Threat analysis in dynamic environments: The case of the smart home

Georgios Kavallieratos*, Vasileios Gkioulos*, Sokratis K. Katsikas*†
Department of Information Security and Communications Technology, NTNU Norwegian University of Science and Technology, Gjøvik, Norway
Open University of Cyprus, School of Pure and Applied Sciences, Latsia, Nicosia, Cyprus
Email: *name.surname@ntnu.no,†sokratis.katsikas@ouc.ac.cy

***Abstract*—The rapid advancement of information and communication technologies has fostered the development and deployment of complex interrelated systems, many of which also present highly dynamic operational characteristics. These are further integrated within highly connected environments such as smart cities, smart homes, and smart cars, continuously adopting new technological developments. In this article, we focus on the smart home environment, as a case study for such ecosystems, where the integration of IoT devices increases the attack surface, evaluating whether existing risk assessment methods can be utilized for the identification and monitoring of risks, while also capturing the dynamic operational aspects. Accordingly, we review existing dynamic risk assessment methodologies and we leverage a smart home reference architecture to identify the security threats of a smart home's physical and communication viewpoints by leveraging the STRIDE methodology and Microsoft's threat modelling tool.**

***Index Terms*—Dynamic risk assessment, Threat analysis, Smart Home, STRIDE, Threat analysis tool**

I. Introduction

A dynamic environment is characterized by changes in its topology, data flows, and operational characteristics such as mobility patterns; these changes can occur periodically, continuously, or be event triggered. The Internet of Things (IoT) is a characteristic example of such an environment, with instantiations across various ecosystems such as smart homes, eHealth, vehicular networks, cloud computing and mobile communications. This dynamicity is accompanied by an enlargement and diversification of existing security risks, and the introduction of new attack vectors, due to the increased interconnectivity and enhanced operational features, such as remote control and management [1].

Smart homes are a characteristic example of rapid ICT penetration, as several types of connected devices and locally or remotely deployed services leverage ICT in order to facilitate the required operations. Several definitions for the concept of "smart home" can be found in the literature [2]–[4]. Smart homes could be defined by taking a technical viewpoint or a social perspective. The former describes the sensors, home appliances and smart devices which are connected in order to facilitate control over the home's ecosystem, whilst the latter describes how smart homes could influence human and social needs. Moreover, a smart home is able to support diversified components and entities, such as utility suppliers, infrastructure providers and third party software or hardware vendors [5]. As the result of this diversity, the security vulnerabilities of a smart home are increasing rapidly, paving the way to an unreliable and insecure ecosystem. To this end, ENISA in [6] identified potential threats and proposed good practices for their mitigation.

Although many risk assessment methods are available, these are mostly suitable for static systems and extract results which become invalid in case of dynamic modifications within the examined environment. Dynamic environments such as those described earlier, require risk assessment approaches which can adapt to the continuous changes of the environment and adjust their results considering such probabilistic changes. In this paper, by leveraging an existing smart home reference architecture, we carry out a threat analysis of the smart home ecosystem, as the first step towards a comprehensive dynamic risk assessment. The contributions of this paper can be summarized as follows: i) Identify dynamic risk assessment methodologies appropriate for identifying and assessing risks within the smart home ecosystem; ii) Conduct a threat analysis on an existing smart home reference architecture focusing on the data flows and cloud services.

The remainder of this study is structured as follows: Section II reviews related work. In Section III we describe the reference architecture of the smart home and in Section IV we briefly discuss the STRIDE method and Microsoft's threat analysis tool and we demonstrate their use in smart home scenarios of various complexity. Finally, in Section V we summarize our conclusions and propose directions for future work.

II. Related work

N. Shukla et al. in [7] present a comparative analysis of information security risk analysis methods. They compared different activities, inputs and outputs that each method requires. Specifically, the survey examines the OCTAVE, CORAS, CRAMM, ISRAM, CORA and IS Risk methodologies and categorizes each method depending on established criteria. V. Agrawal in [8] presents a comparative study of two qualitative (CORAS and CIRA) and two quantitative (ISRAM and IS Risk) methods, using an existing classification scheme proposed by Campbell et al. in [9]. The survey concludes that CIRA, IS and CORAS require the presence of a domain expert in the team, in contrast to ISRAM. However, none of

these methods is compatible with the smart home's dynamic ecosystem, as they examine a static architecture and do not take into consideration potential changes.

