Towards Automated Threat-based Risk Assessment for Cyber Security in Smarthomes

Pankaj Pandey[2], Anastasija Collen[1], Niels Nijdam[1], Marios Anagnostopoulos[2], Sokratis Katsikas[2], and Dimitri Konstantas[1]

[1]University of Geneva, Geneva, Switzerland
[2]Norwegian University of Science & Technology, Gjøvik, Norway

Abstract

Cyber security is a concern of each citizen, especially when it comes to novel technologies surrounding us in our daily lives. Fighting a cyber battle while enjoying your cup of coffee and observing gentle lights dimming when you move from the kitchen to the sitting room to review your today's running training, is no longer science fiction. A multitude of the cyber security solutions are currently under development to satisfy the increasing demand on threats and vulnerabilities identification and private data leakage detection tools. Within this domain, ubiquitous decision making to facilitate the life of the regular end-users is a key feature here. In this paper we present an approach called Negative to Positive modelling to automate the threat-based risk assessment process, tailored specifically to the smart home environments. The calculation model application is demonstrated on derived threat-triggered evaluation scenarios, which were established from analysing the historical evidence of data communication within the smarthome context. The main features of the proposed risk management are identification of the existing risks, estimation of the consequences on possible positive and negative actions and embedding of the mitigation strategies. The application of this modelling approach for automation of risk assessment would lead to a deep understanding on the extent to which decision making could be automated while tracking and controlling the cyber risks within the end-user's accepted level. Through the proposed risk assessment process, common factors and variables are extracted and integrated into a quantified risk model before being embedded in the automated decision making process. This research falls within the *GHOST* (Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control) project, aiming to provide a cyber security solution targeted at the regular citizens.

Keywords– Risk Assessment, IoT, Security, Smarthome

1 Introduction

The goal of the *GHOST* project [1] is to provide a cyber security solution targeted at the regular citizens by raising their awareness and understanding

of the cyber security risks associated with all aspects of cyber security from threats and vulnerabilities identification and private data leakage detection up to making informed decisions affecting their cyber-physical smart home security. *GHOST* aims to transform smart home occupants' decisions into reliable automated security service, promoting user-friendly end-user habits through usable security.

The Risk Engine (RE) is a central component of the *GHOST* software implementation focused on the context-aware real-time risk assessment of the ongoing activities on the network. It gathers information about the current risks, analyses in real-time current network traffic flows and correlates them with the normal behaviour of the smart home. RE is responsible for determining at multiple stages in the processing of the data what the current Risk Level is. This Risk Level is associated with a particular action a device or an end-user is about to take. It validates real-time communication context using the behaviour device profiles, entailing the processing of the communication context properties. The fusion of the permitted risk levels according to user preferences and typical behaviour stored in safety patterns allows an automatic decision making, where risk levels matching and comparison indicates the appropriate security action: allowing or blocking the whole communication stream, or propagating the intervention to the user interface for the end-user approval or correction.

The structure of this paper is as follows. The research method followed for this paper is presented in Section 2. The recent advancements in the field of Behaviour Analysis (BA), Risk Prediction and Estimation (RPE) and Mitigation Techniques (MT) are presented in Section 3. Section 4 explains the Risk Assessment and Modelling (RAM) approach, whereas its model for risk levels calculation are demonstrated in Section 5. The application of the RAM in a selected scenarios is presented in Section 6. Finally, conclusions are summarised in Section 7 to give direction to the further work work.

2 Research Method

Design Science Research Method (DSRM) has been followed for this paper. It relies on the creation of "knowledge and understanding of a design problem, and its solution is acquired in the building and application of an artefact" [2]. Johannesson and Perjons [3] presented a DSRM Framework, which consists of five main activities namely: Explicate Problem, Design Requirements; Design and Development of Artefact, Demonstration, and Evaluation of Artefact.

