11-Mar-2019

IoTSM: An End-to-end Security Model for IoT Ecosystems

Joseph Bugeja

Andreas Jacobsson

Bahtijar Vogel

Rimpu Varshney

MALMÖ UNIVERSITY
INTERNET OF THINGS AND PEOPLE RESEARCH CENTER

KK-stiftelsen

AGENDA

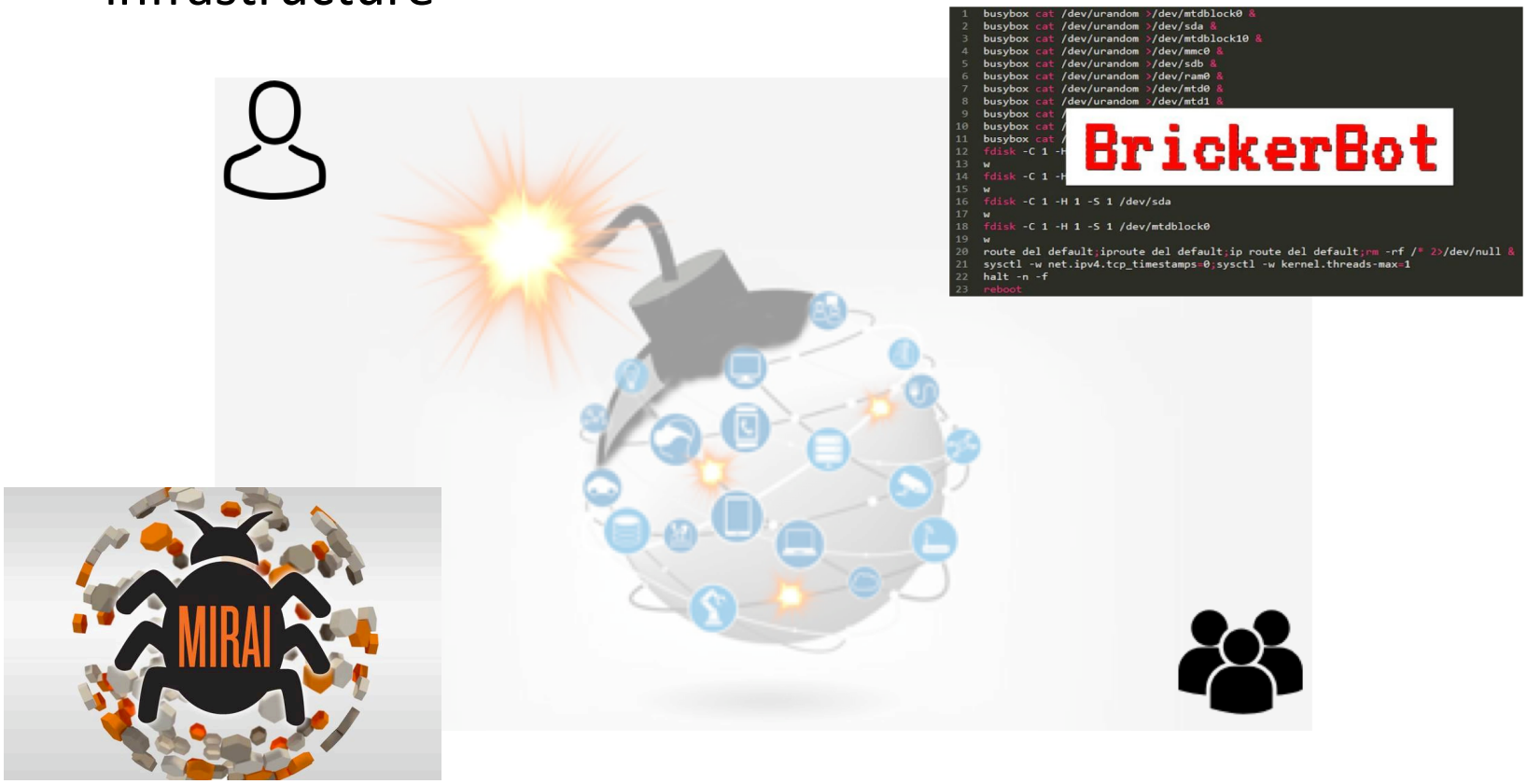
1. Introduction
2. Security Frameworks
3. Research Method
4. The IoTSM
5. Reflections, Remarks & Future Work