On the other hand, other studies have developed risk assessment methodologies for dynamic environments. J. R. W. Merrick et al. in [10] proposed a risk modelling method for maritime transportation. The authors considered simulations, expert judgment and available data, and proposed a method which handles multiple scenarios reflecting past, present and future operating procedures of the vessel's ICT systems. N. Poolsappasit et al. in [11] developed a framework for dynamic risk management that uses Bayesian attack graphs to address security issues in a network system. G. Puppala et al. in [12] proposed a dynamic risk assessment system using an improved attack graph to assess dynamic risks in cloud computing, and proposed appropriate mitigation techniques. The authors used the Common Vulnerability Scoring system to initiate each node's score in the attack graph. The DRAMIA dynamic risk assessment method for the IoT was proposed by C. Kiu et al. in [13]. DRAMIA consists of attack detection agents and sub-systems of dynamic risk assessment, which adopt immune system principles in order to dynamically change the attack detectors and estimate the risk according to the detection results of all attack detection agents. S. Naumov et al. in [14] introduced a dynamic framework to assess cyber risks in continuously changing environments. However, this work is in a preliminary stage. The National technical authority for information assurance in the UK proposed a technical risk assessment and risk treatment standard in [15] that is able to assess risks in dynamic systems or services where components are being regularly upgraded or replaced. A risk assessment engine for assessing cyber risks in real-time was also proposed by the WISER - Wide-Impact cyber Security framework project [16]. Specifically, machine-reliable risk assessment algorithms have been developed in order to facilitate the risk identification in dynamic environments. These algorithms take as inputs the business configuration, the vulnerability assessment, the network constraints and the application layer of the environment, to estimate the cyber risk. The aforementioned risk engines could in principle be used to assess risks in the smart home ecosystem.

The security of the smart home ecosystem has been studied in several works, that seek to identify potential vulnerabilities, threats and risks in this dynamic environment. M. Schiefer in [17] demonstrates the challenges that the risk analysis poses in a smart home installation, due to the heterogeneous nature of the IoT devices. A. Jacobsson et al. in [18] applied an information security risk assessment approach in the development phase of smart home automation systems. The authors identified nine low and four high level risks, and concluded that humans represent the highest risk exposure in smart home automation systems. Further, a risk framework for the smart home was proposed by T. Denning et al. in [19]. This framework focuses on the feasibility of an attack on the system; the attractiveness of the system as a compromised platform; and the damage caused by performing a successful attack. Its drawback is that it examines particular devices of the smart home and does not consider the data flows or the cloud services that are also crucial parts of the smart home's ecosystem. The security of the information flow in the Home Area Network (HAN) of a smart grid was examined by J. Tong et al. in [20]. They identified the security levels of HAN devices and data packets, and proposed a security model which aims to protect such data flows over the HAN network. B. Ali et al. in [4] proposed the use of the OCTAVE Alegro risk assessment method to identify potential risks in the smart home environment. They focused on the cyber and the physical layer of the smart home's architecture, and they identified ten critical cyber and physical assets. Although they carried out a comprehensive risk assessment, they did not take into consideration the complexity of the smart services and devices.

Dynamic risk assessment tailored specifically to smart home environments has been addressed within the EU project GHOST - Safe-Guarding Home IoT Environments with Personalized Real-time Risk Control [21]. The project has proposed a dynamic risk assessment model for real-time security and risk assessment on the ongoing activities over the network of a smart home, that may be implemented by means of a real time risk engine. Consequently, the risk assessment's results remain valid since the engine is able to dynamically identify changes in the environment and to re-assess the risk taking into consideration these changes [22].

