

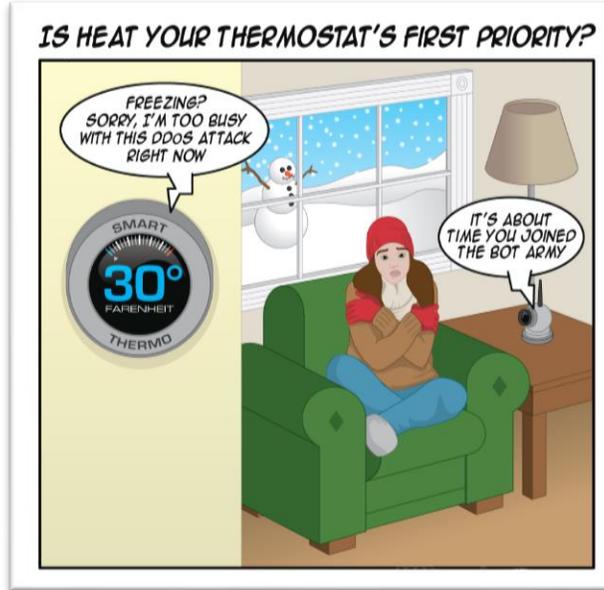
Cybersecurity in IoT

Part 3: Cybersecurity in the Internet of Things

Agenda

- 1** Motivation
- 2** Living in a Smarter World
- 3** Case Studies: Mirai Botnet
- 4** The Good side of the Internet of Things
- 5** Group work on Case Study
- 6** IoT Cybersecurity Challenges
- 7** Cybersecurity Technologies and Regulations for IoT
- 8** Summary and Q&A