Offermann et al. classified the artefacts into eight categories: System Design, Method, Language/Notation, Algorithm, Guideline, Requirements, Pattern, and Metric [4]. According to that classification of artefacts, this paper presents a "Method - Defines the activities to create or interact with a system" and "Metric - A mathematical model that can be used to measure the aspects of systems or methods". The work presented in this paper corresponding to the DSRM activities is presented in the Table 1.

Design Science Activity	Corresponding Section in this Paper
Explicate Problem	Introduction
Design Requirements	Introduction and Related Work
Design and Development of Artefact	Proposed Risk Assessment Model and Risk Level Modelling and Exposure Calculation
Demonstration of Artefact	Demonstration and Evaluation
Evaluation of Artefact	Demonstration and Evaluation

Table 1: DSRM and Paper's correlation

3 Related Work

Schiefer [5] demonstrates the challenges of a Risk Assessment (RA) analysis in a smart home installation due to the heterogeneous nature of the IoT devices. The spectrum of the threats for smart homes is twofold, namely privacy and security related. However, in most cases, the attacks are targeting to exploit both vectors. Unfortunately, the biggest problem still relies in primitive security settings that are ignored by unaware users. According to [6], multiple security incidents involving IoT devices exploit primitive attack vectors such as the use of default passwords or weak communication protocols. The most notorious example is the break out of the Mirai botnet [7], taking over at least 100,000 IoT devices. From the previous, it is evident that a regular user has no way to perceive the full picture of the potential risks involved in the smart home she is living in, and that an automatic monitoring solution is essential. In the followings, we present the recent advancements in the field of BA, RPE and MT tailored for the case of IoT environments.

3.1 Behaviour Analysis

One of the approaches widely used in proactively managing security incidents is behaviour analysis. In the case of smart home security, behaviour analysis can be applied directly on any existing network at the router/gateway entry/exit point of any smart home installation. In terms of the approaches used in behaviour analysis, Machine Learning (ML) is the most common method used for anomaly detection. For example, Saad et al., [8] successfully identified malicious behaviour on the network by comparing application of several existing ML classifiers. Zhao et al., [9] expanded the existing method with the use of the decision trees, allowing zero-day detection of the involvement in botnet activities. The framework proposed by Nari and Ghorbani [10], aimed at detecting malware, is using behaviour graphs, improving the accuracy and false positive detection by incorporating graph attributes. The use of behaviour analysis in cyber security solutions is crucial, as a way to provide additional analysis vector in anomalies detection. *GHOST* is incorporating this approach in RA layer, by extracting the communication context and searching for the anomalies in RE component.

3.2 Risk Prediction and Estimation

In [11] Kitchin and Dodge provide a risk overview for the case of smart cities. This survey can be considered the closest and more recent survey on the risk analysis, vulnerability and mitigation techniques identification on the field of Cyber-Physical System (CPS) security. There, the authors determine five main vulnerability categories for threat modelling: a) Weak software security and data encryption, b) Use of insecure legacy systems and poor ongoing maintenance, c) Many inter-dependencies and large and complex attack surfaces, d) Cascade effects and e) Human error. These five categories are also applicable to the case of a smart home environment.

Furthermore, Almohri et al., [12] suggest to incorporate threat modelling for risk assessment directly at the IoT device design stage, distinguishing three main approaches: attacker-, system- and asset-centric [13]. Rao, et al., [14] present a very promising approach based on the execution time of the processes in a CPS environment. This approach is the closest to *GHOST* work in terms of dynamic real-time risk assessment.

3.3 Mitigation Techniques

Current research in the mitigation techniques does not spread much further than providing generic recommendations for formal risk evaluation processes. The closest work presented in [11], provides guidelines for smart cities environment. The authors recognise three main categories of mitigation techniques: a) Security by design, b) Traditional security mitigation, and c) Formation of the core security teams within the administrative staff supporting infrastructure installations. However, no further dynamic and automatic solutions are presented in the relevant literature.

