Malware Tolerance

Report 6

Michael Denzel <m.denzel@cs.bham.ac.uk>

October 3, 2016

Supervisor: Prof. Mark Ryan
Thesis group: Dr. Flavio Garcia,
Dr. David Parker (RSMG Member)

CONTENTS

List of Abbreviations

APT	Advanced Persistent Threat
DoS	Denial of Service
HIDS	Host Intrusion Detection System
ICS	Industrial Control System
IDS	Intrusion Detection System
MITM	Man-in-the-Middle
MPC	Multi-Party Computation
NIDS	Network Intrusion Detection System
OS	Operating System
RTOS	Real-Time Operating System
SGX	Intel Software Guard Extensions
TCB	Trusted Computing Base
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
WANET	Wireless Ad-Hoc Network

1 Introduction

As recent attacks demonstrate ([3, 7]), it is challenging to give security guarantees about the honesty of a system. Former research focused on minimising the Trusted Computing Base (TCB) and mitigating attacks.

We proposed a new technique, *malware tolerance*, to deal with sophisticated attacks. Our idea is that a system of multiple independent components can distribute trust over these components in such a way that the individual component cannot meaningfully tamper with the resources.

2 Overview of Smart-Homes

Similar to Industrial Control Systems (ICSs), smart-home networks are sensor and actuator networks which control mechanisms mostly autonomous. However, smart-homes have a less structured network and less redundancy in comparison to ICSs. In addition, protocols are very vendor specific and there are various standards, like e.g. Insteon, Z-Wave, Zigbee, Thread, Bluetooth, and WiFi. [4] This lead to the development of so-called smart-home hubs which bridge between the different protocols and radio frequencies.

We assume that users will likely buy one set of products of a company to execute one task, e.g. solar panel, its meter, and its control panel are one set of products. From a vendor perspective, it makes sense that these devices utilise the same protocol – we call them a "zone" of the network. For another task, the user might buy a different set of products which use a different protocol. Thus, these zones can only communicate with each other via bridges or the smart-home hub which support multiple protocols.

Figure 1 shows and overview of a smart-home with devices being coloured depending on the threat targeting them. Critical are especially devices which represent a single point-of-failure:

- The smart-home hub enables communication between the different protocols and zones. It is, therefore, able to isolate, disrupt, and potentially shutdown zones.
- User input devices such as remote controls or Amazon Echo enable the user to adjust functionalities of a smart-home. If an attacker gets access to one of these devices, he will hold the same capabilities, effectively gaining control over the entire network.
- The electricity management system provides the smart-home with power. If an adversary compromises this part of the network, all devices are in danger of disruptions and possibly damage through power surge.
- Depending on the architecture, the home security hub could have dangerous implications on the infrastructure as it grants access to the house and manages smoke and CO detectors. It might also have further capabilities to enable emergency shutdowns in case of fire or similar.
- Lastly, since a lot of devices rely on internet access, the router can disrupt smart devices via Man-in-the-Middle (MITM) attacks or spoofed requests. It is also a central point for network surveillance.

We identified three goals an attacker could pursue: gaining control over the network, sabotage, and information theft. Control of the network likely includes the other two aims. However, sabotage and information theft are also possible without network control.

3 Idea: Malware Tolerant Smart-Home

Malware tolerance is applicable in several parts of the smart-home network, we now present the most promising ones:

- Malware-tolerant smart-home hub: At least, smart-home hub and router need to be hardened. However, it is foreseeable that these two (or more) management devices will be integrated into one device for convenience and cost saving. We, thus, either need a distributed verification mechanism that enables mesh nodes to check upon the hub or an integrated solution for the smart-home hub.
- Malware-tolerant mesh networks: Smart-home networks are moving more and more towards mesh networks, formed already by e.g. speakers to deliver sound in every room. Mesh networks are vulnerable to attacks of its own devices: black hole attacks, Denial of

Service (DoS), routing table overflows, and impersonation.

For Wireless Ad-Hoc Networks (WANETs), Zhang et al. [8] already suggested a distributed Intrusion Detection System (IDS) with local Network Intrusion Detection Systems (NIDSs) which communicate and form a global response to an attack, however, the authors exclusively rely on heuristics. Signature-based IDS are unpopular with WANETs [5, 1].

