Security and Privacy Issues for an IoT based Smart Home

Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino
Gary Steri, and Gianmarco Baldini
European Commission, Joint Research Centre (JRC)
Cyber and Digital Citizens' Security Unit
Via Enrico Fermi 2749, 21027 Ispra, Italy
Email: {firstname.surname}@ec.europa.eu

***Abstract*—Internet of Things (IoT) can support numerous applications and services in various domains, such as smart cities and smart homes. IoT smart objects interact with other components *e.g.,* proxies, mobile devices, and data collectors, for management, data sharing and other activities in the context of the provided service. Though such components contribute to address various societal challenges and provide new advanced services for users, their limited processing capabilities make them vulnerable to well-known security and privacy threats. Until now various research works have studied security and privacy in IoT, validating this claim. However, to the best of our knowledge literature lacks research focusing on security and privacy flaws introduced in IoT through interactions among different devices supporting a smart home architecture. In particular, we set up the scene for a security and privacy threat analysis for a typical smart home architecture using off the shelf components. To do so, we employ a smart home IoT architecture that enables users to interact with it through various devices that support smart house management, and we analyze different scenarios to identify possible security and privacy issues for users.**

I. Introduction

The development of new type of sensors and actuators combined with the deployment of increasingly powerful and pervasive network connectivities is shaping the concept of the Internet of Things (IoT). Several factors are contributing to the evolution of the current Internet into IoT including the lower market price of IoT devices and the higher demand of customers for new services.

Manufactures are now able to provide mobile, wearable or embedded devices with more memory, processing power, and more diverse sensing technology. As a consequence, this increased capability of IoT devices also increases the amount of data available to services and their value to end users. However, even if IoT is capable of supporting new business models, increasing the efficiency of many applications, and enriching the life of citizens with new services, the risks are also significantly higher. The collection of even larger amount of data and merging of the cyber and physical world implies a higher number of privacy and safety issues than the cyber-only Internet.

More specifically our focus in this paper is on a *Smart Home* scenario. In this scenario, the potential for privacy breaches is limited if we consider the direct and explicit collection of data regarding the individuals living in the house. However, the activities of these individuals can be indirectly tracked through the observation of the cyber and physical activities of their connected domestic devices, assisted living systems, or smart meters. The protection of privacy in these complex scenarios where different entities and IoT technologies coexist and work together requires new approaches and solutions. Even if various Privacy Enabling Technologies (PET) have been proposed in literature, their market adoption is still relatively weak and many concrete threats still persist.

In this paper we set up the scene for a security and privacy threat analysis for a typical smart home architecture that relies on existing and readily available market IoT devices and platforms. In contrast to existing security and threat analysis of IoT scenarios, we target a real IoT smart home environment deployed in our testbed focusing on the interactions among the different IoT components. In this architecture, we identify points of interest that an adversary might manipulate either to gain access to unauthorized information or to cause a denial of service. Our contribution, in addition to a concrete threat analysis, is a practical feasibility evaluation of the identified vulnerabilities showing how exploits can be implemented in practice.

The rest of the paper is structured as follows. In Section II we overview a smart home's architecture and in Section III we analyse its threat model. In Section IV we study the realization of the threat model in a test-bed architecture, and analyze possible consequences to end-users in terms of security and privacy. In Section V we provide guidelines and protection measures for eliminating the threats presence, while in Section VI we overview the related work. Finally, in Section VII we conclude this paper and present some pointers for future work.

II. IoT based smart home architecture

Smart home can be defined as the symbiosis of different elements *i.e.,* sensors, connections, and applications that build a dynamic heterogeneous architecture with the aim of efficiently managing home devices, and providing to users advanced services.

