ingenieur
wissenschaften
htw saar

Hochschule für
Technik und Wirtschaft
des Saarlandes
University of
Applied Sciences

STL SYSTEMTECHNIKLABOR

(In)Security in the Internet of Things

Nico Maas

Technical Report – STL-TR-2014-02 – ISSN 2364-7167

stl.htwsaar.de

Technische Berichte des Systemtechniklabors (STL) der htw saar
Technical Reports of the System Technology Lab (STL) at htw saar
ISSN 2364-7167

Nico Maas: (In)Security in the Internet of Things
Technical report id: STL-TR-2014-02

First published: July 2014
Last revision: July 2014
Internal review: André Miede

For the most recent version of this report see: https://stl.htwsaar.de/

Title image source: Flavio Takemoto (flaivoloka), http://www.freeimages.com/photo/1153855

htw saar – Hochschule für Technik und Wirtschaft des Saarlandes (University of Applied Sciences)
Fakultät für Ingenieurwissenschaften (School of Engineering)
STL – Systemtechniklabor (System Technology Lab)
Prof. Dr.-Ing. André Miede (andre.miede@htwsaar.de)
Goebenstraße 40
66117 Saarbrücken, Germany
https://stl.htwsaar.de

(In)Security in the Internet of Things

Nico Maas
Seminar "Past and Future of Science"
htw saar – Hochschule für Technik und Wirtschaft des Saarlandes

***Abstract*—Internet of Things is the latest buzzword beeing used in the media and a new sector for the entire electronics industry. But connecting every electronic device to the internet disconnects everyone's privacy in reality. This paper examines the current problems with an normal homebased "Internet of Things" system and how the information technology industry is more concerned with profit versus user security. Ultimately, we need to decide for ourselves whether we want to continue using these types of technology.**

I. Introduction

A. Ubiquitous computing

In 1991 Xerox PARC scientist Mark Weiser published his article in the Scientific American titled: "The Computer for the 21st Century". He described what at the time was state of the art computer science, therein criticizing that using a computer to solve a problem was too complex because the user was more engaged by using the computer than attempting to solve the problem: "The state of the art is perhaps analogous to the period when scribes had to know as much about making ink or baking clay as they did about writing" [1]. The goal would be to fully integrate computers into our everyday life so that we would not even recognize their presence. We would be using them for mundane tasks such as regulating the room temperature or reading the newspaper. To accomplish that task, hundreds of networked computers in all sizes and formats would be necessary, giving way to what is known as "ubiquitous computing".

B. Internet of Things

In 1999 cosmetics marketer Kevin Ashton, held a conference titled: "Internet of Things" (IoT) at Procter & Gamble (P&G). During his speech he explained how corporations could improve their logistics and supply chains through the use of RFID chips, and also by combining and exchanging data via the Internet [2]. Shortly thereafter, Ashton became the executive director of the newly founded Auto-ID Labs at the Massachusetts Institute of Technology (MIT) [3]. He and his colleges began research on improving the technology and usage of the RFID Chips to our current standards.

C. State of the art

The IoT, as it is meant today consists of both concepts. Mark Weisers "ubiquitous computing", as well as Kevin Ashtons implementation of the RFID chips. Both ideas represent the connection of physical things, such as everyday products to the internet, making them traceable from the production, to the grocery store and then on to the user.

Weiser does occasionally need the user to interact with computer systems for specific functions. For example he imagined an alarm clock which could ask closed questions and react to yes or no answers. The alarm clock would ask the user at the set alarm time whether he/she wanted coffee or not. If so, it would turn on the coffee maker. This is an example of man to machine communication in an quite sophisticated way - using speech as if the user were engaging with another person. But there is another kind of communication, according to Ashton: The machine to machine or M2M communication. As the name implies, humans are not necessarily needed in this kind of system. For example, a parcel would be tracked in an M2M system via scanning the attached barcode or RFID Chip at the different locations it transits on its way to its destination. Another idea which combines M2M and man-to-machine would be the change of temperature, lighting and as well as the kind of music played in a room which would activate as soon as a person enters the room. An RFID chip attached to a person's clothing or watch would let the room know who entered it and change conditions to the likings saved earlier by the person in the smart home database.

