Risk Assessment in IoT
Case Study: Collaborative Robots System

AUTHORS : Salim Chehida, Abdelhakim Baouya, Miquel Cantero, Paul-Emmanuel Brun, and Guillemette Massot

Presented by Salim Chehida (University of Grenoble Alpes) at :

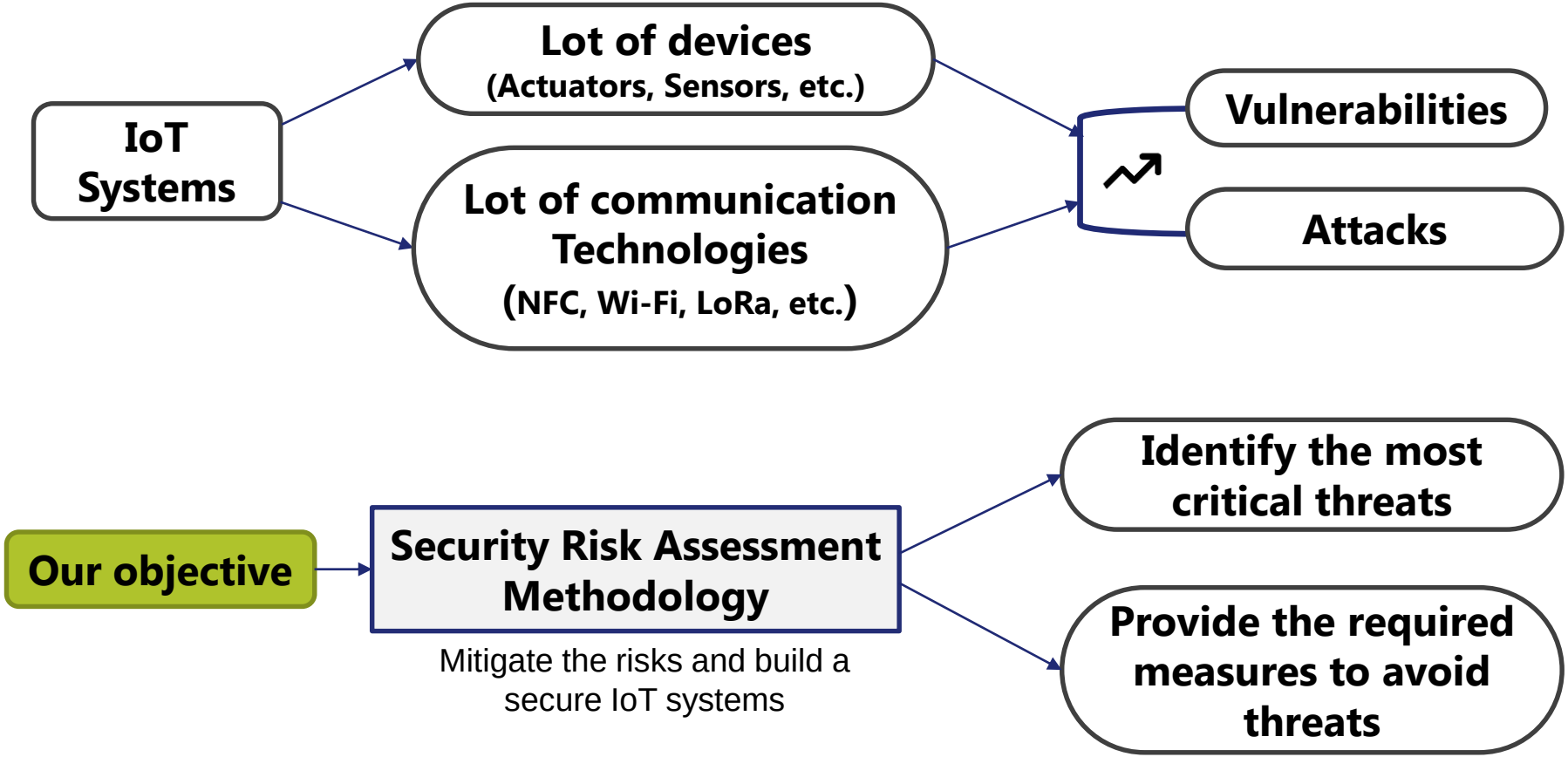
ECLIPSE SAM IoT

VIRTUAL CONFERENCE, SEPTEMBER 17-18, 2020

OUTLINE

- INTRODUCTION
- STATE OF THE ART
- APPROACH
- CASE STUDY
- IDENTIFICATION OF ASSETS
- IDENTIFICATION OF THREATS AND VULNERABILITIES
- SPECIFICATION OF SECURITY OBJECTIVES AND REQUIREMENTS
- CONCLUSION

INTRODUCTION



STATE OF THE ART (SECURITY STANDARDS)

