A Segregated Architecture for a Trust-based Network of Internet of Things

Conference Paper · January 2019

DOI: 10.1109/CCNC.2019.8651703

4 authors, including:

Davide Ferraris
University of Malaga
14 PUBLICATIONS **110** CITATIONS
SEE PROFILE

Carmen Fernandez Gago
University of Malaga
63 PUBLICATIONS **1,101** CITATIONS
SEE PROFILE

Javier Lopez
University of Malaga
400 PUBLICATIONS **10,569** CITATIONS
SEE PROFILE

A Segregated Architecture for a Trust-based Network of Internet of Things

Davide Ferraris[a], Carmen Fernandez Gago[a], Joshua Daniel[b], and Javier Lopez[a]

[a]Network, Information and Computer Security Lab , University of Malaga, 29071 Malaga, Spain {ferraris,mcgago,jlm}@lcc.uma.es , [b]British Telecom,Orion Floor 5 pp10, Adastral Park, Martlesham Heath, IP5 3RE, Ipswich, England {joshua.daniel}@bt.com ,

Abstract

With the ever-increasing number of smart home devices, the issues related to these environments are also growing. With an ever-growing attack surface, there is no standard way to protect homes and their inhabitants from new threats. The inhabitants are rarely aware of the increased security threats that they are exposed to and how to manage them. To tackle this problem, we propose a solution based on segmented architectures similar to the ones used in industrial systems. In this approach, the smart home is segmented into various levels, which can broadly be categorised into an inner level and external level. The external level is protected by a firewall that checks the communication from/to the Internet to/from the external devices. The internal level is protected by an additional firewall that filters the information and the communications between the external and the internal devices. This segmentation guarantees a trusted environment among the entities of the internal network. In this paper, we propose an adaptive trust model that checks the behaviour of the entities and in case the entities violate trust rules they can be put in quarantine or banned from the network.

1 Introduction

With the Internet of Things (IoT) enabling smart homes and smart cities, it is now possible to connect everyday entities that are controlled remotely (i.e. by a smart-phone). To ease this deployment, the manufacturers of such devices allow them to be controlled from a cloud-based command centre, enabling the owners to control them even when they are away from their home network. The functionality has also been extended to enable connected devices to synchronise and take instructions from other connected devices [1] and services [2]. Manufacturers of smart things can use different communica-

[1]http://www2.meethue.com/en-gb/

[2]https://developer.amazon.com/alexa

tion technologies, such as Zigbee or Zwave [20]. These technologies tend to use either proprietary or one of the many standard protocols [9], and they cannot communicate directly with each other [10]. Another issue is the use of different versions of the same technology, in the case of Bluetooth Low Energy (BLE), reverse compatibility with the previous version is not always guaranteed [4]. The solution for this has traditionally been for the manufacturers to create their own IoT hub that corresponds to the devices that they manufacture or intend to support. Considering these aspects, the challenges in building a set of smart objects cooperating with each other grows harder. Ferraris et al. [8] propose a framework to guarantee trust in the development of a smart object in the whole system life cycle. In addition, this framework guarantees a careful planning from the point of view of the developer. From a customer's point of view, without planning, it is possible that a household may end up with devices from multiple manufacturers, creating heterogeneity. In addition, with some IoT hubs corresponding to their respective IoT devices, the complexity of the system grows. Other significant challenges in IoT are those concerning security, trust and privacy issues. These threats may be internal or external from the Internet, targeting the inner and more vulnerable parts of the system. Concerning the security aspect, without a secure architecture, IoT can suffer from malfunctions or attacks. To avoid these problems, IoT needs a holistic approach that secures all the elements, from the physical to the application layer [22]. These security issues are vital to preserve privacy and build a trusted community of devices. Privacy is considered very important by the users [21] and trust is necessary to allow smart things to collaborate with each other in a dynamic and heterogeneous environment like the IoT without compromising privacy [7]. According to Moyano et al. [17], we consider trust as "the personal, unique and temporal expectation that a trustor places on a trustee regarding the outcome of an interaction between them".

