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

Robert Müller, Marcel Waldvogel, Corinna Schmitt

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

Robert Müller[1], Marcel Waldvogel[1], and Corinna Schmitt[2]

[1] Distributed Systems Laboratory, Department of Computer and Information Science, University of Konstanz, 78457 Konstanz, Germany, [robert.mueller|marcel.waldvogel]@uni-konstanz.de

[2] Communication Systems Group CSG, Department of Informatics IfI, University of Zurich UZH Binzmühlestrasse 14, 8050 Zurich, Switzerland, schmitt@ifi.uzh.ch

**Abstract.** Today most used devices are connected with each other building the Internet of Things (IoT). A variety of protocols are used depending on the underlying network infrastructure, application (e.g., Smart City, eHealth), and device capability. The judgment of the security feeling of the data sharing depends on personal settings (e.g., easy to use, encrypted transmission, anonymization support). 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 and usability of mobile device security.

## 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]. 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 views of the users abilities and the deployed network infrastructure in a smart city environment. MoDeNA is an operating system independent application based on a 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.

## 2 Related Work

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 [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.

Work in the field of discovering network topology without network assistance is described in [10]. A user study analyzing security and privacy habits as well as willingness to apply countermeasures is provided by [11]. Another interesting approach is investigated in [12] 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: (1) Central Overview of connected IoT devices, (2) **Automatic Identification** of applied security requirements, (3) **User Interaction** support when no automatic identification happens, and (4) **Control Wireless Radio Connections** to keep track of own IoT devices.

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 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 a

security improvement measure within the application) a new dynamic risk level calculation is executed. Otherwise the algorithm terminates.

Four levels for application security requirements are distinguished: (1) High (green) - key exchange mechanism with no design flaws and transmission encryption, (2) Acceptable (yellow) - key exchange mechanism with design flaws and transmission encryption, (3) Low (red) - insufficient data security, and (4) Undetermined (grey) - by default accepted. This grading can be seen in the **Overview Screen** shown in the shown in the upper part of Figure 2. It presents the user with an Security classification state per connected smart device. Clicking on a row opens the device's **Detail View Screen** shown in the lower part of Figure 2. It advises 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 (e.g., Smart watch + WiFi and/or Bluetooth indicating High security, wireless mouse + WiFi or Bluetooth indicating Acceptable security, hearing aid + Bluetooth indicating Low security).

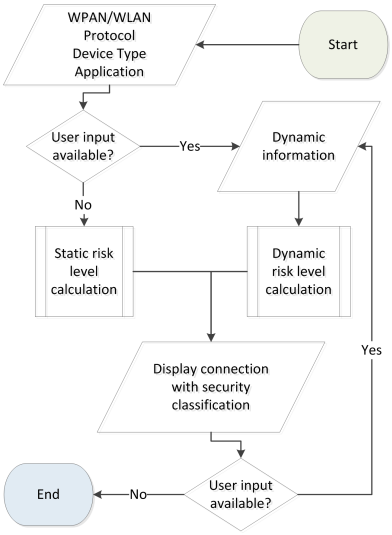


**Fig. 1.** Classification algorithm

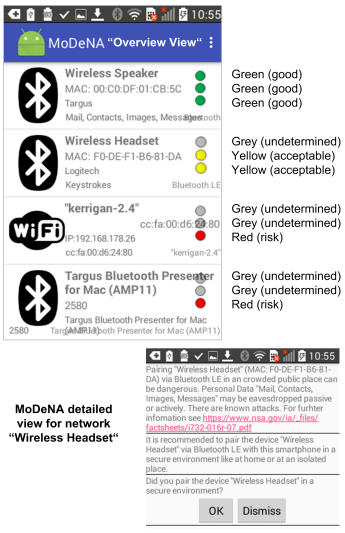


**Fig. 2.** MoDeNA Views

An example for improving the security of a connection is shown for the WLAN "kerrigan-2.4". The WLAN is automatically detected by the smartphone with activated Wi-Fi service as someones private network,which does not require authentication and the smartphone connects to it automatically. When a 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 MoDeNA application. The three bullets indicator is used to show the maximum possible grading available. 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. Further information about the security risk of using specific wireless technologies is provided with links to useful web pages that provide background information and educate the user.

## 4 User Study

A prototype of the application MoDeNA is realized on the Android OS platform, since it is the most widely used operating system to date for smartphones.

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.

(1) **Wireless Network Smartphone Security** 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. Asking the users if they turn off unused wireless protocols showed that 65% 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.

(2) **"Application Specific Wireless Security"** The users were requested to play around and evaluate our prototype implementation of the application MoDeNA. Thus, this 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.

## 5 Conclusions and Future Work

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. In our user study with 23 participants we observed 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.

## 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., 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, 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, 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. 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, June/July 2014, pp. 1–9. 2
10. R. Black, A. Donnelly, and C. Fournet, "Ethernet Topology Discovery without Network Assistance," in *12th IEEE International Conference on Network Protocols*, ser. ICNP, October 2004, pp. 328–339. 2
11. 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. ACM, July 2012, pp. 1–16. 2
12. G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos, "Paranoid Android: Versatile Protection for Smartphones," in *26th Annual Computer Security Applications Conference*, ser. ACSAC. ACM, December 2010, pp. 347–356. 2