Common Standards

ISO/IEC 27002, ISO/IEC 27005, AS/NZS 4360, BS7799 (ISO17799), NIST SP 800-30, NIST SP 800-82, IEEE 1686.

IoT Security Standards

- ITU-T (Y.2060, Y.2063, Y.2066, Y.2067, Y.2068, Y.2075,etc).
- ISO/IEC 30128: covers IoT security related to sensor network application interface.
- ETSI TS103645: gives security practices for consumer devices connected to the Internet.

ISO/IEC 27002

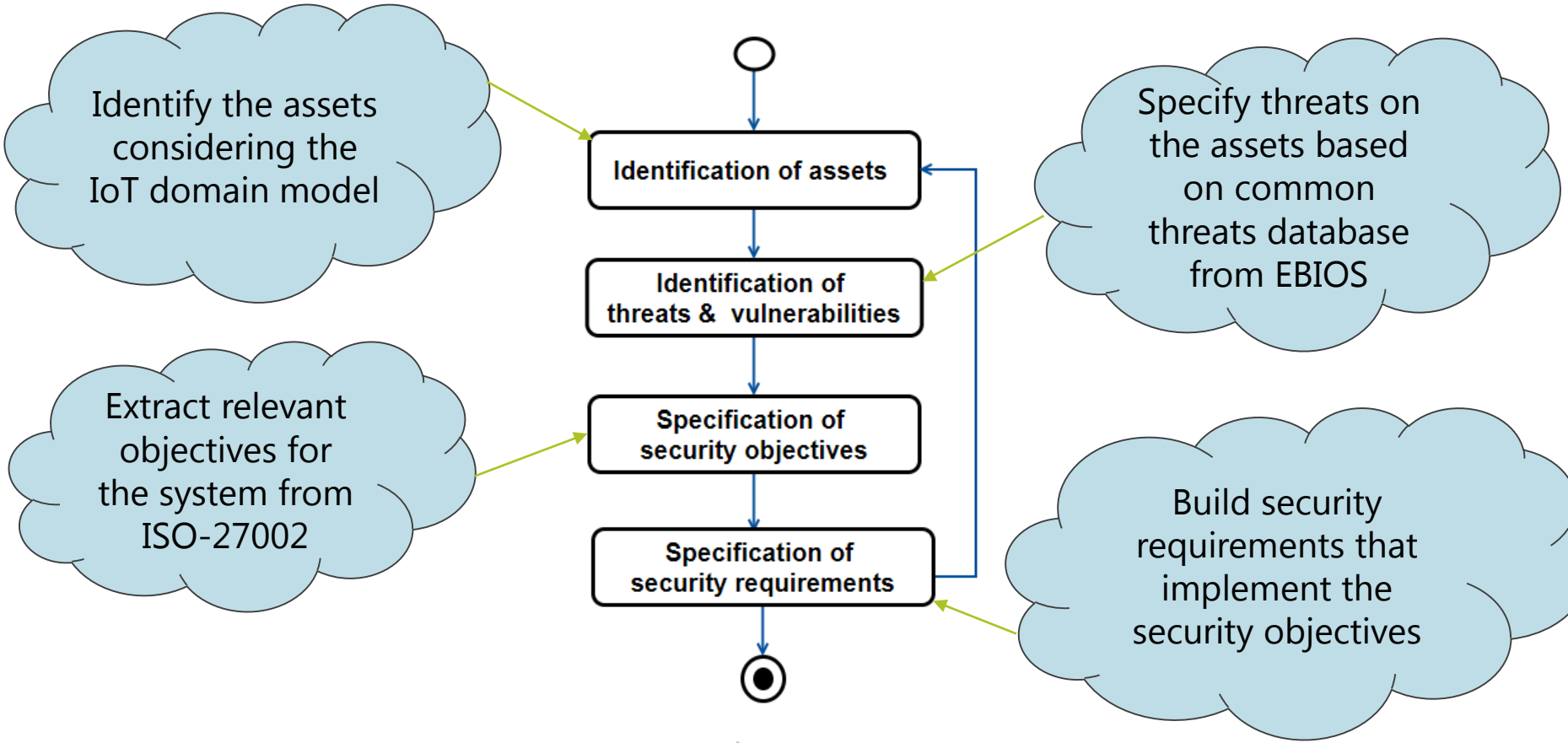
- International standard that gives general guidance on the commonly accepted goals structured around 36 security objectives and 133 controls.