III. Smart Home Reference Architecture

Through the smart home environment, designers and vendors seek to facilitate everyday tasks such as the remote control of the home's functions or the efficient management of energy consumption. A reference architecture can be used as a template in order to develop a specific architectural instance of such an environment, since it provides a common framework around which specific architectural decisions can be anchored [23]. In particular, such a model is able to integrate aspects such as human users, device implementations and server structures providing a more accurate view of the overall environment [24]. Various reference architectures have been proposed for smart homes [25]–[27]. However, most of them provide an abstract view of the home's architecture; hence they cannot be used for conducting a risk assessment. On the other hand, K. Ghirardello et al. in [28] proposed a smart home reference architecture by describing three viewpoints of the ecosystem: (i) Functional, (ii) Physical, and (iii) Communication. In particular, the functional viewpoint consists of the necessary functions that must be supported for the normal operation of the smart home. The next viewpoint describes all the physical components which are required for executing the smart home's functions. The last viewpoint contains the protocols which are necessary for the transmission of control and information flows among the components. A risk assessment to such a reference model allows the extraction of rigorous results since the critical components and services of a smart home are sufficiently described at an adequate level of abstraction. In this work, we leverage this reference model

to carry out a threat analysis, as the first step towards to a comprehensive risk assessment for smart homes.

IV. Threat Analysis

A. Method

Threat analysis is a statement of threats that are related to vulnerabilities of assets and threat agents [29]. As such, threat analysis is part of the risk assessment process [30]. In dynamic environments, it is necessary to use a threat analysis method which is taking into consideration potential changes to the examined environment. A threat analysis method can be based on either the attacker's perspective or the defender's perspective. The former is more complex, whilst the latter examines the targeted systems thoroughly and its scope is to defend them. The methodology to be used is important for the identification of all the attacks, threats and vulnerabilities across a smart home architecture. Focusing on methods which are able to identify threats automatically by means of the use of a supporting tool, we used the STRIDE method which is supported by the Microsoft's threat modelling tool. The method was developed by L. Kohnfelder and P. Garg and has been used by both academia and industry; it allows the extraction of rigorous results for the risks that the target systems face [31] and can be applied as early as the design phase. STRIDE stands for *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege*. The STRIDE threats are described by A. Shostack in [32]. Further explanation of methodology can be found in [33].

In this work we use Microsoft's Threat Modelling tool to identify potential threats which target data flows and back-end services of the reference model of [28]. This tool allows the identification of security problems in processes, data stores and data flows, as the analysis is conducted using Data Flow Diagrams (DFDs). In addition, the threat analysis tool promotes dynamic threat analysis since, through DFDs, the analyst is able to add or remove devices, connections or boundaries and extract the corresponding results automatically. Before the tool can be used, information on the systems to be examined, their interconnections and dependencies must be gathered, and security assumptions about the target environment must be made. An example of such an assumption is that a cloud provider uses encryption on the transmitted data. Data flow diagrams is a key characteristic of the tool; hence, one or more DFDs for the smart home ecosystem, each corresponding to a different topology need to be created. The identification of threats is achieved by using the STRIDE threat taxonomy. The analysis follows specific steps, as depicted in Figure 1. These are discussed in the sequel.

Fig. 1. Threat modelling tool steps

Describe Scenario: The scenario description must include all relevant elements within the scope of the examined environment. In this paper, the focus is on the smart home ecosystem and in particular on the data flows and the back-end services.

Identify Assets: The assets of the target system must be identified. Such assets include information assets and physical assets.

Create DFDs: By leveraging the simplicity of such diagrams, an analyst is able to represent devices, services, and data flows between the assets identified above.

Create constraints for each vulnerability: Each of the identified assets has various security vulnerabilities which have already been analyzed and can be found in existing vulnerability databases, such as [34] and [35].

Determine Threats: The analyst develops different attack scenarios, considering the identified assets and their interconnections. The tool automatically identifies threats, also taking into account the predefined constraints.

B. The case of the smart home ecosystem

In order to demonstrate the use of the method and tool described in the previous subsection to the case of the smart home ecosystem, we developed six distinct smart home scenarios. Our analysis is based on an existing template, modified appropriately to allow the analysis of particular data flows and back end services. Following the methodological steps described above, we first identified the assets in the environment.

The smart home ecosystem includes multiple assets, depending on the viewpoint. In this work we focused on the physical and communication viewpoints, thus we aim at identifying information and physical assets. These are:

- Information Assets
  1) User credential
  2) Information collected by smart devices
  3) Smart home status information
  4) Information about the installed assets
  5) Logs information
  6) Video, Picture, Voice Information
  7) Location tracking information
  8) Personal information: (i) Health information, (ii) Billing data, (iii) Profile data
- Physical Assets
  1) IoT smart devices
  2) IoT hubs
  3) IoT gateways
  4) Sensors/Actuators
  5) Cloud server

Based on the identified assets and various device and back-end service communication scenarios, we then created six scenarios, described by the corresponding data flow diagrams, representing six topologies of varying complexity, so as to approach the dynamic nature of the target environment.