4 Proposed Risk Assessment Model

The management of large amount of personal and device data is one of the key challenges and adequate risk management process is to be adopted for the same. One of the potential methods to use for risk level definition in *GHOST* is to adopt the "Negative to Positive Model" [15]. The "Negative to Positive Model" is based on the four quadrants namely positive value gained from an activity done; positive value if the corresponding activity is not done; negative value if the activity is done; and the negative value if the activity is not done. These four quadrants of Negative to Positive Model have been classified as the four risk levels in the *GHOST* architecture, as follows:

- **Risk Level 1:** What will the positive value be if an activity is done? (e.g. compliance with privacy laws thus at the lowest level of risk in failing the compliance)
- **Risk Level 2:** What will the positive value be if an activity is not done? (e.g. collecting anonymised user information thus at a slightly higher level of risk in the event of failure of anonymisation technique and/or data theft)

- **Risk Level 3:** What will the negative value be if an activity is done? (e.g. collecting personal information and sharing the data with unauthorised third party)
- **Risk Level 4:** What will the negative value be if an activity is not done? (e.g. not anonymising the user data and paying penalty for the misuse of the data)

For the above-mentioned risk levels, the principle Basic Value Model (BMF) is applied for positive (yield/return) and negative (cost) values and it is to be used in conjunction with the negative to positive and the table of the balance sheet that is presented for a complete set of method steps for evaluating and presenting results. The principle of BMF is based upon the three areas with different characteristics as shown in Figure 1.

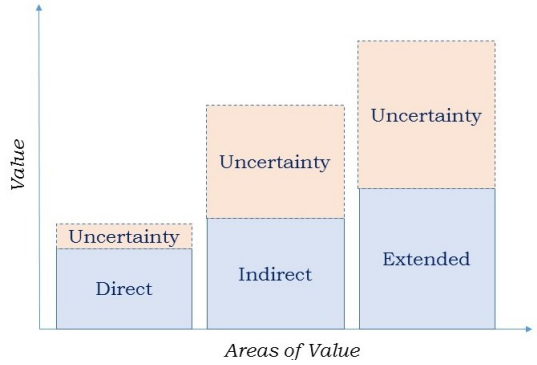

Figure 1: Principle Basic Value Model

- *Direct Values* refer to direct economic values, such as failure of a device, or direct investment based on an occurrence which could be active or passive.
- *Indirect Values* refer to the additional and more intangible values gained or lost. Indirect values have a greater uncertainty and as such they can be within ranges. Examples of indirect values are unavailability of services due to DDoS attacks, increased administrative tasks, etc.
- *Extended Values* reflect the values affected by the direct and indirect values and can be significantly huge. Extended values are also affected by other factors such as impact on society and/or the *GHOST* network as a whole, or share prices of suppliers if relevant, etc. Extended values of items such as brand, reputation, etc. are often difficult to quantify. Extended values are mostly negative but may also be positive as a consequence when information security is applied.

Addressing the above-mentioned four risk levels and corresponding questions in "Negative to Positive Model" in combination with the principle basic value model, Figure 1 will then lead to creation of a balance board as shown in Figure 2.

The use of the model will lead to assurance that all the aspects have been covered. However, there might be duplication of values related to the same

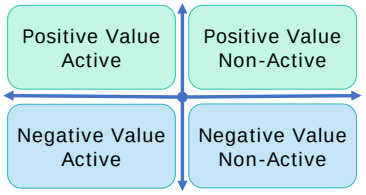

Figure 2: Negative to Positive Model

activity which can be handled by using a simple balance table as shown in Table 2.

