Proceedings of the Federated Conference on Computer Science and Information Systems pp. 449–458
DOI: 10.15439/2019F177
ISSN 2300-5963 ACSIS, Vol. 18

FANE: A Firewall Appliance for the Smart Home

Christoph Haar
Hochschule für Telekommunikation in Leipzig
Gustav-Freytag-Straße 43-45, 04277 Leipzig, Germany
Email: haar@hft-leipzig.de

Erik Buchmann
Hochschule für Telekommunikation in Leipzig
Gustav-Freytag-Straße 43-45, 04277 Leipzig, Germany
Email: buchmann@hft-leipzig.de

***Abstract*—With the advent of the Internet of Things (IoT), many domestic devices have been equipped with information technology. By connecting IoT devices with each other and with the Internet, Smart Home installations exist that allow the automation of complex household tasks. A popular example is Google Nest that controls cooling, heating and home security. However, Smart Home users are tempted to neglect that such IoT devices pose IT-Security risks. Examples like the Mirai malware have already shown that insecure IoT devices can be used for large-scale network attacks. Thus, it is important to adapt security approaches to Smart Home installations. In this paper, we introduce FANE, our concept for a Firewall AppliaNcE for Smart Home installations. FANE makes a few realistic assumptions on the network segmentation and the communication profile of IoT devices. This allows FANE to learn firewall rules automatically. Our prototypical implementation indicates that FANE can secure a wide range of IoT devices without requiring network-security expertise from the Smart Home user.**

I. Introduction

IN THE the last years, the proliferation of Smart Home installations has gained momentum. Today, the consumer market offers a huge number of different Internet-of-Things (IoT) devices.

Smart thermostats, cameras, speakers and even toothbrushes contain information technology that connects the IoT device over the Internet with cloud services or other IoT devices. For example, IoT devices from the Google Nest family [1] provide a straightforward, user-friendly way to control heating, cooling and home security. Smart speakers like Amazon Alexa [2] allow to control many daily activities via voice control. From the perspective of the manufacturers, the Smart Home concept allows new business models, e.g., to sell new product features as digital upgrades for IoT devices.

On the other hand, consumers might be tempted to overlook that the IoT devices pose an IT-Security risk. For example, the lifetime of a traditional security camera ends when the device is broken. In contrast, the lifetime of an IoT security camera that connects over the Internet should come to an end when its manufacturer discontinues security updates, even if the IoT security camera is still working. Otherwise, the IoT security camera might end up as, say, part of the Mirai bot network, which consisted of approx. 500,000 devices in 2016 [3].

From the perspective of a consumer without in-depth expertise of network security, it is next to impossible to find out if the IoT devices present in a Smart Home installation are subject to attacks over the Internet. In this paper, we explore options to integrate a firewall into typical Smart Home installation that can detect and deter such attacks. This is challenging, since the firewall must be compliant with the typical modes of use of a Smart Home installation, and a consumer cannot be expected to evaluate firewall rules or identify false alarms. On the other hand, the IoT devices used differ from general-purpose devices such as smartphones and desktop computers. This might allow for pre-configuration to some extent.

In particular, we make the following contributions:

1) We systematically compare the lifecycle of a classical firewall with the lifecycle of IoT devices in a typical Smart Home installation.
2) We propose FANE, a Firewall AppliaNcE on a Wi-Fi bridge in Smart Home installations.
3) We describe a proof-of-concept implementation of FANE based on a Raspberry Pi, and we evaluate it with three different IoT devices.

We show that it is possible to develop a generic IT-Security concept for IoT devices in a Smart Home installation by making few realistic assumptions, e.g., the IoT network segment is only used by single-purpose IoT devices, which do not fundamentally change their communication profiles. We have implemented this security concept in FANE. Our evaluation indicates that FANE can secure the IoT network segment without requiring the user to possess network-security expertise.

Paper structure: In Section II, we review related work. In Section III we provide a problem statement. We describe FANE in Section IV, followed by a proof-of-concept implementation in Section V and an experimental evaluation in Section VI. Section VII concludes.

II. Related Work

In this section we provide a brief definition of Internet of Things and Smart Home, and we introduce related work on firewalls, firewall management and approaches to generate firewall rules automatically.

A. Internet of Things and Smart Homes

The "'Internet of Things"' (IoT) refers to physical appliances, which have been equipped with information technology in order to connect them with other devices directly or over the Internet [4]. IoT includes a wide range of appliances, from

connected cars over smart buildings to connected machinery in an Industry 4.0 setting. The concept "'Smart Home"' narrows down this range to devices that let end users to control, monitor or access everyday objects of the daily routine [5].

B. Security Challenges

To assess the security properties of Smart Home installations, it is important consider the basic security challenges that occur in installations of IoT devices. One study [6] lists six major security issues:

Identity and Authentication: In IoT environments, numerous devices need to authenticate each other in order to provide trustable services. Thus, reliable techniques for identification and authentication are needed.

Access Control: To create new services it is necessary to aggregate data from different providers. This is challenging, because in typical IoT scenarios each provider has its own access control policy.

Protocol and Network Security: If IoT devices communicate with each other in a distributed network architecture, distributed schemes for key management are needed.

Privacy: The Smart Home concept means that numerous IoT devices monitor the actions of its users in order to devise meaningful responses. Thus, privacy very important from a user perspective.

Trust and Governance: In IoT architectures there are two dimensions of trust. The first dimension is between users and their IoT devices. The other dimension is between the IoT devices. Device A needs to trust the accuracy and integrity of the data produced by device B. Data governance goes in the same direction, in a sense of data and access governance.

Fault Tolerance: Mechanisms for fault tolerance need to be established to counteract faulty or tampered devices.

Other studies [7] list similar challenges.

