Figure 1: Logging Process: Participant accessing the fridge and logging the interaction by reading the respective NFC tag using the smartwatch.

Towards Understanding User Interaction in Future Smart Homes

Sarah Prange
University of Applied Sciences
LMU
Munich, Germany
sarah.prange@hm.edu

Christian Tiefenau
University of Bonn
Bonn, Germany
tiefenau@cs.uni-bonn.de

Emanuel von Zezschwitz
University of Bonn & Fraunhofer FKIE
Bonn, Germany
zezschwitz@cs.uni-bonn.de

Florian Alt
Bundeswehr University
Munich, Germany
florian.alt@unibw.de

ABSTRACT

IoT devices are currently finding their way into people's homes, providing rich functionality by means of various interaction modalities. We see great potential in collecting and analysing data about users' interaction with their smart home devices to gain insights about their daily life behaviour for self-reflection as well as security purposes. We present a methodology to study interaction with IoT devices in users' (smart) homes. Logging daily behaviour usually comes with high effort and often interrupts natural interaction. Hence, we suggest an unobtrusive logging approach by means of a smartwatch and NFC technology. Participants scan interaction with devices using self-placed NFC tags. We tested our method with two flat shares in two cities and provide preliminary insights with regards to the strengths and weaknesses of our study approach.

CHI'19 Workshop, May 5, 2019, Glasgow, Scotland UK

KEYWORDS

IoT; Internet of Things; Smart Home; Smart Devices; NFC; Android; Field Study; Data Collection; In-the-wild

INTRODUCTION & MOTIVATION

Today, IoT-devices are becoming increasingly popular in private environments, such as people's homes. As an example, smart fridges help to keep track of the content, and smart thermostats enable remotely controlling of our home's temperature. These devices come in different form factors (e.g., smart bulbs) and support a wide range of interaction modalities (e.g., speech). In addition, devices in peoples' homes increasingly have access to personal, hence sensitive, data, which opens a need for protection (i.e., authentication). Thinking of a fully connected smart home, new possibilities for authentication methods arise by, e.g., using behavioural biometrics to identify users based on their individual behaviour [4], i.e., by interaction with their devices. Regarding usable security, we are interested in usage patterns of these smart devices which could be used to authenticate a user based on a specific behavioural pattern.

Previous work already investigated user behaviour on smartphones [1], yet focused on one device. At the same time, the relationship of interactions has not been investigated. We investigate user behaviour in a smart home environment, possibly involving multiple modes of interaction with various devices.

Methods of evaluation in smart home environments include, but are not limited to, audio and video recordings [2] or diary studies [3]. However, these methods are highly privacy invasive or require high effort, especially when it comes to participants' behaviour in their own home environment.

We propose a new study approach to understand the interaction with (personal as well as shared) devices in a household. To test our approach, we performed a pre-study with two households with three flatmates each. In this paper, we contribute our new, NFC-based logging tool for studying interaction in participants' homes as well as insights into the strengths and weaknesses of our tool from the pre-study.

APPROACH

Closely related to the workshop's call for papers asking for "methods and approaches for studying the use of interaction with IoT", we present our NFC data logging application which allows to acquire data about daily interaction with IoT devices in participants' homes.

Briefing: *before* the actual field study. Participants need to a) setup the logging environment (i.e., connect smartwatch and smartphone, install our application, distribute NFC tags) and b) self-assess their usage patterns (i.e., which devices do they use in which frequency).

Logging Phase: the actual field study. Participants log interaction with devices in their homes using the smartwatch and NFC technology. In addition, they assess the quality of their logging data by indicating missing data once a day.

Debriefing: *after* a period of logging. Besides returning the hardware, participants self-assess their usage patterns once more.

Sidebar 1: Study Procedure

NFC Data Logging Application

With our NFC-based evaluation platform, we take first steps towards analysing user behaviour in smart home environments unobtrusively and privacy-preserving (e.g. to evaluate if and how data for developing behaviour-based authentication mechanisms in a home environment can be collected). We employed an Android Wear application on a Sony smartwatch, capable of reading NFC tags. We additionally provide a companion smartphone application to add details to log entries, manage registered NFC tags, as well as adding missing logs at the and of each study day.

Procedure

The procedure for our study approach is as follows (cf. Sidebar 1 for an overview).

Briefing: Prior to the study: participants (e.g., families, flat shares) fill in a questionnaire covering the following topics:

- *Previous experience* with smart home devices and smartwatches
- *Patterns and routines* in daily life
- *Potential security issues* with smart home devices

Furthermore, they self-assess their usage of shared and individual devices in their homes of which they could imagine "smart" functionality in the future to serve as a comparison to the logging data.