D. CIA Triad

In 1975, MIT members Jerome H. Saltzer and Michael D. Schroeder wrote the IEEE Paper "The Protection of Information in Computer Systems". They identified three risks to information security (InfoSec): "1) Unauthorized information release [...], 2) Unauthorized information modification [...] [and] 3) Unauthorized denial of use [...]" [4]. These three risks were later known as the CIA Triad composed as abbreviation of the three categories of risks: confidentiality, integrity and availability of information. Due to the fact that the CIA Triad is a well-known and widely accepted model of information security, it will be used as common thread for the following analysis of security risks in the IoT.

E. Typical IoT System

Figure 1. Home IoT System

The model used in this paper will illustrate the typical IoT system as used today in households around the globe (Figure 1). The provider is acquiring data from the IoT Devices and sensors, which are installed in the household of the user, and after analyzing this data it can send back commands to the household system. For example commands which are responsible for regulating the room temperature. Provider and IoT Devices are connected via the Wide Area Network (WAN / here: Internet) Connection terminated at the end points of the Provider and User in form of routers. As the routing system of an IoT Provider is usually more sophisticated than the SOHO products used by the normal Internet User, the main concentration will be placed on the later ones, which will hence be referred to as "access" in the following proceedings.

II. Provider

There are several types of providers. Concerning IoT Devices such as Google's "Nest" Smoke Detector or Smart Meters, it is clear that the accumulated data needs to be collected and analyzed at a central point. In order to further analyze this point, two providers will be used: One for developing IoT Devices, and the other one for analyzing data collected from these devices.

A. Development - mbed.org

ARM microprocessors units (MPUs) are fitted best for IoT designs for multiple reasons: 1.) These MPUs are very small, inexpensive and energy efficient. 2.) ARM does not produce MPUs, but does only design the processor cores. These designs are sold to different companies, which then manufacture those cores with the needed peripheral interfaces (i.e. Analog Digital Converters, Powersystems, etc.). They do this to ensure that the developer can choose the system which fits their need. 3.) All ARM MPUs support the Cortex Microcontroller Software Interface Standard (CMSIS), which allows the developer to program all different ARM systems, which are manufactured by different corporations, in the same way.

mbed.org is a development platform provided by ARM for their MPUs. As the development IDE and system, as well as the data storage works completely online, several security risks are present.

In terms of confidentiality, there are absolutely no guarantees as to whether the Intellectual Property of the Developer could be kept secure over the whole product life cycle. By using an Online IDE, there is always a risk of unauthorized access or data leaks. This could occur due to problems with the used software, hackers or even through the administrators of that service, as the source code is stored on their servers. mbed.org seemed also be affected by the OpenSSL Heartbleed Bug, as they changed their SSL Certificates in April 2014 ([5]) - an proceeding only needed if an earlier compromise of those certificates - due to i.e. this OpenSSL bug has become likely.

As the confidentiality of the developed source code cannot be assured, neither can its integrity. In case of the here discussed online IDE, the implications could be severe: It could be possible to inject malware or backdoors into the source code of the MPU firmware which could later be used to monitor the IoT Device user, or even gain control over those devices. Manipulation of online hosted source code has already occurred several times and therefore is plausible ([6]).

Availability would be the last criteria to be examined: There are always disadvantages to an online IDE, compared to an offline one. The providers need to use multiple backbone connections to the internet in order to ensure an available system. Redundant servers, backups and the use of RAID systems could be implemented in order to prevent system downtimes.

B. Analysis - Xively.com

Xively is a cloud service used to analyze data from IoT Devices. It also maps them, stores them and reacts to events occurring from data changes and set thresholds. To support the development of IoT Devices, Xively provides libraries and examples for all major MPUs, as well as for the mbed.org service - and supports HTTPS, OAuth and other secure forms of communications.

Xively states "While it is possible to communicate with Xively using HTTP, this method is not secure and it is not recommended. It remains a part of the service as an element of legacy support. It is recommended to use HTTPS in all API requests: https://api.xively.com." [7]. Unfortunately, this note cannot be applied to older, 8 bit Microcontroller Units (MCUs) like Arduino Uno (Atmel ATMega328) which are still frequently used for data acquisition. This is due to their price and low energy consumption. As HTTPS is too complex to be used in this context, those MCUs connect to Xively unencrypted via HTTP.

However, even for the new ARM MPUs, mbed.org does not give access to an HTTPS library. Neither uses Xivelys official library on mbed.org the encrypted version of the REST API ([8]). So, even with the new ARM MPUs, data transfer to and from Xively remains unencrypted (Figure 2). Confidentiality as well as integrity of the received data from IoT Devices cannot be trusted because the data could be intercepted and altered without the user's knowledge or consent.