Scenario 1 - IP camera and IoT gateway: The first scenario is a simple DFD which represents the connection between an IP camera and a gateway as depicted in Figure 2. The

ZigBee protocol is used for communication and our analysis focuses on threats which could harm either the physical assets or information transmitted between the devices. We assume that the IP camera is connected directly to the gateway.

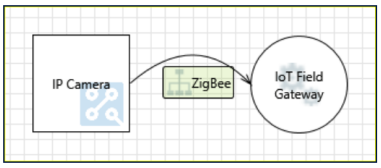

Fig. 2. IP camera and IoT gateway

The threat analysis resulted in identifying thirteen threats, as follows:

1) Spoofing
   - An adversary may gain access to the field gateway by leveraging default login credentials.
   - An adversary may spoof IoT Device with a fake one.
   - An adversary may reuse the authentication tokens of IoT Device in another.
   - An adversary may spoof a device and connect to field gateway.
2) Tampering
   - An adversary may exploit known vulnerabilities in unpatched devices.
   - An adversary may tamper an IoT Device and extract cryptographic key material from it.
   - An adversary may execute unknown code on IoT Field Gateway.
   - An adversary may tamper the OS of a device and launch offline attacks.
3) Repudiation
   - An adversary can deny actions on Field Gateway due to lack of auditing.
4) Information Disclosure
   - An adversary may eavesdrop the communication between the device and the field gateway.
5) Denial of Service
   - N/A
6) Elevation of privileges
   - An adversary may gain unauthorized access to privileged features on IoT Device.
   - An adversary may exploit unused services or features in IoT Field Gateway.
   - An adversary may trigger unauthorized commands on the field gateway.

Most of the threats are related to spoofing and tampering, due to the vulnerable configuration of the IoT device or the weak communication protocol.

Scenario 2 - Unidirectional communication between an IP camera and the cloud: Our second topology represents a connection between an IP camera and a cloud server through two gateways. The communication is established using three different protocols, as can be seen in figure 3. In this scenario, the IP camera sends only a request to the database. The former is connected directly to the gateway through the ZigBee protocol and the latter is a simple database which uses MySQL 2016. The threat analysis resulted in identifying twenty seven threats, some of them common with the first case; spoofing and tampering threats are again the most common:

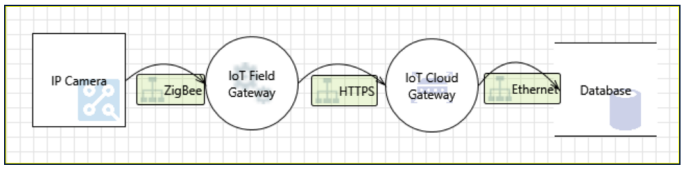

Fig. 3. Unidirectional communication between an IP camera and the cloud

1) Spoofing
   - An adversary may auto-generate valid authentication tokens for IoT Hub.
   - An adversary may replay stolen long-lived SaS tokens of IoT Hub.
   - An adversary may spoof IoT Field Gateway with a fake one.
   - An adversary may reuse the authentication tokens of IoT Field Gateway. in another
2) Tampering
   - An adversary can tamper critical database securables and deny the action.
   - An adversary may leverage the lack of monitoring systems and trigger anomalous traffic to database.
   - An adversary can tamper SSIS packages and cause undesirable consequences.
   - An adversary may gain unauthorized access to IoT Field Gateway and tamper its OS.
   - An adversary may tamper IoT Field Gateway and extract cryptographic key material from it.
3) Repudiation
   - An adversary can deny actions on database due to lack of auditing.
   - An adversary can deny actions on Cloud Gateway due to lack of auditing.
4) Information Disclosure
   - An adversary can gain access to sensitive PII or HBI data in database.
   - An adversary can gain access to sensitive data by performing SQL injection.
   - An adversary may eavesdrop the traffic to cloud gateway.
5) Denial of Service
   - N/A
6) Elevation of privileges
   - An adversary can gain unauthorized access to database due to lack of network access protection.
   - An adversary can gain unauthorized access to database

due to loose authorization rules.
- An adversary may gain elevated privileges on Cloud Gateway.
- An adversary may gain unauthorized access to privileged features on IoT Field Gateway.
- An adversary may exploit unused services or features in IoT Cloud Gateway.