Due to a still missing generic interoperability standard among IoT devices, in this architecture, without loss of generality, the IoT devices organised in islands are connected to a corresponding hub and are not directly accessed by other devices. Moreover, the majority of commercial sensors do not provide direct Internet connectivity; instead the intermediate

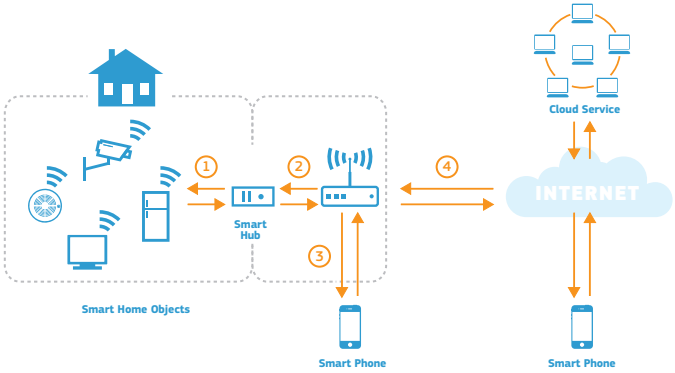

Fig. 1. Architecture of a Smart Home

hub is the component responsible of providing such connectivity.

The communication between the IoT devices and the hub is usually wireless, based on different protocols depending on the device's manufacturer. The most popular are:

- Zigbee[1];
- Z-wave[2].

The hub is then connected to the smart home's router either via an Ethernet or a Wi-Fi interface, depending on its capabilities in order to connect the IoT devices with the outside world.

Users can interact with IoT devices and manage their smart home through different platforms such as PCs, smart phones, and tablets. The interaction modalities are in general two:

1) directly interacting with them using the connectivity and services provided by the hub;
2) accessing Internet cloud services which interact with the IoT hub and the connected IoT devices.

These two scenarios are quite often present at the same time and mixed together to support local and remote interactions with IoT objects. In case of remote management all the information is forwarded to the smart hub through the cloud service, while if the user is acting from the same network where the smart hub is installed the traffic is routed directly to it and thus no Internet access is needed.

However, in order for users to enable IoT devices management, regardless of their location, they must first follow a procedure for correlating their devices with the corresponding hub. In most cases, for an off the shelf based solution to successfully complete this procedure user's physical action is involved, *e.g.,* pressing a button on the smart hub.

Furthermore, IoT manufacturers support protocols such as the Simple Service Discovery Protocol (SSDP) [1] to enable the transparent configuration of the smart home devices in a plug and play mode that requires minimum user interactions. In this case, the smart hub generates a presence announcement

[1]http://www.zigbee.org/
[2]http://www.z-wave.com/

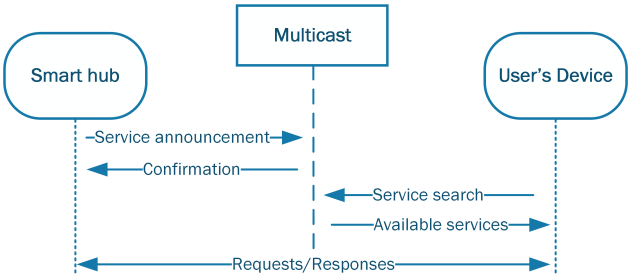

Fig. 2. Plug and play architecture for smart house

to the multicast channel, i.e. the default IoT devices' gateway. Any device that searches for available services sends to the multicast channel a discovery request and receives as a response the available requested services. Then the device can communicate directly with the newly discovered services. This procedure is illustrated in Figure 2.

So consider an example in which a user would like to control the smart home's lights status using his mobile phone, while he is outside the home. To do so, firstly he must have already successfully completed the correlation procedure, otherwise it is not possible to have remote access to the smart home's devices. Once setup, he can launch the mobile application and request the lights' status. This request reaches the cloud service which forwards it on behalf of the user to the hub that is responsible for controlling the lights, using a reverse communication channel kept open, through the house router, by the hub itself. As soon as the hub receives such a request, it sends the corresponding command, *i.e.,* status, to the lights in order to receive back their response, and forwards it to the user via the cloud service. All the interactions between the different components of a smart house are illustrated in Figure 1.

