di.sy

Technical Report
KN–2017–DISY–02

Distributed Systems Laboratory

MoDeNA: Enhancing User Security for Devices in Wireless Personal and Local Area Networks

Robert Müller **Marcel Waldvogel**

Distributed Systems Laboratory
Department of Computer and Information Science
University of Konstanz – Germany

Corinna Schmitt

Communication Systems Group CSG
Department of Informatics IfI
University of Zurich UZH – Switzerland

Today most used devices are connected with each other building the Internet of Things (IoT). They communicate with each other directly and share data with a plethora of other devices indirectly by using the underlying network infrastructure. In both cases a variety of protocols are used depending on infrastructure, application (e.g., Smart City, eHealth), and device capability. But the overall concept of the data sharing is to do it in a secure manner so that different users (e.g., consumer, facilities, provider) can gain benefits. But what does "secure manner" means? This is a big question between the stakeholders, especially when talking of wireless personal and local area networks (WPANs) and wireless local area networks (WLAN), because the judgment of the security feeling depends on personal settings (e.g., easy to use, encrypted transmission, anonymization support). Therefore, MoDeNA – a Mobile Device Network Assistant – was developed offering an opportunity for understanding the judgment of security by bringing the user's concerns and their technology understanding of used devices and protocols into relation. MoDeNA provides a transparent overview over the used wireless security of the user's device giving concrete advices for improving the connection security, helping to improve usability of mobile device security. As a use-case the smart city environment is used, because this is the most common area, where many different WPAN and WLAN connections exist, supported by different underlying infrastructures, and where secure data transmission is essential, because it is an "open communication area".

Table of Contents

1 Motivation

The Internet of Things (IoT) not only includes servers, computers, and routers anymore, but also personal "smart" devices that everyone uses frequently, such as smartphone, sensors, tags, and tablets. All devices collect many data in different application areas and are connected to share the data [1, 2]. It is envisioned that the variety of devices will grow in the future as well as the number of participating devices in the IoT [3]. As long as the user is aware of the established connections using special applications such as tracking options or Bluetooth communications, secure communication is assumed. This fact might be correct, if the user owns the network and has also the ability to configure the infrastructure correctly, including security settings in the device and for the communication way. But as soon as the user lefts the trustworthy environment (e.g., own network, home) the situation changes completely. Assuming the user now walks in a city using all available free wireless connections, the question is if the communication is secure at all. Usually in such a smart city environment different WLANs are established answering the mobility request of the people to be online all the time. Those WLANs are usually configured based on personal setting of the providers building a WPAN. This means for the external user that WPANs normally do not give the users (visitors) the opportunity to configure the security settings as they request them. Sometimes the visitors are even not informed at all what security is used for the connection. This is a big problem as soon as the visitor wants to transmit confidential information (e.g., health data, positioning information, private messages).

Parallel to this problem with the used unknown infrastructure the device capabilities bring another problem to the setting and judging of the security supported. Not every device has the capability to support every security standard (e.g., SSL, TLS, SHA-2, AES), because they are either constraint in memory, power, or computation. Further, not every user knows about this fact or is even able to find out about it and how to configure the device used. Usually, a user is just a user of the device or the application, trusting in the pre-installed security mechanisms.

In order to allow a judgment of the used security, MoDeNA — our **Mo**bile **De**vice **N**etwork **A**ssistant — was developed addressing the aforementioned to views of the users abilities and the deployed network infrastructure in a smart city environment. MoDeNA is an operating system independent application based on an classification algorithm taking into account all available security information from user's device and used infrastructure to make the security setting transparent to the user. Further it recommends the user updates of security settings to improve the mobile device security for the current situation without requiring in-depth know-how. The overall goal of MoDeNA is to raise the user's awareness of security lacks when using WPANs and WLANs to provide countermeasures to avoid data theft.