STATE OF THE ART (RISK ASSESSMENT METHODS)

- **EBIOS** is used for the assessment and treatment of risks associated with an Information System.
- **CRAMM** is a qualitative risk assessment methodology.
- **AURUM** methodology that supports the NIST SP 800-30 standard.
- **CORAS** allows risk assessment, documentation of intermediate results, and presentation of conclusions.
- **MEHARI** aims to provide a risk management model compliant to ISO-27005.
- **OCTAVE** allows to define a risk-based strategic assessment and planning technique for system security.
- **IT-Grundschutz** provides methods, processes, procedures, and measures to establish a system for information security management.

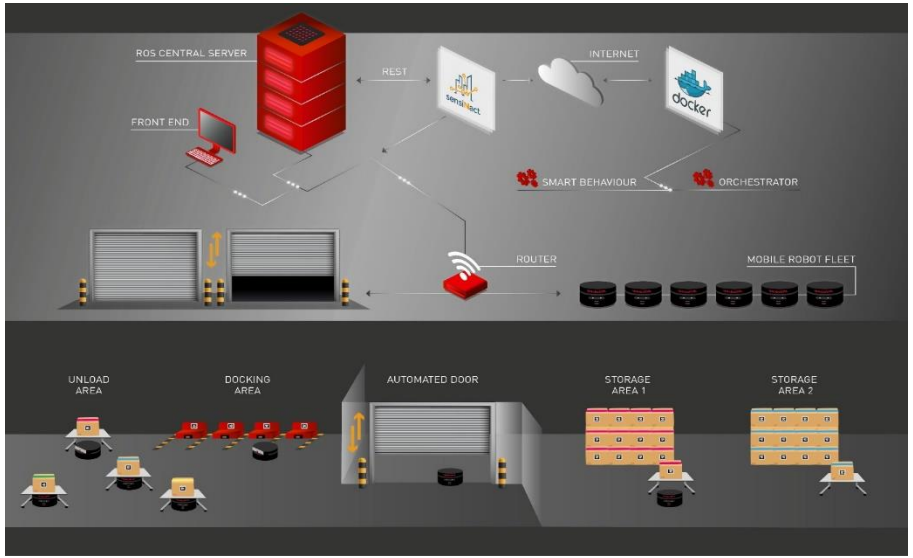
Generic, and they do not consider the complexity and the dynamic of IoT systems

APPROACH


Identify the assets considering the IoT domain model
Identification of assets
Identification of threats & vulnerabilities
Specify threats on the assets based on common threats database from EBIOS
Extract relevant objectives for the system from ISO-27002
Specification of security objectives
Specification of security requirements
Build security requirements that implement the security objectives