We imagine a self-managing mesh network with malware-tolerant routing and cloud assistance to analyse threats. Intrusion detection would be specification-based to detect new threats and signature-based on less powerful devices. In opposite to traditional WANETs, smart-home networks also include powerful devices with continuous power supply like the home computer or a home-server. These devices could be used for heavier computations and in depth local analysis. Likely, Trusted Execution Environments (TEEs) are necessary to analyse malicious code securely.

The cloud is used to check hashes of potentially malicious files. If a file does not exist yet, an extensive set of Host Intrusion Detection System (HIDS) heuristics are applied locally in the mesh network to estimate the risk of the threat while protecting privacy. The anonymous results are uploaded to the cloud. If the file cannot be classified locally, it is uploaded to the cloud where further analysis takes place. In both cases, updates and signatures are created in the cloud and are distributed to all mesh networks.

Before detection, the malware-tolerant routing protocol has to prevent entirely compromised devices (including TEEs) from harming the network. For this, routing has to be tolerant to the aforementioned attacks.

4 Conclusion

Our next steps will be to research malware-tolerant smart-home networks focusing on mesh networks.

References

[1] M Alnaghes and Fayez Gebali. A survey on some currently existing intrusion detection systems for mobile ad hoc networks. In *2nd International Conference on Electrical and Electronics Engineering, Clean Energy and Green Computing (EEECEGC)*, 2015. URL https://www.researchgate.net/profile/Natalie_Walker4/publication/277258314_Proceedings_of_Second_International_Conference_on_Electrical_and_Electronics_Engineering_Clean_Energy_and_Green_Computing_Konya_Turkey_2015/links/556567c008ae89e758fda04f.pdf#page=14. accessed: 2016-09-30.

[2] David Drummond. A new approach to china. online (official Google blog), January 2010. URL https://googleblog.blogspot.co.uk/2010/01/new-approach-to-china.html. accessed: 2016-07-27.

[3] Ralph Langner. Stuxnet: Dissecting a cyberwarfare weapon. *Security & Privacy, IEEE*, 9:49–51, Nov 2011. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5772960. accessed: 2014-08-06.

[4] Chun Liew. The smart home radio protocols war. online, 2015. URL http://www.iot-now.com/2015/08/10/35653-the-smart-home-radio-protocols-war/. accessed: 2016-09-19.