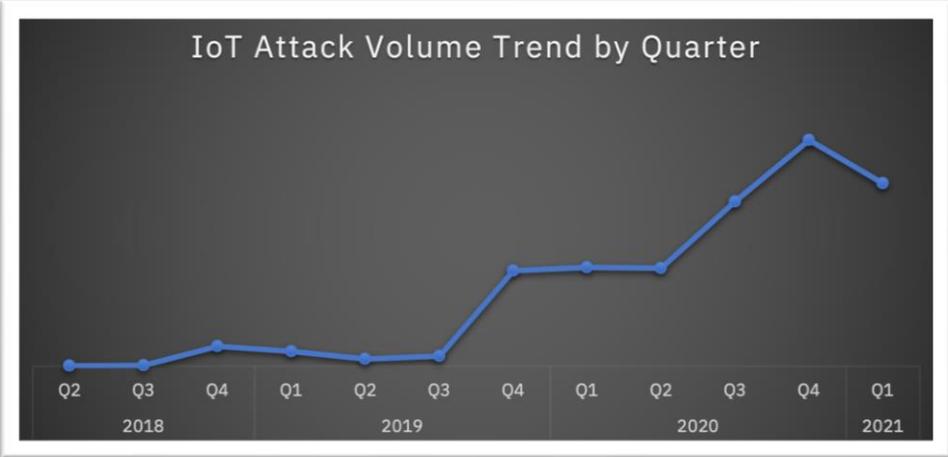
Cybersecurity in IoT: Motivation



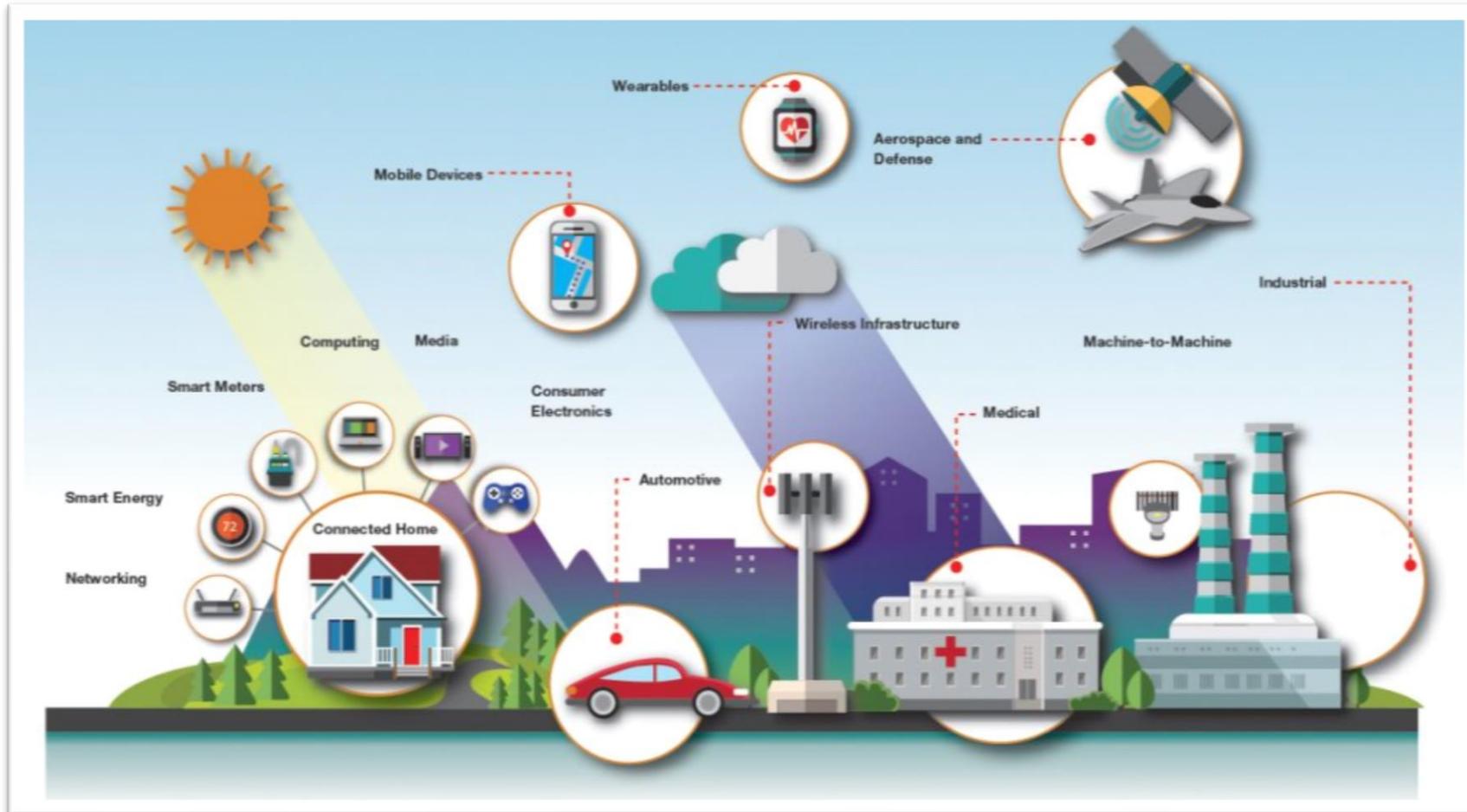
Your Philips Hue light bulbs can still be hacked — and until recently, compromise your network

IoT Insecurity: When Your Vacuum Turns on You

How to Hack and Exploit Printers in Seconds



The Internet of Things Living in a Smarter World



Hyper-connectivity

Millions of new end-points

Millions of new entry-points

Plethora of Information

More automation

Physical limitations to devices

Heterogeneous device landscape

The Internet of Things: Categories

	Description	Risks & Vulnerabilities
Smart Homes	Consumer IoT devices used in homes and buildings, can be connected to a single network and controlled remotely over the internet via a mobile device or computer.	<ul style="list-style-type: none">• High risk of exposing private and sensitive data• Usually private devices and networks are less protected• High number of entry points increases risk
Smart Cities	IoT devices and systems in the utilities, transportation, and infrastructure sectors communicate to create smart-grids, but also collect and share customer usage data to improve efficiency	<ul style="list-style-type: none">• Critical infrastructure like gas pipelines are exposed• Customer and citizen data collected might be sensitive• Increased attack surface for cyber-warfare
Industrial Internet of Things (IIoT)	Networked machines in a production facility can communicate and share information with the goals of improving efficiency, productivity, and performance	<ul style="list-style-type: none">• Increased vulnerability for (D)DoS attacks• Increased risk of IP leakage or sabotage• Increased risk of falling prey to ransomware attacks
Internet of Medical Things (IoMT)	Devices, such as heart monitors and pace makers, collect and send patient health statistics to health care providers for monitoring, analysis, and remote configuration	<ul style="list-style-type: none">• Patient data is more detailed and possibly exposed• An attack on IoMT could result in the loss of life• Most devices are not designed with security in mind

Cybersecurity Challenges in IoT: Mirai Botnet (2016)

Overview

What is Mirai?