C. Firewalls State of the Art

Firewalls are able to control and log the network traffic based on rules set by an administrator or security expert. In literature different firewall generations are distinguished [8]. 1st generation firewalls are known as packet filters which operates on the transport layer. The filtering is based on source and destination IP addresses, ports and protocols. 2nd generation firewalls are also operating on the transport layer and they are known as stateful packet inspection. State tables are used to keep track of the network traffic and filtering is based on state and context of packets. 3rd generation firewalls are operating on the application level and require different proxies for each service. The proxy acts as a middleman between source and destination to reestablish a new session. Current firewall technologies are called next generation firewalls. These next generation firewalls are looking deep into packets and combine traditional firewall technologies with network filtering capabilities on the application level [9]. However, all these generations have in common that an expert is needed to define rules or check them for correctness which motivates our new approach.

D. Firewall Lifecycle

Traditionally, a firewall must be part of the IT-Security process, as described by the ISO 270xx standards family [10], the German BSI Grundschutz Standard 200-2 [11] or the ITIL process for security Management [12]. The IT-Security process starts with a IT-Security policy that has been passed by the management. Based on this policy, business objectives, the assets to be protected and a risk classification can be identified. Subsequently, measures can be defined and implemented that restrict the IT-Security risks to acceptable levels. In the following, the effectiveness of these measures needs to be monitored. Based on this information, corrective actions can be planned and executed [13]. Note that all process steps require a person with IT-Security expertise, which cooperates with various IT experts from the operations department.

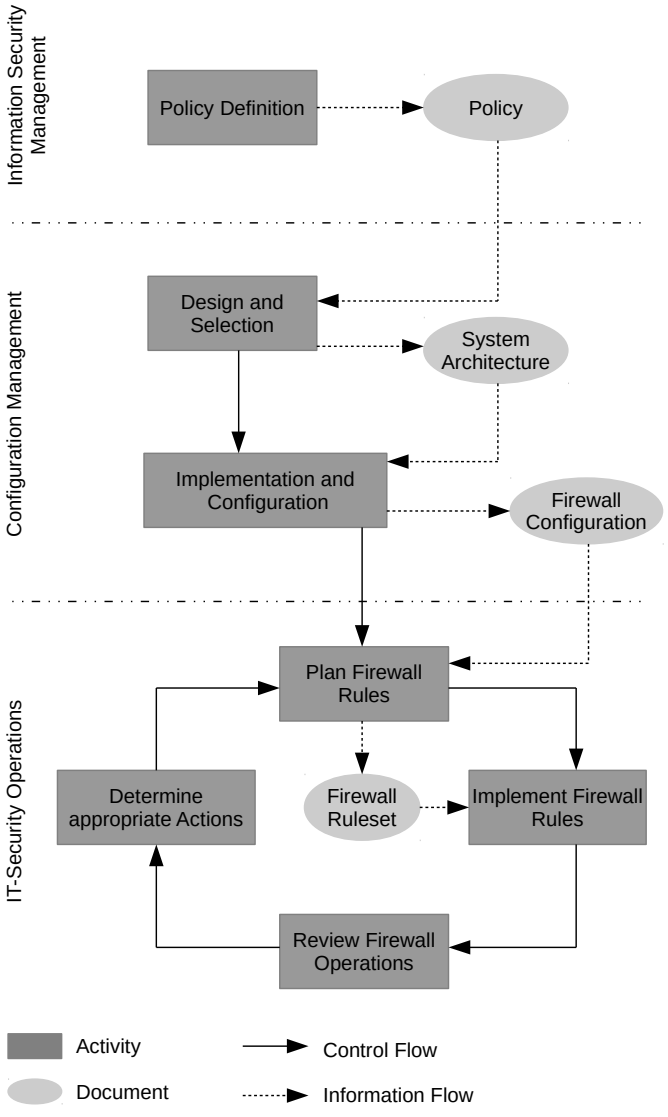

Fig. 1. Traditional Firewall-Lifecycle

A firewall fits into the IT-Security process [14] as shown in Figure 1. In the Information-Security Management phase, the management defines a security policy based on company-wide security objectives. This policy is independent from technical realities. Based on the security policy, an IT-Security expert designs the architecture of the firewall system and selects the firewall system components. In the implementation and configuration phase, the IT-Security expert adapts the firewall system to the system architecture with its network segments, hosts and applications. This includes a preliminary set of firewall rules that define which network packets are allowed to pass the firewall. In the next step, a plan-do-check-act cycle takes place where the firewall rules are designed, implemented, reviewed and improved in a repetitive way. Typically, this cycle is part of IT-Security operations. It allows to adjust the firewall rules to changes such as new business applications, hosts moving from one network segment to another one, or in case of detecting new attacks. Note that not only the management of firewall rules is a cyclic process, but also the IT-Security process. If the management observes that the security policy is ineffective, this policy can be changed as well, and it has an impact on all design decisions further down the IT-Security process chain.

E. Firewall Rules

It is a labor-intensive task for a domain expert to create a rule set for firewalls for manually. One option to obtain firewall rules (semi-)automatically is to use data mining or machine learning on a training set consisting of network packets. This option is based on the assumption all user applications operate as intended while the training set is recorded. Respective approaches [15]–[17] have been proposed for Intrusion Detection systems, but might be adaptable to firewalls as well. By using k-Means, C4.5 decision tree algorithms, Naive Bayes classifier, Neural Networks or Support Vector Machines, it is possible to derive common characteristics of allowed network connections. Those characteristics could be translated into firewall rules. It is also possible to generate firewall rules by mining the firewall log [18] instead of a dump of network packets. However, all approaches require an IT-Security expert to decide which generated rules are relevant to meet the security requirements, and the quality of the generated rules still needs further research.

A different option to generate firewall rules is to deduce them from a formal specification of security requirements by using argumentation logic [19]. This approach allows to automatically obtain a detailed, comprehensive set of rules from a high-level specification. However, creating a specification of the security requirements for a certain system architecture still requires expert knowledge in IT-Security.