In this paper, we propose an architecture for a smart home environment based on the industrial architectures, where the networks are separated in different network levels with different network security controls such as firewalls used to segregate, detect and protect systems (such as SCADA architectures [3]). We have developed an adaptive trust-based access control model to guarantee that the trust relationships are matched either in the inner and outer architecture.

The structure of the paper is as follows. In Section 2 we describe the related work. Then the motivation is described in Section 3. In Section 4 we explain our proposed architecture and in Section 5 our adaptive trust model. A use case scenario is described in Section 6. Finally, in Section 7 we conclude and discuss future work.

2 Related Work

The IoT environment is a worldwide network of interconnected entities locatable, usable and readable through the Internet [22]. It is expected that these objects will have to interact with each other often in a condition of uncertainty. Mechanisms to resolve this lack of information are needed and trust can help address this need [28]. Related to trust, reputation is more objective and it can be a parameter for trust decision [13]. The heterogeneity and dynamicity of IoT have raised questions and led to some possible architectures being put forward. Roman et al. [23] identified four main architectures,

each of them have their strengths and weaknesses. These architectures are centralised, collaborative IoT, connected Intranets of Things and distributed. In a centralised approach, a gateway such as a smart home hub manages a group of devices (mostly passive), with the primary control gateway and logic being in the hub itself. The major risk with this architecture is that, when the smart hub is compromised or is not working properly, the whole architecture fails. As Singh [25] states many such attacks can be performed against the home IoT hub. A message modification attack or a replay attack are examples of two such attacks that can have a major impact on a smart home. With a replayed signal, the attacker can repeat a command indefinitely. For example, an attacker can continuously open and close a window. With a message modification attack, the attacker can change a parameter set by the user or by the system. In the event of a fire, for example, the threshold can be modified and resulting in the alarm being switched on too late or remaining switched off. A problem like this is a huge menace to not only everyone living in that home but also their neighbours. In a distributed approach, all the nodes have determinant rules [23]. This model expects an input which, when it satisfies a condition, the device executes an action locally and independently. A lot more peer-to-peer communication is expected in a network like this [6]. There are variations to this type of architecture, like the one proposed by Parra [19] where some peers are in the middle of the communication, so if they fail the trust assurance, the architecture will also fail. Another big problem with this architecture is that the peers are not protected as well as the smart hub is, and in this case, it can be easier to compromise them. According to Roman et al. [23], the vulnerability of a distributed architecture lies in the fact that the nodes are not protected as well as the central unit. In fact, if an attacker knows how to target a particular node he/she can, for example, leak private information. These architectures are used as the basis to create frameworks used in the IoT field [7], [26] and some of these structures are applied to many fields, such as smart cities, smart grids or smart homes [19]. Some of these architectures are used in industrial systems [27] where the networks are divided into two or more parts, using firewalls to segregate the more vulnerable networks and protect them from direct access to the Internet. This approach enhances security and privacy. They are core characteristics that have to be guaranteed to protect users and things from attacks or theft of information [21]. To solve IoT privacy problems an increasingly important approach is Privacy-by-Design (PbD) as noted in the US Federal Trade Commission (FTC) report on consumer privacy [5].

In IoT, the challenges with respect to privacy principally concern the users and how they have stored their private data in the architecture. Depending on the applications used, privacy issues are very different from each other [21]. Privacy and trust are strictly related, Ferraris et al. [8] developed a framework that guarantees trust in the development of an IoT entity. In this framework, the authors state that trust is strongly related to privacy and other security properties and in the requirement phase it is possible to link these types of requirements to each other to guarantee traceability. Here we focus more on the *need* phase and in its relation to the *utilization* phase. We also take into consideration transversal activities such as threat and risk analysis. In fact, another challenge in IoT is to protect the environments from different known and unknown attacks. Hu et al. [12] focus on IoT environments related to attacks. They state that it is now more important than ever that the proposed architectures have to consider these

attacks and propose solutions to this problem. In our work, we propose an architecture that can prevent such attacks as is demonstrated in the following sections.

