NARA INSTITUTE OF SCIENCE AND TECHNOLOGY
- Outgrow your limits -

Threat Level Assessment of Smart-Home Stakeholders Using EBIOS Risk Manager

N'guessan Yves-Roland Douha, Doudou Fall, Yuzo Taenaka, Youki Kadobayashi

Laboratory for Cyber Resilience, Division of Information Science

Nara Institute of Science and Technology (Japan)

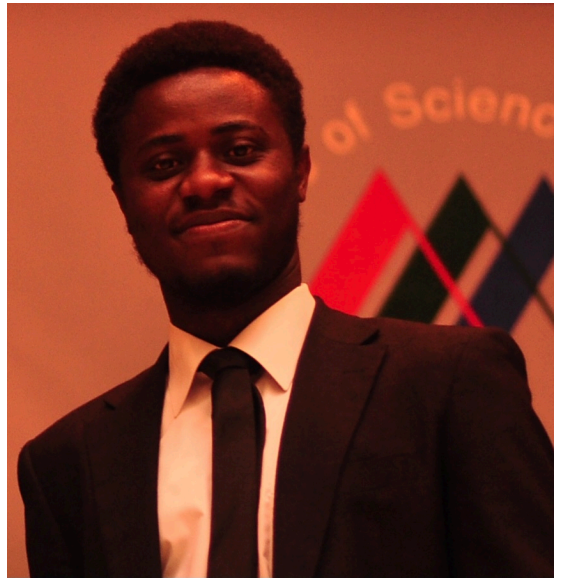
Presenter's email address: douha.nguessan_yves-roland.dn6@is.naist.jp

iplab Laboratory for Cyber Resilience

N'guessan Yves-Roland Douha *received the Master's degree of Engineering - MEng, Information Science and Engineering at Nara Institute of Science and Technology (NAIST), Japan, in 2020.*

He is currently a doctoral student majoring in cybersecurity at the Division of Information Science, NAIST.

His research interests include risk management, machine learning, anomaly detection, game theory, and smart-home security.



INTRODUCTION

- Worldwide revenue of smart homes [1]
  - US$78.9 billion (2020)
  - US$182.3 billion (2025)
- Smart homes attract considerably, not only normal users, but also attackers
  - More than 750,000 Phishing and SPAM emails Launched from “Thingbots” Including Televisions, Fridge [2]
  - Hacked home devices caused massive Internet outage [3]
- Risk assessment becomes necessary to identify and address the security flaws in smart homes to withstand future cyberattacks.

RELATED WORK

Authors	Methods	Contributions
Wongvises, Khurat, Fall, and Kashihara [4]	Fault Tree Analysis	Quantify security risks in a given smart home based on the ”things” it is composed of.
Ali and Awad [5]	Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)	Identify ten critical information assets (e.g., user credentials, log information, mobile application data, and various smart home-related information)
Kavallieratos, Gkioulos, and Katsikas [6]	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE) model	Identify threats to smart-home devices such as IP cameras, smartphones, and alarm systems.
Jacobsson, Boldt, and Carlsson [7]	Information Security Risk Analysis (ISRA) approach [8]	Recognize that third-party stakeholders can access the whole smart home and collect private data on inhabitants.

- Limitations: A lack of study on stakeholders assessment whereas, as mentioned by Bregman [9], stakeholders play a critical role in a smart-home environment. If one or many of these stakeholders get compromised by attackers or fail to secure information transmission, the smart home security could be affected.

PROBLEM

- Individuals within any organization or ecosystem, through actions or inactions, may intentionally or unintentionally facilitate the realization of cyberattack operations.

- **Smart-home stakeholders** may not understand the matter of cybersecurity.

- Attackers may elaborate attack scenarios that leverage one or more smart home stakeholders at strategic positions.

CONTRIBUTIONS

- ❑ We introduce stakeholder-based risk analysis for smart-home security.
- ❑ We evaluate the threat level associated with smart-home stakeholders to identify strategic scenarios that attackers could exploit.
- ❑ We propose an approach of threat classification for risk managers and compare our results with two other classification methods, including the EBIOS RM's.
- ❑ We identify and describe potential high-level attack scenarios that could involve smart-home stakeholders.

METHOD

- Risk analysis of a smart home using EBIOS Risk Manager.
  - EBIOS Risk Manager (EBIOS RM) was published by National Cybersecurity Agency of France (ANSSI) in December 2018.
  - EBIOS RM is a method based on the risk analysis and management methodology called EBIOS.
  - EBIOS (created in 1995): Expression of Needs and Identification of Security Objectives
    - ✓ *A method for risk management of information system security*
    - ✓ *A comprehensive tool that complies with Security Management Policies and international standards such as ISO 27001 (Information security management), ISO 27005 (Information security risk management), and ISO 31000 (Risk management).*

- Unlike other methods (e.g., OCTAVE, STRIDE) mentioned in related work, EBIOS RM focuses on stakeholder analysis.