Table 2: Balance Table for Net Values

	Base	**Activity**	**Positive Value Activity Done**	**Positive Value Activity Not Done**	**Negative Value Activity Done**	**Negative Value Activity Not Done**	**Net**
Ref			A	B	C	D	
1	A possible activity to change the current situation	Activity "XY" done	Value	Not Applicable	Cost	Not Applicable	A1-B1
2	The possible activity not done	Activity "XY" not done	Not Applicable	Value	Not Applicable	Cost	B2-D2

In some cases the amount in cell A1 might be the same as in cell D2, and thus the negative value/cost would turn into a positive value when comparing the net value for the two rows (Row 1 and 2). For a complex activity, further rows can be used but then also the summary should be between current state i.e., the possible activity is not done and when the activity is fully completed.

5 Risk Level Modelling and Exposure Calculation

Estimation of risk exposure at different risk levels is based on incorporation of the multitude of Influence Factors (IF), as identified in Table 3.

While the first three categories of IF are already integrated in the first model of risk level calculation, the last three factors have a *perception* factor, which needs to be further quantified in the risk estimation method.

1. Physical: Sum of the tangible (devices, sensors, etc.) assets in a smart home or the entire *GHOST* network under consideration

2. Intangible/Logical: Sum of the intangible (information, services, etc.) assets in a smart home or network

Table 3: Types of Influencing Factors

Type of IF	**Description**
Physical	Sum of the tangible assets that comprise the *GHOST* network
Customer/User	Smart home residents/owner
Societal	Perception that the society in general has about an appliance/device in the *GHOST* network and network as a whole
Reputational	Perception that competitors, suppliers, customers, shareholders, government and other stakeholders have about the devices in the network and services provided by the *GHOST* network
Intangible/Logical	Intangible assets handled by the *GHOST* network such as user data, forms of consent, blacklisted IP addresses, software integrity, etc.
Legal and Regulatory	Potential sanctions and/or penalties that might result from a breach

3. Legal and Regulatory: Potential sanctions and/or penalties that may arise from breach of data protection regulations, service contracts, etc
4. End-user
5. Societal
6. Reputation

Calculation model

- T : Time Period
- V_1 : Value created by taking an action
- A : Action taken to mitigate the risk
- V_2 : Value created by not taking an action
- AC_1 : Additional internal cost
- C : Cost associated with an action
- AC_2 : Additional external cost

Risk Level 1 $RL_1 = T \times (V_1 \times A)$

Risk Level 2 $RL_2 = T \times (V_2 - AC_1)$

Risk Level 3 $RL_3 = T \times C$

Risk Level 4 $RL_4 = T \times (AC_1 + AC_2)$

Determining the Risk Level

1. Is the risk mitigation action (device removal) completed?
   - If Yes, go to step 2
   - If No, go to step 3
2. Is $RL_1 > RL_3$
   - If Yes, Risk Level is RL_3
   - If No, Risk Level is RL_1
3. Is $RL_2 > RL_4$
   - If Yes, Risk Level is RL_4
   - If No, Risk Level is RL_2

6 Demonstration and Evaluation

We use a scenario based approach, a common practice in DSRM for ongoing work, to demonstrate and evaluate the application of the proposed risk assessment model in the given scenario.

6.1 Example scenario - A to B communication

Internal Internet of Things (IoT) device A (IP camera) is sending data to malicious entity B (malware.com). B is already in the blacklist (iptables).

Device	Exposure	Data
IP static camera	• Wi-Fi connection • Motion detection • Remote control • Night vision • Video & sound capturing • Face recognition	• System status • Configuration data • Video frames • Credentials for remote access • Facial profiles

Actions

1. Block outgoing communication from device A to B
2. Block all outgoing communication from device A
3. Allow outgoing communication from device A to B

Possible Consequences

1.
   - Partial service disruption (–)
   - User discomfort as no alert is received (–)
   - Controlled traffic (+)
   - Avoiding privacy infringement from the IP camera data sent to malware.com (+)
   - Avoiding ransomware attack (+)
2.
   - Full service disruption (–)
   - Exposure to theft (–)
   - Controlled traffic (+)
   - Avoiding ransomware attack (+)
3.
   - Remote control by unauthorised party (–)
   - Privacy violation (–)
   - Involvement in DDoS (–)
   - Potential danger in extreme scenario (–)
   - GDPR regulatory fine (–)
   - Ransomware (–)
   - Continuous monitoring of sick (elderly) person (+)
   - Physical security monitoring (+)

Manual Mitigation

- Remove the device
- Inform the administrator on possible threat

6.2 Application of Proposed Model

The proposed risk assessment model is applied to the above-mentioned scenario, and we made assumptions for the data used in the calculations below to demonstrate the positive and negative values of doing or not doing the required action.