CASE STUDY (SERVICE ROBOTICS SYSTEM)

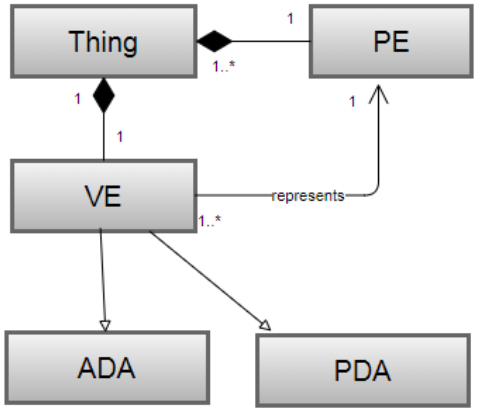
- A fleet of robots installed in a warehouse to support the movement of loads.
- Robots are expected to empty continuously an “unload area”.
- Each robot picks item and places it in a specific storage area following some predefined rules.

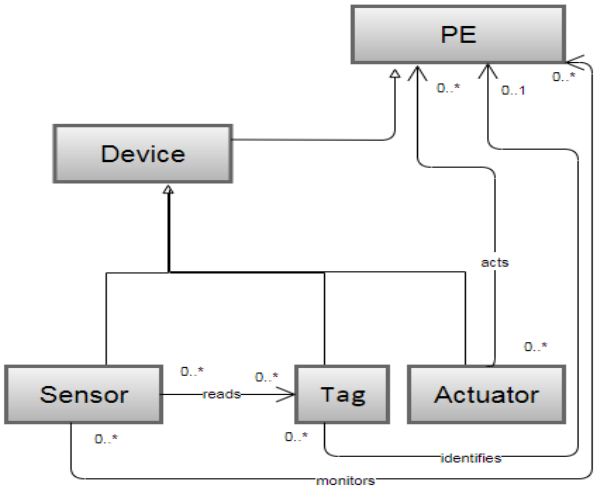


IDENTIFICATION OF ASSETS

- An asset is “any tangible or intangible thing or characteristic that has value to an organization”. [ISO-27001]

IoT Domain Model





IDENTIFICATION OF ASSETS (EXAMPLES)

Asset ID	Asset Description
A1	Mobile Robot: Embedded Computer
A2	Mobile Robot: Motion Control (motor driver)
A3	Mobile Robot: Sensor 1, RGBD Camera
A4	Mobile Robot: Sensor 2, Lidar
A5	Mobile Robot: Sensor 3, Odometry
A6	Mobile Robot: Lift Mechanism
A7	Mobile Robot: Battery (LiFePo)
A8	Mobile Robot: Network (Card)
A9	System: User Computer
A10	System: Network (Router and infrastructure)
A11	System: Mission Command (Outwards)
A12	System: Robot State (Inwards)
A13	Door PLC
A14	PLC WiFi Gateway
A15	PLC: Opening order (Inwards)
A16	Operator HMI

IDENTIFICATION OF THREATS AND VULNERABILITIES

Threat is “a potential cause of an unwanted incident, which may result in harm to a system or organization”. [ISO-27001]
Vulnerability is “weakness that is related to the organizations’ assets, which sometimes could cause an unexpected incident”. [ISO-27001]

EBIOS Threats Database

- Physical damage: T-1010 to T-1050.
- Natural events : T-2010 to T-2050.
- Loss of essential services : T-3010 to T-3030.
- Disturbance due to radiation : T-4010 to T-4030.
- Compromise of information : T-5010 to T-5110.
- Technical failures : T-6010 to T-6050.
- Unauthorized actions : T-7010 to T-7050.
- Compromise of functions :T-8010 to T-8050.

