IOTWeek

Dublin —— June 20-23, 2022

Security & Privacy Threats

Antonio Skarmeta

David Goodman

Francesco Capparelli

Ruben Roex

GLOBAL VISION:

IoT TODAY AND BEYOND

IOTForum

New trends like IoT, 5G and continuum computing provide new opportunities and new threats

This is not only a technological challenge but also normative, legal and societal

We need to consider from the different angles the mechanisms for provide user an increase trustworthiness

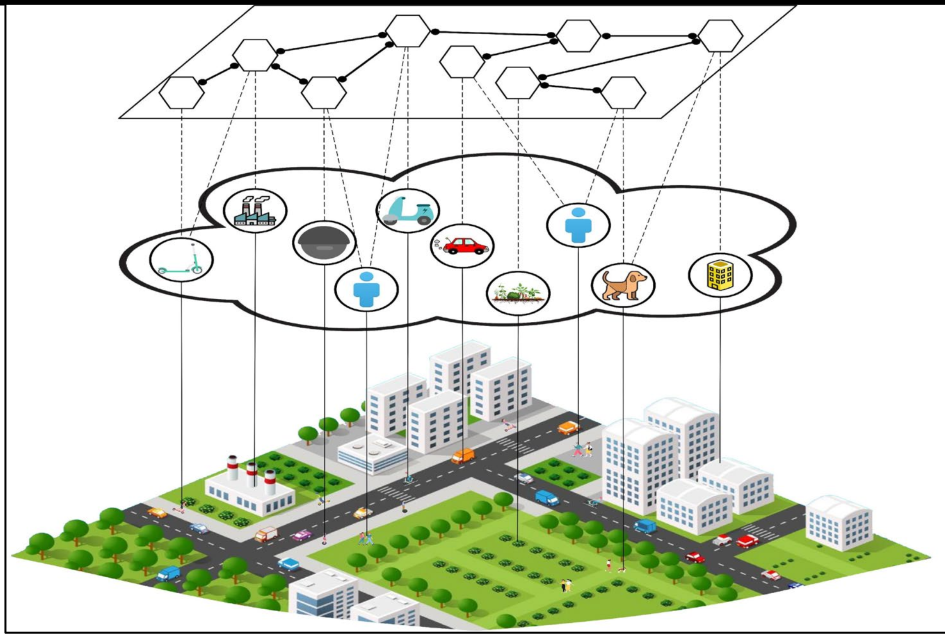
In this panel we will touch several of this issue with the next speakers:

Ruben Roex : TimeLex
Antonio Skarmeta: Universidad de Murcia-Spain
David Goodman: Trust in Digital Life
Francesco Capparelli: Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Antonio Skarmeta

Opportunity

- IoT devices and the emergence of 5G in our daily lives are bringing new data-driven and increasingly autonomous scenarios.
- Possibilities of highly distributed processing capacities from IoT-Edge-Cloud in a continuum:
  - New services requires efficient and effective management of computing and network resources
  - Means to deal with huge amounts of data and at different levels of the future NG infrastructure and manage its security