EBIOS RISK MANAGER

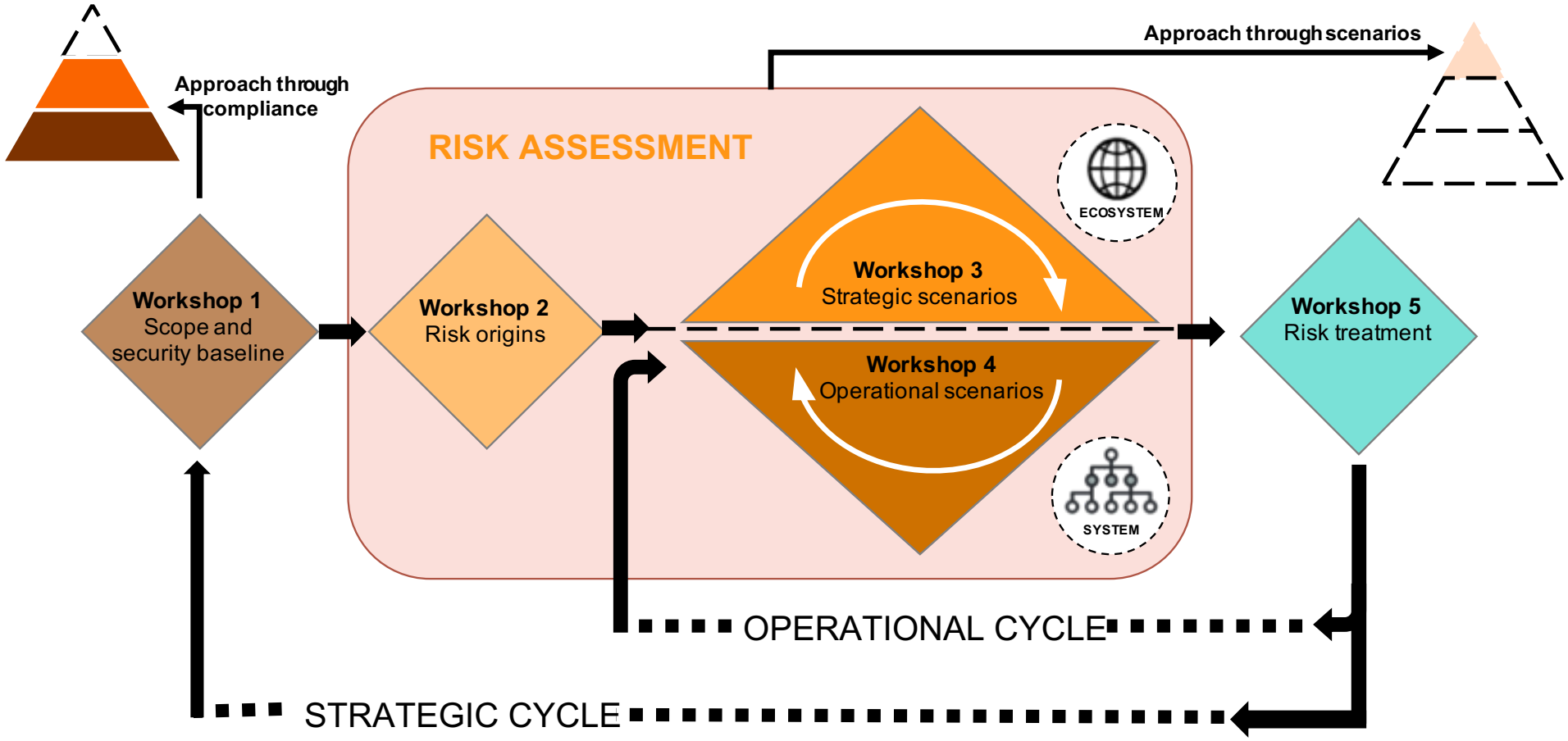


Figure 1. A description of the general workflow of the EBIOS Risk Manager methodology

EBIOS RISK MANAGER

- We focused exclusively on the first three workshops because our purpose is to evaluate the threat level of smart-home stakeholders.