III. Problem Statement

In this section, we explore the differences between traditional firewalls and firewalls needed for IoT devices in a Smart Home installation. In addition, we derive requirements for a Smart Home firewall.

A. Does a Firewall Fit into the Smart Home Concept?

To find out in which ways traditional firewall use cases differ from Smart Home use cases, we consider the modes of use, network architecture, application scenario, user roles and information technology used.

a) Modes of Use: A firewall is an access control mechanism that allows or blocks network traffic between two network segments that have different security properties [20], e.g., an internal network and the Internet that is open for anybody. The firewall enforces a set of firewall rules that allow or prohibit network packets to travel from one segment into the other one. The firewall rules depend on the use cases that are executed over both network segments. For example, a business workflow "'Answer customer requests"' might require that a set of machines in the internal network is allowed to send and receive email to/from the Internet. Thus, firewall rules must be defined by a network-security expert with domain knowledge. If the workflows, the applications or the segment boundaries are changed, the expert must adapt the firewall rules as well. Traditionally, firewalls are tailored for complex multi-purpose scenarios where the hosts execute numerous different applications that change over time.

Smart Home use cases are fundamentally different [21]: A typical IoT device is a physical object that has been extended with information technology to improve its usefulness. For example, a smart toothbrush [22] can tell its user if a tooth has gone unbrushed. Thus, IoT devices are constructed for a single purpose that does not change over time. It only makes sense to install a toothbrush control software on a smart toothbrush. As a result, IoT devices are single-purpose objects. If the device is not needed any more, it will be disposed.

b) Network Architecture: Firewalls depend on the network segmentation. With traditional use cases, a network installation might contain multiple segments protected by multiple firewalls. A prominent example is a perimeter network [20], which contains assets such as Web servers that must be accessible from an external network. Two sets of firewall rules protect the perimeter network against the external network and the internal network against the perimeter *and* the external network. However, the number and architecture of the network segments might be individually different for each network installation.

In contrast, a typical Smart Home installation with IoT devices produces three network segments with different security properties: (a) the untrusted Internet, (b) the home network with trusted devices such as the user's laptop and printer, and (c) an IoT network segment that contains all IoT devices. Since the IoT device and its software comes as an integrated package, the user has little options to influence the security of the IoT device, e.g., by disabling unused network protocols or by removing unused software functionality. Thus, the IoT network segment should be separated from the home network [23], which is used for sensible tasks such as online banking or online shopping. All devices in the IoT network segment can be expected to require an Internet connection, to

provide a service, to obtain updates and upgrades, to allow a remote control via smartphone app, etc.

c) Application Scenario: Firewalls follow the IT-Security lifecycle, as explained in Section II. Based on a general security policy that has been defined from a management perspective, a network-security expert defines the position of the firewall(s) in the network architecture and a set of firewall rules. By using a plan-do-check-act-cycle, the firewall rules as well as the firewall hard- and software must be constantly monitored, evaluated and adapted to changes in the IT infrastructure.

On the opposite side, one of the fundamental principles of the Smart Home concept is to let IoT devices use sensors to observe its environment, in order learn appropriate actions with a minimum of user interaction and without requiring the user to scrutinize the operations of the IoT device on a regular basis. For example, the nest thermostat observes the temperature preferences of its user and if he or she is at home, and controls the heating system accordingly. Furthermore, the duration of use of IoT devices is an one-dimensional process that starts with the deployment of a device and ends with it's disposal, just like non-smart devices [24], i.e., it does not follow a periodic lifecycle where it is constantly monitored and improved. For example, a smart light switch never changes its function, and it cannot be adapted to different needs.

d) User Roles: Setting up a traditional firewall typically requires three distinct roles: The role "'Information Security Management"' defines a security policy by considering the assets and (business) objectives that are relevant for a certain part of the IT infrastructure. Based on the policy, the role "'Configuration Management"' designs a firewall system, selects appropriate firewall components, and provides an initial installation and configuration of the system. Finally, a role "'IT-Security Operation"' constantly monitors and improves the firewall system, both on the level of the firewall rules and of the firewall hard- and software.

In contrast, an IoT device for a Smart Home usually is preconfigured by the manufacturer for typical use cases. The end user can deploy and configure the IoT device with minimal efforts, does not need to monitor it later on and does not need expert knowledge.

e) Information Technology: IoT devices make use of network protocols which have been well established. They use Linux-based operating systems, Cloud resources and Open Source programming libraries. The network security of IoT devices is based on mechanisms for encryption, certification and signatures that have been in use for years. Thus, from a technical point of view, off-the-shelf firewalls can be directly used to control the network traffic of IoT devices.

B. Problem Definition

From a technical perspective, it would be a simple exercise for a network security expert to set up a firewall that controls the network traffic of an IoT device. However, this procedure conflicts with the general understanding how IoT devices should operate in a Smart Home. Thus, a firewall for Smart Homes must differ in the following properties from traditional firewalls:

- **P1** The firewall must be usable without expert knowledge.
- **P2** The firewall must fit to the durations of use of Smart Home components.
- **P3** The firewall must operate in a way that is typical for IoT devices in the Smart Home.

P1 implies not only that the configuration and installation of a firewall in a Smart Home must not require network security expertise. It also means that a user cannot be expected to tell false alarms from real alarms, or to decide if a certain firewall rule is applicable to the home network. From **P2** it follows that such a firewall must deal with IoT devices that are bought once for a certain purpose and never change its basic properties until disposal, and it must operate in the same way. Furthermore, the firewall must operate in the same way. **P3** means that a firewall in a Smart Home needs to operate without permanent care from the user, i.e., it must monitor the network traffic, deduce meaningful firewall rules and provide appropriate reactions to forbidden network packets.

We have ruled out a cloud-based approach [25], [26] that externalizes the firewall to a trusted third party on the Internet. Although such an approach might fulfil the properties described, it requires a permanent Internet connection. In addition, a cloud-based firewall would transfer security-relevant information into the cloud. Thus, both the Internet connection of the firewall and the trusted third party would be a valuable target for an attacker.