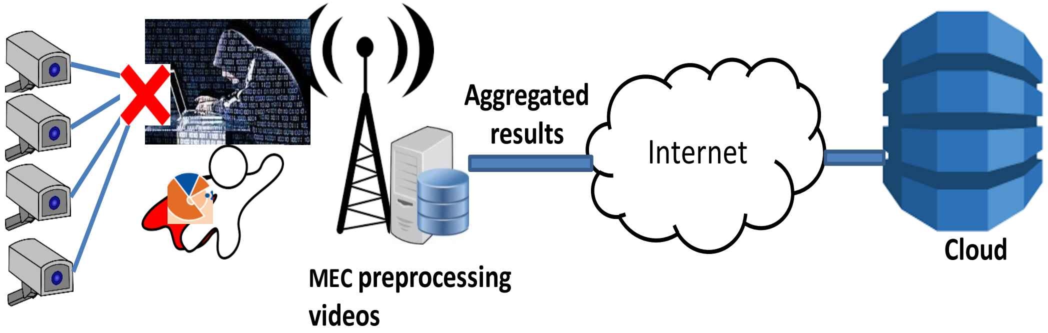


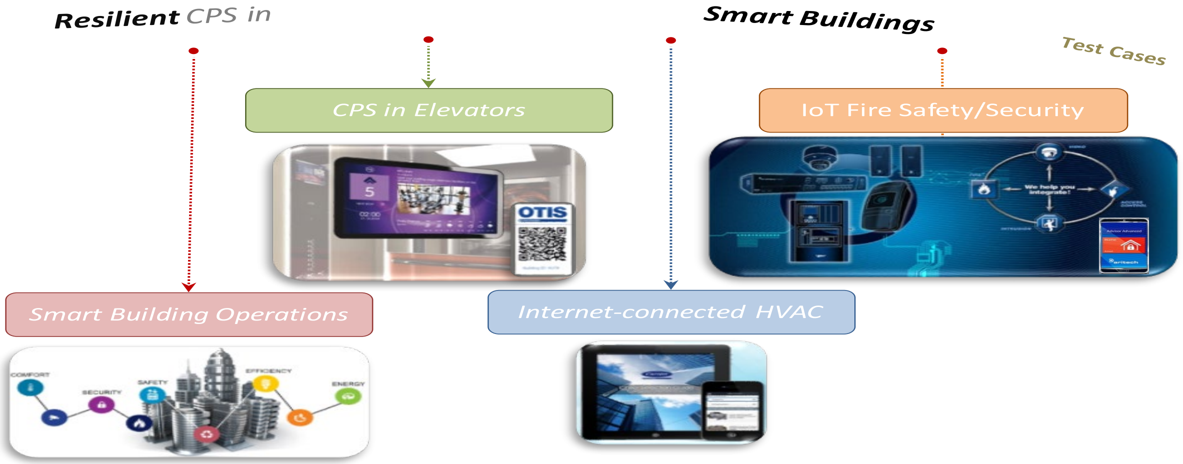
Need for configuration, architecture and coordination of security and privacy processing nodes at different levels: end-device – edge – cloud … and beyond

Attacking IoT

IOTWeek
Dublin — June 20-23, 2022

- Default, weak, and hardcoded credentials
- Difficult to update firmware and OS
- Lack of vendor support for repairing vulnerabilities
- Vulnerable web interfaces (SQL injection, XSS)
- Coding errors (buffer overflow)
- Clear text protocols and unnecessary open ports
- DoS / DDoS
- Physical theft and tampering





Digitalization it is transforming most of the economic sector and it is a quite relevant change

Now ICT are like any other utility like energy or water, and are fundamental to the development of the business and at the same time are because of that a critical factor.

5G and IoT tecnologies providing hyperconnectivity it is also creating new attack vector and provide new opportunites for threats

Trust between the stakeholders in the different value chains are becoming more important and as a consequence the data sharing, privacy aspects etc are new challenges to be managed

Threats

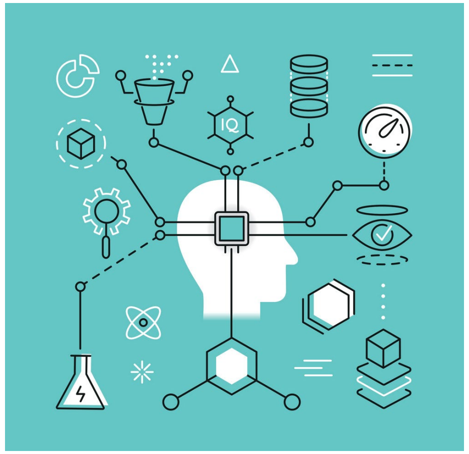
- As companies digitize businesses and automate operations, cyber risks proliferate
- As technology advances, so does the level of cyber risk that organizations must navigate.
- It is no secret that the financial costs of a cyber-attack could be large enough to cripple small and medium-sized businesses.
- Also reputation could affect companies if costumer privacy is being violated, altering consumer trust and long-term brand reputation.

