Moving from Internet of Threats to Internet of Things: A Cyber Security Reference Architecture for Smart Home Environments

J. Augusto-Gonzalez[1], A. Collen[2], S. Evangelatos[3], M. Anagnostopoulos[4], G. Spathoulas[5], K. M. Giannoutakis[6], K. Votis[6], B. Genge[7], E. Gelenbe[8], N. A. Nijdam[2]

[1]*Televes SA*, Santiago de Compostela, Spain

[2]*Centre Universitaire d'Informatique, University of Geneva*, Geneva, Switzerland

[3]*EXUS Software Ltd*, London, United Kingdom

[4]*Center for Cyber and Information Security, Norwegian University of Science and Technology*, Gjøvik, Norway

[5]*Department of Computer Science and Biomedical Informatics, University of Thessaly*, Lamia, Greece

[6]*Information Technologies Institute, Centre for Research and Technology Hellas*, Thessaloniki, Greece

[7]*Kalos Information Systems AS*, Oslo, Norway

[8]*Imperial College London*, London, United Kingdom

[1]jaugusto@televes.com, [2]{anastasija.collen, niels.nijdam}@unige.ch, [3]s.evangelatos@exus.co.uk, [4]marios.anagnostopoulos@ntnu.no, [5]gspathoulas@uth.gr, [6]{kgiannou, kvotis}@iti.gr, [7]bela.genge@kalosis.com, [8]e.gelenbe@imperial.ac.uk

***Abstract*—The H2020 European research project GHOST – Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control – aims to deploy a highly effective security framework for IoT smart home residents through a novel reference architecture for user-centric cyber security in smart homes providing an unobtrusive and user-comprehensible solution. The aforementioned security framework leads to a transparent cyber security environment by increasing the effectiveness of the existing cyber security services and enhancing system's self-defence through disruptive software-enabled network security solutions.**

In this paper GHOST security framework for IoT-based smart homes is presented. It is aiming to address the security challenges posed by several types of attacks, such as network, device and software. The effective design of the overall multi-layered architecture is analysed, with particular emphasis given to the integration aspects through dynamic and re-configurable solutions and the features provided by each one of the architectural layers. Additionally, real-life trials and the associated use cases are described showcasing the competences and potential of the proposed framework.

***Index Terms*—IoT Security; Cyber Attacks; Smart Home; Reference Architecture;**

I. Introduction

Internet of Things (IoT), which has attracted considerable attention during the last decade, presents a huge opportunity for many industrial and business stakeholders in various domains. According to [1], by the year 2020 approximately 50 billion connected devices will be deployed and the total IoT revenue is expected to outreach more than one trillion euros.

As an emerging technology, IoT is prone to cyber security attacks and demands for countermeasures for the protection of such ecosystems are constantly growing. The heterogeneity and diversity of the "Things", as well as new lightweight communication protocols appropriate for IoT technology, create new challenges for the protection of such systems.

GHOST – Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control (https://www.ghost-iot.eu/) – is European Union Horizon 2020 Research and Innovation funded project, aiming at developing a reference architecture for securing smart homes IoT ecosystem. The multi-layer solution integrates traditional cyber security countermeasures, while it introduces new mechanisms for the efficient defence of common to IoT threats. This paper presents the detailed architecture of the solution, and discusses the integration and validation strategy followed for the delivery of the framework on the real life deployments.

The rest of the paper is organised as follows: Section II introduces the related work of security frameworks in IoT and in smart home environments specifically. Section III describes in detail the proposed security framework and its technical architecture, while section IV presents the integration and validation strategy followed for its successful implementation. Section V concludes the paper with the discussion on the results gained and provides possible future directions.

II. Related work

Internet-enabled smart home is one of the most well-known applications of the IoT since heterogeneous devices are networked together to provide smart services to the occupants of the smart home, offices and surrounding environment. The

S. Evangelatos is also with the National & Kapodistrian University of Athens, Department of Physics and Department of Informatics & Telecommunications, Athens, Greece

G. Spathoulas is also with the Center for Cyber and Information Security, Norwegian University of Science and Technology, Gjøvik, Norway

raise of the automation technology and the ubiquitous computing together with the constant growth of lightweight and low-energy devices have made smart homes more technology dependent and, thus, more complex in terms of security to handle.