Scenario 3 - Bidirectional communication between an IP camera and the cloud: The third topology is similar to the second, but now the IoT device communicates with the cloud bidirectionally. The used communication protocols are depicted in Figure 4. This topology inherits the security threats from the previous two topologies. The Spoofing and Information disclosure threats remain the same as in previous topologies, but six additional threats in the Tampering and Elevation of Privileges classes have been also identified.

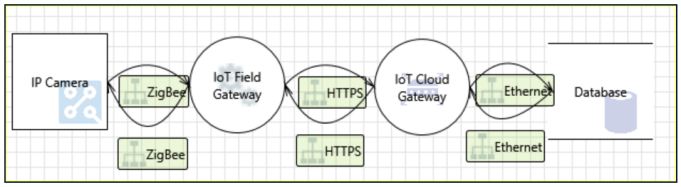

Fig. 4. Bidirectional communication between an IP camera and the cloud

The identified additional STRIDE threats are:

1) Tampering
   - An adversary may leverage the lack of monitoring systems and trigger anamolous traffic to database.
   - An adversary may attempt to intercept encrypted traffic sent to IoT Field Gateway.
   - An adversary may attempt to intercept encrypted traffic sent to IP camera.
2) Repudiation
   - An adversary can deny actions on Field Gateway due to lack of auditing.
3) Elevation of privileges
   - An adversary may exploit unused services or features in IP camera.
   - An adversary may trigger unauthorized commands on the device.

Scenario 4 - Smartphone controlled IP camera: A more complex topology is represented in the next scenario. This topology describes the communication between a smartphone-controlled IP camera and the cloud. The IoT device (smartphone) sends requests to the cloud API in order to control the IP camera through cellular communication. We identified forty-eight security threats in all, of which thirty-four are similar to threats identified in previous topologies.

1) Spoofing
   - An adversary may spoof Database and gain access to Web API.
   - An adversary may spoof IoT Device and gain access to Web API.

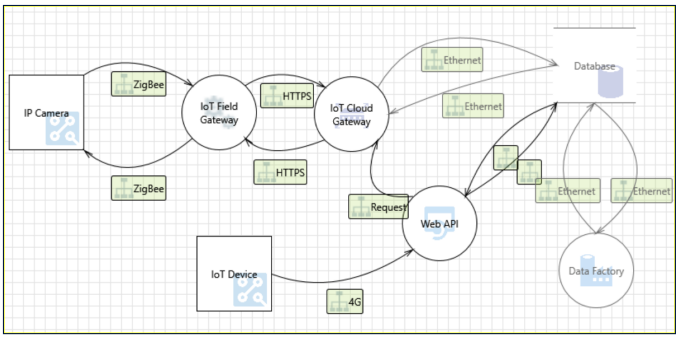

Fig. 5. Smartphone controlled IP camera

2) Tampering
   - An adversary may inject malicious inputs into an API and affect downstream processes.
   - An adversary can gain access to sensitive data by performing SQL injection through Web API.
   - An adversary may tamper the OS of a device and launch offline attacks.
   - An adversary may execute unknown code on IP Camera.
3) Repudiation
   - Attacker can deny a malicious act on an API leading to repudiation. issues
4) Information Disclosure
   - An adversary can gain access to sensitive information from an API through error messages.
   - An adversary can gain access to sensitive data by sniffing traffic to Web API.
   - An adversary can gain access to sensitive data stored in Web API's config files.
5) Denial of Service
   - N/A
6) Elevation of privileges
   - An adversary may gain unauthorized access to Web API due to poor access control checks.
   - An adversary may gain unauthorized access to privileged features on IoT Device.
   - An adversary can gain unauthorized access to resources in an Azure subscription.
   - An adversary may exploit unused services or features in Web API.

Scenario 5 - Smartphone communication with the cloud: The next topology represents the communication between the smartphone and the cloud as illustrated in Figure 6. In this topology we aim to identify potential threats that could provoke damage to the control requests. We identified twenty-three security threats, all of which have already been identified in previous topologies.

