ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY
20 years!

Cybersecurity Measurements Investigation for Smart Buildings

Barnabás SÁNDOR, Ph.D.

Introduction

- Head of Group IT Security @ 4iG Group
- University Lecturer @ Óbuda University
- Lecturer @ LABA Hungary (Robot Dreams)

- PhD – Safety and Security Sciences (ÓE)
- MSc – Safety Technology Engineer (ÓE)
- BSc – Military & Safety Technology Engineer (ÓE)

- CEH
- ISO27k IA

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

The scientific problem

Today's smart buildings are increasingly connected and rely on more IoT devices, increasing their vulnerability to cyber-attacks.

At present, the absence of a comprehensive, adaptive, and real-time responsive cybersecurity framework in the market is a pressing issue, underscoring the need for innovation and improvement in handling the evolving and diverse nature of cyber threats in smart buildings IoT systems.

Thus, my objective was to analyze existing cyber security frameworks and create a new checklist to effectively detect, protect, and respond to cyber threats in the IoT environment of smart buildings.

Objectives

Objectives

Explore the current state of smart buildings' IoT stakeholders, including manufacturers, service providers, and users, as well as their existing practices and capabilities for sharing threat information.

Analyze the benefits and challenges of threat information sharing as a common defense strategy for IoT systems in smart buildings.

Develop a framework for effective and secure threat information sharing among stakeholders, considering privacy concerns, legal considerations, and the diversity of smart building systems.

Objectives

Investigate and analyze different processes and technologies to collect, analyze, and disseminate threat information promptly and effectively.

By conducting experiments to assess the impact of sharing threat information on improving system security, including detection and mitigation of cyber threats in smart buildings and IoT environments, we aim to pave the way for significant advancements in the field.

Develop guidance and recommendations for stakeholders on implementing and adopting effective threat information-sharing practices, including best practices for information-sharing, trust building, and collaborative protection strategies.

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Research methods

Research methods

- Empirical research methods: observation and document analysis;
- Comparative analysis of existing cybersecurity frameworks and standards;
- In-depth interviews with national experts;
- A study of national and international literature and a systematic analysis of previous research findings.

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

New scientific results

New scientific results

- Create a new IoT cybersecurity checklist for Smart Buildings
  - Identify gaps in existing frameworks;
  - 14 areas and 16 themes identified.

- Created a new reference model for Smart Building IoT Security;
- Demonstrated that existing cybersecurity frameworks and standards lack a cybersecurity recommendation for smart buildings.

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

IoT cybersecurity checklist

#	Area	Topic	Task
1	Governance and policy management	IoT security policy review	- Check that the IoT security policy includes technical standards for device security, network protocols and data management. - Check specific policies for the procurement and deployment of IoT devices.
2	Human resource security	Training employees on IoT security	- Evaluate the effectiveness of IoT security training programmes, focusing on technical aspects such as device management and data security.
3	Asset Management	Inventory and classification of IoT devices	- Check that all IoT assets have been inventoried and classified according to their risk and function. - Ensure device inventories include firmware versions and patch status.
4	Access control	Managing access to IoT devices	- Review access control policies for IoT devices, ensuring they include technical measures such as multi-factor authentication.
5	Cryptography	Encryption standards for the IoT	- Assess the implementation of encryption in IoT communications and data storage. - Verify the use of up-to-date and reliable encryption algorithms.
6	Physical and environmental safety	Physical security of IoT devices	- Check physical security measures for IoT devices, especially for devices in accessible locations.
7	Operational safety	Configuration and management of IoT devices	- Assess the security configuration of IoT devices, including default settings and network interfaces. - Verify the implementation of secure management protocols for IoT devices.
8	Communication security	Wi-Fi security	- Assess the security of Wi-Fi networks used by IoT devices, including the use of WPA3 and network segmentation. - Check for the presence of rogue access points and the effectiveness of wireless intrusion prevention systems.

#	Area	Topic	Task
9	Systems procurement, development and maintenance	Secure Software Development Lifecycle (SDLC) for IoT	- Consider integrating security into the SDLC of IoT applications, including secure coding practices and vulnerability testing. - Evaluate the process for updating and patching IoT-based software.
10	Supplier relations	IoT supply chain security	- Assess the security measures of third-party IoT components and services. - Review contracts for cybersecurity liability and incident response clauses.
11	Information security incident management	IoT incident response planning	- Review incident response plans for scenarios involving IoT devices and systems. - Assess the ability to detect and respond to IoT-specific security incidents.
12	Information security aspects of business continuity management	Integrating IoT into business continuity	- Check that IoT devices and systems are properly included in business continuity and disaster recovery plans.
13	Compliance	Regulatory compliance for the IoT	- Check compliance with relevant IoT cybersecurity regulations and standards. - Ensure that IoT data management practices comply with data protection legislation, such as GDPR.
14	IoT-specific technical security checkpoints	Firmware security	- Assess the security of the firmware of IoT devices, including the process for secure updates and protection against firmware tampering. - Verify secure boot mechanisms and firmware integrity checks.
15		Network security	- Assess network security measures specific to IoT, such as network firewalls, intrusion detection systems and secure network protocols. - Check the separation of IoT traffic from critical network segments.
16		IoT data protection	- Review data protection measures for IoT, focusing on data encryption, anonymisation and secure data storage practices. - Assess compliance with data retention and privacy policies.

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Possible uses of the results

Possible uses of the results

- For the forthcoming regulation on a national cybersecurity certification scheme for IoT devices for the Authority;
- For cybersecurity designers who design IoT systems for smart buildings;
- Cybersecurity operators who are taking over existing systems for deployment;
- IoT professionals who want to increase cybersecurity in their IoT devices and systems;
- For companies designing or operating smart buildings;
- I recommend that my results be widely used in the field of cybersecurity at the level of technical recommendation.

Contact

LinkedIn: www.linkedin.com/in/sandorbarnabas

MTMT ID: 10064423

ODT: 32485

ORCID: 0000-0001-7133-8082

Google Scholar: scholar.google.com/citations?user=pSqxGQUAAAAJ&hl

ResearchGate: www.researchgate.net/profile/Barnabas-Sandor

Web of Science: M-7380-2018

IEEE Xplore ID: 37086507551

Academia: independent.academia.edu/BarnabasSandor