

User-Centered Design to Enhance IoT Cybersecurity Awareness of Non-Experts in Smart Buildings

Hanning Zhao, Bilhanan Silverajan
Tampere University, Finland
Email: firstname.lastname@tuni.fi

Abstract—Smart buildings, building automation and operational management have increasingly begun to incorporate Internet of Things (IoT) technology. Therefore, they have become susceptible to common cyber attacks targeting IoT devices. However, there is still a lack of an effective way of monitoring the cybersecurity situation of smart devices, IoT sensors and networks. During the operational lifecycle it may also not be easy for non-experts to discern cybersecurity issues from malfunctioning or physical safety. Therefore, we propose visualization prototypes that provide both safety and cybersecurity status of IoT devices for non-expert users in smart buildings. By utilising a user-centered design method, the visualization dashboards are developed based on requirements of two user roles - House managers and Residents. The user test results have shown the capabilities and effectiveness of leveraging dashboards to increase cybersecurity awareness in smart buildings.

Index Terms—IoT, User-Centered Design, Cybersecurity

I. INTRODUCTION

It is common for smart residential buildings nowadays to have large-scale installations of IoT devices for monitoring physical situations and facilitating housing management by monitoring sensor readings. However many recent cyber-attacks on IoT devices have proven that these devices are manufactured at low cost, may contain security flaws or have poor security. In such an environment, a cybersecurity threat or attack may threaten physical safety, such as when a temperature sensor is manipulated to give a false alarm. However, the cybersecurity awareness for managing and using IoT devices in smart buildings is rather low. Most residents are non-expert or non-technical people while house managers also may have limited expertise in cybersecurity. This poses challenges when a need to identify cybersecurity threats of IoT devices and networks arises. To handle this, we aim to provide a usable visualization system to enhance cybersecurity situational awareness of non-experts users. Previous research has revealed the advantages of utilising visualizations in cybersecurity. However, most visual systems focus on network security and are primarily developed for professional users.

In this work, we describe ongoing work of a visual system to enhance the cybersecurity situational awareness in smart residential buildings fitted with various types of wireless IoT sensors. These IoT sensors are based on the low-power Sigfox [1] technology. A Sigfox network operator is responsible for managing the radio network infrastructure to which these sensors connect. Data subsequently transmitted from a Sigfox sensor is stored in a cloud that is also managed by a national

Sigfox operator. While this provides a high level of convenience in terms of IoT device management, one challenge in such a proprietary network is that the security status of devices is inaccessible for regular consumers. In addition, when Sigfox sensors become unreachable or are delivering unusual data, it is challenging to immediately ascertain the cause of the malfunction, which may range from hardware faults to cybersecurity attacks. As a consequence, end-user security visualization prototypes need to consider both safety and cybersecurity events, to contribute to a better understanding of the situational awareness of IoT sensors and networks.

This short paper describes recent visualization prototypes that focuses on serving security information of IoT sensors to two non-expert user groups - House managers and Residents. The approach considers a user-centered design (UCD) process along with the designed results of visualizations for each user group. We analyse the user requirements obtained from interviews and questionnaires. The developed interactive visualization prototypes are derived from user requirements and have been evaluated from an initial round of user testing.

II. RELATED WORK

User-centered design (UCD) is a well-known method which aims at designing the products by involving users throughout the design process. It refers to several iterations of design with a focus on user needs and requirements [2]. This approach has been widely applied for constructing visualizations for cybersecurity. Mckenna et al. [3] explored UCD for designing a visual dashboard named *BubbleNet* to help network analysts identify cyber threats. *Ocelot*, a visual system was designed based on UCD for threat assessment and quarantining any compromised assets away from the network [4]. However, the majority of visual systems are primarily designed for technical users such as security experts and network engineers.

III. VISUALIZATION DESIGN BASED ON UCD

The UCD method ensures the usability and effectiveness of final product by including end users throughout the design process. We applied this method in designing our visualizations. This allowed us to identify the concrete requirements for the two end-user groups and evaluate the proposed design solutions. More specifically, the UCD process contains four activities specified in ISO 13407 [5]. We adhered to these four phases, which are described in the following subsections.