Scenario 6 - Links among smart devices: Finally, the last topology targets only smart devices (IP camera, alarm system and smartphone) and aims to identify potential threats which

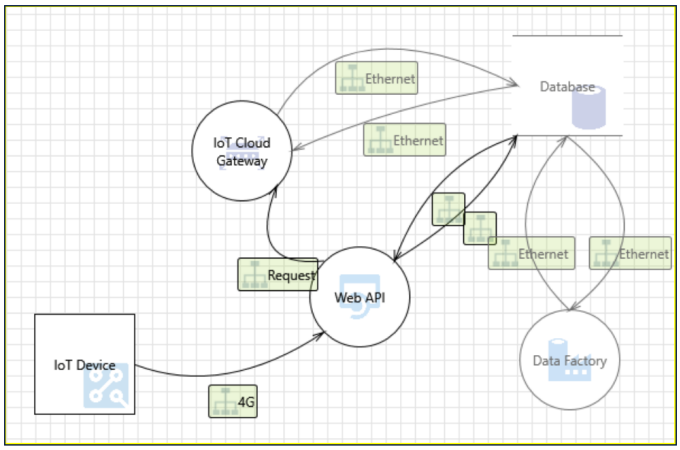

Fig. 6. Smartphone communication with the Cloud

derive from parallel links among these devices. In particular, the IP camera is able to communicate using 4G and the ZigBee protocol. The topology in Figure 7 depicts the interaction of an IP camera with a smartphone and with an alarm system. Sixteen STRIDE threats have been identified and have been categorized according to the communication protocol involved. Among these, nine threats refer to the IP camera, whilst only four and three originate from the smartphone and the alarm system respectively.

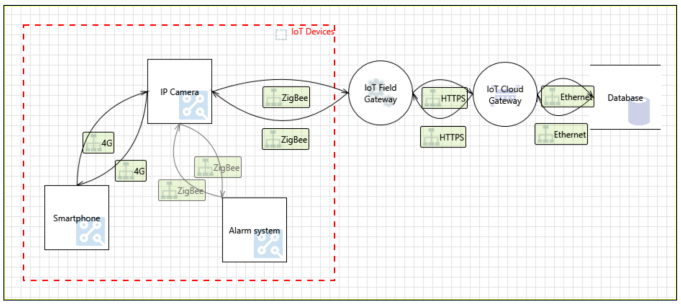

Fig. 7. Links among smart devices

1) Spoofing
   a) ZigBee request
      - An adversary may spoof IP Camera with a fake one.
      - An adversary may reuse the authentication tokens of IP Camera in another.
2) Tampering
   a) 4G Request
      - An adversary may exploit known vulnerabilities in unpatched devices.
      - An adversary may tamper Smartphone and extract cryptographic key material from it.
      - An adversary may execute unknown code on IP Camera.
      - An adversary may tamper the OS of a device and launch offline attacks.
   b) 4G Response
      - An adversary may tamper IP Camera and extract cryptographic key material from it.
      - An adversary may execute unknown code on Smartphone.
   c) ZigBee Request
      - An adversary may execute unknown code on Alarm system.
   d) ZigBee Response
      - An adversary may attempt to intercept encrypted traffic sent to IP Camera.
      - An adversary may tamper Alarm system and extract cryptographic key material from it.
3) Elevation of privileges
   a) 4G Request
      - An adversary may gain unauthorized access to privileged features on Smartphone.
      - An adversary may exploit unused services or features in IP Camera.
   b) 4G Response
      - An adversary may gain unauthorized access to privileged features on IP Camera.
      - An adversary may exploit unused services or features in Smartphone.
   c) ZigBee Response
      - An adversary may trigger unauthorized commands on the device.

The results above lead to the following conclusions on how the dynamic nature of a smart home environment affects the identified threats:

- As the complexity of the topology increases, more security threats are identified.
- More complex topologies inherit the threats that the simpler ones face.
- IoT devices such as IP cameras and smart devices increase the attack surface of the smart home. In particular, an attacker can launch elevation of privileges attacks more efficiently by leveraging vulnerabilities of an IP camera and its communication protocols, particularly ZigBee.
- Devices with transitive or parallel connections, such as an IP camera, are more vulnerable to cyber-attacks since they inherit the security vulnerabilities of each and every protocol.