Setup: Each participant within the household receives a prepared smart watch and a couple of NFC tags. They set up the study in their homes by placing NFC tags on or next to "smart" or "to-become-smart" devices.

Logging: Participants log interaction with the tagged devices as follows: shaking the wrist (i.e., moving the hand/arm towards the device) activates the app. Placing the watch close to the NFC tag while interacting with the tagged device adds a new log entry, providing participants with vibration feedback if successful (cf. Figure 1).

Debriefing: After the logging phase, participants assess their own behaviour once more. They fill in another questionnaire covering the following topics:

- *Patterns and routines* in daily life
- *Potential security issues* with smart home devices

Analysis: With the collected data, we can not only compare self-assessed quantified behaviour vs measured behaviour, but also analyse chains of interactions on shared and individual devices as well as reoccurring patterns of interaction.

PROOF OF CONCEPTS, EARLY INSIGHTS & LESSONS LEARNED

As of now, we conducted two trials with our NFC-based data collection in (smart) homes in two flat shares in different cities. Each flat share logged interactions for one week. From our trials, we learned about challenges with regards to data quality and the setup procedure of our study approach.

Data Quality

We assume that the data logs are incomplete. This may be due to several reasons: a) some participants were away from home during the logging phase, b) participants forgot to log each and every interaction (e.g. while concentrating on another main task). For future studies, we propose to nudge people to logging by, e.g., vibrational reminders via the smartwatch.

Setup Procedure

Furthermore, we encountered minor technical problems (e.g., missing network connection or battery drainage of test devices). In addition, it was unclear for some participants which devices are to be considered relevant. For future studies, we suggest to give specific instructions which devices to tag to gain more specific insights.

APPLICATION AREAS

We propose various application areas for interaction data acquired via our approach: behaviour analysis, home automation, security and privacy, as well as implicit authentication.

Behaviour Analysis

Our approach allows for analysing users' interaction with their devices, while still preserving their privacy. This allows for various further investigations, including, but not limited to: a) investigating differences between self-reported and observed behaviour, which could support further studies on accuracy of self-assessment, b) finding uncommon habits (e.g. irregular preparation of meals) or c) nudging users to a "more secure" behaviour (e.g. reminding them to lock the door if the system detected that the person left the house without locking it).

Home Automation

Investigating users' interaction behaviour in their smart homes can serve as a data source for automating their homes. As an example, if we know users' common interaction patterns, IoT devices could predict and execute the next step (e.g., opening the front door turns on the light in the living room). However, such systems need to take great care of potential threats evolving around automating the IoT (e.g. attackers imitating users' behaviour could get access to their homes).

Security & Privacy

In a fully connected smart home that is able to predict user behaviour, a new threat model arises. An attacker could observe a user's behaviour, and can then possibly impersonate this user when she is not at home and try to get access to, e.g, the smart door lock. Also, such a scenario leads to a privacy critical situation. People could get the feeling of being permanently under observation when their behaviour is tracked continuously. This should be investigated in future work.

Implicit Authentication

Finally, given the fact that IoT devices increasingly acquire and process sensitive data, this enables new mechanisms of authentication (cf. behavioural biometrics [4]). Behaviour can serve as implicit and seamless mechanism for authentication on IoT devices, given that we may be able to identify people by their interaction patterns.

CONCLUSION & FUTURE WORK

In our position paper, we proposed a novel platform that enables researchers to collect data about users' interaction with IoT devices in their homes. It is unintrusive and preserves participants' privacy in their home environment. Future work could a) improve the study setup itself by looking at the validity of the gathered data, b) find a good trade-off between reminding participants of possible missed logs and annoyance, or c) gather more specific data by pre-defining the devices to be tagged or evaluate different settings, such as offices. We are looking forward to discuss further challenges in evaluating interaction with IoT devices at the workshop.

REFERENCES

[1] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 213–230.

[2] Ahmad Jalal and Shaharyar Kamal. 2014. Real-time life logging via a depth silhouette-based human activity recognition system for smart home services. *2014 11th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)* (2014), 74–80.

[3] Shrirang Mare, Mary Baker, and Jeremy Gummeson. 2016. A Study of Authentication in Daily Life. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 189–206. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/mare

[4] Roman V Yampolskiy and Venu Govindaraju. 2010. Taxonomy of behavioural biometrics. In *Behavioral Biometrics for Human Identification: Intelligent Applications*. IGI Global, 1–43.