IV. FANE: A Firewall Appliance

In this section, we introduce FANE, a concept for a Firewall AppliaNcE that is compatible with the Smart Home paradigm.

A. Network Architecture

A firewall separates network segments with different security properties. Typical IoT devices do not allow its user to observe security properties, and to configure security-related aspects, such as disabling unused functions. Furthermore, an IoT device is designed to be used like a classical, non-smart device, i.e., its users are tempted to forget that the device might pose IT-Security risks. For this reason, IoT devices should be placed in network segments that are isolated from all other network segments of the Smart Home.

Thus, FANE operates as a Wi-Fi bridge that connects the IoT network segment to the Internet and includes a firewall, as shown in Figure 2. The IoT network segment only contains single-purpose IoT devices, and the Wi-Fi bridge is the only connection of the IoT segment to other network segments and the Internet. We observe that this allows us to specify the security concept in advance.

B. Security Concept

From Section III it follows that a traditional firewall approach is complex, because the underlying network segmentation and the processes executed over the boundaries of these segments are complex, too, and might change from

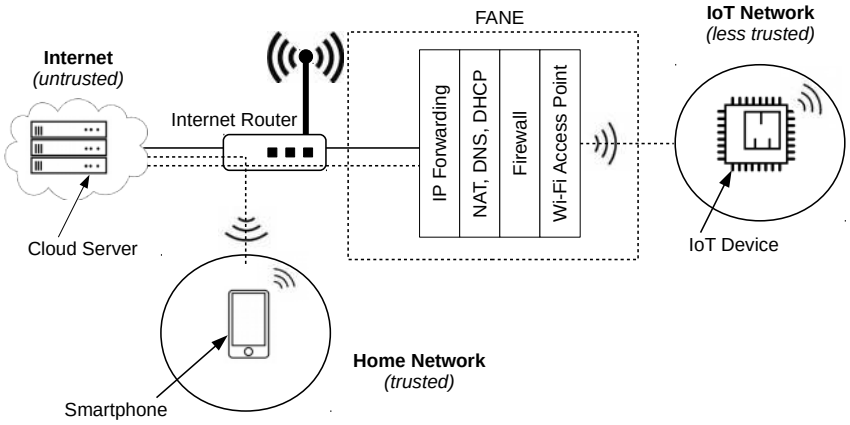

Fig. 2. System Architecture

time to time if a new software is installed on a device in the network. With our network architecture, we have reduced this complexity. We only need to consider three kinds of communication activities:

- An IoT device wants to communicate with a server on the Internet. For example, a smart thermostat wants to communicate with the user's smartphone, which is mediated over a cloud service.
- An IoT device wants to communicate with a device in another network segment. For example, the user installs a control application on a laptop to configure the smart thermostat.
- An IoT device wants to communicate with another IoT device in the same network segment. For example, our smart thermostat wants to directly communicate with the smart air condition.

Since FANE operates as a bridge to the Internet, only the first two kinds of communication have to be monitored, and the security properties of the endpoints of the communication can be specified at production-time of FANE: The open Internet is insecure by default, the IoT devices are less secure, and the devices in other network segments of the Smart Home are trustworthy. This allows to pre-configure the security concept of FANE in advance, i.e., it does not need a user with network-security expertise (Property **P1**):

1) No device on the Internet is allowed to open a network connection to the IoT network segment.
2) An IoT device is allowed to open a connection to the Internet, if this is part of its normal operation.
3) An IoT device is allowed to open a connection to devices in other (trusted) network segments of the Smart Home, if this is part of its normal operation.
4) A device from a trusted segment is allowed to open connections to the IoT network segment.
5) IoT devices are allowed to open connections to other devices in the IoT network segment.

C. Smart Home Firewall Operations

FANE has to meet conflicting requirements: It must meet the expectations provided by Smart Home components (**P2**). In particular, this means that FANE must operate without constant supervision (**P3**). At the same time, as a security component it must not neglect the IT-Security process, including a plan-do-check-act cycle to refine firewall rules. However, this must be possible without requiring the user to possess expert knowledge (**P1**).

We circumvent these conflicts, as shown in Figure 3): We distinguish between pre-configuration management and Smart Home operations. Because we restrict FANE to the network architecture described in Subsection IV-A, the policy definition, the firewall design and a baseline configuration of firewall rules can be done at pre-configuration time. Thus, we shift the initial parts of the IT-Security process into the responsibility of the Smart Home firewall manufacturer who possess IT-Security expertise. Furthermore, we propose to automate the configuration and the plan-do-check-act cycle in a way that it's phases can be started without expert knowledge at operation time. Finally, we define a process step in a way that the user is informed when an IT-Security expert is needed.