III. Smart Home Threat Model

The formulation of a smart home's cyber threat model should consider two types of adversaries; internal and external entities that can act maliciously on a passive or an active way depending on their goal. On one hand, the former category consists of malicious entities that are located close or inside the smart home's premises. On the other hand, external adversaries can interact only through an Internet connection. In both cases adversaries target either the smart home's infrastructure, or the information stored in the related cloud services. Note that in this work we do not consider adversaries having physical access to IoT components. This is because, cybersphere entities have only virtual access to the components of a provided service.

In this context, similar to any other IP based service, adversaries acting passively will try to eavesdrop available communications in order to acquire information that can either be used to monitor users' behaviour or can be accumulated and exploited in a later step of an active attack. Adversaries, to access this type of information, will try to capture the traffic in different points of the smart home architecture depending on their capabilities and goals. In this way, adversaries could impact users' confidentiality and privacy as they can collect information related to the smart home's status. For instance,

taking as example the architecture shown in Figure 1, if the adversary monitors the communication link (1) between the smart hub and the router in the smart house premises, he could identify which entities the smart hub communicates with, while if he monitors the communication link (4) he can deduce the users daily habits *e.g.,* when the lights turn on and off that might correspond to user's absence from home.

On the other side, an active adversary will interact actively with the IoT components, instead of only eavesdropping the underlying communication. He could identify the existence of components by generating the appropriate probes through different network devices. Moreover, the adversary could try to impersonate a legitimate user in order to gain access to the smart home devices. Then he could be able to control them, use them or even extract sensitive information from them. An active adversary could impact not only users privacy and the provided service's confidentiality but also affect data integrity, gain unauthorized access and ultimately disrupt the proper function of provided services.

Obviously in more complex scenarios an adversary could combine a passive and active attack. Consider, for instance the case where a smart socket provides electricity to a health device. If the adversary knows its unique identifiers by eavesdropping the communication traffic, he could cause a denial of service to the IoT that could have an immediate impact on the users safety. For that reason this type of information should be considered of high importance.

Besides the passive and active network layer threats, software exploitation is another aspect that an active adversary will capitalize in order to gain access to otherwise private domains. This is because, IoT relies on light weight versions of well known operating systems that adversaries look to exploit with very few resources. Moreover, most of the largely used IoT devices have a corresponding mobile application that acts as a controller. The mobile application's execution environment could be used as an attack vector for an adversary as he could be in position to exploit well-known software vulnerabilities of the underlying operating system.

Table I overviews the threats and the possible consequences that they can have to a smart home's infrastructure.

IV. IoT based Smart Home Cyber-Flaws

To study the feasibility of the generic threats reported in Section III we deployed a test-bed architecture similar to the one illustrated in Figure 1. This architecture is based on commercial products that provide connectivity to IoT sensors through a smart hub that is connected to a network and to the Internet via a traditional wireless router. Specifically, a computer (A) supported with a WiFi network card and Internet connection is configured as the access point to which the mobile device with the IoT management apps is connected to. In a second computer (B), which is connected to computer's A WiFi for having Internet, the IoT device or Hub (depending on the device type) is attached. This way, computer A monitors the traffic shown in point 3 and 4 of Figure 1, while computer B monitors the traffic of point 2. By running wireshark on both computers we are able to capture all packets passing through the specific points.

TABLE I. IoT Smart home threats overview

Type	Threat	Impact	Target
Passive	Eavesdropping	Confidentiality	User-IoT
Passive	Eavesdropping	Privacy	User
Active	DoS	Availability	User-IoT
Active	Impersonation	Integrity	User
Active	Impersonation	Availability	User-IoT
Active	Impersonation	Unauthorized access	User
Passive	Software exploitation	Confidentiality	User-IoT
Passive	Software exploitation	Privacy	User
Active	Software exploitation	Integrity	User
Active	Software exploitation	Availability	IoT

As our goal is to illustrate the security and privacy issues of IoT in general, and not to criticize a specific product, we do not provide any related information for it. Note that, as we are interested in studying the interaction between the different components, we assume that a powerful adversary [2] can get access to the underlying communication *e.g.,* by exploiting a specific device or protocol vulnerability, using default or common WiFi and router passwords, cracking insecure passwords, social engineering, *etc.*, however, such an analysis is out of scope of this work.