INTRODUCTION

- ✓Over 20 billion Internet of Things (IoT) devices by 2020
- ✓Internet-connected devices will outnumber people at least 2:1
- ✓Global market size of about $457B by 2020
- ✓Applications range from domestic to industry scenarios

INTRODUCTION

✓Surge of attacks targeting individual users to critical infrastructure



PROBLEM

- ✓Security is new to many manufacturers operating in the IoT domain

- ✓Implementing Secure Software Development Life Cycle (SSDLC) methodologies is challenging

- ✓Lack of visibility over which processes are used by actual IoT practitioners

- ✓Shortage of end-to-end comprehensive standards and reference architecture that can help secure IoT development

MAIN RESEARCH OBJECTIVE

Develop a novel security model to help organizations formulate a strategy for developing and for discoursing about end-to-end IoT security

MAIN RESEARCH OBJECTIVE

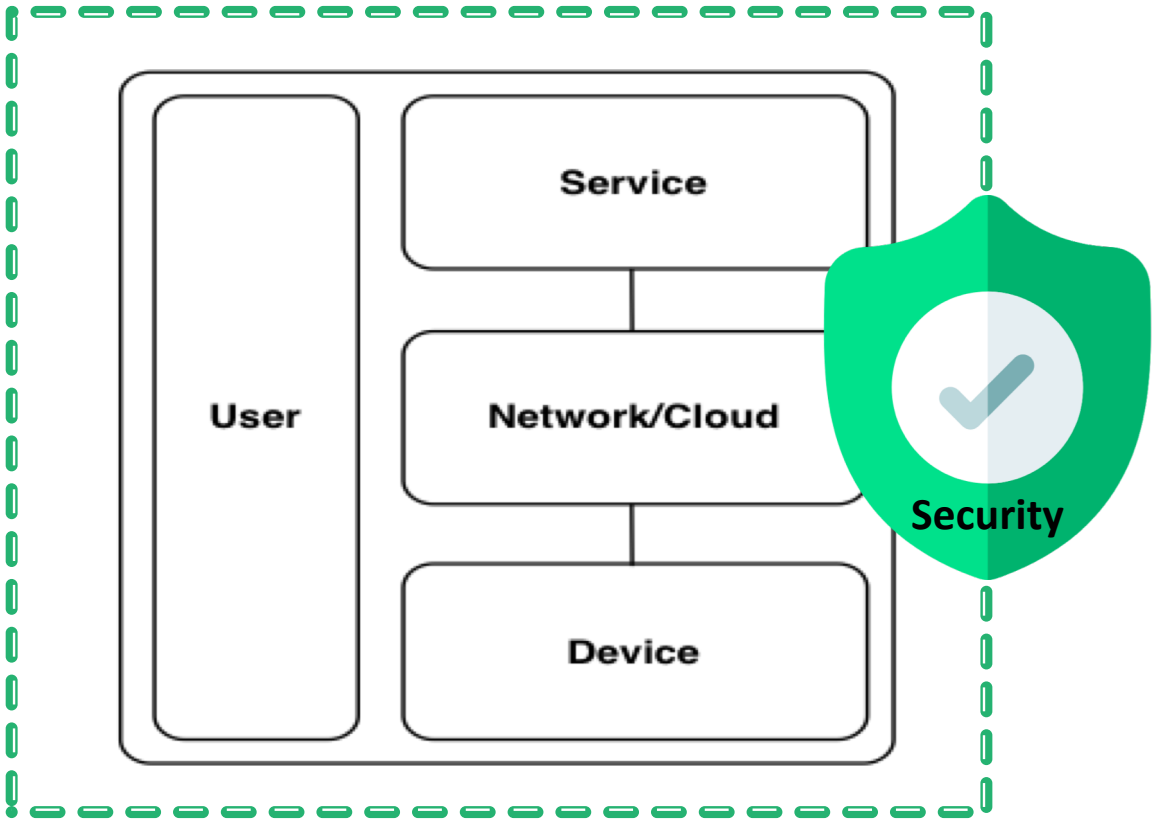
1.  Using existing scholarly literature on IoT security

2.  Leveraging first-hand experience of IoT practitioners

3.  Possibly, basing the model on an existing security framework

END-TO-END IOT SECURITY

High-level IoT architecture with security representing a cross-sectional aspect



SECURITY FRAMEWORKS

Characteristics of different security frameworks:

MSSDL

- Designed to reduce software maintenance costs and increase reliability
- One of the most used in the commercial area
- Mostly intended for large organizations
- No concept of measuring security maturity of an organization

BSIMM

- Measures which software activities are included in an organization
- Based on empirical data
- 16/120 firms are IoT firms
- Includes a concept for measuring an organization's security maturity

SAMM

- Helps organizations formulate and implement a strategy for application security
- Based on the experience of security experts
- It is an open project
- Includes a concept for measuring an organization's security maturity

RESEARCH GAP

Overall, the reviewed models fall short in covering IoT specific security practices and architectures; and are mostly intended for web-based applications.