V. Conclusions

In order to facilitate threat analysis for dynamic environments it is necessary to be able to continuously identify and analyze different components, systems and communication protocols. In this work we conducted a threat analysis for the smart home ecosystem, utilizing the smart home reference architecture of [28], the STRIDE threat analysis method and Microsoft's threat modeling tool, with an eye towards identifying and analyzing potential threats which target both physical components of a smart home environment and data

flows among them. The analysis considered six smart home instances of varying complexity.

Even though the proposed approach has been demonstrated to allow the capture of dynamic changes of devices and/or back-end services in a smart home environment, it does not come without limitations. These are mostly related to the threat analysis tool, which has not managed to identify denial of service threats and cannot handle physical threats that might affect the physical infrastructure. Furthermore, the existing DFD template does not support all the communication protocols that may be used in a smart home; hence our analysis was limited only to the ZigBee, HTTPS and 4G protocols. Moreover, the analysis of existing communication protocols considered only spoofing, tampering and elevation of privileges threats, as repudiation and information disclosure threats are not fully supported. What is more, the currently available template does not allow the examination of transitive attacks over the network. Speicifically, the specific template analyzes each component of the DFD separately and cannot consider malicious actions which, for example, could occur by a stealthy malware.

Despite these limitations, the approach can be used to provide input to one of the dynamic risk assessment methods to identify potential risks to the physical and communication viewpoint. As future work, we intend to develop a more flexible template to reflect the smart home ecosystem in higher fidelity, and use this to carry out a refined threat analysis, to be used as input to the dynamic risk assessment approach taken in the GHOST project. In particular, we will analyze the security of the communication protocols and data packets in more detail in order to contribute in the most crucial part of the Risk Engine which is the risk analysis.

REFERENCES

[1] H. Stuckenschmidt. Ontology-based information in dynamic environments. In *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WET ICE 2003. Proceedings. Twelfth IEEE Int. Workshops on*, page 295. IEEE, 2003.

[2] V. Fabi, G. Spigliantini, and S. P. Corgnati. Insights on smart home concept and occupants interaction with building controls. *Energy Procedia*, 111:759–769, 2017.

[3] N. K. Suryadevara and Subhas Chandra Mukhopadhyay. *Smart homes: design, implementation and issues*, volume 14. Springer, 2015.

[4] B. Ali and A. I. Awad. Cyber and physical security vulnerability assessment for iot-based smart homes. *Sensors*, 18(3):817, 2018.

[5] T. Denning, T. Kohno, and H. M Levy. Computer security and the modern home. *Communications of the ACM*, 56(1):94–103, 2013.

[6] C. Lévy-Bencheton, E. Darra, G. Tétu, G. Dufay, and M. Alattar. Security and resilience of smart home environments good practices and recommendations. *ENISA Google Scholar*, 2015.

[7] N. Shukla and S. Kumar. A comparative study on information security risk analysis practices. *IJCA Special Issue on Issues and Challenges in Networking, Intelligence and Computing Technologies ICNICT (3)*, pages 28–33, 2012.

[8] V. Agrawal. A comparative study on information security risk analysis methods. *JCP*, 12(1):57–67, 2017.

[9] J. E. Stamp and P. L. Campbell. A classification scheme for risk assessment methods. Technical report, Sandia National Laboratories, 2004.

[10] J. RW Merrick, J R. van Dorp, T. A Mazzuchi, and J. R Harrald. Modeling risk in the dynamic environment of maritime transportation. In *Proceedings of the 33nd conference on Winter simulation*, pages 1090–1098. IEEE Computer Society, 2001.

[11] N. Poolsappasit, R. Dewri, and I. Ray. Dynamic security risk management using bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 9(1):61–74, 2012.

[12] G. Puppala and S. K. Pasupuleti. Dynamic security risk assessment in cloud computing using iag. In *Progress in Computing, Analytics and Networking*, pages 105–116. Springer, 2018.

[13] C. Liu, Y. Zhang, J. Zeng, L. Peng, and R. Chen. Research on dynamical security risk assessment for the internet of things inspired by immunology. In *Natural Computation (ICNC), 2012 8th Int. Conference on*, pages 874–878. IEEE, 2012.