A. Motivation

Meng et al., [2] demonstrate the challenges and security concerns in smart home installations and they argue that threats against a smart home environment can lead to security breaches and put at risk the safety and privacy of the unaware users residing in it. Bugeja et al., [3] attribute these security issues to the heterogeneous, dynamic and Internet connected nature of an IoT environment. To this direction, Jacobsson and Davidsson [4] propose a model that integrates security and privacy into the design of smart home services and systems. According to the authors, the security design principles and technologies of a smart home environment should incorporate security-enhancing technologies to protect the user information and provide resilience against malicious actions. Furthermore, Lin and Bergmann [5] suggest that a gateway architecture is most suitable to provide cyber protection to resource constrained devices. They also deduce that existing tools for the implementation of cyber protection in smart homes are applicable only for newly designed devices to be included in a future smart home installation.

B. Security Frameworks

A plethora of competing security frameworks for smart homes have emerged in order to tackle the security attacks that threaten the privacy and safety of the smart home residents. For instance, Park et al., [6] present a traffic monitoring and inspection solution, called IoTGuard. In their work, the authors utilise Bro IDS to detect abnormal behaviours in an IoT environment. The main drawback of their framework though is the requirement to forward all routers traffic to IoT Controller and link each IoT device with the IoT Watchdog in order to target and monitor particular IoT devices using device-specific IoT protocols.

The IDS framework by Pacheco and Hariri [7], based on Anomaly Behaviour Analysis, tries to provide security for existing and hardly changeable smart home installations. Their focus is given to measuring the activities of sensor devices installed in a smart house, and detecting any anomalies in the quantity and quality of the collected measurements. The limitation of their work relies in the ability to apply their analysis only on the primitive IoT devices without direct internet access.

The work by Rafferty et al., [8] is based upon the Agent-based modelling, where agents inside the smart home environment make observations and implement intended behavior. This model requires minimal engagement by the user and it is focused on threat detection. However, it neglects the detection of vulnerable devices within the smart home. Furthermore, the reasoning process, namely the process of deciding what actions to perform to reach a goal, is taking place in the Cloud layer. Finally, the aforementioned framework was not tested against live data, i.e., operating real-time.

A more user-intrusive approach for network security is presented by Habibi et al., [9]. There, the authors propose a whitelist-based intrusion detection technique specific for IoT devices. The proposal aims to prevent IoT devices to get entangled in botnets activities, so it blocks at the gateway level DNS lookups to malicious sites. However, this solution is only applicable for IP-based IoT devices and networks.

Similarly, DeMarinis and Fonseca [10] state that a network-layer architecture is required for the protection of a smart home against external threats and the mitigation of attacks from compromised devices. The authors recommend the implementation of a policy-based framework to restrict malicious traffic. The adopted policies will follow a white-listing approach based on the observed and predictable patterns in network traffic of the IoT devices. The main drawback of this proposal, however, is that each different purpose IoT device exhibits distinct patterns, requiring a monitoring period of the legitimate usage for each IoT device to construct its network pattern. Nevertheless, the work by DeMarinis and Fonseca is in preliminary stage and presents only considerations for designing a novel security layer.

Serror et al., [11] follow a rule-based approach, where every IoT device is allowed a specific behaviour, namely specific set of allowed connections, in order to fulfill its intended functionality. In this work the gateway enforces these rules with traffic filtering and anomaly detection techniques. An apparent drawback is the required definition of the communication rules, whereas in the case of the lack of which by the manufacturer or a certification authority, should be provided by the end-users.

A different approach is followed by Dorri et al., [12], where the authors propose a blockchain-based solution for decentralised security and privacy in a smart home environment. Specifically, they utilise a local and private blockchain to control and audit the communications internal and external to a smart home. This way an access control policy to the IoT devices and their data is enforced. However, the proposed mechanism exhibits a relative large overhead regarding traffic, processing time and energy consumption, as it requires each smart home to be equipped with a high-resource miner for the administration of the blockchain.