DATA COLLECTION

✓Peer-reviewed articles focusing on IoT security

- **Inc:** keywords: “IoT”, “CPS”, “security”
- **Exc:** non-English articles, pre-2000, articles focusing on other topics, e.g., privacy

AND

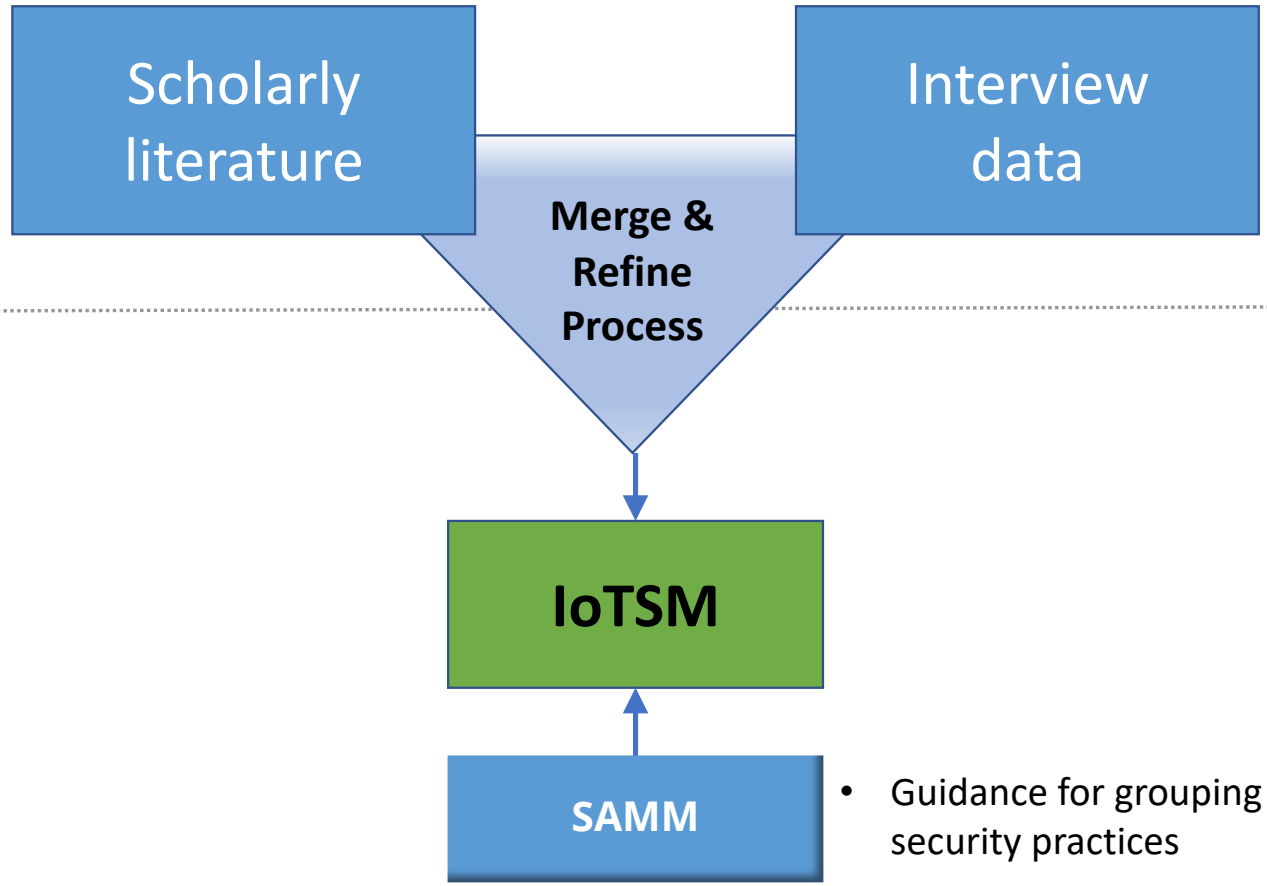
✓Qualitative one-to-one interviews with 6 industry experts