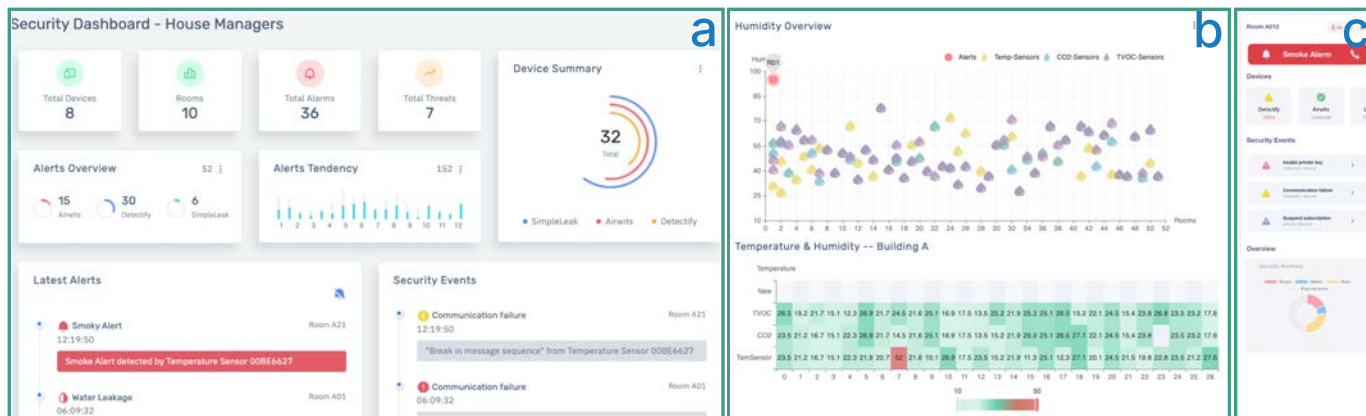
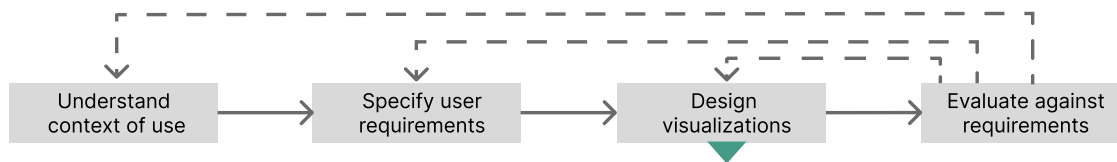


Figure 1: The overview of UCD process, (a) security situation for the smart buildings, (b) scatter chart for all humidity values while heatmap visualises all temperature values, (c) mobile UI of individual smart apartment.

Figure 1 illustrates the entire design process and the developed visualization prototypes.

A. Understanding Context of Use

The context of use significantly shapes the design of visualization. In our work, we focus on a smart residential building scenarios with various types IoT devices installed for monitoring temperature, humidity and air quality data. In such a scenario, the cybersecurity situation of IoT devices and networks is critical and any malicious events should be reported in time. Thus, the goal of the security visualizations in this paper is to support non-expert users to achieve a context-specific comprehension and management of devices in smart buildings. In addition, the safety status in these smart buildings needs to be displayed and users alerted to unusual readings.

B. Specifying User Requirements

Knowing the users is a high priority as it helps to clarify their actual requirements for a usable design. In our design, two major user groups - *House managers* and *Residents* are identified. Given that they are mostly non-expert users with respect to cybersecurity, their technical background and needs vary from IT professionals. By utilizing interviews and questionnaires, we analyzed the background of two user groups and defined two user roles:

- *House managers*, who are in charge of the overall security of the smart buildings. They are assumed to have little to limited knowledge in cybersecurity.
- *Residents*, who are living in apartments within a smart building and get physical alerts from IoT devices to their mobile app. Residents are usually not technically skilled, and they are assumed to have no background in IT networks and cybersecurity.

Based on user research results, the visualization designed for *House managers* is expected to provide at-one-glance information of overall cybersecurity status instead of technical details and packet view of network traffic. The ongoing attacks of devices and networks need to be visualized while historical data can support further analysis and predictions. *House managers* also require safety information about buildings. *Residents* require a view of cybersecurity health of IoT sensors installed in their apartments. The cybersecurity health information can be supplied to them by IT support, external security analysts or data provided to the house managers. Based on questionnaires and interviews, both user groups prefer an easy-to-follow design and be able to provide effective responses to anomalous events through visualizations.

C. Designing Visualizations

We selected different visualization techniques for each user role and the following subsections describe the proposed design solutions. The visualizations for the house manager is a web-based dashboard based on an open-source library, ECharts, while the mobile application for residents is built on Ionic, which is an open-source mobile toolkit for cross-platform design.

1) *Visualizations for House Managers*: The security visualization aims to provide a comprehensive view of cybersecurity and safety posture in smart buildings. Figure 1a and 1b show the visualization interfaces for house managers. The security visualization dashboard consists of various components including the safety and cybersecurity data of three types of IoT devices provided by the Sigfox solution provider: Airwits (temperature sensor), Detectify (motion sensor) and Simple-Leak (sensor for water detection). As shown in Figure 1a, the overall information of devices and raised alerts are displayed

and both ongoing safety alarms as well as cybersecurity events are visualized. In addition, all temperature and humidity values are displayed as scatter and heatmap charts as shown in Figure 1b. While not shown in the figure, the air quality data is similarly visualized in a scatter chart. Such visualizations give a holistic view of the state of a smart buildings in terms of safety matters such as smoke alarm, water leakage and so on. These visualizations also reveal potential cyber threats or attacks by highlighting abnormal device reading or behaviour with contrasting colors. When hovering on a single node, the tool-tip provides detailed information about the device and its location. In addition to the view for all devices, the information of each device is displayed in a collapsed card design.