3 Motivation

In an industrial system, the idea is to define and create fixed boundaries between networks to make the system less vulnerable and to reduce the possibility of attacks carried out by malicious external agents [18]. In a smart home environment these boundaries are not anticipated by the end consumers and so the typical architectures are either centralised or distributed [19]. Hard boundaries are not defined by the various internal networks or with the external networks. A way ahead towards solving this architectural dilemma is to apply the industrial systems architecture to a smart home environment. This would enable a clear network segmentation and security controls to be injected, such as firewalls at interfaces and a SCADA-like system to protect the home devices that are directly connected to the Internet. The most common risks of these smart home architectures are cyber risks (i.e ransomware, malware) and physical risks (i.e. fire, theft). The causes of these risks can be zero-day attacks with attackers using Phishing or Spear-phishing to target the end consumer. These types of attacks, which intrude on networks are currently on the rise with the increased impact [14] of payloads such as Wannacry [16]. The manipulation of these Internet-connected critical systems at home can, however, have grave consequences up to and including death (attack on health monitoring) [11]. One required practical consideration lies in the network segmentation between the smart objects, smart hubs, the Internet and the network used by the consumer for critical functions such as banking. This type of connection represents a significant risk and protection is needed to divide the internal network into parts to protect the inner level [27]. Network subnets, intrusion detection and prevention systems, firewalls and other such security controls are also needed to protect and monitor the network, and allow only specified ports to perform the actions needed.

In this paper, we propose an architecture that guarantees a segregated trusted environment where the sharing of information/logic with multiple hubs could be stored and processed in a trusted way. This is a new way of trying to solve the principal problems of security, trust and privacy issues related to the classic IoT architectures [24].

4 Architecture

The main objective of this paper is to protect IoT entities by means of a segregated trust architecture. By *segregated trust*, we mean that the IoT entities inside the internal network can trust the entities which are allowed to interact with. This segregation is guaranteed by the internal architecture, that is designed to prevent external and internal threats. This architecture is similar to Obregon's work [18]. Moving further from this work, we have developed the model shown in Figure 1, which is divided into six levels plus a Demilitarized Zone (DMZ). We can see that the levels are grouped mainly into two zones: the blue zone is related to the internal network and the green zone is related to the external network.

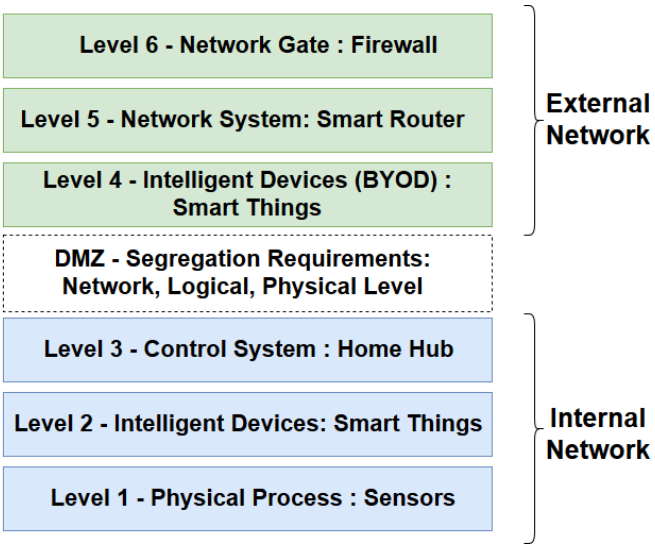

Figure 1: Hierarchy Levels of the Segregated Architecture

Starting from the bottom, the first level concerns the physical processes. In a smart home environment, this level comprises the sensors, which collect raw data from the field and send it to the level above, where the intelligent devices or smart things are. These devices have to process and analyse the raw data originated in the sensors and, when necessary, act. For example, a smart smoke sensor can detect smoke and, if higher than a threshold, the sensor triggers the smoke alarm. The third level is for the control system, where there is a central unit (like a home hub) that has to monitor the other smart objects and be the bridge between them and the higher levels and the Internet. The first segregation takes place at this level. This level is the highest of the lower zone. The home hub is connected to the Internet through a DMZ. This zone prevents the lower level from being compromised by outside threats and a firewall monitors both inbound and outbound traffic. This DMZ must satisfy the segregation requirements for the network, logical and physical levels.