6.2.1 Risk Level 1: Positive Value – Activity Done

Let us assume that by removing the device from the network, we gain a positive value of EUR 5000 (from the positive consequences as listed in outlined scenario and annotated with (+)). Time period under consideration is 1 day. Risk reduction for the GHOST network in the given home is 90%.

Hence, $T = 1$, $V_1 = 5000$, $A = 90\%$. Therefore, $RL_1 = 1 \times (5000 \times 0.9) = 4500$.

6.2.2 Risk Level 2: Positive Value – Activity Not Done

Let us assume that by not removing the device from the network, we gain a positive value of EUR 3000 (from the positive consequences as listed in outlined scenario and annotated with (+)). Further, there is an additional cost associated with the unwanted data flow between A to B, which we assume as EUR 1000.

Hence, $T = 1$, $V_2 = 3000$, $AC_1 = 1000$. Therefore, $RL_2 = 1 \times (3000 - 1000) = 2000$.

6.2.3 Risk Level 3: Negative Value – Activity Done

Let us assume that the negative consequences are critical in nature and by applying a method like Cyber Value-at-Risk (CVaR) for the above consequences as listed in outlined scenario and annotated with (–), we get an estimated cost (negative consequence) of EUR 8000.

Hence, $T = 1$, $C = -8000$. Therefore, $RL_3 = 1 \times (-8000) = -8000$.

6.2.4 Risk Level 4: Negative Value – Activity Not Done

Since the device is not removed, the associated external cost is estimated by using a method like Single Loss Expectancy (SLE) for the above-mentioned negative consequences as listed in outlined scenario and annotated with (–). Let us assume that by applying SLE we get EUR 10000.

Hence, $T = 1$, $AC_1 = 1000$, $AC_2 = -10000$. Therefore, $RL_4 = 1 \times (1000 + (-10000)) = -9000$.

7 Conclusion and Future Work

The Risk Level model presented in this paper is currently an ongoing research and development effort and is at the heart of the *GHOST* solution for risk assessment. Deployed at the network traffic capture level, the incoming data is constantly monitored and fed into several distinct analysers. The resulting output is a set (zero or more) of risk related properties. Further grouped into identified risks, they serve as a base for the exposure value calculation. Various risk levels at multiple stages of data processing are evaluated and monitored to ensure permitted risk levels of current activity at each case, practically determining the required action to be taken.

Experimental evaluation of the risk boundaries is enabling further fine-tuning of the calculation model to achieve automatic risks assessment. It is envisioned to perform several iterations of the model values refinement through the data obtained during the trials.

Furthermore, a process on effective allocation and association of the mitigation actions should be identified. The current prototype relies on the hard-coded set of the actions extracted from the set of predefined attack scenarios.

Nowadays, a typical smart home installation contains an enormous variety of IoT devices communicating with the controlling gateway and/or with each other through various wireless protocols. Threats against smart homes can put at risk the security and privacy of the unaware users residing on it. However, the traditional cyber security risk assessment approaches fail to address the

heterogeneous nature of such environment. *GHOST* project aims to close this security gap by providing a cyber security solution targeted at the regular citizens. In our work, we present an approach called Negative to Positive modelling to automate the threat-based risk assessment process, tailored specifically to the smart home environments. The RA layer is a core layer of the *GHOST* software implementation focused on the context-aware real-time risk assessment. As we discuss, the main purpose of this layer is to provide the real-time security and privacy risk assessment of the ongoing activities on the network. It gathers information about the current risks, analyses in real-time current network traffic flows and correlates them with the normal behaviour of the smart home.