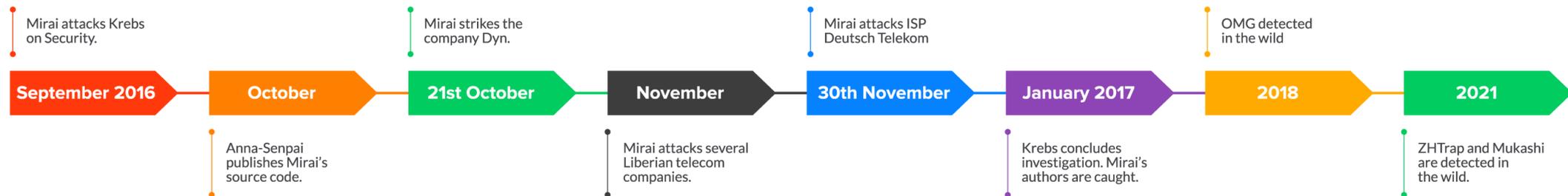
- The Mirai internet of things (IoT) botnet is infamous for targeting connected household consumer products
- Targets mainly cameras, alarm systems and personal routers

Why is Mirai dangerous?

- It conducts attacks fully automatic and can grow rapidly
- Its main attacks are (D)DoS attacks bringing down infrastructure
- It also has the capability of spying and collecting data in big scale

Who was targeted?

- Deutsche Telekom: More than 1 Million customers fall victim
- Lonestar Cell (Libarian Telecom): 616 attacks in a few months
- DYN: Impacted Netflix, Amazon, AirBnB, Twitter, Reddit and HBO