C. Emerging advancements

Nowadays, the absence of IoT standards and the intrinsic complexity demand for proper security layers constitute the need of holistic IoT security solutions imperative. Apart from some notable exceptions, such as [13] where the authors propose a methodology to validate and certify different technological solutions in large-scale conditions and [14] where the cyber security aspect regarding the communication between IoT devices and external entities is addressed, there is still a long way until the total armour of the IoT.

Several research papers, derived by the work done in various EU funded projects, exist in the literature mainly focusing on

crucial aspects of the IoT domain, such as the interoperability in different IoT environments [15] and for heterogeneous testbeds [16], privacy [17] in terms of authorisation and sensitive information handling, cloudification [18] and smart applications and services towards an open IoT ecosystem [19], just to name a few. Nevertheless, there are numerous issues left open for further discussion, with the most prominent one being the security in IoT.

GHOST project aims to close this security gap by providing a generic, hardware agnostic, security solution for smart home installations. It takes into account multiple different protocols and monitors the behaviour of all installed IoT devices along with the activity of the smart home gateway. The system automatically handles detected security events, while self defending mechanisms have also been employed to ensure its normal operation. It requests user intervention only when this is absolutely required, while a lot of effort has been concentrated on the usability of the interfaces used for user interaction. Additionally, GHOST solution has been designed upon the restriction that it should be functional while running on limited hardware resources, an evident constraint for smart home gateways. The developed algorithms are performance efficient and require minimal resources. In a few cases where additional hardware resources are required, a lot of attention has been given to preventing sensitive personal data of smart home inhabitants leave the gateway, and thus any privacy implications are eliminated. Finally, while blockchain technology has been employed, there is no requirement for significant hardware resources. A modular architecture has been implemented, that enables the blockchain related components, to either connect to external blockchain nodes or run a local lightweight node inside the smart-home gateway.

III. System Architecture

The conceptual design of the GHOST architecture [20] relies on the thorough identification of all crucial elements of the wide attack vector applicable for the smart home environments. Due to the numerous constraints depicted in related works, GHOST follows a network monitoring and anomaly detection approach, allowing to preserve the existing heterogeneity of the IoT devices deployed in the smart home and focusing on the analysis of the generated network activity. The conceptual design was further enhanced through the functional requirements extraction process directly from the end-user need analysis and advancements in the research on a security intelligence available within the consortium. To this end, GHOST pursues a layered system architecture approach, allowing independent development of the separate components, while preserving a high inter-dependency within the framework. This section describes in details GHOST's system logical layers depicted in Fig. 1.

A. Gateway (GW)

This layer focuses on linking an already existing gateway software environment with GHOST solution, mostly composed of the Interoperability Middleware (IM). Its main goal is

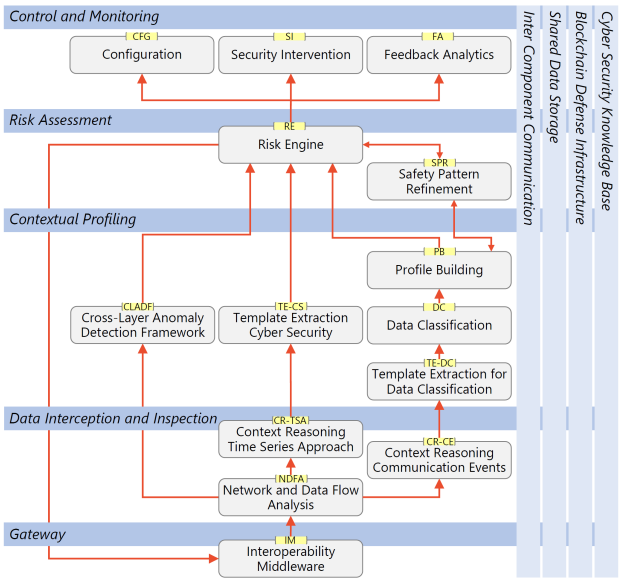

Fig. 1. GHOST system architecture

to provide a uniform access to the gateways managing IoT devices in the smart homes. This is where the actual traffic packet capture is realised, ensuring consistent implementation across different protocols supported. An important effort is devoted to gaining a near real-time performance, and part of the research is to strike a balance between having real-time and a low as possible resource use impact. Furthermore, this layer is responsible for the sensitive operations at the core of the system, such as modifications to the *iptables*, aggregation of device events for inclusion in the risk assessment and direct control on IoT devices. For example, *iptables* cannot be used for Bluetooth communication, it is therefore not possible to block a certain Bluetooth communication flow. Instead the whole device can be excluded if necessary through the control commands through the unified API, exposed to the internal modules.