IDENTIFICATION OF THREATS AND VULNERABILITIES (EXAMPLES)

ID	Threats Description	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16
T-1010	Fire	X	X	X	X	X	X	X	X	X	X			X	X		
T-1020	Water damage	X	X	X	X	X	X	X	X	X	X			X	X		
T-1030	Pollution	X	X	X	X	X	X	X	X	X	X			X	X		
T-1040	Major Accident	X	X	X	X	X	X	X	X	X	X			X	X		
T-1050	Destruction of equipment or media	X	X	X	X	X	X	X	X	X	X			X	X		
T-2010	Climatic Phenomenon	X	X	X	X	X	X	X	X	X	X			X	X		
T-2020	Seismic Phenomenon	X	X	X	X	X	X	X	X	X	X			X	X		
T-2030	Volcanic Phenomenon	X	X	X	X	X	X	X	X	X	X			X	X		
T-2040	Meteorological Phenomenon	X	X	X	X	X	X	X	X	X	X			X	X		
T-2050	Flood	X	X	X	X	X	X	X	X	X	X			X	X		
T-3010	Failure of air-conditioning	X	X							X				X			
T-3020	Loss of power supply	X	X	X	X	X	X	X	X	X	X			X	X		
T-3030	Failure of telecommunication equipment	X							X		X	X	X		X	X	X
T-4010	Electromagnetic radiation								X		X	X	X		X	X	X
T-4020	thermal radiation	X	X	X	X	X	X	X	X	X	X			X	X		
T-4030	Electromagnetic pulses	X	X	X	X	X	X	X	X	X	X			X	X		
T-5010	Interception of compromising interference signals										X	X	X		X	X	X
T-5020	remote spying			X													X
T-5030	eavesdropping	X							X		X	X	X		X	X	
T-5040	Theft of media or documents													X	X		
T-5050	Theft of Equipment	X	X	X	X	X	X	X	X	X	X			X	X		
T-5060	Retrieval or recycled or discarded media																X

SPECIFICATION OF SECURITY OBJECTIVES

- Extract security objectives needed to protect the system assets against the identified threats from ISO-27002 generic list.
- Map each security objective with the threat list.

ID	Security Objective	Security Objective Description	Threats
O1010	Protection Against Malicious Code	Prevent and detect the allocation of any malicious code, as well as connections of any unprivileged user to the robot network	T-50xx
O1020	Backup	The data from the initial robot setup and the robot firmware require regular backup	T-10XX T-20XX
O1030	Network Security Management	Protect the information and communication in network from a client to robot. Sending REST Command once authenticated in the same network can modify the operations	T-5030 T-5090 T-7010 T-7020 T-7040
O1040	Exchange of information	Secure the interaction between the platform and robot system	T-5070 T-5080
O1050	Monitoring	Logs and robot system state shall be secured to prevent a bad usage (i.e. a door opened)	T-5030 T-5040 T-60xx T-70xx T-80xx

SPECIFICATION OF SECURITY REQUIREMENTS

- Define security requirements needed to ensure each security objective.

Objective ID	Requirement ID	Requirements Description
O-1010	R-1010-0010	REST API must detect malformed commands
	R-1010-0020	Access to the REST API must be authenticated
	R-1010-0030	Robot firewall should block all the connection except SSH
	R-1010-0040	SSH connection should be restricted to unprivileged users
O-1020	R-1020-0010	Robot firmware should be stored in a non-erasable memory
O-1030	R-1030-0010	Network access must require authentication
	R-1030-0020	Network communication from a client with a robot must be authenticated and encrypted
O-1040	R-1040-0010	Communication from platform to robot must be authenticated and encrypted (e.g: using protocol like TLS1.2 minimum)
O-1050	R-1050-0010	Access to log information must be limited to authorized person only

CONCLUSION

Advantage of our method :

- Considers IoT domain model to identify all system assets.
- Follows security standards to define security requirements of IoT systems.
- Iterative approach that responds to the need for evolution.

Applications :

- Collaborative Robots System
- Water Management Infrastructure

CONTACTS

SALIM CHEHIDA

RESEARCHER, UNIVERSITY OF GRENOBLE ALPES

Salim.Chehida@univ-grenoble-alpes.fr