- Participants’ portfolio: IoT devices, cloud-based services, security solutions, etc.
- Questions: IoT security mechanisms, technical constraints, operational challenges

ID	Participant role	Organization function
P1	Security architect	Mobile communications
P2	Senior IoT architect	IoT solutions
P3	Technology leader	Industry automation
P4	Technology expert	Home security
P5	Security coach	Home surveillance
P6	Security expert	Data security

DATA ANALYSIS

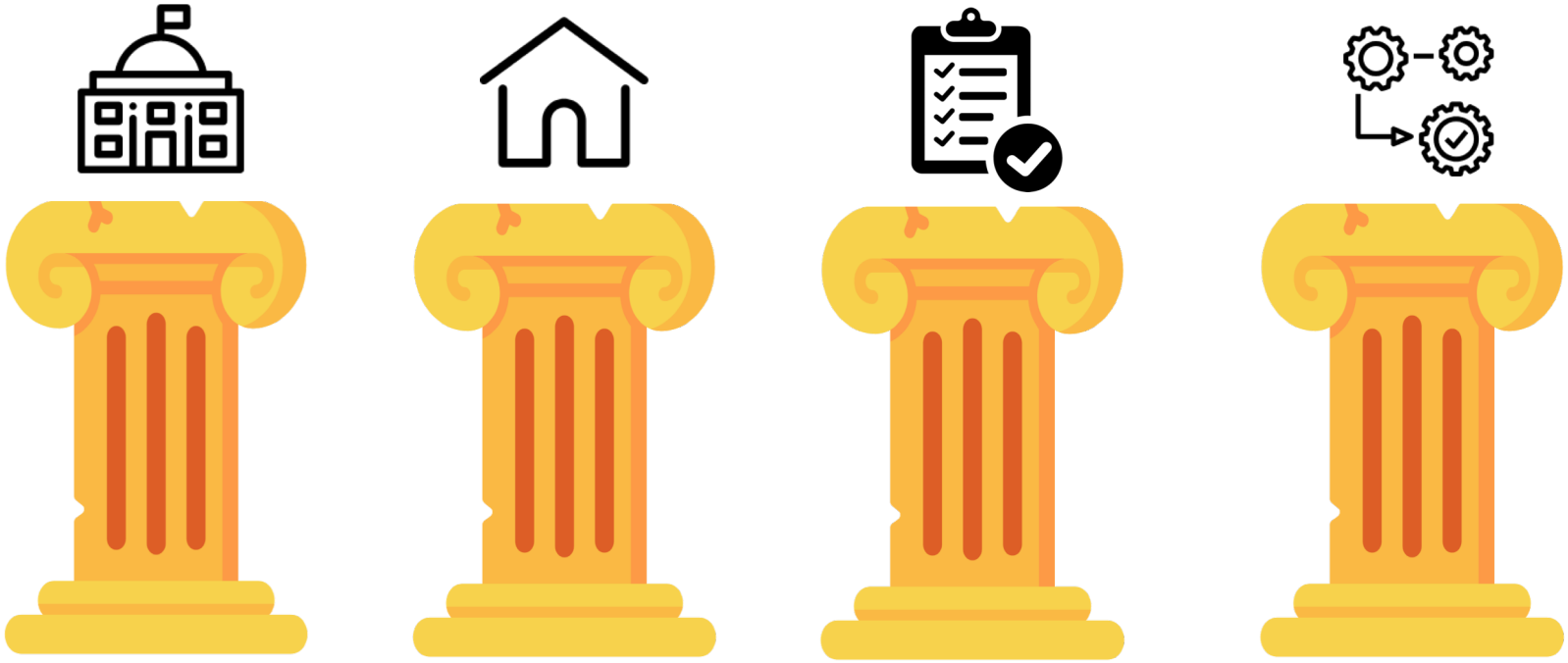
- Selected peer-reviewed articles



- Transcribed interview data
- Guidance for grouping security practices

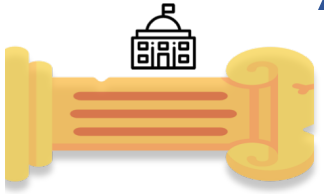
IOTSM PILLARS

Main grouping was motivated by SAMM but enhanced with additional security practices