The remainder is structured as follows. First, in Section 2 background information about classic used WPANs and WLANs in smart city environments is presented with focus on used protocols. Followed by a model design description for MoDeNA's security classification algorithm in Section 3. Implementation details are presented in Section 4. As a proof of concept a smart city environment is assumed to allow a user study of MoDeNA as presented in Section 5. Finally, the paper is concluded and future steps are mentioned in Section 6 to improve the current version of MoDeNA.

2 Related Work

The challenge of providing security to WPAN and WLAN for connecting a users personal devices is a research field actively studied for IoT devices.

While there are calls for novel security challenges for the services of the IoT like encryption and authentication [4], proposals for securing the IoT with protocols like Lithe (lightweight DTLS) [5], TinyDTLS [6, 7] are available. Additionally, analyzes exist that investigate the technical challenges and limitations of the IP-based IoT [8, 9], though the aspect of involving the user in the security of the connection between IoT devices is not considered. To our knowledge there is no known approach to involve the user in the wireless network security, particularly not for IoT devices.

Since version 6.0 of the Android OS, there is a build-in permissions app that lets the users specify which information third party applications are allowed to access on the smartphone, e.g., calendar items, storage, sensors, or location information [10]. This allows users to restrict access for less trusted applications. However, it does not cover wireless network usage and wireless network security yet. Work in the field of discovering network topology without network assistance is described in [11]. A user study analyzing security and privacy habits as well as willingness to apply counter measurements is provided by [12]. Another interesting approach is investigated in [13] by moving privacy-sensitive tasks to remote security servers which offer higher protection capabilities than smartphones.

3 MoDeNA's Security Classification Algorithm

Based on the presented challenges in Section 2 with existing solutions, the following goals were set for MoDeNA to build a security classification scheme:

Central Overview. Connected IoT devices for different types of used wireless networks shall be displayed in a single view.

Automatical Identification. Security requirements in the communication way between the IoT device and its application shall be automatically identified by MoDeNA.

User Interaction. MoDeNA interaction with the user shall be possible, in case information is not available, by answering concrete questions about the setting (e.g., Was the pairing within proximity of 2 meters? Did you enter a PIN code for pairing? Were there any other device nearby that could have been wrongly paired? Were there suspicious strangers nearby? Can you uniquely identify the one device being paired with?).

Control Wireless Radio Connections. It shall be easy for the user to keep track of wireless communications to his/her IoT devices with MoDeNA.

In order to address the first goal the connected IoT devices are classified according to the security standard required by the data transmitted. Reading device specific information, such as shared services for communication, applications used, and identifying device classes can achieve this without user interaction required for an automatic identification. Additional information provided

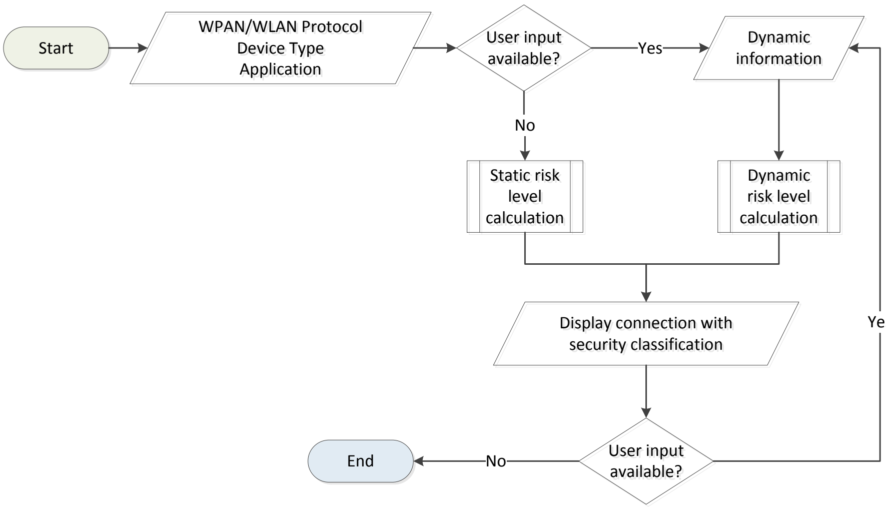


Fig. 1. MoDeNA classification algorithm

by the user about the pairing process, if available, is used for a more precise identification of security requirements.