The firewall allows the traffic from the DMZ to the internal network. This configuration can protect the internal network from the external threats, preserving privacy by protecting the stored data inside the protected zone and guaranteeing trusted zones for information exchange and data when necessary. For instance, when a part of the home is physically compromised it is possible to transfer the data to another secure area.

Beyond the inner zone, there is a fourth level. In this level, we have all the entities classified under the Bring Your Own Device (BYOD) paradigm [15]. These devices are, for example, smart-phones or laptops that the owner can carry with him or her in external networks. For this reason, they have to be segregated from the internal network but they can communicate with it through the DMZ.

Then we have level five and it is related to the Network System, that communicates with the Internet through the upper level. In this level, we have the smart router

that could block some communication or forward them to the layer below (in the case coming from the Internet) or to the layer above (in the case coming from the level 4). Finally, there is the sixth level where we can find the firewall, protecting the external layer from the Internet threats. Both the firewall and the smart router of layer five can be implemented to let pass or block communication in both directions. This implementation is strongly dependent on the context and the environment.

5 Adaptive Trust Model

The adaptive trust model works in different situations. According to Ferraris et al. [8], during the *utilization* phase, an entity can join, stay or leave a network. For the join and stay actions, a trust estimation must be computed. The trust level computed will be fundamental to allow the new entity to join or stay in the network. The smart hub is the device that will compute the values and it has the rights to access to the Databases (DB). It could store information related to the actions performed by the entities for forensics purpose (but this is out of the scope of the paper). We assume the Smart Hub cannot be compromised because it has a Root of Trust[3].

5.1 Trust Estimation

In our model, trust estimation is central and is done with different criteria. It is done to decide whether a new entity can join the network and to decide whether an entity can stay in the internal or the external part of the network. The criteria taken into consideration are: reputation DB, threats DB, risk calculation and context

Threats DB. The known vulnerabilities of the smart devices are collected in this DB. In the case there are no known attacks related to the device its trust value is higher. In the case of known attacks, the greater the danger the lower the trust value.

Reputation DB. The reputation DB is used to store the devices old reputation values. For example, in the case a new device tries to join the network again, but in the past, it has been banned, the smart hub will deny its access. We assume that a ban is done only after a serious security issue, for this reason a banned device cannot join the network again. Furthermore, avoiding a second opportunity we prevent Whitewashing Attacks (WA). We assume that both the DBs are secured and encrypted. In addition, they are stored in the internal network where we assume that a malicious entity cannot access because of the implementation of the join, stay and leave phases (as we will show later).

Context. The context depends on the environment, on the purpose and on the services that the device provides alone or with the other smart devices. The more important a device is the higher the necessary level of trust.

Risk Calculation. Risk can be provoked by attacks, system failures, adding or changing devices. In the state of the art there are a lot of techniques related to risk estimation [2]. We consider three parameters to calculate the risk. The first parameter is the likelihood (L) of an event; this is the probability that a situation that harms the

[3]https://www.synopsys.com/designware-ip/technical-bulletin/secure-iot-system.html

system can occur (either an attack or a malfunction). The second parameter is the severity (S) of the effect that a malfunction or an attack can have on the system, the more critical the component involved is, the more critical the threat is for the whole system. Finally, there is a parameter that is usually not taken into consideration but one which we think is crucial to calculate the risk: the detectability (D). The detectability is the possibility of a malfunction or an infected device can be detected. If an attack is occurring and we cannot detect it, the system will fail or will be manipulated. We have considered either detectability and likelihood separately because the likelihood is related only to the probability that an event occurs even if we detect it or not. As shown in Tables 1, 2 and 3 the risk values have different meanings according to their typology.