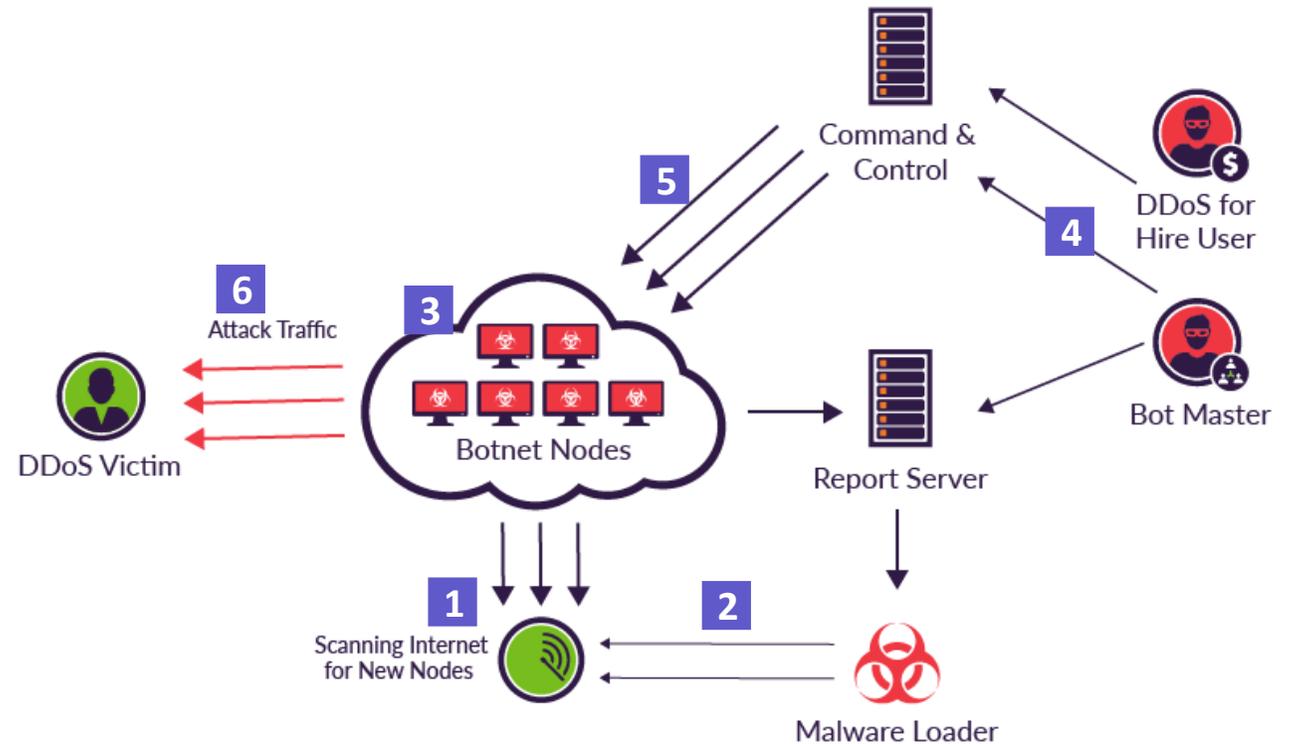


Cybersecurity Challenges in IoT: Mirai Botnet (2016)

The Landscape

- 1** Mirai scans the internet for vulnerable IoT devices (e.g. if default password set)
 - 2** Deploying malware customized to the attacked device
 - 3** The device joins the ranks of the botnet army, repeating the process
 - 4** The bot master issues an attack command to the command and control server
 - 5** The command and control system tells each node in the botnet to launch an attack
 - 6** Once the node receives an attack command it immediately executes the desired attack
-
- A** To protect itself it deletes itself from the file system once the malware is running and changes its name
 - B** As soon as it breaks into the system, it tries to prevent anyone else from breaking in using any other methods

Mirai at a Glance



Cybersecurity in IoT

The Good Side of the Internet of Things

Automation and Control

- Control manufacturing
- Control of smart-homes remotely and intelligent

Access Information in Real-Time

- Critical infrastructure can be monitored with sensors
- Fully automated intelligent warehouse

Improve Monitoring with Sensors

- Internet-connected tags on supermarket products
- Enhanced inventory control

Machine-to-Machine Communication

- Tracking of mileage and routes in cars
- Car-to-car communication

Better Quality of Life

- Smart devices in medicine
- Connected traffic lights
- Smart-home

Cost Reduction

- Light sensors result in lower utility costs
- More efficient production based on M2M com.

Increased Efficiency and Productivity of Businesses

- Improved data collection
- M2M communication
- Including the customer directly into the value chain

Big Data

- Prediction of customer behavior
- More efficient infrastructure

Cybersecurity in IoT

IoT as a Security Enabler

Home Security

- Connected remote accessible cameras enable people to check if everything is alright
- Connected sensors like smoke detector and heating enable early threat detection
- Remote controlled or automated devices like window shutter add security layer

Authentication & Sensors

- Authentication can be enhanced with 2FA and continuous authentication
- SIEM solutions are more sophisticated based on the number of sensors connected
- Platform security can be enabled to add another security layer into networks

Health related devices

- Remotely accessible Insulin pumps and sensors that detect blood sugar levels
- Heart pacer that can be updated and monitored remotely
- Activity tracker nowadays monitor many vital functions and can help detect threats early

Car-to-car communication

- Cars can talk to each other and warn each other about hazards on the way
- Distances can be monitored and automated breaking implemented

Group-work: «Task»

Case Study: The Jeep Hack (2015)



Watch

Watch the following YouTube video:

[Hackers Remotely Kill a Jeep on a Highway | WIRED - YouTube](#)



Task

- Time: 30 minutes
- Collaboration: Team up and work together
- Task:
 - Summarize the jeep hack briefly in your words
 - What IoT related challenges are being used? (see slide 4)
 - What is the danger here? How could that attack be mis-used?
 - What security principle (CIA) is attacked? (with explanation)
 - Discuss how this attack could be mitigated (CIA?)