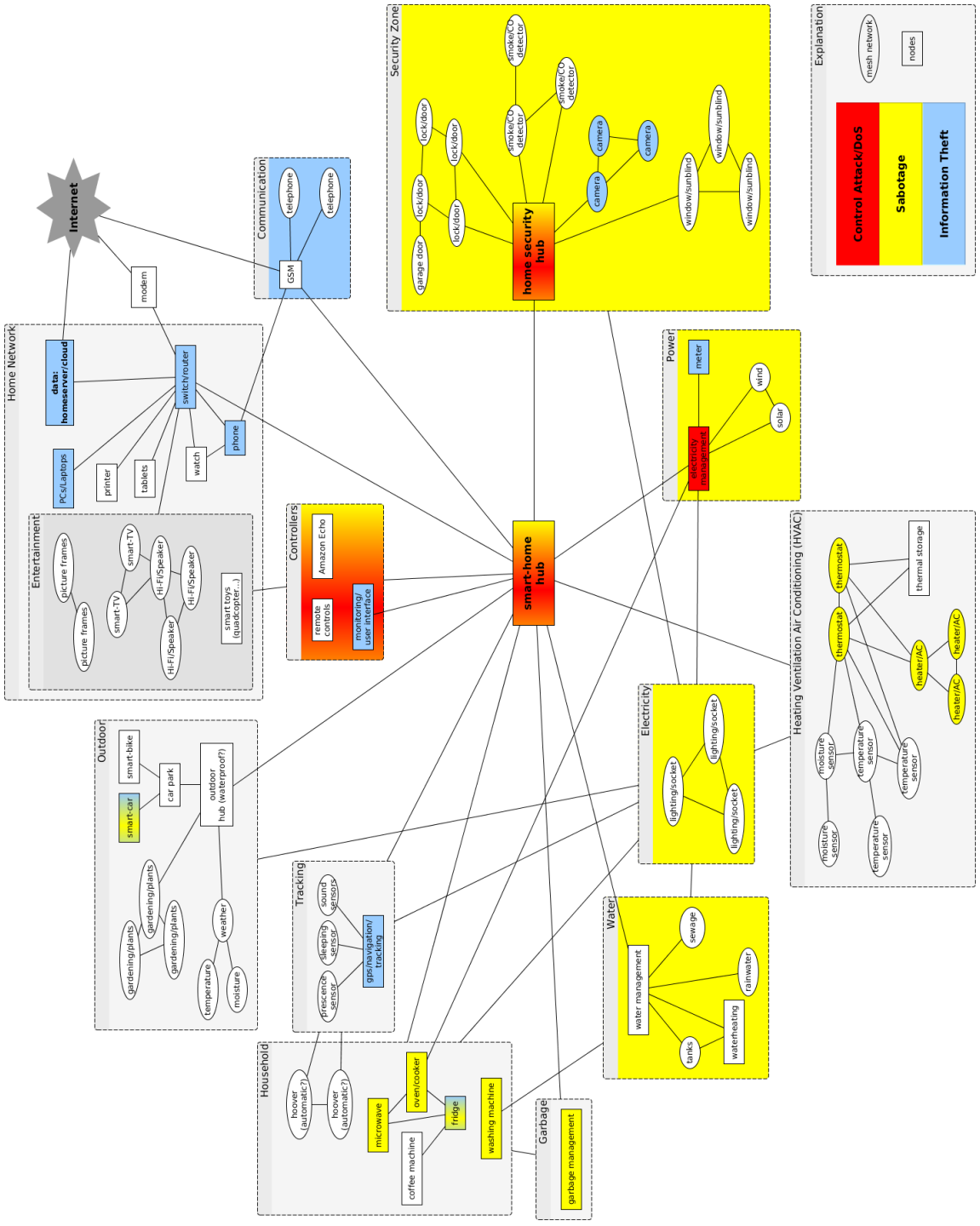
[5] Amitabh Mishra, Ketan Nadkarni, and Animesh Patcha. Intrusion detection in wireless ad hoc networks. *IEEE wireless communications*, 11(1):48–60, 2004. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1269717. accessed: 2016-09-30.

[6] Craig Schmugar. More details on "operation aurora". online (McAfee), January 2010. URL https://blogs.mcafee.com/mcafee-labs/more-details-on-operation-aurora/. accessed: 2016-07-27.

[7] Nikos Virvilis, Dimitris Gritzalis, and Theodoros Apostolopoulos. Trusted computing vs. advanced persistent threats: Can a defender win this game? In *10th International Conference on Ubiquitous Intelligence and*

Figure 1: Example Network of a Smart-Home

Threats are coloured for their severity: red are attacks that control most of the network; yellow are sabotage attacks on one part of the network; blue are devices which hold personal data. Mesh networks are displayed in circles.



Computing and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC), pages 396–403. IEEE, 2013. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6726235. accessed: 2015-02-13.

[8] Yongguang Zhang and Wenke Lee. Intrusion detection in wireless ad-hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 275–283. ACM, 2000. URL http://dl.acm.org/citation.cfm?id=345958. accessed: 2016-09-30.