Value	**Meaning**
Low (1)	The event is unlikely to happen
Medium (3)	The event can quite probably happen
High (9)	The event is almost certain to happen

Table 1: Likelihood

Value	**Meaning**
Low (1)	The network is not damaged
Medium (3)	The network can be partially damaged
High (9)	The network can become completely useless

Table 2: Severity

Value	**Meaning**
Low (1)	The problem is easily detectable
Medium (3)	The problem cannot be entirely detected
High (9)	It is not possible to detect the problem

Table 3: Detectability

We have considered only three values for each parameter to keep the calculation simpler. The values are combined between them using a multiplication. This is a common approach used in many risk methods [2]. If the result is lower than 9, we have a low risk. If the result is between 9 and 27, we have a medium risk. If the value is higher than 27, we have a high risk. The overall risk value has been chosen according to the following criteria:

1. It is the same level of the all parameters if they belong to the same level (i.e low if L, S and D are low).
2. Low, if there is a medium parameter only and the other two parameters are low.
3. High, if there are two or more parameters set to high or two parameters set to medium and one set to high.

4. Medium, otherwise.

In the case that the calculated risk is high the device cannot be added to the network or it must be banned. In the case the risk value is low or medium the device can join or stay in the network depending on other criteria.

5.2 Join, Stay and Leave

Join. When the smart homeowner allows a new entity to connect to the network, it contacts the centralised monitor (i.e. a smart hub) and it asks to join the network and the other entities. The smart hub checks the entity's rights (i.e. owner, password, risk calculation), instructs the entity how to join the other entities and gives the proper key for exchanging messages. The rule for joining an entity depends on the trust estimation. The network decision is based on whether or not the new entity is a BYOD. If it is a BYOD the new entity can join the external network only.

The join procedure is similar to the SDP[4] technique. When the new device joins the network, it sends a broadcast message to communicate with the smart hub and asks permission to join the network (action 1). The smart hub checks the permissions of the new device (i.e. password, owner key, rights) and makes the join decision. If the access to the network is denied, the smart hub signals the new device that it is not allowed to join the network. If access is granted, the smart hub signals the new device that it can join the network and with which other devices it is allowed to interact (action 2). Afterwards, the smart hub informs the devices already present in the network that they can interact with the new device (action 3). In both actions 2 and 3, the smart hub gives a symmetric key to the allowed device and to the devices already present in the network to enable the communication between them. The devices must acknowledge the smart hub and, from that moment, the interaction between the devices can start.

Stay. When an entity stays in a network, it must be monitored, according to external and internal factors. During the monitoring, the smart hub checks whether the entities are behaving normally. If something not expected occurs (depending on the context, risk calculation and entity involved) a trust estimation is needed to decide whether the entity is behaving maliciously or not. During trust estimation, the context and the risk calculation of the action are all taken into consideration, together with the data of the reputation DB where the history of the entities is stored and a threat DB updated with the latest known attacks. The smart hub can allow the entity to stay or it can decide to ban or put the entity in quarantine. When an entity is put on quarantine, it remains in the network without be able to communicate with the other entities. The entity can only receive communications from the smart hub. The quarantine will continue until new information are available (i.e. known attacks or vulnerabilities related to the entity). In the case an entity is banned or put in quarantine, the smart hub must communicate the decision to the entities having a connection with the banned one. The model for stay decision is similar to the work of Atlam et al. [1]. They have proposed a risk-based access control model for IoT to calculate the risk associated with the access request to a particular resource. We extend this model using risk calculation as a parameter for trust estimation.