WORKSHOP 1: **scope and security baseline**	WORKSHOP 2: **risk origins**	WORKSHOP 3: **strategic scenarios**
This workshop aims to identify the scope of our study, its assets, and its primary missions. Then, it **determines the severity of feared events associated with its assets.**	This workshop aims to **identify the RO/TO pairs.** This pair comprises risk origins (RO) and their high-level targets, namely target objectives (TO).	This workshop includes the threat level assessment, establishes **a mapping of threat agents**, and **provides high-level scenarios**, called strategic scenarios. These scenarios describe the attack paths a risk origin could use to reach its target objective.

WORKSHOP 1

FEARED EVENTS

Energy Management

FEAR EVENTS

Triggering power outage, tampering consumed energy amount, and alteration of heating, ventilation, and air conditioning.

IMPACT

Quality of service (QoS), comfort, safety, security of dwellers, and financial losses

(Severity: S3 or S4)

TABLE I. A DESCRIPTION OF SEVERITY LEVELS REGARDING THE POTENTIAL IMPACTS OF FEARED EVENTS.

SECURITY LEVEL	DESCRIPTION
S4 (CRITICAL)	Incapacity for the smart home to ensure all or a portion of its functioning. Severe impacts on the safety and security of dwellers, data, and assets.
S3 (SERIOUS)	High degradation in the performance of the smart home. Significant impacts on the safety and security of dwellers, data, and assets.
S2 (SIGNIFICANT)	Degradation in the performance of the smart home. No direct impact on the safety and security of dwellers, data, and assets.
S1 (MINOR)	Minor or no impact on operations or performances of the smart home. Minor or no impact on the safety and security of dwellers, data, and assets.

Safety and Security

FEAR EVENTS

Disabling of alarm system, smart door lock, or network security services, and detection of human activities by an attacker.

IMPACT

QoS, data security, privacy, safety, and security of dwellers

(Severity: S2, S3, or S4)

Healthcare

FEAR EVENTS

Leaking medical data records of dwellers and altering medical data records

IMPACT

Safety and privacy of dwellers and involve financial losses

(Severity: S3 or S4)

Home Automation

FEAR EVENTS

Altering the automation configuration and remote control by an attacker.

IMPACT

Comfort, privacy, safety, and security of dwellers

(Severity: S1, S2, or S3)

Entertainment

FEAR EVENTS

Leaking personal data of dwellers.

IMPACT

Safety and privacy of dwellers and involve financial losses

(Severity: S3 or S4)

WORKSHOP 2

RISK ORIGIN /TARGET OBJECTIVE

TABLE II. A DESCRIPTION OF RO/TO PERTINENCE

Identification		Scoring		Assessment
Risk origins (RO)	Target objectives (TO)	Motivation	Resources	Resources
Amateur	Challenge	Low	Limited	Low
Avenger	Obstacle to functioning; Spying	Low	Limited	Low
Competitor and organized crime	Profit; Strategic pre-positioning; Terrorism	High	Significant	Fair
Hacker	Challenge; Profit; Spying; Strategic pre-positioning	High	Significant	Fair
Hacktivist	Terrorism	Fair	Significant	Fair
Inadvertent attacker	N/A–does not intend to attack	Very low	Very low	Low
Specialized outfits	Profit; Challenge; Spying; Strategic pre-positioning	High	Considerable	High
State-related	Terrorism; Spying	High	Unlimited	High
Terrorist	Terrorism; Spying	Highly motivated	Considerable	High
Thief	Spying; Obstacle to functioning; Profit	Fair	Significant	Fair