References

[1] A. Collen, N. A. Nijdam, J. Augusto-Gonzalez, S. K. Katsikas, K. M. Giannoutakis, G. Spathoulas, E. Gelenbe, K. Votis, D. Tzovaras, N. Ghavami, M. Volkamer, P. Haller, A. Sánchez, and M. Dimas. GHOST - Safe-guarding home IoT environments with personalised real-time risk control. In *Communications in Computer and Information Science*, volume 821, pages 68–78, 2018.

[2] Olusola Samuel-Ojo, Doris Shimabukuro, Samir Chatterjee, Musangi Muthui, Tom Babineau, Pimpaka Prasertsilp, Shaimaa Ewais, and Mark Young. Meta-analysis of design science research within the IS community: Trends, patterns, and outcomes. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 6105 LNCS, pages 124–138. Springer, 2010.

[3] Paul Johannesson and Erik Perjons. *An introduction to design science*, volume 9783319106. Springer International Publishing Switzerland, 2014.

[4] Offermann P., Blom S., Schönherr M., and Bub U. Artifact Types in Information Systems Design Science – A Literature Review. In *Lecture Notes in Computer Science*, page Vol 6105. Springer, 2010.

[5] Michael Schiefer. Smart Home Definition and Security Threats. *Proceedings - 9th International Conference on IT Security Incident Management and IT Forensics, IMF 2015*, pages 114–118, 2015.

[6] Vijay Sivaraman, Hassan Habibi Gharakheili, and Clinton Fernandes. Inside job: Security and privacy threats for smart-home IoT devices. Technical report, Australian Communications Consumer Action Network, Sydney, 2017.

[7] Elisa Bertino and Nayeem Islam. Botnets and Internet of Things Security. *Computer*, 50(2):76–79, 2017.

[8] Sherif Saad, Issa Traore, Ali Ghorbani, Bassam Sayed, David Zhao, Wei Lu, John Felix, and Payman Hakimian. Detecting P2P botnets through network behavior analysis and machine learning. In *2011 Ninth Annual*

International Conference on Privacy, Security and Trust, pages 174–180. IEEE, 7 2011.

[9] David Zhao, Issa Traore, Bassam Sayed, Wei Lu, Sherif Saad, Ali Ghorbani, and Dan Garant. Botnet detection based on traffic behavior analysis and flow intervals. *Computers & Security*, 39(PARTA):2–16, 11 2013.

[10] Saeed Nari and Ali A. Ghorbani. Automated malware classification based on network behavior. In *2013 International Conference on Computing, Networking and Communications (ICNC)*, pages 642–647. IEEE, 1 2013.

[11] Rob Kitchin and Martin Dodge. The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *Journal of Urban Technology*, 0(0):1–19, 2017.

[12] Hussain Almohri, Long Cheng, Danfeng Yao, and Homa Alemzadeh. On Threat Modeling and Mitigation of Medical Cyber-Physical Systems. *Proceedings - 2017 IEEE 2nd International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2017*, pages 114–119, 2017.

[13] G Martins, S Bhatia, X Koutsoukos, K Stouffer, C Tang, and R Candell. Towards a systematic threat modeling approach for cyber-physical systems. *Resilience Week (RWS), 2015*, pages 1–6, 2015.

[14] Aakarsh Rao, Nadir Carreon, Roman Lysecky, and Jerzy Rozenblit. Probabilistic Threat Detection for Risk Management in Cyber-physical Medical Systems. *IEEE Software*, 35(1):38–43, 2018.

[15] ISO/IEC TR 27016:2014 Information technology – Security techniques – Information security management – Organizational economics ISO/IEC. Technical Report 1, International Organization for Standardization, Geneva, CH, 2014.