ConnectivityControl: A Model Ecosystem for Advanced Smart Home Privacy

Philipp Thalhammer
thalhammerphilipp@gmail.com
LMU Munich
Munich, Germany

David Müller
david.muelle2@web.de
LMU Munich
Munich, Germany

Alexander Schmidt
mail@alxschmidt.com
LMU Munich
Munich, Germany

Michael Huber
mail@hubermichi.de
LMU Munich
Munich, Germany

Albrecht Schmidt
albrecht.schmidt@ifi.lmu.de
LMU Munich
Munich, Germany

Sebastian S. Feger
sebastian.feger@ifi.lmu.de
LMU Munich
Munich, Germany

Figure 1: Ecosystem Demonstration of Connectivity Control visualizing the data flow between two smart devices, a hub, a router, and two tablets

ABSTRACT

Smart home devices with their sophisticated sensing technologies raise many privacy concerns. In most cases, they only function when fully connected to the internet in which case privacy exposure is greatest. Users currently have to either accept these privacy risks or remove devices from the internet or power plug, rendering them useless. Our demo is based on recent work advocating for advanced smart device configuration options across a spectrum of connectivity control options. We introduce a model ecosystem with four connectivity levels and a privacy label that informs about connectivity-feature trade-offs across those four modes. The presented ecosystem introduces two functional smart devices and demonstrates intuitively how configuration decisions impact information flow.

MUM '23, December 03–06, 2023, Vienna, Austria

ACM ISBN 979-8-4007-0921-0/23/12.
https://doi.org/10.1145/3626705.3631876

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**.

KEYWORDS

Smart home, Internet of Things, Privacy, Security, User-controlled privacy

ACM Reference Format:
Philipp Thalhammer, David Müller, Alexander Schmidt, Michael Huber, Albrecht Schmidt, and Sebastian S. Feger. 2023. ConnectivityControl: A Model Ecosystem for Advanced Smart Home Privacy. In *International Conference on Mobile and Ubiquitous Multimedia (MUM '23), December 03–06, 2023, Vienna, Austria.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3626705.3631876

1 INTRODUCTION

Today, connected devices have become omnipresent. Some projections [6] predict that by 2025, as many as 100 billion connected devices will be in use worldwide. Even if a lot of the data that is being collected might appear insignificant at first sight, the data collected by a smart meter for example can be enough to reveal information about eating habits, sleeping routines, and the number of people that are present in a household [5]. While a lot of data can be collected by smart devices, research also indicates that many users are unaware of what happens to their data, as demonstrated by Malkin et al. [4] in their research about smart speakers. It has been shown that many users are reluctant to adopt IoT devices into their lives because they fear what could potentially happen to their data [3]. Findings from the work of Jin et al. [2] have unveiled, that "users heavily rely on ad hoc approaches at the physical layer (e.g., physical blocking, manual powering off)" [2] when it comes to privacy protection with smart devices. To address these issues, we propose a connectivity-based control model that empowers users with greater data control, as outlined by Feger et al. [1]. We show that this approach is feasible, by implementing two standalone smart devices: one security camera and one thermometer. Our demo aims at enabling interaction with this model ecosystem and intuitively communicating data flow and configuration consequences.

2 CONNECTIVITYCONTROL DEMO: THE MODEL ECOSYSTEM

We implemented a four-stage connectivity model for connected devices. For each mode, there is a list of supported features and potential privacy/security risks which are documented on a standardized label shown in *Figure 2c*.

Stage 1 (Offline): The device is not connected at all and is only usable in a manual way (e.g. reading information from a display) which is the most limited mode regarding features but also it poses no security risk whatsoever.

Stage 2 (Access Point): The device opens a WiFi Access Point for direct connections and information exchange.

Stage 3 (Network Mode): The device is accessible only from within the user's private network.

Stage 4 (Online Mode): The device is fully connected to the internet and usable from anywhere. To access it, the user needs to log in to our web application and link his account to the corresponding hub via its unique ID. This stage offers the most features and is most pleasant to use, but also comes with the most security/privacy risks.

