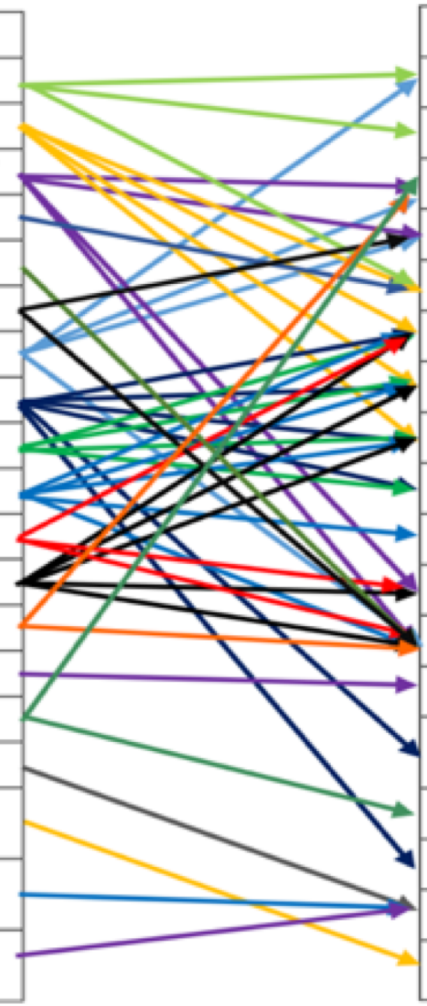
THREAT MODEL



Countermeasures

SUMMARY OF IOT SECURITY THREATS AND COUNTERMEASURES

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

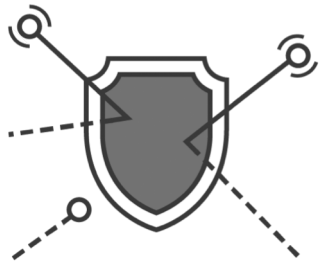


Countermeasures
Side-channel signal analysis
Trojan activation methods
IDSs
Securing firmware update
Circuit/design modification
Kill/sleep command
Isolation
Blocking
Anonymous tag
Distance estimation
Personal firewall
Cryptographic schemes
Reliable routing
De-patterning and Decentralization
Role-based authorization
Information Flooding
Pre-testing
Outlier detection

DEFENDING AGAINST DOS ATTACKS

IoT Devices

Intrusion Detection System



- ✓ IDSs provide a reliable approach to defend against battery-draining and sleep deprivation attacks by detecting unusual requests to the node
- ✓ Certain IDSs are designed to meet the requirements of IPv6 connected nodes of IoT, making it possible to detect various routing attacks
- ✓ IDSs can also detect the existence of a malicious node that tries to inject invalid information, including code injection attacks, into the system or violate a policy

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

DEFENDING AGAINST MALICIOUS INJECTIONS

IoT Services

Pre-testing

- ✓ Pre-testing attempts to identify the set of possible attack scenarios and simulate these scenarios to see how the system responds
- ✓ It also specifies what information should be logged and what information is too sensitive to be stored
- ✓ In addition, the input files should be closely examined to prevent the danger of malicious injection. For example, the attacker should not be able to execute any command by injecting it into the input files

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

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