WORKSHOP 3

SMART-HOME STAKEHOLDERS

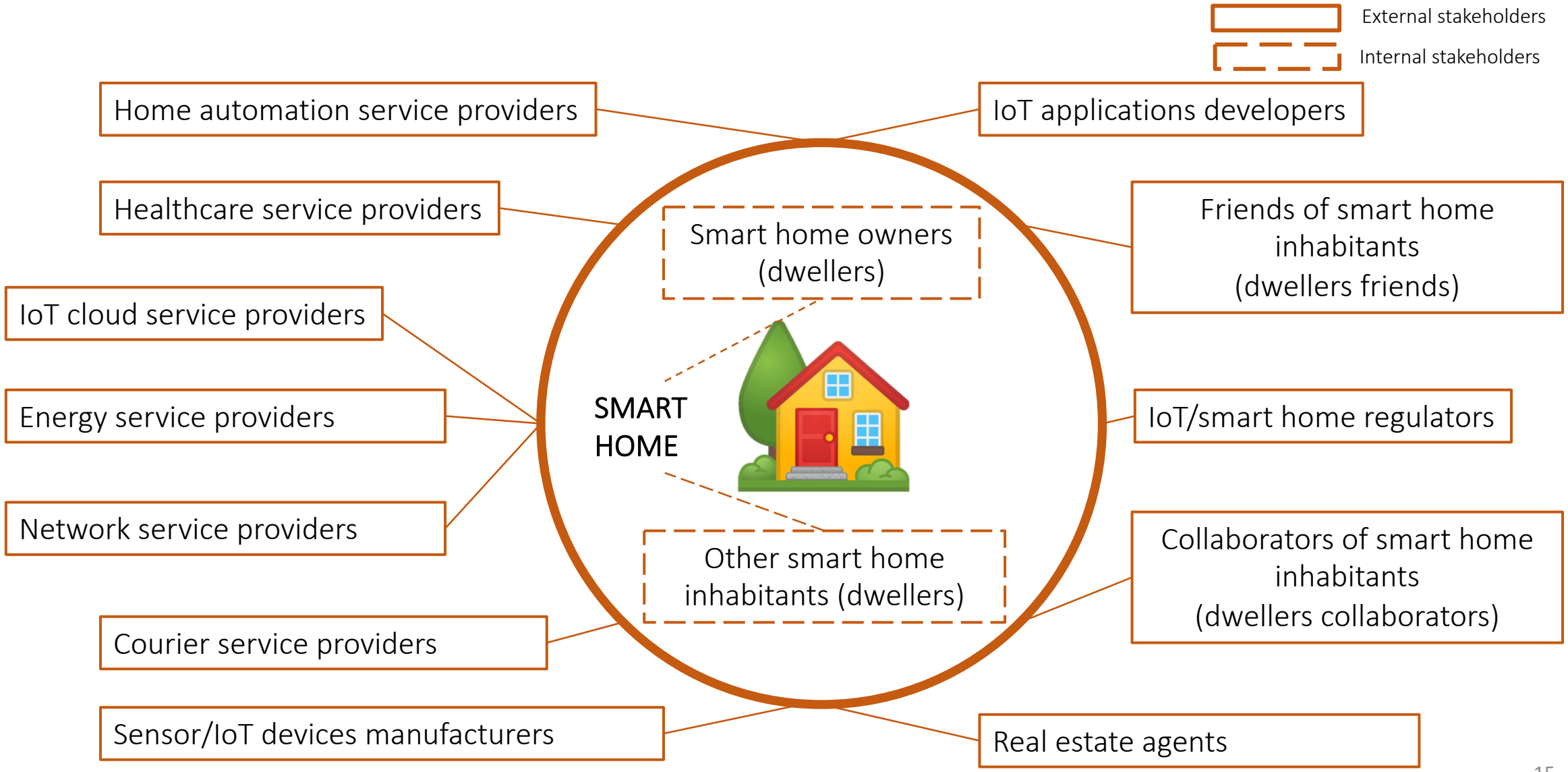


Figure 2. A description of smart-home stakeholders

THREAT LEVEL ASSESSMENT

- Metrics and formula recommended by EBIOS RM.

$$\text{Threat Level} = \frac{\text{Dependency X Penetration}}{\text{Cyber Maturity X Trust}}$$

- ***Dependency*** *evaluates the degree of relationship between the stakeholder and the smart home.*
- ***Penetration*** *assesses how far the stakeholder could access the smart home assets (including physical and remote access).*
- ***Cyber Maturity*** *measures the ability of stakeholders to understand and implement cybersecurity best practices in their daily activities.*
- ***Trust*** *measures the level of confidence the system should have regarding the intention of stakeholders.*

THREAT LEVEL ASSESSMENT

❑ Data collection

- Online survey questionnaire
  - 17 security specialists from academia and industry
  - We use a 5-point Likert scale to collect data from security specialists for the risk assessment.
  - Evaluation Stakeholders evaluation for each metric (dependency, penetration, cyber maturity, and trust).
    - ✓ For example: *Please rate the dependency levels between each stakeholder and the smart home on a scale of 1 to 5.*

TABLE III. A DESCRIPTION OF THE ONLINE SURVEY QUESTIONNAIRE

	1: Very low	2: Low	3: Moderate	4: High	5: Very high
Stakeholder 1	◯	◯	◯	◯	◯
Stakeholder 2	◯	◯	◯	◯	◯
…	…	…	…	…	…
Stakeholder n	◯	◯	◯	◯	◯

THREAT MAPPING

- The figure describes the threat levels of smart-home stakeholders according to the classification provided by EBIOS RM

Danger zone
10% of the stakeholders with the highest threat levels.
Control zone
40% of the next stakeholders
Watch zone
40% of the next stakeholders
Out-of-scope
The remaining 10%

The danger zone contains *Smart-homes owners (dwellers)* and *Other smart-home inhabitants (dwellers).*
The watch zone contains the other stakeholders.