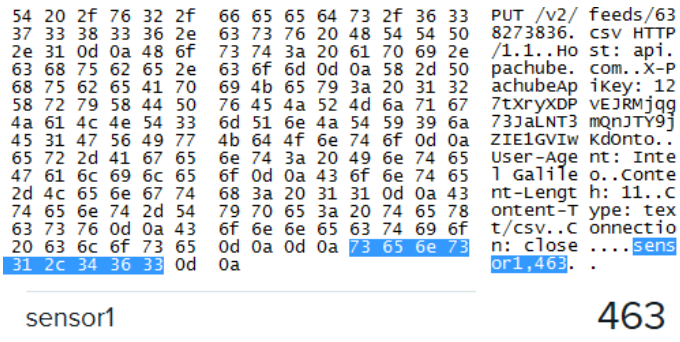

Figure 2. Wireshark Capture of HTTP Post from Intel Galileo to Xively

The collected data could also be abused in different ways, from selling the data to using it for private, perhaps even

nefarious, purposes. A quick search on Google for the words "Xively Door Sensor" gave access to the unsecured feed of an Xively IoT Device with the current state of a door - together with its GPS location data ([9]). The problem within this case is not simply a flaw in the system, but the unprotected usage of it.

As well as mbed.org, Xively seemed to be prone to the Heartbleed Bug. Even tough this was not publicly announced, the company behind Xively, LogMeIn, did explain that most of their products were affected by the Bug, due to their use of OpenSSL ([10]).

In conclusion, availability would be limited by the use of redundant systems, data lines, power supplies, storage as well as Backups.

III. Access

As previously mentioned, with Access Device the SOHO Router is meant, which connects the Home Network and IoT Devices to the Internet and to the IoT Providers. To simplify and accelerate the development of such devices, most corporations began using Linux as the operating system of their SOHO Routers several years ago. The disadvantage of this development was that unlike a specialized OS like windriver, system complexity of routers broke down to that point that it became far easier for outsiders to find errors and use them to hack the system. Once a backdoor was installed on the router, the hacker could attack the local network from the inside and gain access to other resources. In addition, they were also able to log data transfers, manipulate and pry-open SSL connections or even use multiple hacked routers as Botnet to drive a Distributed-Denial-of-Service (DDoS) attack against other hosts or networks.

A. Confidentiality

There are several other aspects which could harm the confidentiality of the data transmitted via an router. If not directly compromised by a hack router security can be altered by two other factors: a) autoconfiguration by using tools such as Universal Plug and Play (UPnP) and b) autoconfiguration by the Internet Service Provider (ISP) via TR-069. UPnP i.e. enables computers in the home network to alter certain features of the router which then allow their software to communicate with the Internet. In most cases, UPnP is used to automatically configure firewall settings on the router. It can disable firewall protection on different ports, making the use of it an potential security risk - as this open port could be used to attack the OS and eventually the entire network. TR-069 even enhances those possibilities to that extend, that the ISP can configure every setting in the router and can even push software updates to the device. Manipulation of the ISPs Auto Configuration Server could therefore compromise a large number of SOHO Devices.

B. Integrity

In order to ensure the integrity of user data which is transmitted via the router - secure configuration is vital as well as access to the latest firmware updates. Even though this has not changed in the last few years, AVM is currently one of the first corporations to include a automatic firmware update during their latest release [11]. Because Linux is used, potential security risks could linger unknown to the owner of the system. It will normally remain unknown to the user until the bug is found in an different context, for example on an Linux server with the same key component (i.e. OpenSSL). These security gaps can then be used to attack these deprecated devices which are still in use.