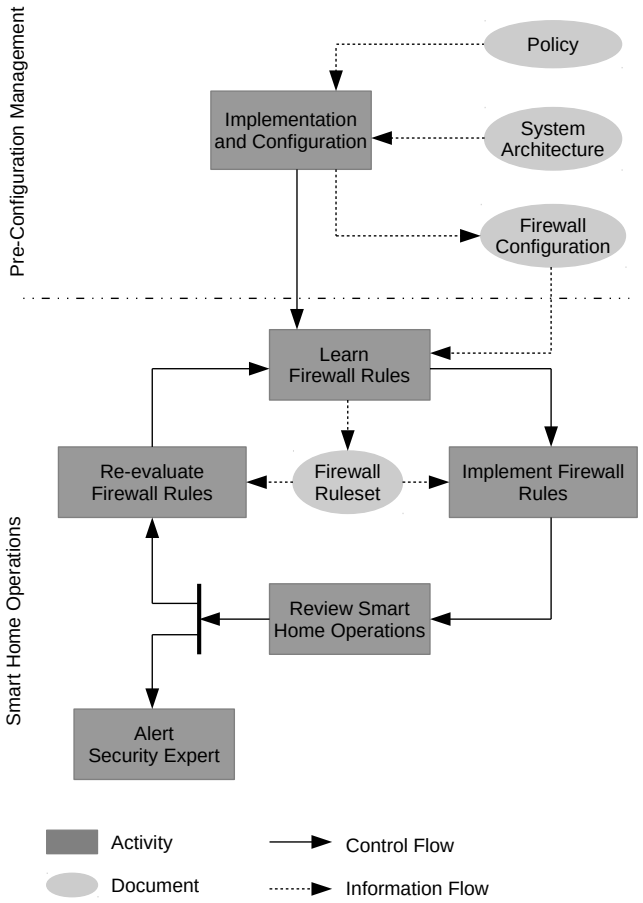

Fig. 3. FANE Operations

D. User Interaction

After having defined the operations of FANE, we can define the user interactions needed. Observe that no interaction requires expert knowledge (Property **P1**). FANE comes as an IoT device that runs out-of-the-box after being connected to a power outlet and the Internet.

When FANE is connected to the Smart Home installation for the first time or if new IoT devices are added, the user can tell FANE to **learn** new firewall rules by observing the network packets of the IoT devices. Assume an IoT device uses a functionality that has not been used during the learning stage, or the device has been updated and a new network connection is now blocked by FANE. In this case, the user has the option to let FANE **re-evaluate** the rule set. That is, FANE executes a learning stage on a certain device with the option to discard rules that have been learned before. The rules from the security concept (Subsection IV-B) cannot be discarded.

If FANE blocks a large number of network packets per time-interval, it generates an **alert**. The alert shows the user that immediate action needs to be taken, i.e., something happens that cannot be handled automatically by FANE. For example, the IoT network segment might face a denial-of-service attack from the Internet, or an IoT device has been taken over and tries to connect to the attacker's command and control server on the Internet. In such cases, the user might decide to call the customer support of the IoT device, or ask an IT-Security expert for further investigations.

V. Proof-of-Concept Implementation

In this section, we describe the software and hardware components of our FANE prototype, how FANE learns firewall rules and in which way it interacts with the user.

A. Our FANE prototype

We have realized FANE on the basis of a Raspberry Pi, which executes several linux shell scripts to configure and operate an iptables packet filter (see Subsection II-C). Figure 4 illustrates our hardware configuration and the main software packages used.

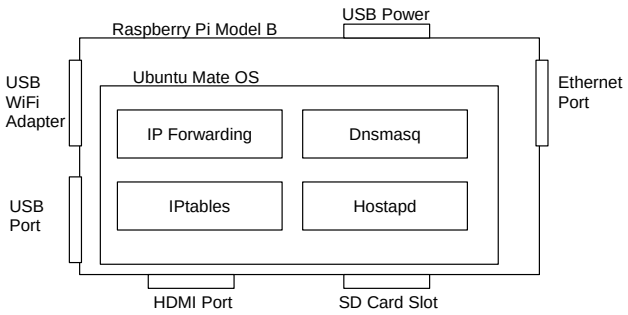

Fig. 4. Our FANE prototype

a) Hardware: From Section IV it follows that FANE must provide a Wi-Fi access point that creates a network segment for IoT devices. The IoT devices might want to communicate with other devices in the same segment, the home network segment and the Internet. Thus, FANE must be connected to the Internet, and its firewall must control all incoming and outgoing network packets of the IoT network segment.

We have implemented this approach on a third-generation Raspberry Pi model B. This is a credit-card sized single board computer containing a quad-core processor with 1.2GHz, 1 GB main memory and various network and connection interfaces. Because the on-board Wi-Fi chip cannot be configured as a Wi-Fi access point, we have connected an external Wi-Fi module via USB. We have used a 32 GB SD Card for permanent storage.

We would need only two switches to initiate the learning- and re-evaluation stage of the user interface, and one LED indicating an alert. The IT-Security expert, which might be needed to handle serious attacks on the IoT nework segment, would be able to obtain firewall logs and other information by using an SSH connection. This way, our FANE prototype

costs less than 60 EUR. However, to ease development we have used an external USB keyboard and a LCD monitor.

b) Software: We have used the Ubuntu Mate Linux operating system as a basis of our software configuration. On top of a minimal OS installation, we need the following software packages and services:

- awk (script language to edit text files)
- cron (timed execution of processes)
- dnsmasq (DHCP client and DNS cache)
- hostapd (Wi-Fi access point)
- inotify-tools (monitor changes in files)
- iptables (network address translation and firewall)
- tcpdump (record network packets)

By configuring the Ethernet interface *eth0* as a DHCP client, our Raspberry Pi can be connected to any Internet router without further configuration. We have configured the *wlan0* interface with a static IP address and subnet mask, and we have configured it as a Wi-Fi access point by using *hostapd*. Our Smart Home firewall must act as a bridge between *eth0* (Internet) and *wlan0* (Wi-Fi segment for IoT devices). Thus, we have used *iptables* and *sysctl* to activate IP forwarding, including network-address translation and masquerading. With *dnsmasq*, we have realized a DHCP service.

B. Learning Firewall Rules

For our FANE prototype, we have used a straightforward approach to learn firewall rules. For more elaborate approaches, see Section II. The learning stage consists of two phases, a *monitoring phase* and a *rule generation phase*. We assume that all network traffic recorded during the monitoring phase is allowed, i.e., we assume that no IoT device has been manipulated or attacked before the monitoring phase ends.

When FANE is connected to power and Internet for the first time, or if the user wants FANE to learn new rules, it enters the monitoring phase for a certain period of time. In this phase, FANE waits for new IoT devices connecting to the access point, and logs the network packets. We have implemented this phase as follows:

At boot time, a *cron* task with the time prefix *@reboot* starts a script that finds out if the set of firewall rules is the one that has been pre-configured from the security concept (Subsection IV-B). Alternatively, a user command starts the monitoring phase manually. In the monitoring phase, FANE uses the monitoring tool *inotify* to find out if the *dhcp.leases* file changes. This indicates new devices using the access point. In this case, inotify executes a script that obtains the IP address of the device from dhcp.leases. At the same time, FANE uses tcpdump to create a log file containing all network packets sent or received during the monitoring phase.

