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

Pankaj Pandey[1], Anastasija Collen[2], Niels A. Nijdam[2], Marios Anagnostopoulos[1], Sokratis Katsikas[1,3] and Dimitri Konstantas[2]
[1]Norwegian University of Science & Technology, Gjøvik, Norway
[2]University of Geneva, Geneva, Switzerland
[3]Open University of Cyprus, Nicosia, Cyprus
Pankaj.Pandey@ntnu.no
Anastasija.Collen@unige.ch
Niels.Nijdam@unige.ch
Marios.Anagnostopoulos@ntnu.no
Sokratis.Katsikas@ntnu.no
Dimitri.Konstantas@unige.ch

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 a Risk Assessment Model (RAM), originating from Negative to Positive approach, to automate the threat-based Risk Assessment (RA) 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 RAM 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 RA 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 risk level. Through the proposed RAM, 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 (Collen *et al*, 2018) is to provide a cyber security solution targeted at the non-expert citizens by raising their awareness and understanding of the security risks associated with all aspects of cyber security from threats and vulnerabilities identification and personal data leakage detection up to making informed decisions affecting their cyber-physical smart home. GHOST aims to transform smart home occupants' decisions into reliable automated security service, promoting user-friendly end-user habits through usable security.

The Risk Assessment (RA) is a central functionality of the GHOST software implementation focused on the context-aware real-time threat protection. 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. RA is responsible for determining at multiple stages in the processing of the data what the current Risk Level (RL) is. This RL is associated with a particular action a device or an end-user is about to take. RA validates real-time communication context using device behaviour profiles, entailing the processing of the communication context properties. The fusion of the RLs accepted according to user preferences and of typical behaviour stored in security patterns allows an automatic decision making, where RLs 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's approval or correction.

The structure of this paper is as follows. The recent advancements in the field of Behaviour Analysis (BA), Risk Prediction and Estimation (RPE) and Mitigation Techniques (MT) are presented in Section 2. Section 3 explains the Risk Assessment and Modelling (RAM) approach, whereas the calculation of the RLs is demonstrated in Section 4. The application of RAM in a selected scenario is presented in Section 5. Finally, conclusions and directions for further work are summarised in Section 6.

2. Related Work

Schiefer (2015) demonstrates the challenges that RA poses 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 both aspects. Unfortunately, the biggest problem still relies in primitive security settings that are ignored by unaware users. According to (Sivaraman, Habibi Gharakheili and Fernandes, 2017), 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 (Bertino and Islam, 2017), that took over at least 100,000 IoT devices. From the above, it is evident that a non-expert 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 security risk monitoring solution is essential.

Behaviour Analysis: One of the approaches widely used in proactively managing security incidents is BA. In the case of smart home security, BA 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 BA, Machine Learning is the most common method used for anomaly detection. For example, Saad et al (2011), successfully identified malicious behaviour on the network by comparing application of several existing ML classifiers. Zhao et al, (2013) 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 (2013), aimed at detecting malware, is using behaviour graphs, improving the accuracy and false positive detection by incorporating graph attributes.

Risk Prediction and Estimation: In Kitchin and Dodge (2017) provide a risk overview for the case of smart cities. This survey can be considered the closest on the risk analysis, vulnerability and MT identification in the field of Cyber-Physical System (CPS) security. There, the authors determine five main vulnerability categories: 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. The same categories are also applicable to the case of a smart home environment. Furthermore, Almohri et al, (2017) suggest to incorporate threat modelling for RA directly at the IoT device design stage, distinguishing three main approaches: attacker-, system- and asset-centric (Martins *et al*, 2015). Rao et al, (Rao *et al.*, 2018) present a very promising approach, based on the execution time of the processes in a CPS environment. This approach is the closest to the work in GHOST, in terms of dynamic real-time RA.

Mitigation Techniques: Current research in the MT does not spread much further than providing generic recommendations for formal risk evaluation processes. The closest work presented in (Kitchin and Dodge, 2017), provides guidelines for smart cities environment. The authors recognise three main categories of MT: 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.

3. Proposed Risk Assessment Model

The approach taken for RA in GHOST involves the use of predefined Risk Levels (RL). "Negative to Positive Model" (*ISO/IEC TR 27016:2014*, 2014) was adapted for RL definition relying on four-dimensional correlation between values and activities. This model assesses risk on the basis of the cost (or benefit) associated with the option to either proceed with an action or not and turns negative values (cost) to positive (yield/return). Use of this model in our case results into the definition of four RLs, as shown in **Table 1**.