C. Availability

The availability and therefore the functionality of the IoT Device and Service is largely defined by the performance of the connection to the ISP. If this connection fails, the service will be cut off. As in the other scenarios like the Provider case - availability can be increased by a second line to another ISP, and the use of different technologies. There are different routers which also support dialup or a UMTS connection which can be used as a backup in case the primary broadband connection should fail. Availability is also decreased by security flaws in the OS. The mentioned UPnP system i.e. has also been implemented in insecure ways by several router manufactures. Metasploit developer Rapid7 disclosed that more than 81 million networked systems did respond to UPnP queries - which they should not, as UPnP should only be available on the inside of the network. Even more concerning, Rapid7 stated that "23 million fingerprints match a version of libupnp that exposes the system to remote code execution." [12], which means that 23 million devices could be used to run any given code - and therefore compromise the whole network. But UPnP is not the only possibility which is known - and has not been repaired - to enter the system: In January 2014, IT journal Golem released an news article which stated that reverse engineer Eloi Vanderbeken had found an open port on his Linksys SOHO router [13]. By using telnet on the undocumented Port 32764, he could access the configuration data of the router, as well as change it, paving the way for further attacks. As he decided to look further into this problem, he found out that not only Linksys, but also Netgear, Diamond, Cisco and other routers were vulnerable to this attack. The reason for this vulnerability was due to the fact that all of these manufactures used DSL Modems by the Taiwan Corporation Sercomm, which added this debug interface to their chipsets. Netgear did react to those claims and released new firmware for several routers to address this problem. When Vanderbeken conducted a follow up analysis, he found the backdoor was still present [14]. The only change was that the backdoor had to be activated by a specially crafted packet. Once activated it would perform the same way. The only problematic thing was, that from this point on, the backdoor could only be triggered by attacking from inside the LAN or attacking directly from the ISP. But using the well-known techniques of Cross Site Request Forgery and DNS Rebinding, introduced by Craig Heffner at the Blackhat 2010 [15], even those "limitations" seemed unproblematic.

IV. IoT Devices

IoT Devices come in different shapes and functions, just like Mark Weiser already predicted. The range includes simple environmental sensors like smoke detectors, internet enabled actuators like lamps, TV screens and more - forming complex home, city or power grid control systems - consisting of many simple sensors and actuators, combined through software and big data analysis. The possibilities are endless, but so are the pitfalls to privacy. The IoT is not only present in a niche, but in very different types of use. There are IoT Applications for Smartgrids, Smarthomes, Smartcities - as well as applications in the Wearables and Medical sector.

As there are so many different types of IoT Devices and usage scenarios there are also a nearly endless amount of corporations, research institutes and private hobbyists who have designed different frameworks. Even the European Union had their own consortium, IoT-A, to conduct research on the IoT sector. Because there are so many different frameworks, architectures and vendor-specific implementations there are also many different kinds of security problems, in addition to those written about in George Orwells "1984".

A. Confidentiality

As shown in the described case of the Sercomm DSL Modem, there is always the risk of backdoors integrated on a IoT Device. This can happen with or without the knowledge of the manufacturer. This was made evident with the recent case concerning the interception and manipulation of Cisco Equipment by the NSA [16]. With those modifications in place it would be possible to access stored information and even compromise their integrity and the overall availability of the device.

The same thing applies to the concept of master-codes which were previously used to unlock a device if an administrator had forgotten their password. Today, the possibility to use such hidden master-codes via networked connections could become a security threat.

There were common security measures to ensure that the user, which claimed to be at the site and resetting the password of an server, was really in front of the server. Therefore meaning they were allowed to make changes. Cisco accomplished this on an older version of their Voice over IP System called "Callmanager" in terms of having the user insert and eject the main cd into the cd drive. That used to be a good idea, but as those servers are no longer physical, inserting and ejecting a cd became mounting and un-mounting an image file - which could be done from anywhere.

As already mentioned while discussing the providers, implementing secure encryption for both data storage and data communication is vital to uphold the confidentitality of the captured or processed data.

B. Integrity

While secure encryption can keep the confidentiality of data, it is also important to secure data integrity in terms of the use of hash algorithms and similar concepts. As corporations start to realize the huge gap between the need for strong security (i.e. private / public key algorithms) and the inexpensive and simple IoT Devices, different projects were founded to ensure the communication of IoT Devices would work according to the Security Goals of the CIA Triad.

One of these projects was the "E-Lock" Chip, presented by the electronics publisher Elektor in March 2014 [17]. The publisher even held a competition about hacking the E-Lock, which ended in May 2014 without a successful hack. Devices like those are certainly the right way to ensure security in IoT, however, these devices need ongoing firmware support to prevent security breaches. Additionally, hardware encryption chips with reliable and proven security measures will also be needed.

For example, Atmel among other corporations does produce chips for hardware security like the ATECC108, performing Elliptic Curve Digital Signature Algorithm (ECDSA) - an asymmetric cryptographic measure, in order to ensure confidentiality and integrity of data communication [18]. However, this algorithm uses elliptic curves, which are known to have been exploited during their development by the NSA [19]. In theory, this chip would perform its task secure and correctly. The result may not be as secure as the implemented algorithm could have some pre-programmed weak points.