In the following subsections we discuss the implementation of the threats described in Section III considering information that we gather from our test-bed architecture as well as other related research reports.

A. *Eavesdropping*

An adversary might use different tools and techniques for capturing the traffic among the different components of an IoT based smart home infrastructure, considering its heterogeneous architecture. These techniques are highly related with the attacker's location and capabilities.

If the attacker manages to connect to smart home network components, *e.g.,* adsl router, he is able to capture all the traffic between the smart hub and the local or the remote users; that corresponds to reference points 2, 3 and 4 of Figure 1. In that case the adversary relies on well known tools such as tcpdump[3], wireshark[4], *etc.*, to gain access to the data. In case the communication is wireless, the adversary might use specific hardware equipment, for instance the WiFi Pineapple[5], that can spoof access points and intercept the underlying communication; this corresponds to reference points 1, 2, 4 of Figure 1.

So taking into consideration an adversary that intercepts the traffic among the reference points 1,2 and 3, he can identify:

1) whether or not the smart hub communicates with a cloud supported service *e.g.,* (cloud.iot.com:80)
2) the user device's type (*e.g.,* Linux, Android 7.1.1; Nexus 5X Build/NMF26F)
3) unique identifiers for user's access to the smart hub services
4) the device's status through traffic analysis
5) the smart hub's operating system (*e.g.,* unix like OS)
6) methods that can be used to send commands to the smart hub (*e.g.,* POST, GET, DELETE, *etc.*)

[3]http://www.tcpdump.org/
[4]https://www.wireshark.org/
[5]https://wifipineapple.com/

```
NOTIFY * HTTP/1.1
HOST: 239.255.255.250:1900
CACHE-CONTROL: max-age=100
LOCATION: http://192.168.1.24:80/description.xml
SERVER: Ubuntu UPnP/1.0
NTS: ssdp:alive
BridgeId: 40285567791489150
```

Listing 1. An SSDP NOTIFY message example for service announcement

Listing 1 illustrates the example of an eavesdropped message during a smart hub service announcement in the local network. In this case the adversary can deduce the operating system that the smart hub runs, its IP address, and its unique ID. In this point it should be mentioned that this information might be slightly changed depending on the IoT manufacturer.

B. Impersonation

An adversary could try to impersonate and act on behalf of a legitimate user. To do so, he requires either access to users' credentials or to any other information that provide access to the IoT resources. The former case is used in IoT architectures requiring access to the IoT devices remotely, while the latter is normally used to access the IoT resources from the local network (an example of key information needed in this case is for instance the unique identifier that the smart hub generates during device registration for enabling local access). Note that the smart hub often recognizes the location of the user based on his IP address. So if the adversary captures such a message, he can impersonate the user and can consequently interact with the smart hub on behalf of the user. This can be achieved by simply crafting the appropriate request towards the smart hub's resources with the appropriate parameters, *e.g.,*: `http://ip-address/api/unique-id/rsrc`

Recall that the adversary can intercept the unique identifier during an eavesdropping attack. In this category we also classify replay attacks as the adversary reuses previous requests either towards the hub or the cloud based service so that the user does not have the proper information about the status of his devices. Though this type of attack assumes that the adversary acts on the same network that the smart hub belongs to, it introduces a vulnerability in the smart home architecture in case that the adversary can reach the smart home router from outside world.

C. DoS

Similarly, to other IP based services, the adversary using different techniques might try to cause a Denial of Service (DoS) either to the hub or to the sensors themselves. As the adversary knows the smart hub's IP through eavesdropping, he can easily launch a single DoS or a Distributed DoS (DDoS) attack against it by simply sending numerous requests to it. Note that as IoT devices rely on low capabilities processing hardware they are susceptible to low rate DoS [3] as well.