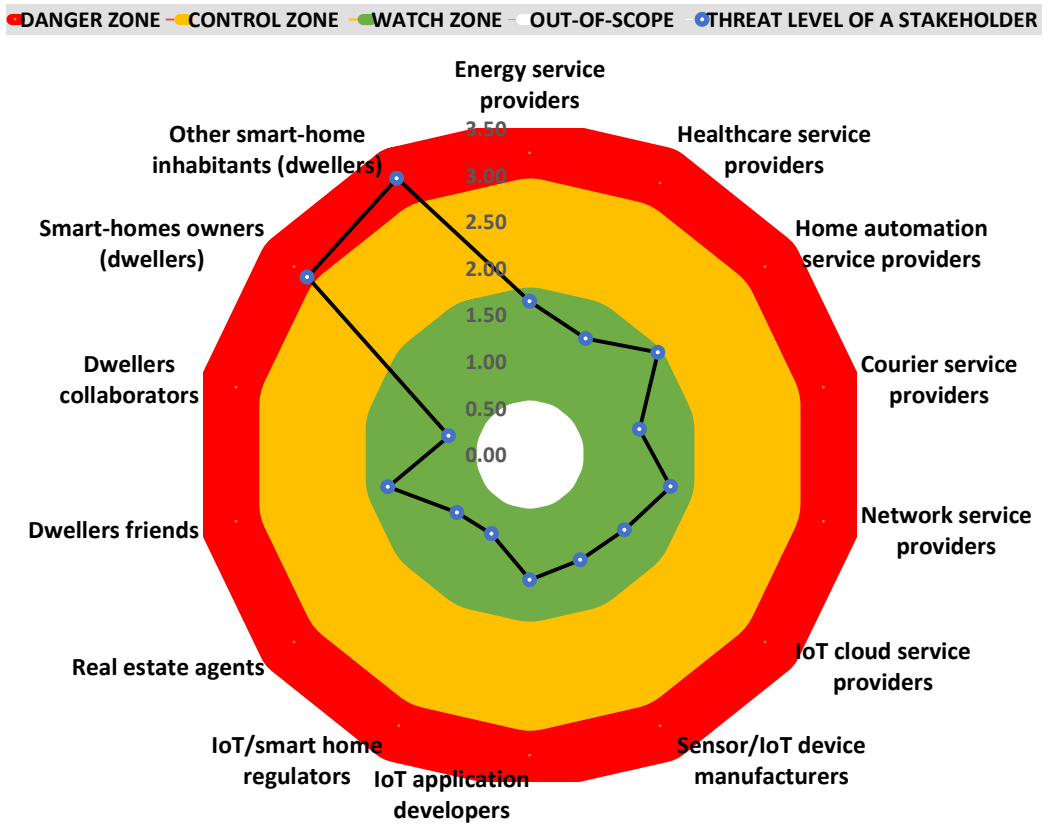


Figure 3. A description of threat agents using EBIOS RM classification

THREAT MAPPING

- The figure describes the threat levels of smart-home stakeholders based on a simplified classification.

Danger zone
3 ≤ Threat level ≤ 4

Control zone
2 ≤ Threat level < 3

Watch zone
1 ≤ Threat level < 2

Out-of-scope
0 ≤ Threat level < 1

The danger zone contains *Smart-home owners (dwellers)* and *Other smart-home inhabitants (dwellers).*

The out-of-scope contains *Dwellers collaborators* and *IoT/smart home regulators.*

The watch zone contains the other stakeholders.