At the end of the monitoring phase, FANE stops tcpdump and enters the rule generation phase. In this phase, FANE parses the log file from tcpdump into firewall rules according to the IP addresses of the IoT devices that have used the access point in the monitoring phase. In particular, FANE uses a *sed* command to filter the log for incoming and outgoing IP addresses and ports. This set of addresses and ports is reduced to unique entries in a second step. The odd lines in Figure 5 show, how the set of addresses and ports looks like after FANE has removed surplus information and duplicats from the log file. In a third step, a shell scripts parses the remaining addresses and ports into firewall rules that allow such packets for the *iptables* chain "'FORWARD"'. The odd lines in Figure 5 illustrate this step. We have used the iptables policy "'DROP"', i.e., FANE drops all packets that are not allowed by the rules generated.

```
1  15:23:18 IP 10.200.65.101.1080 > 35.158.162.95.80:
2  iptables -A FORWARD -s 10.200.65.101 -sport
       1024:65535 -d 35.158.162.95 -dport 80
       -p tcp -j ACCEPT

3  15:23:22 IP 10.200.65.101.8553 > 35.157.158.75.1883:
4  iptables -A FORWARD -s 10.200.65.101 -sport
       1024:65535 -d 35.157.158.75 -dport 1024:65535
       -p tcp -j ACCEPT

5  15:24:36 IP 10.200.65.101.8653 > 35.156.40.103.1883:
6  iptables -A FORWARD -s 10.200.65.101 -sport
       1024:65535 -d 35.156.40.103 -dport 1024:65535
       -p tcp -j ACCEPT

7  15:25:07 IP 10.200.65.101.8554 > 35.157.255.122.80:
8  iptables -A FORWARD -s 10.200.65.101 -sport
       1024:65535 -d 35.157.255.122 -dport 80
       -p tcp -j ACCEPT
```

Fig. 5. Firewall rules learned from an adjusted packet log

Note that this procedure can be extended easily to extended firewall features, e.g., to include the iptables options for stateful inspection. At the end of the rule generation phase, FANE installs the rules and is ready for operation.

If an IoT device is not working properly, if a new IoT device is added to the IoT network segment or if an existing device is used in a way it has never been used before, the user can order FANE to re-evaluate the rule set. In this case, the user has the option to discard rules from preceding learning procedures, and to re-start the monitoring- and rule-generation phase.

VI. Experimental Evaluation

In this section, we explore the applicability of FANE with three different Smart Home appliances.

A. Setup

Figure 6 shows our experimental setup. FANE is directly connected to the Internet router, and its integrated access point spans a Wi-Fi network segment for IoT devices. The Internet router creates a Wi-Fi home network that connects a smartphone to the Internet. Different cloud services connect the smartphone to the IoT devices. A cloud service might use a load balancer, i.e., the IP addresses the IoT devices connect to might change from time to time.

We have tested three different devices, which communicate differently with a control app on the user's smartphone:

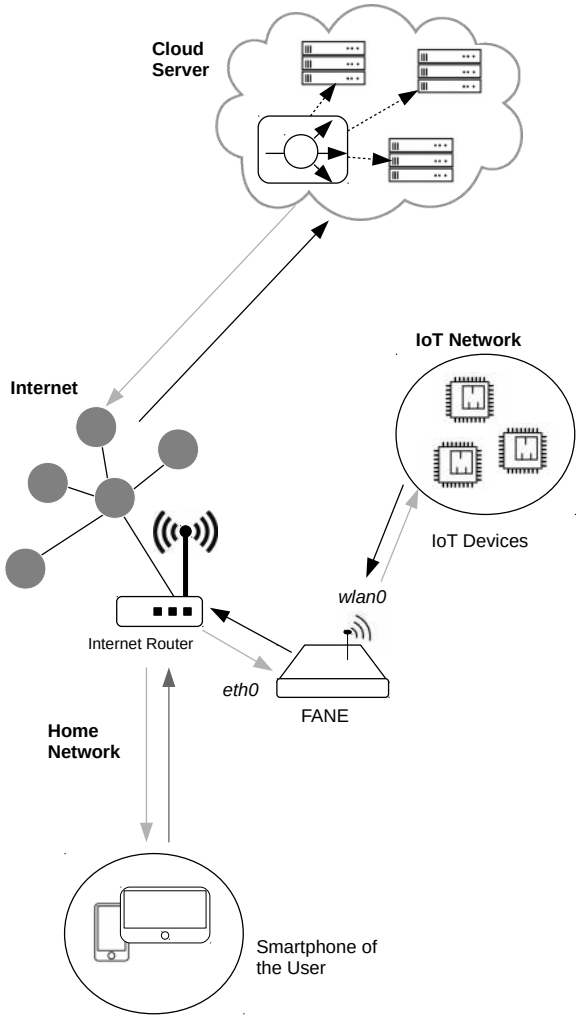

Fig. 6. Our experimental setup

1) An electrical IoT relay.
2) An IoT power outlet.
3) An IoT security camera.

The IoT devices do not communicate directly with each other, but with the user's smartphone and the Internet. Thus, for our experiments we do not need to preconfigure rule 5 from our security concept (see Subsection IV-B). We have configured each device for FANE's IoT network segment. We have used a monitoring phase of 40 minutes, and we have operated each device periodically during this phase. In the following, we briefly introduce each IoT device, and we describe what we have learned by using FANE as described.