Alternatively, the adversary might try to craft specific messages *e.g.,* malformed messages, so that the provided service cannot process them properly and cause either a DoS or provide unauthorized access.

DoS can also take place directly at the IoT devices, without passing through the smart hub. An adversary having the appropriate hardware that enables him to use the IoT devices' protocols can send directly messages to them and attempt to interfere with their proper functioning.

Finally, a DoS attack can also take place at the router or the cloud service. This may be a general attack, not linked to IoT, but the consequences for the end user would be the same. Without a working router or a could service, he will not be able to access his smart home's IoT devices through the Internet.

D. Software exploitation

Malicious software (malware) can affect the IoT services and devices. As IoT devices run autonomously light weight versions of well known operating systems adversaries will search for software vulnerabilities and exploit them to gain access to otherwise private information.

However, currently IoT is becoming an attack target for executing DoS in order to increase the amplification factor of the generated traffic to break down a target. For instance, IoT devices have been exploited for launching a DoS attack [4] against DNS servers in order to paralyze Internet access. In such cases the adversaries exploit the fact that these devices are running over the Internet with default configurations, *e.g.,* default passwords, while most of these devices are not patched in most of the cases against security flaws.

The malware can reach the IoT devices through different channels:

1) Device Acquisition: When the device is bought by an end user there is a risk of buying malware infected devices. For instance, an adversary could purchase many new devices, infect them, and sell them to users through online auction sites (*e.g.,* eBay[6]).

2) Firmware Upgrade and Trusted Boot: Orthogonal to device infection during acquisition, adversaries might be able to upgrade IoT firmware with a malicious acting version. For instance, this was a channel that adversaries exploited in the case of Mirai malware [5].

3) Apps and services: Users control their IoT devices through corresponding applications and online services. Lately, the most common way to manage one's devices is to use a mobile application on the user's mobile device. Almost all manufacturers provide such applications that can be downloaded directly from the mobile operating system's application market. Since these applications are executed on the user's personal device, they can be infected by malware that is already present on the device, or exploited directly by an adversary that takes advantage of either the mobile application's or the operating system's vulnerabilities.

Moreover, several IoT manufacturers assume that they can delegate security on the smart home's underlying architecture, such as the router's firewall. However, this assumption should not be taken for granted. As Sivaraman *et al.* demonstrate with their work [6], the security measures deployed at one's

[6] http://www.ebay.com/

smart home could easily be bypassed with a malware mobile application.

Similarly to mobile applications, online services that interact directly with the smart hub could pose a weak point in the IoT architecture chain. If one manages to access them through standard web services attack methods, he could then easily manipulate all connected IoT devices.

V. Discussion

Considering the above mentioned discussion in current smart home architectures, adversaries can gain access to underlying infrastructure and exploit it. As a result, smart homes should deal with security "flaws" in the same manner other IP based services with advanced resources do.

So in the case of smart home, adversaries can eavesdrop the underlying communication and extract different information due to the lack of an end-to-end encryption between the different components of IoT. This is also a flaw for the existing protocols that IoT builds on; for instance, the SSDP protocol does not use any encryption and thus the adversary could exploit this fact and identify available smart hubs and their capabilities.

Furthermore, the current access control approaches that smart home deployments follow, *e.g.,* generating unique identifiers during correlation of user's device with the smart hub, expose IoT services to impersonation attacks as the adversary can eavesdrop the unique identifier, and use it for future attack attempts. However, these types of attacks can be mitigated if the appropriate integrity and authentication mechanisms are deployed.

Protection against DoS and their distributed counterpart (DDoS) is a challenging task especially for IoT architecture considering its limited capabilities, while currently we even lack effective solutions for IP based services that are supported by high power security infrastructures. To the best of our knowledge, only research related solutions such as [7] have been proposed for the protection of IoT against DoS attacks. However, such approaches do not focus on the application layer, but are mainly dealing with network layer protection.