B. Data Interception and Inspection (DII)

Responsible for the direct network data gathering and extraction, this layer is composed of three modules: Network and Data Flow Analysis (NDFA) Context Reasoning Time Series Approach (CR-TSA) and Context Reasoning Communication Events (CR-CE). The NDFA component takes incoming network traffic that is going through the IM and extracts 'valuable' data, to be utilised by other components afterwards for anomaly detection. For all supported protocols (IP, Bluetooth, Z-wave, RF869) full packet data are being retained for a certain time-frame in the Shared Data Storage (SDS). Consecutively, a data release strategy, based on time interval & size, is applied. Whenever a new packet or flow is detected, the NDFA directly propagates this event through the Inter Component Communication (ICC) to all subscribed components, which in turn will access the SDS for its related data.

The CR-CE component extracts meaningful context information (*generic metrics*) and CR-TSA extracts metrics specific for attack detection (*cyber security metrics*). The context information is further utilised by the upper layer's components to identify user data, with a special focus on the privacy monitoring. Its focus lies on knowledge about similarities and repetition of similar events, and deduction of the reasoning for each particular communication. Using the data flow information prior processed by NDFA, the components process these data to identify the communications related to distinct events occurring for smart home devices.

C. Contextual Profiling (CP)

This layer provides current state of data identification and related behaviour of the IoT devices' generated network data and is relying on the performance of several components: Template Extraction Cyber Security (TE-CS), Template Extraction for Data Classification (TE-DC), Data Classification (DC), Profile Building (PB) and Cross Layer Anomaly Detection Framework (CLADF). TE-DC is using the context information (*generic metrics*) to create templates according to the communication patterns of the devices. For example, a motion sensor template can contain the type of packets being sent to the Gateway (GW), their frequency, the number of device or personal packets sent during a day. TE-CS utilises the *cyber security metrics* which are based on *cloud trained Artificial Intelligence (AI)* to detect attacks with a probability which is then fed to the Risk Engine (RE) through the SDS.

The DC component is responsible for classifying data as content data (user-related data) and device events. It applies a variety of algorithms together with the templates from the TE-DC to process incoming traffic. A certain probability is given to each captured packet or flow and its classification. The communication between the TE-CS and the DC follows a reinforcement learning scheme. Information regarding the classification quality, when ground truth class labels are available through user feedback, is provided back to the TE-DC, to probe different configurations for more accurate classifications.

The PB component is responsible for building behavioural profiles of devices. Its purpose is to guide the detection of abnormal behaviours in communications and of new devices that enter the network. It incorporates the results from the DC and the metrics from the NDFA for building *behaviour graphs*. Its self-improvement mechanisms are relying on the feedback intelligence distributed by the Safety Pattern Refinement (SPR) from the Cyber Security Knowledge Base (CSKB).

The main purpose of the CLADF is to utilise existing cyber security features and combine them in a unified output. The output of the CLADF is used by the RE directly to perform a risk assessment and to provide visual support in the representation of any reported event by the Feedback Analytics (FA). A significant aspect targeted by CLADF is the correlation and combination of different events. Even though a particular cyber attack may trigger several alarms in different tools, it is important to understand the semantics of the events and to find a possible correlation by combining several apparently distinct events into a unified output, including data on the possible source, time, magnitude, and severity on the event.