Fast, secure and reliable firmware upgrades are also vital for the security and functionality of IoT Devices.

C. Availability

The need for the availability of an IoT Device is largely defined by its role and purpose. For example, if a single temperature sensor would reboot every day for the duration of a minute, it would not be that problematic in a privately owned weather station. In contrast if large parts of a smart grid system would repeatedly "go down" this could have dramatic effects, which have been simulated in different scenarios - where a worm had infected smart meters and began to under- and over load power plants. Depending on the usage and importance of the device it can be necessary to provide a backup in case the primary device fails. The same back-up principle applies to both the device and to the network connection to the router.

V. Stakeholders

The final factor to consider in IoT Security is the human factor. There are many different stakeholders involved in the IoT with different, and sometimes conflicting, purposes and ideas.

A. IoT developing Corporations

For different corporations in the high technology sector, IoT is the next big thing. Millions of households should be equipped with smartmeters, complete cities with sensor arrays and car companies want to include car2car communication. It is clear that every corporation is highly competitive on the market and that is one reason why it is very difficult to get those corporations to cooperate on certain aspects of IoT.

B. IoT using Corporations

The just in time production with limited storage capacities of today would not be possible without IoT technology, such as: 2D barcodes, RFID chips, GPS and real time tracking. Especially corporations in the logistics, vehicle, environmental and health market could profit from the new solutions and increase production efficiency and improve their products.

C. Governments

Governments try to save costs and improve the quality of life of their citizens. In the interest of public safety many governments have started to monitor not only their citizens, but also other nations. This trend will continue to increase with the installation of more and more IoT Devices. The magazine "Wired" wrote about former CIA Director David Petraeus's enthusiasm for IoT in 2012: "We'll Spy on You Through Your Dishwasher" [20].

D. Citizens

Normal citizens want to streamline their lives with personal digital assistants, increase comfort with smart homes, and reduce overall costs and energy consumption. Recent generations tend to become "early adopters" who quickly use the latest technology as soon as it hits the market. They are decreasingly concerned about protecting their privacy and are used to paying for convenience with their personal privacy. This trend is alarming and can only be changed temporarily through massive security flaws like discovered on WhatsApp, pushing the User to look for secure alternatives. Shortly after these incidents, users return to unsecure applications because of comfort.

E. Criminals

For criminals, the IoT gives completely new possibilities in terms of taking control over such networked systems. This could manifest itself in rather boring attacks with turning on and off light bulbs or flushing IoT enabled toilets [21], to the extent of cutting off whole countries from energy grids. If criminals are not trying to attack IoT Devices to spy on persons or to cause harm, they could still use these devices to attack other systems. This already happened as security corporation Proofpoint has shown in their recent tech report: "More than 750,000 Phishing and SPAM emails [were] Launched from 'Thingbots' Including Televisions, Fridge[s]" [22]. A user could not only manipulate the IoT Devices to spam the net with unwanted advertisements, but criminals could also use these devices to create Distributed Denial of Service (DDoS) attacks, as with the afore mentioned SOHO routers.

VI. Conclusion

The IoT is an interesting and powerful idea which will rapidly expand within the next few years and ultimately become commonplace. However, there are still a lot of different and extensive security problems. It is important for the industry to implement more standardized solutions and develop secure means of communication such as: authentication and authorization in the context of IoT infrastructures, as well as secure processing of this data and automated firmware updates. This also includes longer support life spans for IoT enabled devices, which most manufactures refuse to implement due to the corresponding costs. As Bruce Schneier put it, "We have to put pressure on embedded system vendors to design their systems better." [23]. In my opinion, we need to decide for ourselves whether we want to continue using these types of technology - or not.

References

[1] M. Weiser, "The Computer for the 21st Century," *Scientific American*, pp. 94–104, September 1991. [Online]. Available: http://doi.acm.org/10.1145/329124.329126

[2] K. Ashton. (2009, June) That 'Internet of Things' Thing. RFIDJournal. Last visited: 2014.06.11. [Online]. Available: http://www.rfidjournal.com/articles/view?4986

[3] J. McHugh, "Attention, Shoppers: You Can Now Speed Straight Through Checkout Lines!" *wired*, vol. 12.07, July 2004.