As the majority of low cost IoT manufacturers do not usually consider mechanisms for validating firmware integrity during installations, upgrades and on execution, for instance using a trusted boot, IoT devices are exposed to possible software flaws. To eliminate software exploitation users should also use applications and services provided through well known channels, as unknown third party applications can manipulate the existing infrastructure introducing backdoors for future attacks.

One major issue is the possibility to deploy IoT installations using the default configurations. As explained in the previous section this is what made the DNS attack [4] possible. A recommendation in this could be to force users to properly configure the devices, otherwise the services cannot be started (*i.e.,* routers cannot have ports open by default, remote login can be enabled only if you set a strong password, IoT services can be started and accessed only if a good password was set.) Next to this, for what concerns wireless communications, open connections should not come as default configuration, the router can be started only if the default password was changed, vulnerable protocols should be deprecated and removed from configuration options.

VI. Related Work

Jacobsson *et al.* in [8], [9] presents the results of a risk analysis of a smart home automation system developed in a research project involving leading industrial actors. Their architecture was identical to the one discussed in this paper including sensors/devices, in-house gateway, cloud server, mobile devices and apps. The risk analysis was performed during collaborative workshop sessions with nine persons including security experts, domain experts, and smart home system developers. The discussion was organized using an open information security risk assessment questionnaire used to reason, identify, analyze, and evaluate threats. The identified threats were linked to the respective system vulnerabilities and the corresponding probability, likeliness of occurrence, and potential impact associated with each threat was estimated by each participant using a five level scale (1-5) from unlikely/negligible to likely/disastrous. The risk analysis results were organized in five categories relating to: software, hardware, information, communication, and human-related risks. The higher ranking risks in each category were related respectively to the software security in apps and APIs, inadequate physical security, inadequate access control policy/mechanisms, inadequate authentication and confidentiality, and poor password management. The results of their risk analysis are presented in a high-level and are in-line with our findings in this paper. Furthermore, in their work the a main observation was the need of empirically based methods that support the evaluation of risks in smart home environments, which is precisely the focus of this paper.

Kozlov *et al.* in [10] describe a threat analysis for an overall IoT architecture including security, privacy, and trust issues. Their threat analysis is mostly a high-level selection of threats discussed in the literature considering many scenarios and application domains (e.g., smart home, road transportation, smart energy meters, and mobile apps). The scenarios discussed illustrate threats to personal data privacy, availability, and also safety, for example, when an exploited vulnerability in a road traffic system could cause an accident. In contrast to their work, the analysis performed in this paper is more concrete with respect to the threats and vulnerabilities identified, and is also focused specifically on a deployed smart home scenario. We show not only the high-level issues but also demonstrate how they can be realized by attackers in real IoT devices.

Perera et al. propose in [11] a privacy-by-design framework for assessing IoT applications and platforms, which is proposed as a systematic method to guide privacy analysis and design in IoT based on a set of 30 guidelines. Each guideline should be applied during different phases of the data lifecycle including consent and data acquisition, data pre-processing, data processing and analysis, data storage, and data redistribution. The major privacy risks addressed by the guidelines are unauthorized access and secondary usage of information, meaning the use of already collected data for purposes not initially allowed by the data owners. The authors show the application of their framework in two open source IoT middleware platforms: OpenIoT and Eclipse SmartHome. For each

middleware a table was constructed showing if the guideline is supported, extendible, or not supported considering each of the phases in the data lifecycle. An extendible support means the middleware provides a plug-in mechanism that could make it straightforward to implement the functionality. By comparing the support for each guideline it is possible to compare the middleware with respect to their privacy-by-design features and gaps; in a sense more compliance to the guidelines implies a lower privacy risk. In contrast to the technical contributions in this paper the proposed guidelines are more abstract (*e.g.,* data anonymization, encryption, *etc.*) and can be mapped to the threats and vulnerabilities detailed in this paper.