2) *Visualizations for Residents*: Residents are able to obtain safety and cybersecurity specific information for IoT devices installed in their own residences, with a mobile application. Figure 1c illustrates the homepage of the visualization. The design contains different sections. Owing to the risk of physical harm, safety alerts are given a higher priority and are more prominent than other threats. The overall information of installed devices is listed. The section of security event focuses on cybersecurity data and raises alerts related to devices or network anomalies. In addition to real-time notifications, the overview panel presents summary data of the cybersecurity situation of IoT devices as a doughnut chart. Historical data is also provided in order to detail past malicious events.

D. Evaluating Design Against Requirements

Evaluation is the process for testing of the design of visualizations align with users requirements. We conducted the interviews and heuristic evaluations [6] for identifying the strengths and weakness of the visualizations. The overall feedback is positive and shows a high usability of the visualizations. The most common feedback from users are *"the dashboard is clear and they can find the information easily"*. However, a major issue is mentioned by multiple users that *"the term 'private key' is hard to understand"*. Another concern from house managers is how the design can be applied and used with larger scale data sets, for example, if thousands of devices are installed in future. All received feedback and suggestions will be used in future design iterations.

IV. DISCUSSION AND REFLECTION

The developed security visualizations effectively deliver the overall security posture in smart buildings for non-expert users. Different visualization techniques affect the user experience and effectiveness of understanding the security information and alerts. According to the conducted usability testing, we found out that the scatter plot and heatmap are very effective methods of visualizing large scale data. Both of them are scalable and using different colors allows users can easily locate the anomalous readings.

One difficulty for all non-expert users is related to the terms shown in the dashboard. For example, users had difficulty in grasping the concept of what a private key is. This should be taken into account, when describing technical or cybersecurity

terms within visualization prototypes. Additional feedback received pertains to how such visualization can incorporate collaborations with other user groups, particularly when cybersecurity events are detected and confirmed. As an example, residents would want to report anomalous device behavior to house managers, whereas house managers indicated a strong desire to correspond with technical personnel to co-ordinate follow-up action upon detection. We intend to resolve these issues in future work.

V. CONCLUSION AND FUTURE WORK

Security visualization plays a vital role in supporting non-experts in cybersecurity management in IoT smart environments. In our work, we proposed the visualization dashboards for two different user groups. Through the developed visualizations, both house managers and residents get an overview of security status and the first usability testing showed the usability and effectiveness of the design.

As future work, we intend to iterate the design and conduct additional user tests. Moreover, the visualization techniques for large scale data such as for hundreds of rooms needs to be explored. One proposed solution is a bubble chart which allows a zoom-in/out feature. Also how to enhance the security information sharing through visualization, is being explored.

However, based on the current practices and evaluation, we believe that proper visualization methods contribute to better comprehension and deeper insight into gathered information. This will pave the way for better cyber security management in other IoT ecosystems.

VI. ACKNOWLEDGEMENTS

The work was funded via Business Finland's S²ERC Apia IoTSpace and the DIMECC Sea4Value Future Fairway Navigation programs. The authors thank Marko Helenius and Tiina Schafeitel-Tähtinen for their valuable and constructive feedback during the design of the visualization prototypes.

REFERENCES

- [1] A. Lavric, A. I. Petrariu, and V. Popa, "Sigfox communication protocol: The new era of iot?" in *2019 International Conference on Sensing and Instrumentation in IoT Era (ISSI)*. IEEE, 2019, pp. 1–4.
- [2] C. Abras, D. Maloney-Krichmar, J. Preece *et al.*, "User-centered design," *Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications*, vol. 37, no. 4, pp. 445–456, 2004.
- [3] S. McKenna, D. Staheli, and M. Meyer, "Unlocking user-centered design methods for building cyber security visualizations," in *2015 IEEE Symposium on Visualization for Cyber Security (VizSec)*. IEEE, 2015, pp. 1–8.
- [4] D. L. Arendt, R. Burtner, D. M. Best, N. D. Bos, J. R. Gersh, C. D. Piatko, and C. L. Paul, "Ocelot: user-centered design of a decision support visualization for network quarantine," in *2015 IEEE Symposium on Visualization for Cyber Security (VizSec)*. IEEE, 2015, pp. 1–8.
- [5] T. Jokela, N. Iivari, J. Matero, and M. Karukka, "The standard of user-centered design and the standard definition of usability: analyzing iso 13407 against iso 9241-11," in *Proceedings of the Latin American conference on Human-computer interaction*, 2003, pp. 53–60.
- [6] Nielson, Jakob, "10 Usability Heuristics for User Interface Design," [Online; accessed 7-June-2022]. [Online]. Available: <https://www.nngroup.com/articles/ten-usability-heuristics/>