B. IoT Relay

Our first use case is an electrical relay "'10A Wi-Fi smart switch"', sold for less than 9 EUR, manufactured by Sonoff [27]. The IoT relay can be turned on or off via smartphone app, which allows a technician to integrate non-smart electrical devices into a straightforward Smart Home installation. Sending commands from the app to the relay requires an Internet connection, i.e., there is no option to directly connect the smartphone app to the IoT device. After the relay is connected to the access point provided by FANE, and the user has installed the smartphone app, the relay is ready to use.

In our monitoring phase of 40 minutes, we have switched the relay on and off frequently via smartphone app for 10 minutes. After that, we have waited for a period of 20 minutes. Finally, we have operated the relay for further 10 minutes.

After completing the monitoring phase, FANE has written 1,800 lines in the packet log. All packets followed the TCP protocol and were sent/received to/from one singular IP address located at a dedicated server leased from Amazon. Thus, the rule generation phase has generated only one rule for in- and outgoing packets. The IoT relay was working properly after FANE has activated the firewall rule set generated. Figure 7 shows an example from the traffic log FANE has recorded from the IoT relay.

```
1  13:41:31.551813 IP 10.200.65.109.55147 >
       52.71.154.91.443: Flags [F.], ...

2  13:41:31.551870 IP 10.200.65.109.55145 >
       52.71.154.91.443: Flags [F.], ...

3  13:41:31.551914 IP 10.200.65.109.55161 >
       52.71.154.91.443: Flags [.], ...

4  13:41:31.668878 IP 52.71.154.91.443 >
       10.200.65.109.55161: Flags [.], ...

5  13:41:31.669239 IP 52.71.154.91.443 >
       10.200.65.109.55161: Flags [P.], ...
```

Fig. 7. Fragment of the packet log of the IoT relay

C. IoT Power Outlet

Our second use case is an IoT power outlet "'Smart Wi-Fi Socket Model SWA1"', sold for 18 EUR, produced by Shenzhen Lingan Intelligent Technology [28]. Similarly to the IoT relay, the IoT power outlet can be turned on or off via smartphone app. In addition, it can be controlled with Amazon Alexa or Google Home, which allows to integrate non-smart electrical devices into an elaborate Smart Home concept without requiring a technician. Any command to the IoT power outlet is handled by a cloud service over the Internet.

In our monitoring phase, we have used the IoT power outlet via smartphone in the same way as the relay for 40 minutes. At the end of the monitoring phase, FANE has collected a packet log of approx. 2,600 lines, all of them TCP packets. The rule generation phase has generated rules that allow five

different IP addresses, all of them in the address range of the Amazon AWS cloud.

The IoT power outlet was fully operational after FANE has started to filter network connections. We have observed that only one of the five addresses in the firewall rule set was actually used to operate the outlet via smartphone app. We assume that some network connections are used only for analyzing customer behavior or similar purposes, i.e., blocking them would not reduce the functionality of the device.

D. IoT Security Camera

The most complex IoT device tested was a "'720P HD IP Wireless security camera"', sold for 37 EUR and manufactured by XinweiYa [29]. The IoT security camera sends a live video stream to the smartphone of the user. Furthermore, the smartphone app allows to restart the IoT security camera, and to rotate it around two axes. After connecting the IoT security camera to a power outlet, it can be configured with a smartphone app to use FANE's access point.

During our monitoring phase of 40 minutes, we have restarted the IoT security camera, we have let the IoT security camera sent a live video stream of 10 minutes to the smartphone, we have waited for 20 minutes, and we have restarted it again for another live stream of 10 minutes. After 40 minutes, FANE has collected 8 MB packet log of approx. 27,000 lines, most of them UDP packets.

The rule generation phase produces a rule set of 20 rules for this device. Those rules allow services like Network Time Protocol (NTP) or Domain Name System (DNS) as well as cloud services hosted on Amazon AWS, the Microsoft cloud and the Alibaba cloud.

We have observed that the IoT security camera was not working properly, after FANE started to filter network packets. Our investigations have shown that this due to a specific load balancer. The IP address of the load balancer was allowed by the firewall rule set generated. But the load balancer referred the IoT security camera frequently to IP addresses unknown to FANE. However, it would be possible to adapt the learning approach to cope with such a load balancer. For example, FANE could detect and accept IP addresses that are close by addresses that are already allowed by the rule set.

The packet log has also shown that the IoT security camera first tries to reach the smartphone app in the same network segment directly, via multicast. Thus, even if the IoT security camera makes use of the Internet connection, it might be able to provide its basic functionality without the Internet. From this observation we conclude that there might be options for FANE to distinguish between communication needed for the normal operation of an IoT device, and other communication needed for advertising purposes or usage analytics that can be blocked without undesired side-effects.

Finally, we have observed that the IoT security camera produces more network load by an order of magnitude than the other IoT devices tested. While this has slowed down the rule generation phase, it did not overstrain the IP forwarding capacity of our Raspberry Pi during normal operation.

E. Discussion

Our three use cases have provided evidence that a straightforward learning approach is applicable to many IoT devices used in Smart Home scenarios. Two of our three IoT devices remained fully operative after FANE has monitored the network activities of our devices for 40 minutes, and has subsequently generated and activated firewall rules. Furthermore, our observations have shown that it would be easily possible to extend our learning approach to consider load balancers. As there is no communication standard for IoT devices, it is problematic to generalize our findings to all IoT devices used in the Smart Home. However, using a cloud service seems to be typical for many use cases. Only network packets can pass FANE that are allowed by a specific rule. Thus, FANE increases the security of the Smart Home installation.

FANE operates without requiring the user to possess expert knowledge, by making three assumptions: First, the network segment created by FANE's access point contains IoT devices only. This allows to specify a security policy in advance, before FANE is delivered to the user. Second, the IoT devices operate as single-purpose appliances that do not fundamentally change their communication profiles. Due to this assumption, FANE can learn a rule set that remains stable over a long period of time, which makes it compatible with the Smart Home concept. Third, we assume that the IoT devices are working properly during the monitoring phase. This allows FANE to learn firewall rules unattended.