***Note:** This task is mandatory for course completion. It can be done now or later, but will be part of the work-product of this session.*

The Internet of Things Cybersecurity Challenges I

	 Background	 Challenge	 Mitigation
1	<ul style="list-style-type: none">• Heterogeneous device landscape• Number of devices• No central platform to manage updates	Outdated Hardware and Software	<ul style="list-style-type: none">• Using device management systems• Implementing patch governance processes• Individuals: Focus on entree-points (router)
2	<ul style="list-style-type: none">• Lack of awareness by users• Number of devices• Plug-and-play default	Weak and default credentials	<ul style="list-style-type: none">• Trainings and security awareness• Enhanced Authorization and Authentication• Individuals: Focus on entrée-points (router)
3	<ul style="list-style-type: none">• Plethora of Information• High value of data and information• Lack in base-security raises attractiveness	Risk to privacy and data security	<ul style="list-style-type: none">• Trainings and security awareness• Restrict access of devices (need to know)• Enhanced passwords and protocols
4	<ul style="list-style-type: none">• New technology, regulations are behind• Legacy regulation standards, how to implement and what applies?	Regulations and Compliance	<ul style="list-style-type: none">• Following existing guidelines• Go through vulnerability and compliance assessment when acquiring smart devices

The Internet of Things Cybersecurity Challenges II

	 Background	 Challenge	 Mitigation
5	<ul style="list-style-type: none">• Number of sensors in a smart home• High number of entry-points (low security)• Hyper-connectivity	Home invasion	<ul style="list-style-type: none">• Limit capabilities of devices• Update passwords, protocols and patch• Separate devices and create safe rooms
6	<ul style="list-style-type: none">• Physical limitations to devices• Often lack of security by design	Lack of encryption	<ul style="list-style-type: none">• Implementing defense in-depth• Limit physical access• Vulnerability assessment and risk accept.
7	<ul style="list-style-type: none">• Large attack surface (many entry points)• Weak security standards• Attractive targets	Vulnerable to botnet attacks	<ul style="list-style-type: none">• Improve endpoint and network protection• Update passwords, protocols and patch• Network segregation
8	<ul style="list-style-type: none">• Possible gain from an attack is high• Security is often not properly implemented• Attack-shift to private households	Criticality and impact of attacks	<ul style="list-style-type: none">• Awareness and device landscape assessment• Protect critical assets with highest standards and countermeasures

IoT Device Management Platform

What is a IoT Device Management Platform?

Provisioning and authentication

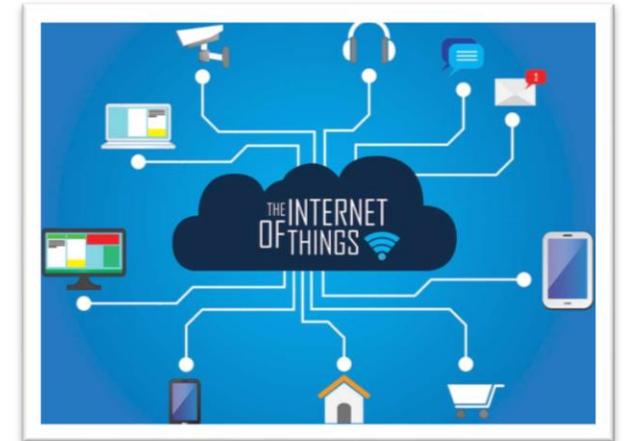
Remote configuration and management

Data collection and reporting

Real-time monitoring

Software deployments for updates and patches

Easy IoT device onboarding and offboarding



How does it improve IoT Cybersecurity?

Improves Update and Patch Management

Enables Incident and Event Monitoring

Enhances IAM Capabilities

Enables encrypted channels and sub-net configuration

General Data Protection Regulation (GDPR) Overview

What is GDPR?

General Data Protection Regulation published by the European Union

A set of unified rules regulating the protection of data

Relevant for all EU countries and impacting companies globally



What are the main goals?

The protection of personal and sensitive data

Improving data privacy rights of all European citizens

Return some control of personal data back to the owner

Impacts all companies that store or process data of European citizens

General Data Protection Regulation (GDPR)

Benefits for Data Owners

What is personal and sensitive data?