D. Risk Assessment (RA)

This layer combines intelligence reports regarding noticeable alerts and performs real-time risk assessment. It is composed of RE and SPR. The RE is responsible for the risk assessment for any communication, correlating device activity on the network with the prior established metrics and profiles available from the Contextual Profiling (CP) layer. The communication is being processed through a variety of analysers, handling different aspects of the incoming data, such as the *behaviour* support by the PB component, the *payload* related to the DC and NDFA, the *blocking rules* interfacing with the IM component and the *alert processor* for handling detected attacks/anomalies by the CLADF and the TE-CS. In addition, it is enhanced with the Blockchain Defense Infrastructure (BDI) protection to ensure the reliability and trustworthiness of the automated decisions.

SPR is optimising the performance and efficiency of the PB and RE components and acts as an intermediate for providing safety insights to the RE's operations and strengthening the PB device profiles. These insights are foremost coming from the CSKB and indirectly from the RE and PB themselves. The information from the CSKB is based on the *user feedback* decisions on blocking communications aggregated and analysed from all connected GHOST installations.

E. Control and Monitoring (CM)

Visualisation of the available risk reports through user friendly interactions is ensured by components of this layer: Configuration (CFG), Security Intervention (SI) and FA.

The CFG provides the means and functionality to the user to control and configure the GHOST platform. It has two stages, the first being the *first time usage* and second the *regular usage* of the configuration pages. All configuration options are stored in the SDS and are mostly directly related with the RE component itself, calibrating the risk assessment parameters. A key focus is given to the effortless and usable design of the configuration setup process and further settings review and fine-tuning of applied configuration policies. These include, *authentication management* and *factory reset* at its highest level and control over the *blocking rules*, personalising the *risk levels* and *awareness automation* directly related to the risk assessment.

The SI serves for user friendly visualisation of the risk tracking and evaluation results. The appropriate visualisation and human-machine interaction mechanisms are put in place to allow users to effortlessly and effectively review security issues and *take key decisions* that affect their privacy and security. Visualisations are fed by data analysis and results from the RE component, tailored in relation to the usability studies and results from real life trials. A set of scenarios have

been extracted in which a certain mitigation action by the RE is realised.

The FA component is responsible for providing high-level monitoring and analysis of data originating from the Data Interception and Inspection (DII), CP and Risk Assessment (RA) layers. The input data include historical and current packet flow behaviours, risk levels, device profiles, packet classification scores and any metrics available and deemed suitable for display. The input data are used in order to provide visual and intuitive presentations and reports of the smart home security status, including visualisations of packet features through time, visual monitoring and distinction of packet/flow behaviours, and visual identification of potential anomalies and vulnerabilities. For this purpose, existing visualisation techniques, employing multimodal graph-based visualisations, will be adapted to the data generated in the home environment.

F. Blockchain Defense Infrastructure (BDI)

In order to ensure the integrity of the data exchanged among devices for central decision making for risk assessment, GHOST uses a variation of the default blockchain approach.

a) Public blacklisting: The RE is able to assess the risk imposed by the connections and communications between internal with external end points, which may result in a mitigation action to push a malicious IP onto the blockchain. Here, a list of malicious IPs is collaboratively created and maintained by different installations.

b) Forms of consent: As part of the operation of the BDI network, records of transactions are hashed by the miner nodes in an encrypted format, including potentially sensitive user data, such as records from medical devices. Informing the users about the operating principles of the network as well as to request the acceptance of the principles by the users is done by digitally signing a *Form of Consent*.

c) Software integrity: The BDI network can utilise a new firmware update scheme, based on a synergy between the Blockchain network and a BitTorrent network. That way, the version of the firmware can be checked securely, its correctness can be validated and the installation of the most up-to-date firmware on all the devices of the network can be ensured.

G. Cyber Security Knowledge Base (CSKB)

The CSKB is a cloud-based knowledge repository, which collects anonymised security intelligence and insights from external web sources and other GHOST instances. It maintains a list of malicious actors and properties (IP addresses, domains, URLs, file hashes). These data are produced by feedback from the users through the FA and SI components; scraped regularly from open online research; collected from specific commercial feed publishers; generated by correlation triggers and malware analysis engine. The information is further analysed and propagated to the SPR for enhancing each individual GHOST platform.

