Security Risk Analysis of a Smart Home Using EBIOS Risk Manager

Douha N'guessan Yves-Roland
<douha.nguessan_yves-roland.dn6@is.naist.jp>

Abstract

- The smart home is among the emerging technologies designed to improve in-house quality of life by supplying many services, such as home automation, healthcare, and energy management.
- Recent cyberattacks on smart homes affecting home dwellers' privacy, safety, and security could slow down smart homes' adoption. To identify and reduce smart home attack surfaces, we propose a risk assessment using the EBIOS methodology to evaluate smart home stakeholders' security risks.
- Our contributions include assessing smart home stakeholders, classifying these stakeholders into different threat zones, and identifying attack scenarios in which they could be involved.

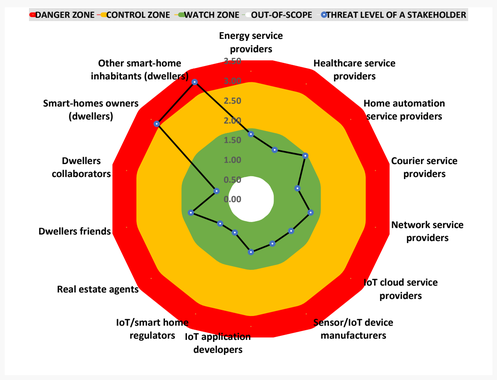
Background & Motivation

- "A complete set of risks to a system may not be identified without an understanding of system configuration, interactions with other systems, stakeholders' goals, rights and responsibilities, and human-machine interactions [1]."
- What are the responsibilities of the smart home stakeholders toward a smart home security?
- Previous studies related to the risk assessment of a smart home did not evaluate the smart home stakeholders' security level.

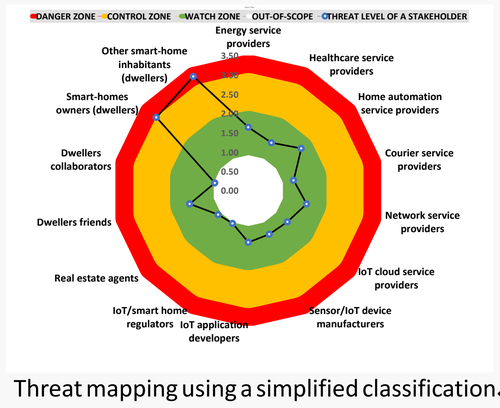
[1] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K., 2016. A review of cyber security risk assessment methods for SCADA systems. Computers & security, 56, pp.1-27.

Result

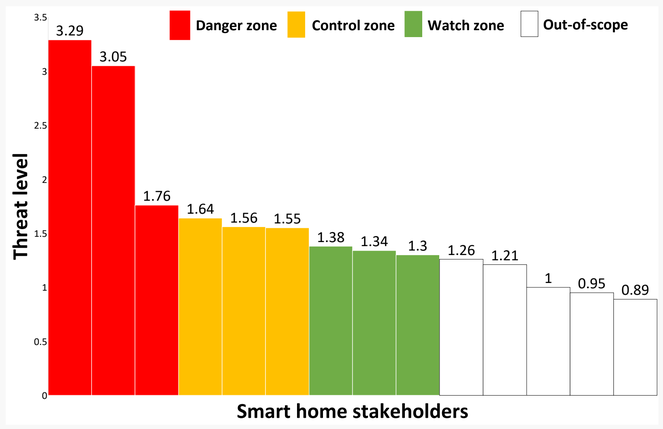
- We classify the threat levels into danger zone, control zone, watch zone, and out-of-scope.



Threat mapping using EBIOS RM classification.



Threat mapping using a simplified classification.



Threat levels classification using a three-level Pareto chart.

- On the contrary to the other methods, our approach can effectively distribute the threats in every threat zone.

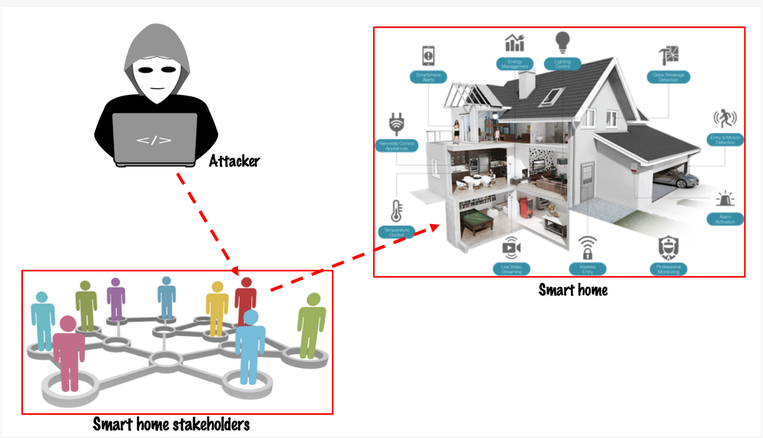
	Danger zone	Control zone	Watch zone	Out-of-scope
EBIOS RM –based classification	2	0	12	0
Simplified classification	2	0	10	2
Our approach	3	3	3	5

Comparison of three approaches for threats classification.

Proposed Idea and Methodology

- We use the EBIOS Risk Manager to identify and evaluate the threat levels of the smart home stakeholders.

$$ThreatLevel = \frac{Dependency\ X\ Penetration}{CyberMaturity\ X\ Trust}$$



An attacker is targeting a smart home after compromising a smart home stakeholder.

- We use a 5-point Likert scale to collect data from security professionals in industry and academia areas to conduct this risk assessment and choose the *mean* for measurement.
- The choice of this measure is motivated by Boone et al. [2], who stated that if one designs a series of questions that, when combined, measure a particular trait, then one has created a Likert scale. In this case, the authors recommended the mean and standard deviation to describe the scale.
- We propose a three-level Pareto chart to classify the smart home stakeholders into different threat zones and compare our result with two other classification methods.

[2] Boone, H.N. and Boone, D.A., 2012. Analyzing Likert data. Journal of extension, 50(2), pp.1-5.

Conclusion and Future Work

- Identification and classification of smart home stakeholders into different threat zones.
- This investigation will contribute to designing security systems and policies for strengthening the smart home ecosystem's security.