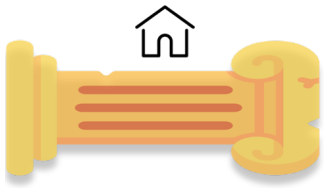


Governance **Construction** **Verification** **Operations**

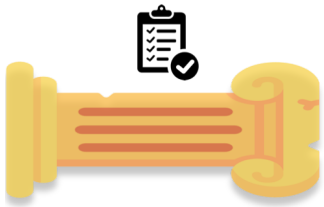
IOTSM PILLARS



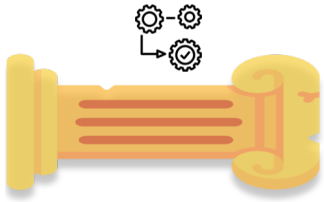
Governance: Related to how an organization manages the overall software development activities



Construction: Deals with how an organization defines its goals and develops software



Verification: Focuses on the activities related to how an organization tests its artifacts like source code and design documentation



Operations: Involves processes that are related to how an organization releases products to end-users, including operating in the runtime environment

GOVERNANCE

- ✓**Security education and awareness:** Educate both the end-user as the consumer of the IoT system and developers about securing IoT devices

P4

"Lack of awareness [startups] about security practices, e.g., w.r.t. threat modeling"

- ✓**Regulations and compliance:** Given the heterogeneity of IoT devices and data they are dealing with regulations and compliance are core to enable a secure environment

P1

"[Regulations] act as new drivers to functionality but may hamper developers' freedom"

- ✓**Security-by-design processes and standards:** Security should be embedded into the IoT devices at the outset, and follow a standardized approach

P6

"More than 600 different protocols in IoT"

CONSTRUCTION

- ✓**Continuous and automated risk assessment:** An automated process to continuously identify, estimate, and prioritize risks to an organization's resources

P5

"RA is crucial for prioritizing IoT security work"

- ✓**Data and application threat modeling:** Structured approach for systematically identifying and categorizing the threats that are most likely to affect a system

P6

"Threat modelling is core to understand security risks"

- ✓**Security requirements and architecture:** Specification and the adoption of principles for the creation of secure functionality, e.g., physical/device security, network/cloud security, service security.

P6

"Requirements such as resilience are increasingly important"

VERIFICATION

✓**Artifact review:** Security focused design and code reviews possibly based on checklists to assist in early vulnerability discovery and related mitigation activities

P5

"code reviews are essential to build secure software and embed quality…"

✓**Security testing:** Inspecting the software, e.g., through security penetration testing, in order to discover exploitable vulnerabilities

P1

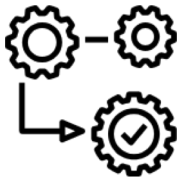
"…need for PT before purchasing an IoT product"

OPERATIONS

✓**Secure operations and maintenance:** IoT system must be kept updated for new vulnerabilities in order to operate securely

P1

"time is a critical element to deliver patches in an IoT system"