H. Shared Data Storage (SDS)

At the core of the SDS lies a PostgreSQL database and a service that provides easy access to it. All internal GHOST components have the option to directly access the database, whereas a more secured interaction is provided by the service for *external* access. For example, for the GW itself and the exchange of configuration data or information regarding the devices which are subscribed to the GW. Additionally, the data encryption mechanisms are put in place to comply with security requirements.

I. Inter Component Communication (ICC)

The ICC component is the glue between all the components for direct communication and, based on ZeroMQ[1], it offers two exchange patterns:

- Request/Reply, a client connects to a service and performs a *request*.
- Publish/Subscribe, a client(service) sends data to a set of *subscribed* clients, with the possibility to set an intermediate broker.

Furthermore, messages between the components are encoded by Protocol Buffer[2], efficient method to serialise structured data.

IV. Integration and validation strategy

GHOST project tackles several challenges in terms of integration of the solution due to its modular and interrelated architecture presented in previous section. Therefore, the development process that has been followed relies on the use of a funnel approach, both in terms of innovation and development.

A. Innovation and development approaches

GHOST follows a user-centred methodology where several experiments have been defined to lead the road from the conceptual idea to the final market solution. To this end, the initial stages of the project have involved the user through online questionnaires and focus groups with potential users of the system. These experiments led to the conclusions that there was a lack of awareness of the potential risks associated to cyber security [21] and the need of assistance in the configuration and management of the system (tips and tricks, baseline guides, etc.). During the lifetime of the project, the realisation of trials in real life installations, involving up to 200 people is envisioned. In this way, the GHOST's functional design is being continuously evaluated to find the most useful and usable features and characteristics through the continuous involvement of users within the development process, fostering the innovation of the solution and the route to the market.

[1]http://zeromq.org/

[2]https://developers.google.com/protocol-buffers/docs/overview

B. Cyber security validation

In addition to the innovation path, technical feasibility and robustness of the system, GHOST validation strategy is also focused on the demonstration of its capabilities to detect and prevent cyber threats. To this end, three possible types of attacks have been defined and analysed from the GHOST perspective:

a) Physical attacks: related to physical actuation over one or several devices leading to malfunctioning of these devices. This category is formed by attacks such as physical damage caused by the removal of the battery, shut down of the proper device or physical breaking of the device, injection of an actual device with malicious objectives in the network or mechanical exhaustion of physical buttons or triggers that creates, in the long term, malfunctioning of the device. GHOST addresses these type of attacks through the detection of changes in the communication patterns between the devices and the gateway, where the rate of communication increases, decreases or becomes absent all together.

b) Network attacks: related to direct actuation over the network traffic to cause malfunctioning of the system or capturing relevant information. This category includes well-known traditional attacks normally based on IP protocols (such as network scanning and enumeration techniques as TCP/IP and UDP related scan, Denial-of-service (DoS) or Distributed denial-of-service (DDoS)), device impersonation attacks where the attacker injects packets captured from an authorised device to trigger other devices or sniff communications, or artificial creation of network activity causing battery drains by eliminating, for example, idle times of devices. GHOST solution is dealing with these attacks through the analysis of changes in the communication templates characterising each device in the network and monitoring the evolution of flow based communication profiles between different devices within the network.

c) Software attacks: based on gaining access to a device within the network and using or altering its software to provoke malfunctioning of the specific device or of the service. In addition to the well-know traditional software-based attacks that implies the exploitation of software flaws through the use of viruses, worms or malicious script executions, this category also analyses specific to IoT attacks, such as software compromising in the gateway or in the devices (where the attacker gains access to the software inside the device and modifies somehow its behaviour), the injection of unexpected commands or communications between two devices on the same network by utilising gateway legitimate communication channels for malicious purposes or sleep deprivation of the device leading to battery drains (where the attacker is able to change the logic of the device forcing longer wake up times than usual and affecting directly the service). The specific blockchain-based integrity checking mechanisms defined for the GHOST solution in combination with the network monitoring and analysing tools of the system are key assets for protecting the smart home against this type of attacks.