Personal data:

- Name
- E-mail / phone number
- Credit card information
- Address
- Other identifiers (like cookies)

Sensitive data:

- Biometric data
- Health information
- Genetic data

Data owners rights based on GDPR?

Right to Access

Data subjects have the right to request access to their data. Data controllers have to provide this access free of charge.

Right to Erasure

Data subjects may ask to exercise their right to erasure. Erasure means that the data controller has to delete the personal data. (There are certain limitations)

Right to Data Portability

Data subjects can request that the data be transferred either to themselves or to another controller.

Right to Rectification

Data subjects have the right to request rectification of incorrect or incomplete data. The data controller then has to correct the information as soon as possible.

Right to Restriction of Processing

Data subjects may request restriction. Restriction means that the data controller has to stop processing data for certain things. (not stop processing)

Right to Object

Data subjects have the right to object to the processing of their data if they have not given their consent. While there are exceptions this is generally true.

General Data Protection Regulation (GDPR)

Impact on Companies and Business

Data lifecycle changes

- Very big impact on almost every step in the cycle
- For big companies that means that all departments that collect or work with customer data need to be re-assessed and possibly adapted

Data monitoring & tagging

- Data needs to be continuously monitored
- Companies awareness of customer enhanced
- Information needs tagging and descriptions so it can be found and acted upon as required

Data processors validation

- A Data Protection Officer (CPO) is mandatory for companies of a certain size
- All possible processors of information need to be validated for the requirements as defined by GDPR

Consequences of data breaches

- Reporting of a data breach must happen in 72 hours
- Or a fine of up to 20Mio Euro (or 4% global revenue)
- This created large focus on data protection, because the impact of a data breach is affecting the risk



European Union Agency for Cybersecurity (ENISA)

Overview

The European Union Agency for Cybersecurity assists the **Commission**, the **member states** and, consequently, the **business community** in meeting the requirements of **network** and **information security**, including present and future **EU legislation**.

ENISA: IoT and Smart Infrastructures

ENISA focuses on the following **five domains** as part of their effort to **provide security guidance** for the Internet of Things and Smart infrastructures

- Internet of Things
- Smart Infrastructure
- Smart Transport
- Smartphone Guidelines
- Artificial Intelligence

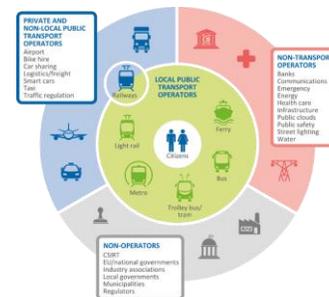
Internet of Things

ENISA developed a **Good practices** for IoT guideline and a **Smart Infrastructures Tool** to support individuals and companies on their path to a more **secure** IoT infra.



Smart Infrastructure

Develops **guidance** to secure **Smart Infrastructures** from cyber threats, by highlighting good **security practices** and proposing **recommendations**. Focus on **Smart Cities, Smart Homes, Smart Hospitals and Smart Grids**.



Smart Transport

Focuses on the security and safety of **smart cars** and **intelligent road systems**.



Cybersecurity in IoT

Summary

- **Living in a smarter world:**
 - The **good**: How IoT has **benefits** that are **outweighing** their downsides. (including benefits to cybersecurity)
 - The **bad**: Many **cybersecurity challenges** arise as the technology paradigm gains momentum
 - The **ugly**: There are many challenges around the IoT that can be attributed to a **lack of awareness** and **understanding**
- **IoT Cybersecurity challenges** (with case study)
 - We saw at multiple examples that IoT has truly some **cybersecurity challenges** that need mitigation and awareness
 - Especially the **number of devices, hyper-connectivity and device limitations** combined with **new sensors** and **criticality of information** they are able to access this is a hot topic
 - This results in challenges like botnets, lack of patch and password management, risk to privacy and lack of encryption
- **Cybersecurity Technologies and Regulations** for IoT
 - **IoT Device Management Platform** – enables companies to **control** and **manage** their IoT landscape **centrally**
 - **GDPR** – an EU regulation that addresses **data protection** for all citizens of the European Union
 - **ENISA** – an EU institution that develops **cybersecurity guidelines** and **frameworks** for countries, companies and individuals



Thank you!