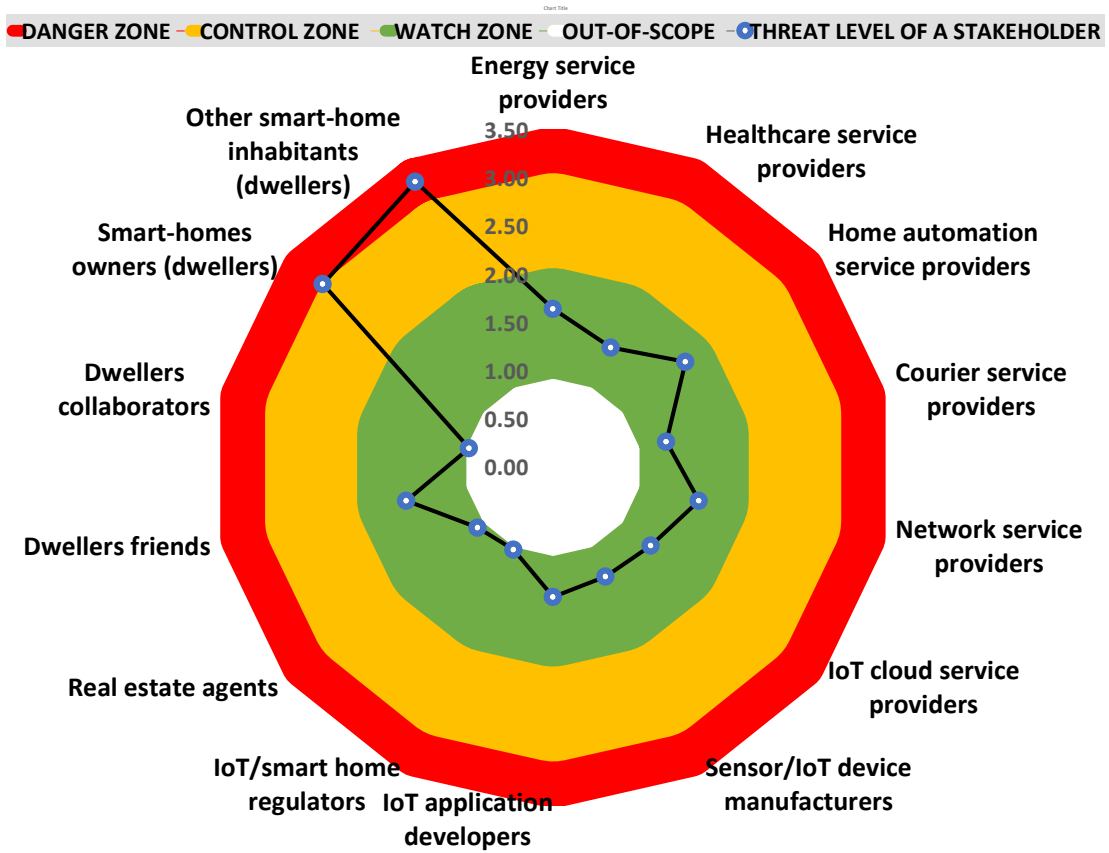


Figure 4. A description of threat agents using a simplified classification

THREAT MAPPING

- The figure describes the threat levels of smart-home stakeholders according to a Pareto-based classification.

Danger zone

1.64 < Threat level ≤ 4

Control zone

1.38 < Threat level < 1.64

Watch zone

1.26 < Threat level < 1.38

Out-of-scope

0 ≤ Threat level ≤ 1.26

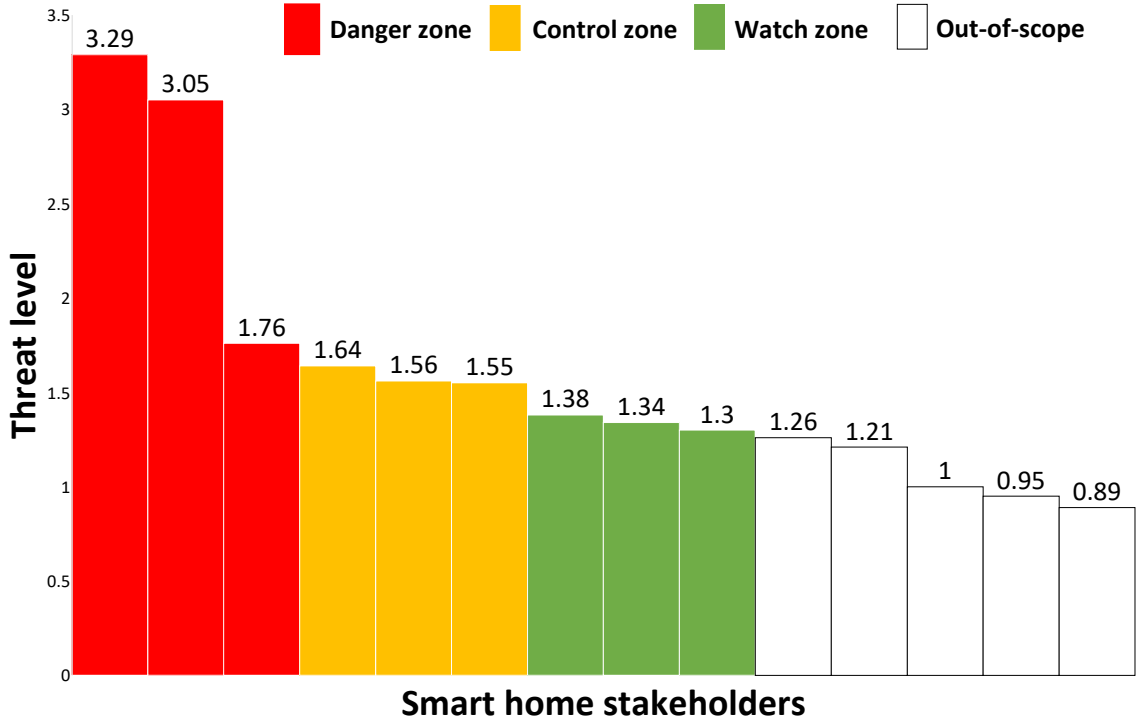


Figure 5. A description of threat agents using a simplified classification

The danger zone contains Smart-homes owners (dwellers) and Other smart-home inhabitants (dwellers), and Home automation service providers.