The classification itself is a process that needs to be adopted for the various available device types and WPAN/WLAN protocols. Therefore, existing parameters for classification were used building the "static input (e.g., device identifiers, announced services, Universally Unique Identifier UUID) and if necessary "dynamic input" based on the user's manual input. The general security classification algorithm is illustrated in a flow diagram in Figure 1.

The MoDeNA classification algorithm takes the protocol type, device type and application of the device to be connected with as input values. They are obtained automatically by the WPAN/WLAN network sensors and connection information published in the network (e.g. via network service) by the device. If there is input regarding connection purpose available from the user ("Dynamic Information"), this information is considered for a dynamic risk level calculation. Otherwise a static risk level calculation without additional user input is applied. Afterwards the newly established connection is displayed together with its security classification. If new user input becomes available (i.e. the user confirms an security improvement measure within the application) a new dynamic risk level calculation is executed. Otherwise the algorithm terminates.

After performing this security classification algorithm a judgment of the existing settings is done concerning application security requirements and risk classification of the connection. Concerning the application security requirements three levels are distinguished having user-friendly grading in mind:

- High connection security provides state-of the art security enabled by a key exchange mechanism with no known practically exploitable design flaws and a secure transmission encryption, such as AES.
- Acceptable connection security indicates security consisting of a key exchange mechanism with design flaws which cannot easily be exploited. It also uses a secure transmission encryption and no significant general protocol weakness that may only be broken with very high effort.

- Low connection security provides insufficient data security for personal data and should only be used for non-private or non-confidential data. For the broken protocol there are known attacks against, based on the key exchange or the data transmission with weak ciphers or the complete absence of cryptography.

In order to present the user the current security status for each established WPAN/WLAN connection between his device and the connected device (e.g., network, router, other mobile device) a risk classification is visualized using MoDeNA. The classification is indicated by a four-level color code: s

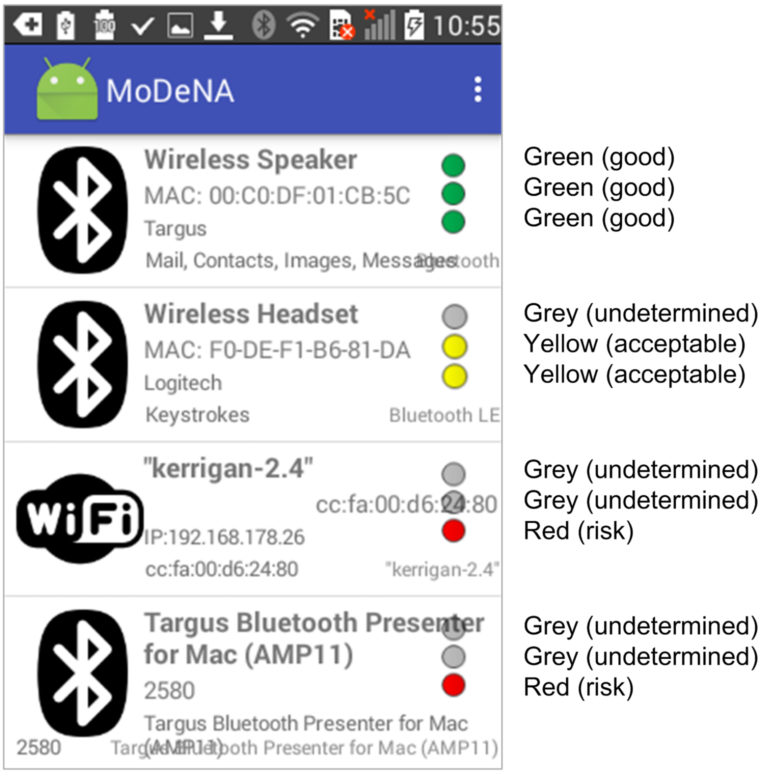
- Good (green) The risk of data theft for the type of transmitted data via the used WPAN/WLAN protocol is good. Devices communicating at acceptable good risk are by default flagged by a green indicator.
- Acceptable (yellow) The risk of data theft for the type of transmitted data via the used WPAN/WLAN protocol is sufficient. Devices communicating through a medium risk connection are flagged yellow.
- At risk (red) The risk of data theft for the type of transmitted data via the used WPAN/WLAN protocol is insufficient. Devices communicating at risk are by default flagged by a red indicator. The protocol is not secure for the used application and IoT device. This is not recommended!
- Undetermined (grey) Devices that the user is well aware of and which he does not want to be warned about by opting out manually in the detail view. Devices communicating at undetermined risk are by default flagged by a grey indicator.