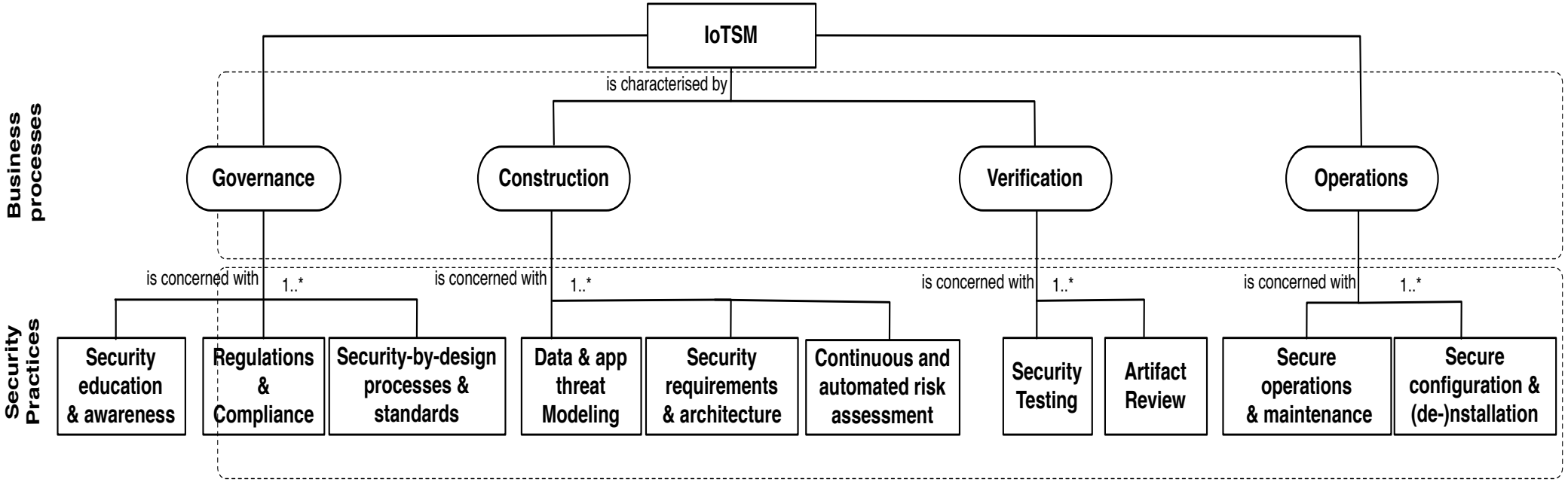
✓**Secure configuration and (de-)installation:** An IoT system should be configured and installed securely, and likewise securely decommissioned

P3

"…and also such configurations should be audited…."

THE IOTSM

Graphical illustration of the IoTSM business processes and security practices



A PRELIMINARY IOT SECURITY MATURITY MODEL

An IoT security maturity model M is a tuple (b, C, p, f_p). The components of *M* are:

- b: finite set of utilized business functions $\subseteq$ {governance, construction, verification, operations}
- C: finite set of IoT components $\subseteq$ {service, network, cloud, device, user}
- p: finite set of adopted security practices with each practice with a corresponding maturity score, *m*, where $m \geq 0$, and a set of target IoT components, *c*, where $c \subseteq C$
- f_p: The organization security posture. This is represented as a function $f_p : p \times b \rightarrow s$

A PRELIMINARY IOT SECURITY MATURITY MODEL

- *End-to-end IoT security (e2e):* representing the overall security maturity of an IoT company
- A company has *e2e*, if $|s| > 0$, $B - b = \varnothing$, and there exists a p with $m > 0$, for each $c \in C$
- If we assume a common scheme for *m,* e.g., 1=low-security, 2=medium-security, 3=high-security, we can come up with a way to measure the overall security maturity of an organization

SOME REFLECTIONS

Comparing the IoTSM security practices with different security frameworks

Security practice	IoTSM	SAMM	BSIMM	MSSDL
Security education and awareness	●	●	●	●
Regulations and compliance	●	●	●	–
Security-by-design processes and standards	●	●	●	●
Continuous and automated risk assessment	●	–	–	–
Data and application threat modeling	●	◗	◗	◗
Security requirements and architecture	●	◗	◗	◗
Artifact review	●	●	●	●
Security testing	●	●	●	●
Secure operation and maintenance	●	●	●	◗
Secure configuration and (de-)installation	●	◗	◗	◗
Continuous monitoring and auditing	●	–	–	–

- ✓ Continuous and automated risk assessment have not been incorporated in the reviewed frameworks
- ✓ Some practices have only been partially implemented in existing frameworks, e.g., the application of threat modeling to data
- ✓ In addition to the CIA requirements there may be more important security goals, e.g., related to ‘controlability’

CLOSING REMARKS

- ✓In general, IoT vendors lack insight into what is required to develop an end-to-end secure product
- ✓Most of the existing security methodologies and models do not capture the dynamic characteristics of the IoT
- ✓IoTSM can be used by security analysts to start formulating a strategy and discourse about IoT security
- ✓Conceptual framework can be developed by security researchers as a tool to formally analyze, describe, and measure the security posture of an IoT organization

FUTURE WORK

- ✓ **Interview data:** Conduct interviews with a broader sample of IoT practitioners

- ✓ **Concrete guidelines:** Evolve the proposed security practices into concrete guidelines for IoT developers

- ✓ **Security metrics:** Introduce sophisticated metrics and have their effectiveness evaluated against IoT companies

THANK YOU FOR *YOUR* ATTENTION !

joseph.bugeja@mau.se