Table 1: Risk Level Definitions

	Question	Example
RL_1	What will the positive value be if an activity is done?	compliance with privacy laws thus at the lowest level of risk in failing the compliance
RL_2	What will the positive value be if an activity is not done?	collecting anonymised user information thus at a slightly higher level of risk in the event of failure of anonymisation technique and/or data theft
RL_3	What will the negative value be if an activity is done?	collecting personal information and sharing the data with unauthorised third party
RL_4	What will the negative value be if an activity is not done?	not anonymising the user data and paying penalty for the misuse of the data

The Basic Value Model (BVM) (*ISO/IEC TR 27016:2014*, 2014) is used to estimate the positive or negative value involved in each RL. The principle of BVM which is based on three different characteristics is shown in Figure 1.

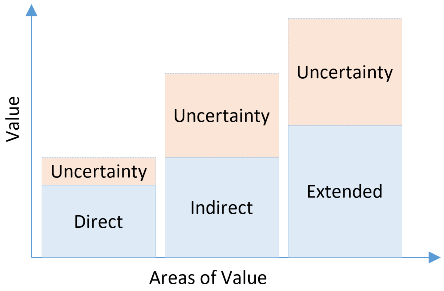

Figure 1: Principle Basic Value Model

With reference to the BVM, the following definitions apply:
Direct Values: direct economic values, such as failure of a device, or direct investment based on an occurrence which could be active or passive.
Indirect Values: the additional and more intangible values gained or lost, having a greater uncertainty and as such they can be within ranges. For example, the unavailability of services due to DDoS attacks or increased administrative tasks.
Extended Values: reflect the values affected by the direct and indirect values and can be significantly huge and are also affected by other factors, such as impact on society and/or the GHOST network as a whole. Extended values of items such as brand or reputation 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 four RLs and corresponding questions (**Table 1**) in combination with the principle BVM, led to the creation of a balance board to assure coverage of all risk relevant aspects. The potential duplication of the values related to the same activity is consecutively handled by using a simple balance table as shown in **Table 2**. Note that the factor C (Cost) is not applicable to the formulation used, but is part of the original BVM model.

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

4. Risk Exposure Calculation

Estimation of risk exposure at different RLs is based on incorporating a multitude of Influence Factors (IF). Their listing along with the current integration status in the RAM is outlined in **Table 3**.

Table 3: Types of Influencing Factors

Type of IF	Description	Status	Reasoning
Physical	Sum of the tangible assets that comprise the GHOST network	Yes	Devices, sensors, or any IoT assets in a smart home
Customer/User	Smart home residents/owner	No	Perception factor, to be quantified
Societal	Perception that the society in general has about an appliance/device in the GHOST network and network as a whole	No	Perception factor, to be quantified
Reputational	Perception that competitors, suppliers, customers, government and other stakeholders have about the devices in the network and services provided by the GHOST network	No	Perception factor, to be quantified

Intangible/ Logical	Intangible assets handled by the GHOST network such as user data, forms of consent, blacklisted IP addresses, software integrity, etc.	Yes	Information/data and services generated/available in a smart home
Legal and Regulatory	Potential sanctions and/or penalties that might result from a breach	Yes	Data protection regulations, service contracts and legal obligations

The calculation model for RLs is defined as follows and is based on the balance table (**Table 2**):

$$RL_1=T\times(V_1\times A) \qquad RL_2=T\times(V_2-AC_1) \qquad RL_3=T\times C \qquad RL_4=T\times(AC_1+AC_2)$$

Where *T* = Time period, V_1= Value created by taking an action, *A* = Risk reduction as a result of action taken, 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. Steps determining the RL in relation to an action taken:

1. If the action is completed, then go to step 2 else go to step 3.
2. If $RL_1 > RL_3$, then RL = RL_3 else RL = RL_1
3. If $RL_2 > RL_4$, then RL = RL_4 else RL = RL_2

5. Demonstration and Evaluation

We use a scenario based approach, a common practice in Design Science Research Method (Samuel-Ojo *et al*, 2010) for ongoing work, to demonstrate and evaluate the application of the proposed RAM in the given scenario. **Example scenario – A to B communication:** Internal IoT device A (**Table 4**) is sending data to malicious entity B (malware.com). B is already blocked by GHOST firewall (e.g. iptables).

Table 4: Device Exposure Vectors

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, Facial profiles

Possible GHOST actions to take on this suspicious situation are listed in **Table 5**.