[4]https://cloudsecurityalliance.org/download/software-defined-perimeter/

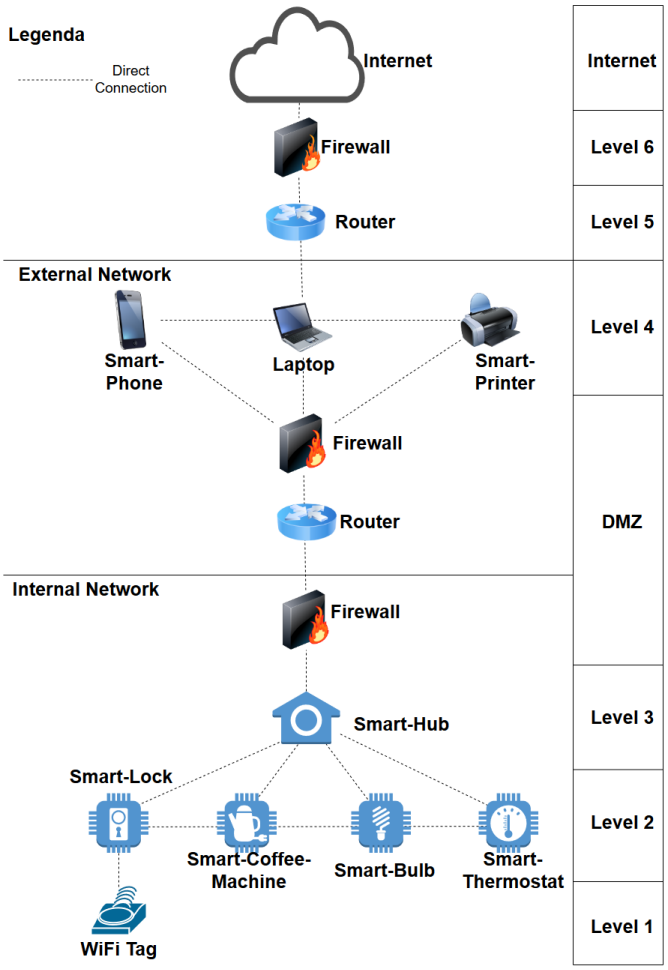

Figure 2: Smart Home: Segregated Trust Architecture

Leave. When an entity leaves the internal or external network, it must announce its intention to leave to the smart hub and to the related entities. For an enhanced security, the smart hub must communicate the change to its related entities.

6 Smart Home Scenario

The smart home architecture is shown in Figure 2. On the right side of the figure, there are the levels related to Figure 1. As it can be seen, it is composed of two networks: one internal and another external. The internal network comprises a smart-lock, a smart-coffee-machine, a smart-bulb and a smart-thermostat. These entities are only allowed to communicate with another entity according to its purpose. The link for

the communication is represented by the dotted lines in Figure 2. The smart-lock has no connections at all with the smart-coffee-machine because there is no reason for them to communicate directly with each other. On the contrary, the smart-bulb can receive information from the smart-lock. In fact, when the door is opening, the smart-lock sends a signal to the smart-bulb to switch the lights on (in case it is night). All these devices communicate directly with the smart hub, which monitors their activities, allowing them to communicate directly only for determined purposes. The internal network is separated from the external network containing a smart-phone, a laptop and a smart-printer. These three objects belong to the BYOD paradigm. They cannot join the internal network because they can join other networks and be compromised. Let us assume that the homeowner needs a new smart-lock and smart-phone.

6.1 Smart-Lock

When the smart-lock joins the network, a broadcast message is sent to all the network devices. The smart devices do not recognize the ID of the new device and they are not allowed to answer. The smart hub recognises the object as belonging to the smart homeowner, in fact, we assume that before joining a network the smart homeowner validates the devices. After this message, the smart hub starts the trust estimation. The smart hub checks the reputation DB to see whether the smart-lock has previously been part of the network, although we assume that the device is completely new. The threat DB is checked to find known vulnerabilities with respect to smart-lock model and it finds a known vulnerability. The risk calculation takes into consideration the parameters L, S and D. For L, the smart hub decides to assign a *medium* value because the known vulnerability could be exploited. Regarding the parameter S, the smart hub decides to give a *high* value because in the case of malfunctions or attacks the smart-lock completely loses its functionalities. Finally, the D value is *low* because the vendor has designed the smart-lock to provide feedback on its functionality. In summary, we have a high value for S (9), a medium value for L (3) and a low value for D (1). According to these values, the overall risk estimation is medium (27). Finally, the smart hub checks the context of the device. The context is related to the lock's cooperation with the smart-bulb so in the case it displays malicious behaviour or suffers malfunction on the part of the lock, the smart-bulb can also be affected. In addition, the smart-lock is of critical importance to the smart home environment because, in the case of malicious behaviour, it can allow strangers to enter the house or it can keep the homeowner out. The trust estimation take into consideration the following parameters: the risk value is medium, the cooperation with the smart-bulb and the (Context) and the known vulnerability found in the threat DB. After the trust estimation, the smart hub decides to not allow the smart-lock to join the network. This denies action protects the internal entities to be threatened by the new device and keep the trust level in the internal network.