Figure 2 illustrated the "MoDeNA Overview screen" assuming the used smartphone has four possible wireless connections in range at the moment. Three of them, namely Wireless Speaker, Wireless Headset, and Bluetooth Presenter for Mac (AMP11), are identified as Bluetooth devices with their Bluetooth address and category of usage. The security is is classified as good, acceptable and at risk respectively as indicated by the bullets on the right part of the screen. The fourth connection, called kerrigan-2.4, is identified as Wi-Fi network including its MAC- and IP-address with a not secure connection. The fourth classification (undetermined / grey) is not shown in this sample.

Figure 3 shows the "Detail view" for one device (here: Wireless Headset). The view contains the rationale for the security classification and useful hints. A user can answer an additional question to increase the security level, which causes the security classification to be recalculated by the MoDeNA algorithm.

Besides the current analysis of the security status at the moment MoDeNA also provides information how to improve the connection, e.g., moving from red to yellow or yellow to green. This is done for the specific connections by offering the user a link to a more detailed web page presenting background information about the connection type, the known security risks, and recommendations for security enhancements as illustrated in Figure 3.

For example, take the wireless LAN "kerrigan-2.4" shown in Figure 2. It is automatically detected by the smartphone with activated Wi-Fi service as someones private network, though it does not require authentication via WEP/WPA2 and the smartphone connects to it automatically. When an user of MoDeNA application detects it in the Overview Screen, it is listed as a network interfaced with. Since there is no authentication provided, it is rated not secure by the



10:55

MoDeNA

Wireless Speaker
MAC: 00:C0:DF:01:CB:5C
Targus
Mail, Contacts, Images, Messages Bluetooth

Green (good)
Green (good)
Green (good)

Wireless Headset
MAC: F0-DE-F1-B6-81-DA
Logitech
Keystrokes Bluetooth LE

Grey (undetermined)
Yellow (acceptable)
Yellow (acceptable)

"kerrigan-2.4"
cc:fa:00:d6:24:80
IP:192.168.178.26
cc:fa:00:d6:24:80 "kerrigan-2.4"

Grey (undetermined)
Grey (undetermined)
Red (risk)

Targus Bluetooth Presenter for Mac (AMP11)
2580
Targus Bluetooth Presenter for Mac (AMP11)
2580 Targus Bluetooth Presenter for Mac (AMP11)

Grey (undetermined)
Grey (undetermined)
Red (risk)