VII. Conclusion

The last years have brought a plethora of Internet-of-Things (IoT) devices dedicated to Smart Home installations. While such IoT devices have numerous practical use cases, observations have shown that many of them come with IT-Security risks. For example, the Mirai botnet consisted of approax. 500,000 baby-phones, security cameras and other insecure IoT devices that were able to execute distributed denial-of-service attacks with 1 Tbit/s network bandwidth. However, typical Smart Home users do not possess the network-security knowledge needed to identify and deter attacks on IoT devices. Furthermore, the Smart Home concept encourages the users to leave IoT devices unattended for long periods of time.

In this paper, we have introduced FANE, our concept for a Firewall AppliaNcE for Smart Home installations. FANE makes a few realistic assumptions on the network segmentation and the communication profile of IoT devices. This allows to pre-configure FANE with a generic security concept. It also enables FANE to learn firewall rules automatically by observing the network traffic of IoT devices.

Experiments with a prototypical implementation have provided evidence that FANE can secure ordinary IoT devices without requiring network-security expertise from the Smart Home user. Only one device was not working properly after FANE has activated its firewall rules due to a specific load balancer. However, this problem could be solved by accepting IP addresses close to addresses that FANE already knows.

ACKNOWLEDGMENT

We would like to thank Eric Ilgunas for his exceptional work on realizing and evaluating the FANE prototype.

REFERENCES

[1] Nest Labs, *Nest*, https://nest.com/, Accessed: 2019-02-25.

[2] Wareable Ltd., *Amazon Echo voice control*, https://www.the-ambient.com/guides/best-amazon-alexa-commands-280, Accessed: 2019-02-25.

[3] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[4] P. P. Gaikwad, J. P. Gabhane, and S. S. Golait, "A survey based on smart homes system using internet-of-things," in *2015 International Conference on Computation of Power, Energy, Information and Communication*, IEEE, 2015, pp. 0330–0335.

[5] L. Jiang, D.-Y. Liu, and B. Yang, "Smart home research," in *Proceedings of 2004 International Conference on Machine Learning and Cybernetics (IEEE Cat. No. 04EX826)*, IEEE, vol. 2, 2004, pp. 659–663.

[6] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[7] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the ip-based internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.

[8] K. Neupane, R. Haddad, and L. Chen, "Next generation firewall for network security: A survey," in *SoutheastCon 2018*, IEEE, 2018, pp. 1–6.

[9] J. Surana, K. Singh, N. Bairagi, N. Mehto, and N. Jaiswal, "Survey on next generation firewall," *International Journal of Engineering Research and Development*, vol. 5, no. 2, pp. 984–988, 2017.

[10] G. Disterer, "Iso/iec 27000, 27001 and 27002 for information security management," 2013.

[11] Bundesamt für Sicherheit in der Informationstechnik, "BSI-Standard 200-2, IT-Grundschutz-Methodik," *https://www.bsi.bund.de*, 2017.

[12] O. of Government Commerce, *Introduction to ITIL, The key to managing IT services*. Van Haren Publishing, 2005.

[13] S. Fenz, G. Goluch, A. Ekelhart, B. Riedl, and E. Weippl, "Information security fortification by ontological mapping of the iso/iec 27001 standard," in *13th Pacific Rim International Symposium on Dependable Computing*, IEEE, 2007, pp. 381–388.

[14] S. W. Lodin and C. L. Schuba, "Firewalls fend off invasions from the net," *IEEE spectrum*, vol. 35, no. 2, pp. 26–34, 1998.

[15] K. Jaswal, P. Kumar, and S. Rawat, "Design and development of a prototype application for intrusion detection using data mining," in *2015 4th international conference on reliability, infocom technologies and optimization*, IEEE, 2015, pp. 1–6.

[16] L. S. Parihar and A. Tiwari, "Survey on intrusion detection using data mining methods," *International Journal for Science and Advanced Research in Technology*, vol. 3, no. 12, pp. 342–7, 2016.

[17] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[18] K. Golnabi, R. K. Min, L. Khan, and E. Al-Shaer, "Analysis of firewall policy rules using data mining techniques," in *2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006*, IEEE, 2006, pp. 305–315.

[19] A. K. Bandara, A. C. Kakas, E. C. Lupu, and A. Russo, "Using argumentation logic for firewall configuration management," in *2009 IFIP/IEEE International Symposium on Integrated Network Management*, IEEE, 2009, pp. 180–187.

[20] D. B. Chapman, E. D. Zwicky, and D. Russell, *Building internet firewalls*. O'Reilly & Associates, Inc., 1995.

[21] G. Kortuem, F. Kawsar, V. Sundramoorthy, D. Fitton, *et al.*, "Smart objects as building blocks for the internet of things," *IEEE Internet Computing*, vol. 14, no. 1, pp. 44–51, 2009.

[22] Procter & Gamble, *Oral-b genius electric toothbrushes*, https://www.oralb.co.uk/en-gb/products/electric-toothbrushes/oral-b-genius, Accessed: 2019-04-25.

[23] N. Gupta, V. Naik, and S. Sengupta, "A firewall for internet of things," in *2017 9th International Conference on Communication Systems and Networks*, IEEE, 2017, pp. 411–412.

[24] J. Stark, "Product lifecycle management," in *Product lifecycle management*, Springer, 2015.

[25] A. R. Khakpour and A. X. Liu, "First step toward cloud-based firewalling," in *2012 IEEE 31st Symposium on Reliable Distributed Systems*, IEEE, 2012, pp. 41–50.

[26] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *Journal of network and computer applications*, vol. 36, no. 1, pp. 42–57, 2013.

[27] ewelink, *Sonoff relay*, http://ewelink.coolkit.cc, Accessed: 2019-04-25.

[28] lingansmart, *Power outlet*, http://www.lingansmart.com, Accessed: 2019-04-25.

[29] XinweiYa Co.,Ltd., *Security camera*, http://www.cctvgood.com, Accessed: 2019-04-25.