The device mode can be changed either on the device with a physical slider or from the user interfaces in stages 2-4. The general model used for this is also described in detail by Feger et al. [1]. As proof of concept, we implemented two smart home devices: a smart thermometer and a smart security camera. Both devices utilize MQTT for the transmission of sensor data and mode change commands to a local device hub. This hub is responsible for regulating the accessibility of specific data to individual clients depending on the device's stage.

2.1 Prototype Devices: Smart Thermometer and Smart Security Camera

The thermometer (see *Figure 2b*) is capable of measuring temperature, humidity, and pressure. During offline mode, the display will only show the temperature reading. In Access Point mode, the device initiates a dedicated WiFi network with a DNS server that redirects users to a low-complexity user interface. This interface provides easy access to WiFi setup and real-time information about the temperature and humidity. The network and online mode are managed within a user interface that is provided to the local network by the device hub. In network mode, the user gets access to this rich user interface from anywhere within his home network. For online mode, the same user interface is provided with the addition of a device history and the ability to access the device from anywhere.

The smart camera (see *Figure 2a*) in Offline Mode provides the ability to store videos locally on an SD card for added privacy and control, while Access-Point Mode adds live streaming capabilities to connected consumer devices. Network Mode offers local streaming for real-time monitoring, and Online Mode provides remote accessibility from anywhere.

2.2 Ecosystem Demonstration

For the ecosystem presentation (see *Figure 1*) we chose the schematic of a house with all relevant devices (the thermometer, the camera, the hub, a router, and an input device) inside, and one input device outside of it. All devices are connected using a total of 7 LED strips that visualize the data flow between the devices. The input device inside the house represents a user within the home network and the outside device represents a user connecting from somewhere that is not the home network. When the mode of the devices gets changed, the data flow changes accordingly: Exemplary, if the thermometer is in online mode, data flows from the device to the hub, from the hub to the router, and from the router to the outside user. In Access-point mode the data flows directly from the device to the inside user. Visitors can interact with both smart devices using the two provided tablets or on their own smartphone if the respective device is in Access-Point Mode.

3 CONCLUSION

Our four-stage model for connected devices empowers users to customize the functionality and security of their IoT devices. By categorizing these stages and providing standardized labels, we enable users to make informed choices. Our practical implementation with smart home devices demonstrates the model's feasibility and we believe this concept has the potential to enhance IoT security and customization, putting users in control of their devices and data.

(a) Smart Security Camera **(b) Smart Thermometer** **(c) Standardized label for the smart thermometer**

Figure 2: The smart Security Camera, smart Thermometer & the standardized label for the Thermometer

REFERENCES

[1] Sebastian S. Feger, Maximiliane Windl, Jesse Grootjen, and Albrecht Schmidt. 2023. ConnectivityControl: Providing Smart Home Users with Real Privacy Configuration Options. In *End-User Development*, Lucio Davide Spano, Albrecht Schmidt, Carmen Santoro, and Simone Stumpf (Eds.). Springer Nature Switzerland, Cham, 180–188. https://doi.org/10.1007/978-3-031-34433-6_11

[2] Haojian Jin, Boyuan Guo, Rituparna Roychoudhury, Yaxing Yao, Swarun Kumar, Yuvraj Agarwal, and Jason I. Hong. 2022. Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 449, 19 pages. https://doi.org/10.1145/3491102.3517602

[3] Evan Lafontaine, Aafaq Sabir, and Anupam Das. 2021. Understanding People's Attitude and Concerns towards Adopting IoT Devices. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI EA '21)*. Association for Computing Machinery, New York, NY, USA, Article 307, 10 pages. https://doi.org/10.1145/3411763.3451633

[4] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019). https://doi.org/10.2478/popets-2019-0068

[5] Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin. 2010. Private Memoirs of a Smart Meter. In *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building* (Zurich, Switzerland) *(BuildSys '10)*. Association for Computing Machinery, New York, NY, USA, 61–66. https://doi.org/10.1145/1878431.1878446

[6] Karen Rose, Scott Eldridge, and Lyman Chapin. 2015. The internet of things: An overview. *The internet society (ISOC)* 80 (2015), 1–50.