[14] S. Naumov and I. Kabanov. Dynamic framework for assessing cyber security risks in a changing environment. In *Information Science and Communications Technologies (ICISCT), Int. Conference on*, pages 1–4. IEEE, 2016.

[15] National Technical Authority for information Assurance. Hmg ia standard numbers 1 2 - supplement, standard no. 1 2 supplement technical risk assessment and risk treatment, 2012.

[16] R. Daz C. H. Arce D. Machnicki A. Cernivec A. Zitnik A. Refsdal A. L. Biasibetti S. Poidomani J. Bastiaensens A. Ivarez, S. Gonzlez and R. Cascella. Wide impact cyber security risk framework, 2015.

[17] M. Schiefer. Smart home definition and security threats. In *2015 9th int. conference on IT security incident management & IT forensics*, pages 114–118. IEEE, 2015.

[18] A. Jacobsson, M. Boldt, and B. Carlsson. A risk analysis of a smart home automation system. *Future Generation Computer Systems*, 56:719–733, 2016.

[19] T. Denning, T. Kohno, and H. M Levy. Computer security and the modern home. *Communications of the ACM*, 56(1):94–103, 2013.

[20] J. Tong, W. Sun, and L. Wang. An information flow security model for home area network of smart grid. In *Cyber Technology in Automation, Control and Intelligent Systems (CYBER), 2013 IEEE 3rd Annual Int. Conference on*, pages 456–461. IEEE, 2013.

[21] A Collen, NA Nijdam, J Augusto-Gonzalez, SK Katsikas, KM Giannoutakis, G Spathoulas, E Gelenbe, K Votis, D Tzovaras, N Ghavami, et al. Ghost-safe-guarding home iot environments with personalised real-time risk control. In *Int. ISCIS Security Workshop*, pages 68–78. Springer, 2018.

[22] N.A. Nijdam M. Anagnostopoulos S. Katsikas P. Pandey, A. Collen and D. Konstantas. Towards automated threat based risk assessment for cyber security in smart homes. In *18th European Conference on Cyber Warfareand Security (ECCWS 2019), accepted for presentation*, 2019.

[23] SW Lin, B Miller, J Durand, G Bleakley, A Chigani, R Martin, and M Crawford. The industrial internet of things, volume g1: Reference architecture. *Industrial Internet Consortium*, 2017.

[24] M. Weyrich and C. Ebert. Reference architectures for the internet of things. *IEEE Software*, 33(1):112–116, 2016.

[25] M. A. Chauhan and M. A. Babar. Using reference architectures for design and evaluation of web of things systems: A case of smart homes domain. In *Managing the Web of Things*, pages 205–228. Elsevier, 2017.

[26] C. Hu, S. Chen, L. Guo, C. Chootong, and L. Hui. Home care with iot support: Architecture design and functionality. In *Ubi-media Computing and Workshops (Ubi-Media), 2017 10th Int. Conference on*, pages 1–6. IEEE, 2017.

[27] ISO. Internet of things (lot) – reference architecture, 2018.

[28] K Ghirardello, C Maple, D Ng, and P Kearney. Cyber security of smart homes: Development of a reference architecture for attack surface analysis. 2018.

[29] S. Vidalis. A critical discussion of risk and threat analysis methods and methodologies. *School of Computing Technical Report CS-04-03, University of Glamorgan*, 2004.

[30] Information technology – Security techniques – Information security risk management. Standard, International Organization for Standardization, Geneva, CH, 2018.

[31] S. Hussain, A. Kamal, S. Ahmad, G. Rasool, and S. Iqbal. Threat modelling methodologies: A survey. 26:1607–1609, 01 2014.

[32] A. Shostack. *Threat Modeling: Designing for Security*, volume Wiley Publishing. 2014.

[33] G. Kavallieratos, S. Katsikas, and V. Gkioulos. Cyber-attacks against the autonomous ship. In *Computer Security*, pages 20–36, Cham, 2019. Springer International Publishing.

[34] Common Vulnerabilities. Exposures (cve). http. *cve.mitre.org*.

[35] National Vulnerability Database, March 2008. [online] https://nvd.nist.gov/.