The control zone contains Energy service providers, Dwellers friends, and Network service providers.

out-of-scope contains Sensor/IoT device manufacturers and Courier service providers, Real estate agents, IoT/smart home regulators, and Dwellers collaborators.

The watch zone contains Healthcare service providers, IoT application developers, and IoT cloud service providers.

COMPARISON OF APPROACHES

- The table illustrates that the Pareto-based classification can distribute the stakeholders' threats to every threat zone identified. Hence, a three-level Pareto chart can provide better results than the two other approaches.

TABLE IV. A DESCRIPTION OF THE ONLINE SURVEY QUESTIONNAIRE

	Danger zone		Control zone		Watch zone		Out-of-scope	
	Range of the likelihood (L)	Number of stakeholders	Range of the likelihood (L)	Number of stakeholders	Range of the likelihood (L)	Number of stakeholders	Range of the likelihood (L)	Number of stakeholders
EBIOS RM's classification	$4 \geq L \geq 2.96$	2	$2.96 > L \geq 1.77$	0	$1.77 > L \geq 0.59$	12	$0.59 > L \geq 0$	0
Simplified threat classification	$4 \geq L \geq 3$	2	$3 > L \geq 2$	0	$2 > L \geq 1$	10	$1 > L \geq 0$	2
Proposed Pareto's classification	$4 \geq L > 1.64$	3	$1.64 \geq L > 1.38$	3	$1.38 \geq L > 1.26$	3	$1.26 \geq L \geq 0$	5