Ziegeldorf *et al.* in [12] classify and examine RFID privacy threats in a broad sense with the goal of presenting relevant challenges that should be overcome in future deployments. In their reference model, they consider the collection of information by devices in the user environment, the processing and dissemination of the information by services that exploit the RFID technology. In their analysis they list the main threats to privacy, namely: identification, localization, tracking, profiling, privacy-violating interaction and presentation, decommissioning of devices, inventory attacks, and linkage of RFID related components. As a result of their analysis profiling is considered the most severe threat. In contrast to our approach this work focuses on RFID based IoT systems, while we concentrate on smart home components threat analysis.

VII. Conclusions & Future Work

IoT architectures will be an important component of future Internet as it closes the gap between physical and virtual objects. Among others, smart home is one of the main developments of IoT environments as it enhances the user's experience when using home devices.

Albeit the advantages that IoT offers to smart home users do not only expose homes to well known attacks but also the (IoT) sensors should deal with flaws that have not been previously considered. This is due to the fact that such devices are of limited processing power, and rely on heterogeneous network architectures that increase the attack surface of the provided service.

In this paper, we introduced a smart home threat model, and analysed it in our test bed architecture considering off the shelf components. Our initial analysis demonstrates that existing smart home IoT infrastructure could be vulnerable to eavesdropping, impersonation, DoS and software exploitation attack vectors under specific conditions *e.g.,* considering an attacker that manages to get access to the underlying network.

Currently, we are planning to extend our analysis demonstrating in detail the consequences and the impact of the different threats on users and the IoT infrastructure, as well as introduce the appropriate countermeasures for enhancing smart home security. In this direction, we envisage a framework that is able to automatically identify vulnerable points in a smart home architecture.

References

[1] U. forum Members, "UPnP Device Architecture 1.1." [Online]. Available: http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf

[2] J. King, K. Lakkaraju, and A. Slagell, "A taxonomy and adversarial model for attacks against network log anonymization," in *Proceedings of the 2009 ACM Symposium on Applied Computing*, ser. SAC '09. New York, NY, USA: ACM, 2009, pp. 1286–1293. [Online]. Available: http://doi.acm.org/10.1145/1529282.1529572

[3] "LOIC." [Online]. Available: https://sourceforge.net/projects/loic/

[4] M. Smith, "IoT botnets used in unprecedented DDoS against Dyn DNS; FBI, DHS investigating," Oct. 2016. [Online]. Available: http://www.networkworld.com/article/3134093/security/iot-botnets-used-in-unprecedented-ddos-against-dyn-dns-fbi-dhs-investigating.html

[5] "Hacker Claims To Push Malicious Firmware Update to 3.2 Million Home Routers." [Online]. Available: https://motherboard.vice.com/en_us/article/hacker-claims-to-push-malicious-firmware-update-to-32-million-home-routers

[6] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, "Smart-phones attacking smart-homes," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec '16. New York, NY, USA: ACM, 2016, pp. 195–200. [Online]. Available: http://doi.acm.org/10.1145/2939918.2939925

[7] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6lowpan based internet of things," in *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct 2013, pp. 600–607.

[8] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system," *Future Generation Computer Systems*, vol. 56, pp. 719 – 733, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X15002812

[9] A. Jacobsson and P. Davidsson, "Towards a model of privacy and security for smart homes," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Dec 2015, pp. 727–732.

[10] D. Kozlov, J. Veijalainen, and Y. Ali, "Security and Privacy Threats in IoT Architectures," in *Proceedings of the 7th International Conference on Body Area Networks*, ser. BodyNets '12. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, pp. 256–262. [Online]. Available: http://dl.acm.org/citation.cfm?id=2442691.2442750

[11] C. Perera, C. McCormick, A. K. Bandara, B. A. Price, and B. Nuseibeh, "Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms," in *Proceedings of the 6th International Conference on the Internet of Things*, ser. IoT'16. New York, NY, USA: ACM, 2016, pp. 83–92. [Online]. Available: http://doi.acm.org/10.1145/2991561.2991566

[12] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: threats andchallenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, 2014. [Online]. Available: http://dx.doi.org/10.1002/sec.795