The GHOST architecture has been designed to cover a broad set of attacks due to the monitoring of critical parameters, probably affected by any attack designed, covering possible omitted attack vectors. The combination of data analysis (for extracting templates of devices and for analysing changes in the data within the network), blockchain (for protecting the integrity of the firmware of devices) and other security-related technologies enables a multi-sided cyber security tool for smart homes. GHOST detection and prevention capabilities against above identified attacks will be tested in specific testbeds in the partners' facilities, to avoid leakage or burden risks to the end-users participating in the real life trials.

C. Integration methodology

Layered and multimodal architecture of the GHOST, the device-agnostic concept and the use of state-of-the-art tools and technologies raise the complexity of the integration process. To overcome this complexity a combination of development methodologies to make the most of the development efforts was used. At early stages a waterfall approach was followed until the release of the first prototype. Additionally, it was combined with an iterative agile approach for continuous feature improvement. The waterfall approach in early stages of the project ensured the clarification of the basic requirements of the solution and the coherence in the development in spite of the interdependence of modules. However, it showed limited effectiveness for managing the continuous integration and, therefore, the continuous change of the requirements when incorporating the feedback of the end-users.

To solve this lack of flexibility, GHOST adopted a SCRUM-based approach (OpenProject[3]). Designating a product owner for each GHOST module, based on the interrelation between modules. The product owner is the main user of the information generated by each module and/or the interfaces, where the product owner is in direct contact with the end-users (incorporating the user's feedback in the technical development).

The product owner creates monthly sprints by prioritising the tasks in the backlog of each of the modules according to the needs of the user. Consecutively, monthly releases of the GHOST platform are remotely uploaded to the gateways within the trials and directly presented to the end-users.

V. Discussion and future work

This paper proposes a cyber security reference architecture, tailored for smart homes consisting of Internet of Things devices. The work performed under the European research project GHOST targets efficient countermeasures for defencing cyber attacks on lightweight smart homes gateways. The design of the functional elements of the architecture was derived from thorough analysis of the IoT infrastructures and particularities of smart homes environments, further enhanced by the specific needs of the end-users. The different architectural layers presented, despite their high inter-dependencies, cover different scopes for the detection and mitigation of attacks,

[3]https://www.openproject.org/

from network analysis and reasoning to security intervention and analytics.

The followed user-centred approach and the continuous involvement of the end-users in the design and evaluation phase of the project, made the validation and integration more complex. To overcome the complexity of these tasks, a detailed validation plan has been developed, while an agile development and integration approach has been adopted, providing the required flexibility to the project in comparison to waterfall based approaches.

The real life trials, executed in three phases, where the actual deployment of the system on smart homes will take place, will offer significant feedback on the usability and validation of the system to realistic cyber security incidents. Continuous improvements, through the agile approach and the iterative real life trials, will construct a solid and effective solution for the protection of smart homes using lightweight gateways.

ACKNOWLEDGEMENT

This work has received funding by the European Union's Horizon 2020 Research and Innovation Programme through GHOST project (https://www.ghost-iot.eu/) under Grant Agreement No. 740923. This paper reflects only the authors views; the European Union is not liable for any use that may be made of the information contained therein.

REFERENCES

[1] H. Jayakumar, K. Lee, W. S. Lee, A. Raha, Y. Kim, and V. Raghunathan, "Powering the Internet of Things," in *Proceedings of the 2014 International Symposium on Low Power Electronics and Design*. ACM, 2014, pp. 375–380.

[2] Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, "Securing Consumer IoT in the Smart Home: Architecture, Challenges, and Countermeasures," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 53–59, 2018.

[3] J. Bugeja, A. Jacobsson, and P. Davidsson, "On Privacy and Security Challenges in Smart Connected Homes," in *2016 European Intelligence and Security Informatics Conference*, 2016, pp. 172 – 175.

[4] A. Jacobsson and P. Davidsson, "Towards a model of privacy and security for smart homes," in *IEEE World Forum on Internet of Things, WF-IoT 2015 - Proceedings*, 2015, pp. 727–732.

[5] H. Lin and N. W. Bergmann, "Iot privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, 2016.