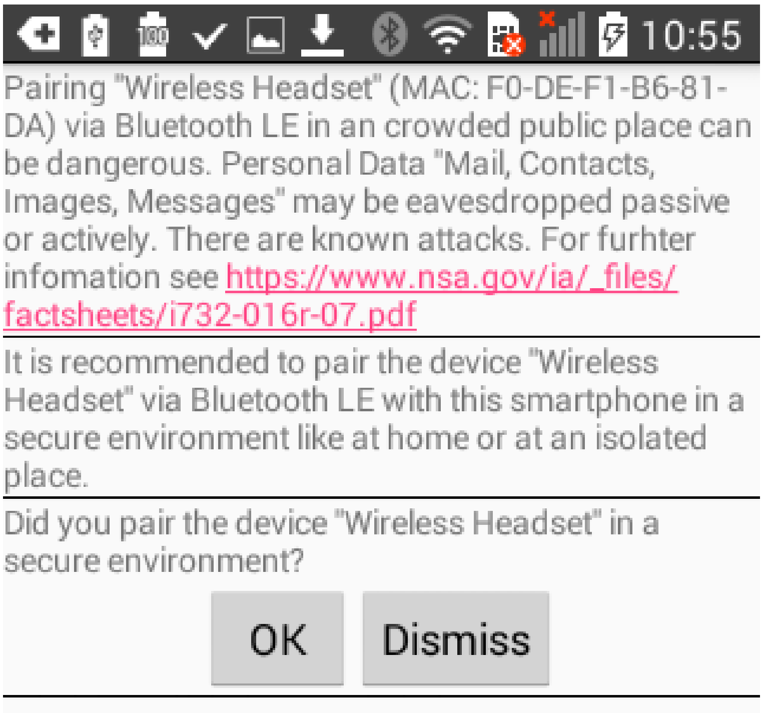
Fig. 2. MoDeNA view with connected WPAN/WLAN devices.

MoDeNA application. If the user now clicks on the list entry, he/she is brought to the detail view, which shows the reason for this security classification (red indicator) and what measures can be applied to improve connection security with “kerrigan-2.4” by adopting them. Settings and measurements made for known networks can be saved automatically by MoDeNA.

For further information about the security risks of using a specific WPAN/ WLAN technology to communicate with a device the application presents the user with links to useful web pages on the Internet that provide further information about what causes the risk and it’s severity plus background information. This is also used to educate the user about the wireless network protocols used. To omit security improvement recommendations, opting-out of a classification for a new connection by choosing “I know the risk!” at the detail screen is provided for any special cases.

4 Implementation

To analyze our classification algorithm with a physical device we implemented a prototype of the application MoDeNA. It is realized on the Android OS platform, since it is the most widely used operating system to date for smartphones. The application MoDeNA was then also used for the following user study in Section 5. For the physical WPAN/WLAN interfaces we use the available interfaces for



Pairing "Wireless Headset" (MAC: F0-DE-F1-B6-81-DA) via Bluetooth LE in an crowded public place can be dangerous. Personal Data "Mail, Contacts, Images, Messages" may be eavesdropped passive or actively. There are known attacks. For furhter infomation see https://www.nsa.gov/ia/_files/factsheets/i732-016r-07.pdf

It is recommended to pair the device "Wireless Headset" via Bluetooth LE with this smartphone in a secure environment like at home or at an isolated place.

Did you pair the device "Wireless Headset" in a secure environment?

Fig. 3. MoDeNA Detail View with security recommendations.

two current and widely spread smartphones of the manufacturers Apple [14] and Samsung [15].

The user interface is separated into two views: (1) Overview screen and (2) Detailed view screen.
The **Overview Screen** shown in Figure 2 presents the user with an Security classification state per connected smart device. Clicking on a row opens the devices Detail View screen.

The **Detail View Screen** shown in Figure 3 presents the user with practical security hints and asks for input of environmental parameters to improve classification. The application back-end provides adapter implementations for the supported physical network interfaces and listens asynchronously for connected devices available. First, it identifies whether a device was previously connected. For new detected devices, the MoDeNA application collects the protocol- and device specific information and creates a new entry in the devices database. Previously known devices can be recognized and the security classification is based on the available device history. For each device the database stores a dataset consisting of: device name, type, address, last security classification, performed security improvements by the user and used application. Based on this information, the MoDeNA algorithm is applied to determine the security requirements and obtain the security classification. This is then used to provide the user with recommendations for each specific combination of device type and security requirement. Table 1 shows a selection of identified available IoT devices (column "Device") with various Wi-Fi and Bluetooth capabilities (column "Protocol").