Appendices

A Dissertation Outline

1. Introduction
   - 1.1. Motivation: Rootkits, Advanced Persistent Threat (APT) attacks, Shodan vulnerability scan, ICS attacks (Stuxnet [3], Operation Aurora [2, 6] etc.)
   - 1.2. Previous research: Mitigating attacks, IDS, detection, defending against a few attacks (signature/anomaly/specification based)
   - 1.3. Contributions
2. Literature review
   - 2.1. APT attacks
   - 2.2. Software vulnerabilities
   - 2.3. Intrusion detection/tolerance/prevention
   - 2.4. Sandboxing
   - 2.5. Trusted Execution Environments
     - 2.5.1. Hardware (new architectures, additional devices)
     - 2.5.2. Software (compiler)
     - 2.5.3. Virtualisation and hypervisor
     - 2.5.4. Integrated hardware (Intel Intel Software Guard Extensions (SGX), TrustZone/Knox, Trusted Platform Module (TPM))
   - 2.6. Multi-Party Computation (MPC)
   - 2.7. Self-healing systems
3. The malware tolerance concept
   - 3.1. Definition
   - 3.2. Scenarios
     - 3.2.1. E-voting
     - 3.2.2. Online banking
     - 3.2.3. ICS
     - 3.2.4. Smart-homes
     - 3.2.5. (Cloud)
     - 3.2.6. (Bitcoin)
     - 3.2.7. (Anonymity, TOR)
   - 3.3. Assumptions and attacker model
   - 3.4. Multiple TCB model
4. ARM TrustZone
   - 4.1. In-depth Presentation
   - 4.2. Security Analysis
   - 4.3. Performance Analysis TrustZone
5. User input: Smart-Guard
   - 5.1. Introduction/problem
   - 5.2. Contributions
   - 5.3. Methods: Overview

B Timetable

Table 1: Milestones

2014-03-14	Start
2014-05-19	**Report 1**
2014-06	Literature review
2014-09-20	**Report 2**
2014-10	Explored scenario “storage” under two assumptions
2014-12	Idea: double encryption
2015-01	Researched formal representation of distributed systems, Idea: Trusted input (“sign-what-you-type”)
2015-02/-03	**Report 3:** Thesis proposal
2015-05	Expanded trusted input idea, verification with ProVerif
2015-06	**Paper 1:** Smart-Guard
2015-07	Presentation at CryptoForma Workshop (CSF 2015)
2015-08	Researched TrustZone (papers, OS, *FriendlyARM* board)
2015-09-20	**Report 4**
2015-10	Researched Multi-Party Computation/Industrial Control Systems
2015-12	Reworked Smart-Guard paper
2016-01	Examined TrustZone of *FriendlyARM Mini6410*
2016-02	Researched self-healing systems; adjusted *FreeRTOS* to run on *FriendlyARM* board
2016-03/-04	Improved scenario of Smart-Guard; adjusted *FreeRTOS* to run on *FreeScale i.MX53*
2016-04-03	**Report 5**
2016-07	Smart-Guard accepted and presented at ATC 2016 (Best paper award)
2016-08	**Paper 2:** A self-healing ICS using TrustZone (submitted to NDSS)
2016-09	Researched Smart-Homes, Timing-Analysis of TrustZone
2016-10-02	**Report 6**
2017-01	**Paper 3:** Malware-Tolerant Smart-Homes
2017-03-13	Start of fourth year
2017-04-09	Report 7
2017-10-08	Report 8
2018-03-13	Submission deadline

C Attended Workshops

Table 2: Attended Workshops

Date	Workshop/Conference	Location
7th May 2014	Google Hack Day (Certificate Transparency)	Google London
19th-23rd May 2014	Academic Writing Seminar	University of Birmingham
27th-28th May 2014	CryptoForma 2014	University of York
14th-18th Jul 2014	Enterprise Summer School	University of Birmingham
23rd-24th Jul 2014	Publishing Academic Journals, Editing your writing	University of Birmingham
22nd Oct 2014	Time Management	University of Birmingham
Oct 2014 - Jan 2015	Research Skills Seminar	University of Birmingham
18th Nov 2014	Speed Reading	University of Birmingham
24th Nov 2014	Note Taking	University of Birmingham
2014	Cryptography 1	University of Stanford (Coursera)
2014 - 2015	Writing in the Sciences	University of Stanford (Coursera)
14th-15th Jan 2015	CryptoForma 2015	University of Kent
13th July 2015	CryptoForma Workshop at CSF 2015	University of Verona
31th Aug-5th Sept 2015	FOSAD Summer School 2015	University Residential Centre of Bertinoro
29th Jan 2016	RITICS meeting	Imperial College London
11th Jul-12th Jul 2016	ACE-CSR 2016	Solihull, Birmingham
18th Jul-21st Jul 2016	ATC 2016 (Best paper award)	University Paul Sabatier of Toulouse
23th Aug-26 Aug 2016	ICS-CSR 2016	Queens University Belfast