6.2 Smart-Phone

The second device bought by the homeowner is a smart-phone. The device has never joined the network before, so the reputation DB has no data for it. The threat DB

has no known attacks related to the smart-phone model and version. The risk value is calculated as low (3) because the L and D parameters are considered low (1) and the S parameter is considered medium (3) because in the case of malfunction or malicious activity the network can be partially damaged. The context is related to all the devices belonging to the external network and the smart hub of the internal network because. Finally, it belongs to the BYOD paradigm so in case of acceptance it will be allowed to only join the external network. After all these parameters are considered, the smart-phone is allowed to join the external network and its behaviour is monitored to anticipate possible threats. Let us assume that after a few weeks, the smart-phone has been manipulated by a malicious entity and tries to communicate with the other smart entities to gain control of them. The architecture allows the smart-phone to pass through the smart hub to communicate with the smart entities in the internal network. We assume that the smart-phone repeatedly sends a command to the smart-bulb to switch the lights on and off every five seconds. The smart hub catches this abnormal behaviour and using the adaptive model decides to block the communications belonging to the smart-phone and set it in quarantine. The smart hub, checking the threat DB, recognises that a replay attack has been carried out by the smart-phone. The reputation DB is set with a low value and the owner of the smart home is notified of the event.

To conclude, we have shown two scenarios related to a smart home environment. The proposed architecture can increase the security level of the smart homes and can notify to the owners if a smart entity has been compromised or if a smart entity cannot join the network for security reason.

7 Conclusions and Future Work

We have proposed a segregated trust architecture and an adaptive trust-based access control model. The architecture comprises two layers. The internal layer contains static entities and it has a higher protection. The external layer contains entities belonging to the BYOD paradigm. This layer is protected too and can communicate with the internal layer through a central smart hub. In accordance with this architecture, we have proposed a model that monitor the entities behaviour and the steps that an entity has to take when it joins and leaves a network. Finally, there is a behavioural control to decide whether an entity can stay in the internal or external network.

For future work, we will validate this architecture and we will test this environment in a real smart home, we will expand the use cases with more entities and we will also insert other guest devices. In addition, we will expand the risk values to have more risk levels. We will also test the architecture against known attacks. Furthermore, we will focus more on the usability feature considering the possibility that the smart hub denies access to a non-malicious devices. In this case, we will design the system to inform the owner about this event.

Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No. 675320. This work reflects only the author's view and the Research Executive Agency is not responsible for any use that may be made of the information it contains.

References

[1] Hany F Atlam, Ahmed Alenezi, Robert J Walters, Gary B Wills, and Joshua Daniel. Developing an adaptive risk-based access control model for the internet of things. 2017.

[2] Armaghan Behnia, Rafhana Abd Rashid, and Junaid Ahsenali Chaudhry. A survey of information security risk analysis methods. *SmartCR*, 2(1):79–94, 2012.

[3] Stuart A Boyer. *SCADA: supervisory control and data acquisition*. International Society of Automation, 2009.

[4] Walter Bronzi, Raphael Frank, German Castignani, and Thomas Engel. Bluetooth low energy performance and robustness analysis for inter-vehicular communications. *Ad Hoc Networks*, 37:76–86, 2016.

[5] US Federal Trade Commission et al. Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers. *FTC Report*, 2012.

[6] Angelika Dohr, Robert Modre-Opsrian, Mario Drobics, Dieter Hayn, and Günter Schreier. The internet of things for ambient assisted living. In *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on*, pages 804–809. Ieee, 2010.

[7] Carmen Fernandez-Gago, Francisco Moyano, and Javier Lopez. Modelling trust dynamics in the internet of things. *Information Sciences*, 396:72–82, 2017.