Table 5: Action and Consequence Correlation

Action	Positive Consequences	Negative Consequences
Block outgoing communication from device A to B	Controlled traffic, Avoiding privacy infringement of data sent to malware.com, Avoiding ransomware attack	Partial service disruption, User discomfort as no alert is received
Block all outgoing communication from device A	Controlled traffic, Avoiding ransomware attack	Full service disruption, Exposure to theft
Allow outgoing communication from device A to B	Continuous monitoring of sick (elderly) person, Physical security monitoring	Remote control by unauthorised party, Privacy violation, Involvement in DDoS, Potential danger in extreme scenario, GDPR regulatory fine, Ransomware

Application of the Proposed Model: The proposed RAM is applied to the above-mentioned scenario, and few assumptions are made for the data used in the calculations below to demonstrate the positive and negative values of doing or not doing the required action.

RL_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). Time period under consideration is 1 day. Risk reduction for the GHOST network in the given home is 90%.

Hence, T = 1, V1 = 5000, A = 90%. Therefore, RL1 = 1 × (5000 × 0.9) = 4500.

RL_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). 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, V2 = 3000, AC1 = 1000. Therefore, RL2 = 1×(3000−1000) = 2000.

RL_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, we get an estimated cost (negative consequence) of EUR 8000.

Hence, T = 1, C = −8000. Therefore, RL3 = 1 × (−8000) = −8000.

RL_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. Let us assume that by applying SLE we get EUR 10000.

Hence, T = 1, AC1 = 1000, AC2 = −10000. Therefore, RL4 = 1 × (1000 + (−10000)) = −9000.

Based on the output values at the respective risk levels for the given scenario, the user can take an appropriate risk management decision whether or not to take the underlying action.

6. Conclusion and Future Work

The RAM presented in this paper is currently an ongoing research and development effort and is at the heart of the GHOST solution for RA. 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 RLs at multiple stages of data processing are evaluated and monitored to ensure permitted RLs 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.

7. Acknowledgements

This work is partially funded by the European Union's Horizon 2020 Research and Innovation Programme through GHOST project under Grant Agreement No. 740923.

References

Almohri, H. *et al.* (2017) '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*, pp. 114–119. doi: 10.1109/CHASE.2017.69.

Bertino, E. and Islam, N. (2017) 'Botnets and Internet of Things Security', *Computer*, 50(2), pp. 76–79. doi: 10.1109/MC.2017.62.

Collen, A. *et al.* (2018) 'GHOST - Safe-guarding home IoT environments with personalised real-time risk control', in *Communications in Computer and Information Science*, pp. 68–78. doi: 10.1007/978-3-319-95189-8_7.

ISO/IEC TR 27016:2014 Information technology -- Security techniques -- Information security management -- Organizational economics ISO/IEC (2014). Geneva, CH.

Kitchin, R. and Dodge, M. (2017) 'The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention', *Journal of Urban Technology*. Taylor & Francis, 0(0), pp. 1–19. doi: 10.1080/10630732.2017.1408002.

Martins, G. *et al.* (2015) 'Towards a systematic threat modeling approach for cyber-physical systems', *Resilience Week (RWS), 2015*, pp. 1–6. doi: 10.1109/RWEEK.2015.7287428.

Nari, S. and Ghorbani, A. A. (2013) 'Automated malware classification based on network behavior', in *2013 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, pp. 642–647. doi: 10.1109/ICCNC.2013.6504162.

Rao, A. *et al.* (2018) 'Probabilistic Threat Detection for Risk Management in Cyber-physical Medical Systems', *IEEE Software*, 35(1), pp. 38–43. doi: 10.1109/MS.2017.4541031.

Saad, S. *et al.* (2011) 'Detecting P2P botnets through network behavior analysis and machine learning', in *2011 Ninth Annual International Conference on Privacy, Security and Trust*. IEEE, pp. 174–180. doi: 10.1109/PST.2011.5971980.

Samuel-Ojo, O. *et al.* (2010) '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)*. Springer, pp. 124–138. doi: 10.1007/978-3-642-13335-0_9.

Schiefer, M. (2015) 'Smart Home Definition and Security Threats', *Proceedings - 9th International Conference on IT Security Incident Management and IT Forensics, IMF 2015*, pp. 114–118. doi: 10.1109/IMF.2015.17.

Sivaraman, V., Habibi Gharakheili, H. and Fernandes, C. (2017) *Inside job: Security and privacy threats for smart-*

home IoT devices, *Australian Communications Consumer Action Network*. Sydney. Available at: https://www.runnersworld.com/running-gear/inside-job.

Zhao, D. *et al.* (2013) 'Botnet detection based on traffic behavior analysis and flow intervals', *Computers & Security*. Elsevier Ltd, 39(PARTA), pp. 2–16. doi: 10.1016/j.cose.2013.04.007.