[4] J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308, Sept 1975.

[5] S. Paulger. (2014, April) mbed.org SSL certificate change. Last visited: 2014.06.13. [Online]. Available: https://mbed.org/blog/entry/mbedorg-SSL-certificate-change/

[6] G. Himmelein. (2012, March) GitHub-Sicherheitslücke kompromittiert alle Projekte. heise. Last visited: 2014.06.13. [Online]. Available: http://www.heise.de/security/meldung/GitHub-Sicherheitsluecke-kompromittiert-alle-Projekte-1463891.html

[7] Xively. (2014, June) Xively REST API Security. Last visited: 2014.06.13. [Online]. Available: https://xively.com/dev/docs/api/security/

[8] ——. (2013, November) Xively Jumpstart Demo. Last visited: 2014.06.13. [Online]. Available: http://mbed.org/users/xively/code/xively-jumpstart-demo/

[9] xose. (2013, January) Door Sensor. Last visited: 2014.06.13. [Online]. Available: https://xively.com/feeds/95931

[10] LogMeIn. (2014, June) Heartbleed FAQ. Last visited: 2014.06.13. [Online]. Available: http://help.logmein.com/SelfServiceKnowledgeRenderer?type=FAQ&id=kA0a0000000siJ3CAI

[11] M. Förster. (2014, June) FritzBox aktualisiert sich künftig automatisch. Last visited: 2014.06.13. [Online]. Available: http://www.heise.de/security/meldung/FritzBox-aktualisiert-sich-kuenftig-automatisch-2217755.html

[12] H. Moore, "Security Flaws in Universal Plug and Play," Rapid7, Whitepaper, January 2013, Last visited: 2014.06.15. [Online]. Available: https://community.rapid7.com/docs/DOC-2150

[13] F. Greis. (2014, January) Hintertür in WLAN-Routern entdeckt. Last visited: 2014.06.15. [Online]. Available: http://www.golem.de/news/sicherheit-hintertuer-in-wlan-routern-entdeckt-1401-103685.html

[14] E. Vanderbeken, "How Sercomm saved my Easter!" synacktiv, Tech. Rep., April 2014, Last visited: 2014.06.15. [Online]. Available: http://www.synacktiv.com/ressources/TCP32764_backdoor_again.pdf

[15] C. Heffner, "How to Hack Millions of Routers," Blackhat, Tech. Rep., 2010, Last visited: 2014.06.15. [Online]. Available: http://media.blackhat.com/bh-us-10/presentations/Heffner/BlackHat-USA-2010-Heffner-How-to-Hack-Millions-of-Routers-slides.pdf

[16] S. Gallagher. (2014, May) Photos of an NSA 'upgrade' factory show Cisco router getting implant. arstechnica. Last visited: 2014.06.15. [Online]. Available: http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

[17] elektor. (2014, April) E-Lock makes the Internet of Things 100% secure. elektor. Last visited: 2014.06.15. [Online]. Available: http://www.elektor.com/e-lock

[18] Atmel, *Atmel ATECC108 Datasheet*, Atmel, October 2013, Last visited: 2014.06.15. [Online]. Available: http://www.atmel.com/Images/Atmel-8873S-CryptoAuth-ATECC108-Datasheet-Summary.pdf

[19] J. Menn. (2014, March) Exclusive: NSA infiltrated RSA security more deeply than thought - study. Last visited: 2014.06.15. [Online]. Available: http://www.reuters.com/article/2014/03/31/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331

[20] S. Ackerman. (2012, March) CIA Chief: We'll Spy on You Through Your Dishwasher. wired. Last visited: 2014.06.16. [Online]. Available: http://www.wired.com/2012/03/petraeus-tv-remote/

[21] J. Thoma. (2014, Juni) Internet of Things: Angriffe auf den Haushalt. heise. Last visited: 2014.06.16. [Online]. Available: http://www.golem.de/news/internet-of-things-angriffe-auf-den-haushalt-1406-107172.html

[22] I. Proofpoint. (2014, January) Proofpoint Uncovers Internet of Things (IoT) Cyberattack. Last visited: 2014.06.11. [Online]. Available: http://www.proofpoint.com/about-us/press-releases/01162014.php

[23] B. Schneier. (2014, January) The Internet of Things Is Wildly Insecure - And Often Unpatchable. Last visited: 2014.06.16. [Online]. Available: https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html