Threat Intelligence Challenges and Opportunities cooperation

From Data to Intelligence

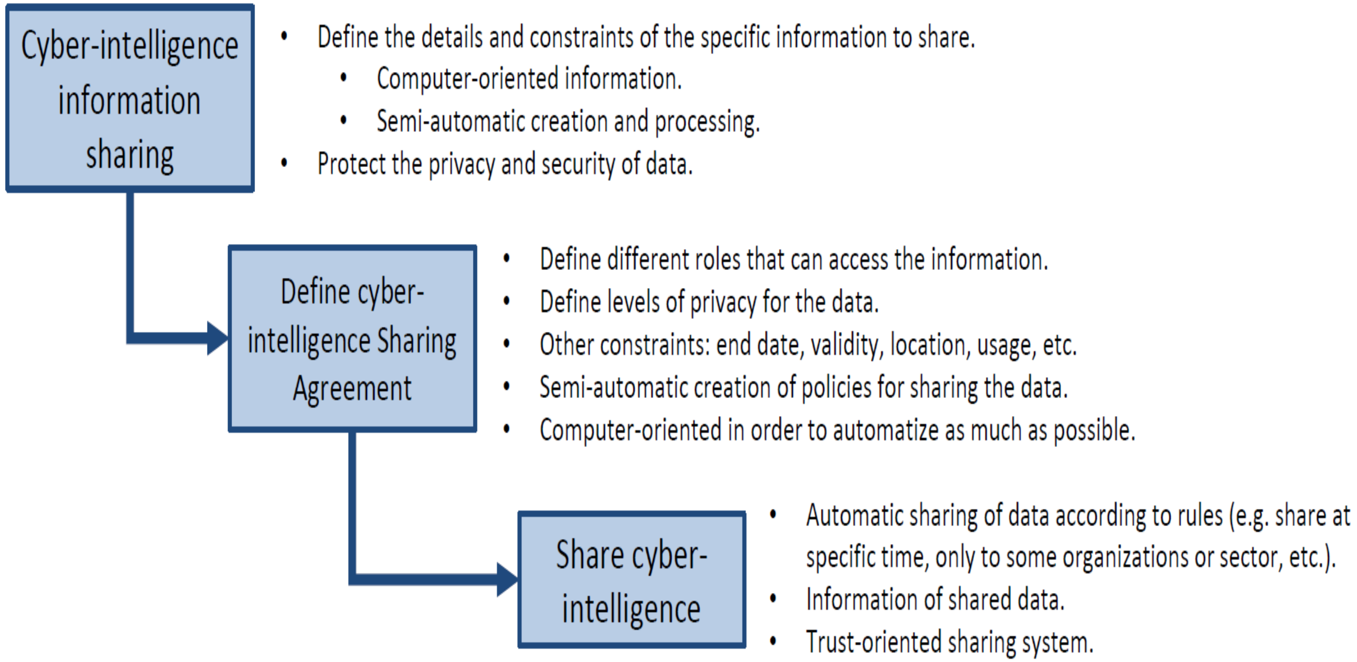
High volume of data needs to be stored, processed, analysed and used to react.

We need to automate it



Heterogeneous data, formats and sources, even regulation.
Companies can share this information and identify common attacks

BUT how to maintain privacy and critical information under control



Cyber-intelligence information sharing

- Define the details and constraints of the specific information to share.
  - Computer-oriented information.
  - Semi-automatic creation and processing.
- Protect the privacy and security of data.

Define cyber-intelligence Sharing Agreement

- Define different roles that can access the information.
- Define levels of privacy for the data.
- Other constraints: end date, validity, location, usage, etc.
- Semi-automatic creation of policies for sharing the data.
- Computer-oriented in order to automatize as much as possible.

Share cyber-intelligence

- Automatic sharing of data according to rules (e.g. share at specific time, only to some organizations or sector, etc.).
- Information of shared data.
- Trust-oriented sharing system.

In the age of analytics and intelligence,

- AI-driven or human-driven attacks
  - AI-driven malware to start mimicking behavior
  - Advanced human attacker groups utilizing AI-driven techniques to improve their attacks
- But also !!! AI shifts the advantage from Cyber Criminals to Cyber Defenders
  - AI systems are now able to aggregate and analyze massive amounts of data
    - to detect hidden threats
    - ML systems to improve the accuracy and efficiency of its data analysis
  - AI enable the automatic prevention, detection, and response to cyber threats at a new level of accuracy and speed
  - AI helps on increasing the autonomy in the response and fast reaction → important for distributed paradigms
- AI will support both cyber defence but also offense: learning policies and identification innovative ways to counter attacks

Compliance and Trust

Today, compliance, data protection, privacy preservation, green and responsible data operations are difficult to handle in such multi-actor and fragmented environments.

Difficult for data owners (data subjects, companies and public administrations) and the other stakeholders to have a transparent and comprehensive view of such data processing activities.

This turns accountable compliance in multi-actor data spaces even more challenging and can consequently seriously hamper the necessary trustworthy, user-friendly, safe and fair sharing and manipulation of data within and across data spaces,

There is a need to enhance protection and compliance management of data, while preventing digital fragmentation of services and data

Challenges

Lack of economic incentives for data protection

Non control over data disclosure

Difficulties to implement PET or data protection

Accountability of data provided by IoT

Data analytics improve the interrelation of up to now disconnected data

Privacy Enforcement in distributed scenarios

Doubt 1: Is it possible to connect anything to the Internet?

Doubt 2: Do we want to connect everything to the Internet?

- Business protection
- Security and Privacy
- Trustworthy

GOOD AFTERNOON MR. HENFENNEL! HEMORRHOID CREAM AISLE SIX!
Beep!
TOO MUCH INFORMATION IN MY MEDICAL I.D. CHIP.
DON'T FORGET MOUTHWASH. I FIGURED THAT ONE OUT BY MYSELF.
TOLES
10-6 © 2004 THE WASHINGTON POST

IOTWeek

Dublin —— June 20-23, 2022

Thank you!

Find more:

UNIVERSIDAD DE **MURCIA**

Cyber Security for Europe

iotweek.org