[6] Y. Park, S. Daftari, P. Inamdar, S. Salavi, A. Savanand, and Y. Kim, "IoTGuard: Scalable and agile safeguards for Internet of Things," in *MILCOM 2016 - 2016 IEEE Military Communications Conference*, Nov 2016, pp. 61–66.

[7] J. Pacheco and S. Hariri, "IoT Security Framework for Smart Cyber Infrastructures," in *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W)*, Sep. 2016, pp. 242–247.

[8] L. Rafferty, F. Iqbal, S. Aleem, Z. Lu, S. C. Huang, and P. C. Hung, "Intelligent multi-agent collaboration model for smart home IoT security," in *Proceedings - 2018 IEEE International Congress on Internet of Things, ICIOT 2018 - Part of the 2018 IEEE World Congress on Services*, 2018, pp. 65–71.

[9] J. Habibi, D. Midi, A. Mudgerikar, and E. Bertino, "Heimdall: Mitigating the Internet of Insecure Things," *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 968–978, 2017.

[10] N. DeMarinis and R. Fonseca, "Toward Usable Network Traffic Policies for IoT Devices in Consumer Networks," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy - IoTS&P '17*, 2017, pp. 43–48.

[11] M. Serror, M. Henze, S. Hack, M. Schuba, and K. Wehrle, "Towards In-Network Security for Smart Homes," in *Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018*, 2018, pp. 1–8.

[12] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, 2017, pp. 618–623.

[13] S. Perez, J. A. Martinez, A. F. Skarmeta, M. Mateus, B. Almeida, and P. Malo, "ARMOUR: Large-scale experiments for IoT security & trust," in *2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016*, 2017, pp. 553–558.

[14] C. S. Kouzinopoulos, K. M. Giannoutakis, K. Votis, D. Tzovaras, A. Collen, N. A. Nijdam, D. Konstantas, G. Spathoulas, P. Pandey, and S. Katsikas, "Implementing a Forms of Consent Smart Contract on an IoT-based Blockchain to promote user trust," in *2018 Innovations in Intelligent Systems and Applications (INISTA)*. IEEE, jul 2018, pp. 1–6.

[15] G. Carrozzo, M. Pardi, P. Tedeschi, G. Piro, M. Dobski, K. Leszczyski, A. Carminati, and M. Di Fraia, "Interoperation of IoT Platforms in Confined Smart Spaces: The SymbIoTe Smart Space Architecture," in *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*. IEEE, oct 2018, pp. 38–45.

[16] R. Agarwal, D. G. Fernandez, T. Elsaleh, A. Gyrard, J. Lanza, L. Sanchez, N. Georgantas, and V. Issarny, "Unified IoT ontology to enable interoperability and federation of testbeds," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. IEEE, dec 2016, pp. 70–75.

[17] J. Hernandez-Serrano, J. L. Munoz, O. Leon, L. Mikkelsen, H.-P. Schwefel, and A. Broring, "Privacy risk analysis in the IoT domain," in *2018 Global Internet of Things Summit (GIoTS)*. IEEE, jun 2018, pp. 1–6.

[18] C. Pham and M. Diop, "Demo: WAZIUP, an Open and Versatile Long-range IoT Framework to Fully Take Advantage of the Cloudification of the IoT," in *2018 3rd Cloudification of the Internet of Things (CIoT)*. IEEE, jul 2018, pp. 1–2.

[19] A. F. Skarmeta, J. Santa, M. J. Beliatis, M. Presser, and E. al., "IoTCrawler: Browsing the Internet of Things," *GIoT 2018 proceedings , IEEE Communications Society*, 2018.

[20] 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 *Security in Computer and Information Sciences*, E. Gelenbe, P. Campegiani, T. Czachórski, S. K. Katsikas, I. Komnios, L. Romano, and D. Tzovaras, Eds. Cham: Springer International Publishing, 2018, pp. 68–78.

[21] N. Gerber, B. Reinheimer, and M. Volkamer, "Home Sweet Home ? Investigating Users ' Awareness of Smart Home Privacy Threats," in *USENIX Symposium on Usable Privacy and Security (SOUPS) 2018*, 2018, pp. 0–3.