ATTACK SCENARIOS

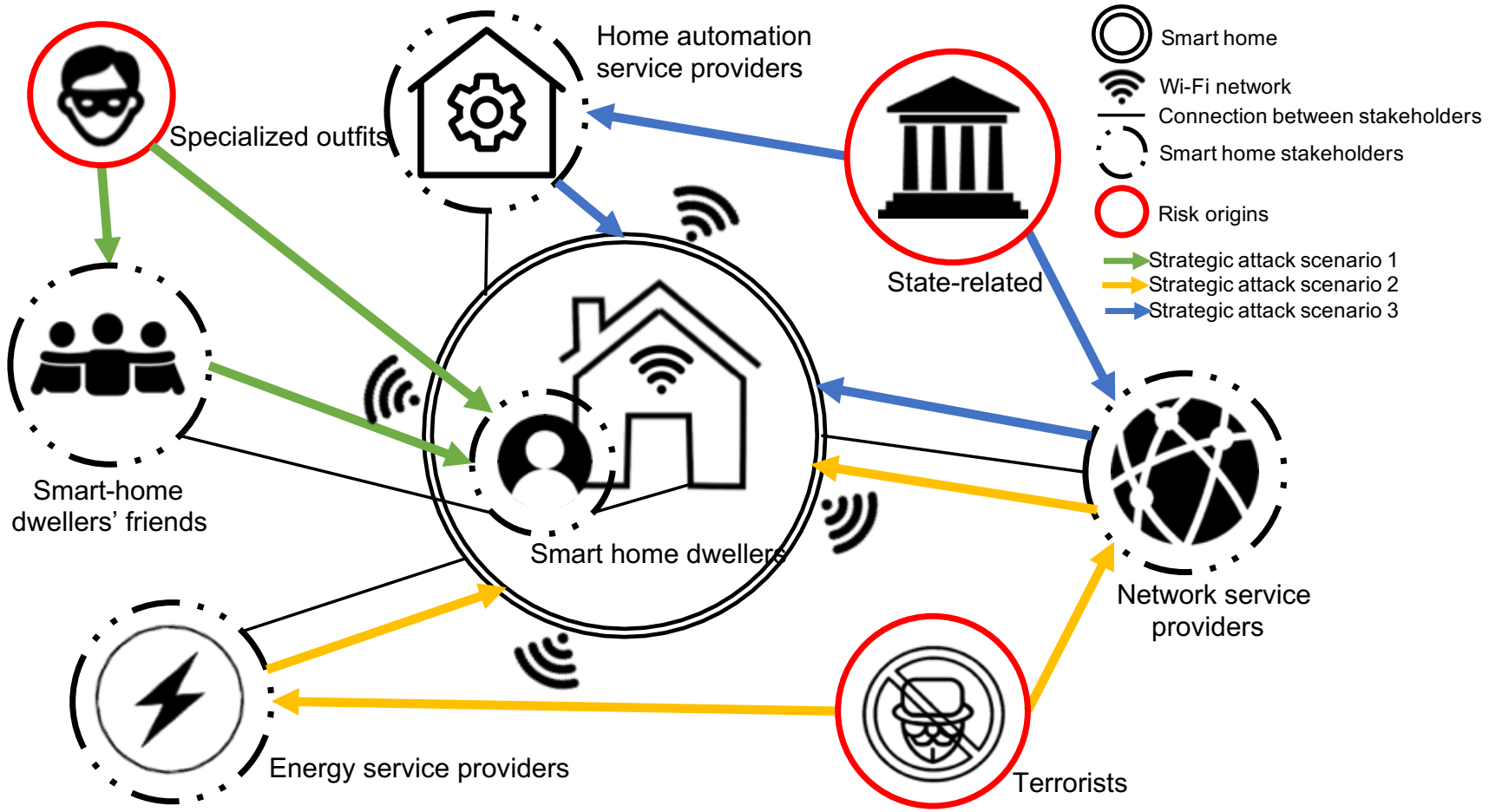


Figure 6. A description of proposed attack scenarios on smart homes involving stakeholders.

CONCLUSION AND FUTURE WORK

Problem

- Smart-home security is still a challenging and crucial topic since users safety and security are involved.
- The perspective of smart home security with a focus on stakeholders security issues have not been explored in the previous studies.

Actions

- We elaborated the security risk analysis of a smart home using EBIOS RM with a focus on the threat level assessment of smart-home stakeholders in the role of threat agents.
- We provided high-level attack scenarios involving smart-home stakeholders after a step-by-step process to identify risk origins, target objectives, fear events and their severity, threat agents and their threat level.

CONCLUSION AND FUTURE WORK

Findings

- Our results showed that the threat levels of successful attack scenarios involving smart-home inhabitants and smart-home automation service providers are very high.

Next milestones

- Identification and risk assessment of each operational scenario (Workshop 4) and risk treatment (Workshop 5).
- Designing of security systems and policies considering stakeholders for smart-home security.
- Multi-layered security cooperation for smart-home security could be possible in the future
- Investigating cybersecurity awareness and education using game theory

REFERENCES

[1] Statista, “Smart Home Report 2021,” 2021, retrieved: October, 2021.[Online]. Available: https://www.statista.com/study/42112/smart-home-report/

[2] Proofpoint, “More than 750,000 Phishing and SPAM emails Launched from “Thingbots” Including Televisions, Fridge,” 2014, retrieved: October, 2021. [Online]. Available: https://www:proofpoint:com/us/proofpoint-uncovers-internet-things-iot-cyberattack

[3] E. Blumenthal and E. Weise, “Hacked home devices caused massive Internet outage,” 2016, retrieved: October, 2021.[Online]. Available: https://www:usatoday:com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/

[4] C. Wongvises, A. Khurat, D. Fall, and S. Kashihara, “Fault tree analysisbased risk quantification of smart homes,” in 2017 2nd International Conference on Information Technology (INCIT). IEEE, 2017, pp. 1–6

[5] B. Ali and A. I. Awad, “Cyber and physical security vulnerability assessment for IoT-based smart homes,” Sensors, vol. 18, no. 3, p. 817, 2018.

[6] G. Kavallieratos, V. Gkioulos, and S. K. Katsikas, “Threat analysis in dynamic environments: The case of the smart home,” in 2019 15th International Conference on Distributed Computing in Sensor Systems(DCOSS). IEEE, 2019, pp. 234–240.

[7] A. Jacobsson, M. Boldt, and B. Carlsson, “A risk analysis of a smart home automation system,” Future Generation Computer Systems, vol. 56, pp. 719–733, 2016.

[8] T. R. Peltier, Information security risk analysis. CRC press, 2005

[9] D. Bregman, “Smart home intelligence–the ehome that learns,”Interna-tional journal of smart home, vol. 4, no. 4, pp. 35–46, 2010.

NARA INSTITUTE OF SCIENCE AND TECHNOLOGY
- Outgrow your limits -

IARIA

Thank you for your attention.

Comments? Questions?

Presenter's email address: douha.nguessan_yves-roland.dn6@is.naist.jp

iplab
Laboratory for
Cyber Resilience