Device	**Protocol**	**Security**
Smart Watch	Wi-Fi , Bluetooth	High
Wearable Fitness	Wi-Fi, Bluetooth	Low/Acceptable/High
Wireless Speaker	Wi-Fi, Bluetooth	Low
Wireless Headphone	Wi-Fi, Bluetooth	Acceptable
Wireless Headset	Wi-Fi, Bluetooth	Acceptable
Hearing Aid	Bluetooth	Low
Wireless Keyboard	Wi-Fi, Bluetooth	High
Wireless Mouse	Wi-Fi, Bluetooth	Acceptable
Wireless Door key	Wi-Fi, Bluetooth, Bluetooth LE	High
Wireless Presentator	Wi-Fi, Bluetooth, Bluetooth LE	Acceptable

Table 1. IoT devices and typical network protocols

The column "Security" gives the identified security requirement for the IoT devices based on the used protocol(s).

5 User Study

We conducted a two-part user study to analyze usage of IoT devices connected to smartphones via WPAN/WLAN and to rate the use of our application. The participants were asked to fill in a questionnaire with 23 questions while using the application MoDeNA for the second part of the study. For the evaluation, we used a mock-up of our proposed application without the implementation of the classification of the real network connections. The following limitations apply to the generalization of the results presented in our study. 11 out of 23 participants come from a technical background and are more likely to be interested in the technical mechanism of WPAN/WLAN and aware of data security than the average smartphone user. Therefore we decide to differentiate the results for certain answers based on this question. The age group is distributed with the majority participants in the age group of 26-35. For a universal conclusion more participants would be required.

The performed user study was divided in two parts: (1) Wireless Network Smartphone Security and (2) Application Specific Wireless Security. The users were asked to voluntarily provide free-form feedback on the MoDeNA app. The selection of users was done randomly and included participants with many technical knowhow and less knowhow, as well as were split over different age ranges. Looking on the two different evaluation part of the study, the following results were received.

Focusing on "Wireless Network Smartphone Security" (Part 1) 48% of our participants have a technical background (work or education). The interest rate in understanding wireless smartphone communication is 91% for non-technical and 67% for technical users. 87% of participants would rate data on their smartphones as private data. 70% know about security concerns of data stored on smartphones but they accept the possible risks. 87% of the participants ask for more protection of their personal data stored on their smartphone. In questions 14 and 15, we asked the users whether they turn off unused wireless protocols. 65% of the users do turn off radio, but for reasons like battery, radiation and others, only 22% of them do it also because of security concerns. 83% of participants state that they would apply security measures, if their smartphone recommended them to do so.

Focusing on "Application Specific Wireless Security" (Part 2) the users were requested to play around and evaluate our prototype implementation of the application MoDeNA. Thus, these received feedback was user-specific and highly influenced by individual knowhow.74% of participants state that they gained insight in the security of wireless smartphone communication. The same percentage of participants also claimed, that they think the application MoDeNA would improve the security when used. 87% expect MoDeNA would improve the WPAN/WLAN security of their smartphones.

Summarizing the received feedback from the performed user study it can be stated that the feedback was manifold and gave us many interesting aspects how to improve the current prototype. The user's feedback included the following main requests that are currently investigated for the envisioned upgrade go MoDeNA:

- The upcoming prototype should include a more detailed classification scheme, including an option for interested users to gain more information about the lightning system used.
- For users it would be handsome if MoDeNA would be combined with a service functionality that automatically starts when a new connection is established as well as request for manual interaction if the connection is accepted or not.
- In general, to improve the acceptance of MoDeNA itself, a tutorial should be included guiding new users how to use avoiding faulty users as well as a drop down menu to have a better overview of offered functionalities by MoDeNA (e.g., setting options, legend for lightning system).