[8] Davide Ferraris, Carmen Fernandez-Gago, and Javier Lopez. A trust by design framework for the internet of things. In *NTMS'2018 - Security Track (NTMS 2018 Security Track)*, Paris, France, February 2018.

[9] Vangelis Gazis. A survey of standards for machine-to-machine and the internet of things. *IEEE Communications Surveys & Tutorials*, 19(1):482–511, 2017.

[10] Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu. A zigbee-based home automation system. *IEEE Transactions on consumer Electronics*, 55(2), 2009.

[11] Xiali Hei, Xiaojiang Du, Shan Lin, and Insup Lee. Pipac: patient infusion pattern based access control scheme for wireless insulin pump system. In *INFOCOM, 2013 Proceedings IEEE*, pages 3030–3038. IEEE, 2013.

[12] Fei Hu. *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations*. CRC Press, 2016.

[13] Audun Jøsang, Roslan Ismail, and Colin Boyd. A survey of trust and reputation systems for online service provision. *Decision support systems*, 43(2):618–644, 2007.

[14] Guy Martin, James Kinross, and Chris Hankin. Effective cybersecurity is fundamental to patient safety, 2017.

[15] Keith W Miller, Jeffrey Voas, and George F Hurlburt. Byod: Security and privacy considerations. *It Professional*, 14(5):53–55, 2012.

[16] Savita Mohurle and Manisha Patil. A brief study of wannacry threat: Ransomware attack 2017. *International Journal*, 8(5), 2017.

[17] Francisco Moyano, Carmen Fernandez-Gago, and Javier Lopez. A conceptual framework for trust models. In *9th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2012*, volume 7449 of Lectures Notes in Computer Science, pages 93–104. Springer Verlag, Sep 2012.

[18] L Obregon. Secure architecture for industrial control systems. *SANS Institute InfoSec Reading Room*, 2015.

[19] Jorge Parra, M Anwar Hossain, Aitor Uribarren, Eduardo Jacob, and Abdulmotaleb El Saddik. Flexible smart home architecture using device profile for web services: A peer-to-peer approach. *International Journal of Smart Home*, 3(2):39–56, 2009.

[20] Zhongmin Pei, Zhidong Deng, Bo Yang, and Xiaoliang Cheng. Application-oriented wireless sensor network communication protocols and hardware platforms: A survey. In *Industrial Technology, 2008. ICIT 2008. IEEE International Conference on*, pages 1–6. IEEE, 2008.

[21] Pawani Porambage, Mika Ylianttila, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, and Athanasios V Vasilakos. The quest for privacy in the internet of things. *IEEE Cloud Computing*, 3(2):36–45, 2016.

[22] Rodrigo Roman, Pablo Najera, and Javier Lopez. Securing the internet of things. *Computer*, 44(9):51–58, 2011.

[23] Rodrigo Roman, Jianying Zhou, and Javier Lopez. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10):2266–2279, 2013.

[24] Dhananjay Singh, Gaurav Tripathi, and Antonio J Jara. A survey of internet-of-things: Future vision, architecture, challenges and services. In *Internet of things (WF-IoT), 2014 IEEE world forum on*, pages 287–292. IEEE, 2014.

[25] Saurabh Singh, Pradip Kumar Sharma, and Jong Hyuk Park. Sh-secnet: An enhanced secure network architecture for the diagnosis of security threats in a smart home. *Sustainability*, 9(4):513, 2017.

[26] Biljana L Risteska Stojkoska and Kire V Trivodaliev. A review of internet of things for smart home: Challenges and solutions. *Journal of Cleaner Production*, 140:1454–1464, 2017.

[27] Keith Stouffer, Joe Falco, and Karen Scarfone. Guide to industrial control systems (ics) security. *NIST special publication*, 800(82):16–16, 2011.

[28] Zheng Yan, Peng Zhang, and Athanasios V Vasilakos. A survey on trust management for internet of things. *Journal of network and computer applications*, 42:120–134, 2014.