6 Conclusions and Future Work

The security of smartphones communicating with IoT devices via wireless personal area networks (WPAN) and wireless local area networks (WLAN) is this works research domain. It is a non-homogenous field of various network protocols and applications with diverse security requirements. We present MoDeNA, a framework for detection and classification of WPAN/WLAN connection security and a prototype smartphone application for Android OS to (semi-)automatically rate the security of connected WPAN/WLAN devices and provide advices to the user. We performed a user study with 23 participants to identify the demand for and benefits of our application. In our study we showed that 70% of participants are generally aware of security risks when transmitting data wirelessly from a smartphone to any other device but nevertheless use the functionality. 78% of our participants have heard or know about security risks for WPAN/WLAN protocols. MoDeNA is rated by 90% of our user study participants to be helpful to feel more secure with smart devices in WPAN/WLAN. Comments which arose from the user study to provide a direct integration in the OS pairing mechanism of MoDeNA will further improve the acceptance of the system.

References

[1] S. Greengard, *The Internet of Things (MIT Press Essential Knowledge)*. The MIT Press, May 2015. 1

[2] International Telecommunication Union, “The Internet of Things,” *ITU Internet Reports*, 2005. 1

[3] A. Vesola, W. Schulte, and B. Lheureux, “Hype Cycle for the Internet of Things, 2016,” Gartner Inc., Stanford, U.S.A., Tech. Rep., July 2016. 1

[4] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of Things,” in *IEEE Computer Journal*, vol. 44, no. 9. New York, NY, USA: IEEE, September 2011, pp. 51–58. 2

[5] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, “Lithe: Lightweight Secure CoAP for the Internet of Things,” in *IEEE Sensors Journal*, vol. 13, no. 10. New York, NY, USA: IEEE, October 2013, pp. 3711 – 3720. 2

[6] C. Schmitt, T. Kothmayr, and W. Hu, “Two-way Authentication for the Internet-of-Things,” in *Internet of Things: Novel Advances and Envisioned Applications*, D. Acharjya and M. Kalaiselvi Geetha, Eds. New York, NY, USA: Springer, March 2017, ch. 2, pp. 27–56. 2

[7] T. Kothmayr, W. Schmitt, C. an Hu, M. Bruenig, and G. Carle, “DTLS Based Security and Two-way Authentication for the Internet of Things,” *ELSEVIER Ad Hoc Networks*, vol. 11, no. 8, pp. 2710–2723, November 2013. 2

[8] 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, December 2011. [Online]. Available: http://dx.doi.org/10.1007/s11277-011-0385-5 2

[9] R. Hummen, H. Shafagh, S. Raza, T. Voigt, and K. Wehrle, “Delegation-based Authentication and Authorization of the Ip-based Internet of Things,” in *11th Annual IEEE International Conference on Sensing, Communicatio, and Networking*, ser. SECON. New York, NY, USA: IEEE, June/July 2014, pp. 1–9. 2

[10] Google Inc., “Control your app permissions on Android 6.0 and up,” http://tinyurl.com/control-your-app, May 2016. 2

[11] R. Black, A. Donnelly, and C. Fournet, “Ethernet Topology Discovery without Network Assistance,” in *12th IEEE International Conference on Network Protocols*, ser. ICNP. New York, NY, USA: IEEE Computer Society, October 2004, pp. 328–339. 2

[12] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, “Measuring User Confidence in Smartphone Security and Privacy,” in *8th Symposium on Usable Privacy and Security*, ser. SOUPS. New York, NY, USA: ACM, July 2012, pp. 1–16. 2

[13] G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos, “Paranoid Android: Versatile Protection for Smartphones,” in *26th Annual Computer Security Applications Conference*, ser. ACSAC. New York, NY, USA: ACM, December 2010, pp. 347–356. 2

[14] Apple Computer Inc., “iPhone User Guide for iOS 8.4 Software,” Apple Computer Inc., California, United States, Tech. Rep., January 2016. [Online]. Available: https://itunes.apple.com/us/book/iphone-user-guide-for-ios-8-4/id917482340?mt=11 4

[15] Samsung Electronics Co Ltd, “Samsung User Manual SM-G920F SM-G920FQ SM-G920I,” Samsung Electronics Co Ltd, Seoul, South Korea, Tech. Rep., Januarya 2016. 4