Towards Building Better Context-Aware Smart Homes for Security and Privacy

Weijia He
Dartmouth College / The University of Southampton

Jingjie Li
The University of Edinburgh

Smart home systems, including smart speakers, home cameras, and robot vacuums, serve the diverse needs of everyday users. Facing users who often have limited technical knowledge, smart home systems prioritize usability and autonomously react to a dynamic environment. However, using smart home systems is accompanied by various security and privacy considerations, such as the acceptability of inter-personal data sharing. These considerations are driven by complex contextual factors (e.g., users' security and privacy attitudes, social and environmental dynamics in smart homes), which may arise and evolve in different phases of the life cycle of a smart home system.

Capturing these contextual factors is an essential, yet non-trivial, task for researchers, service providers, and smart home systems to address users' security and privacy requirements. This talk summarizes the key insights from the authors' research efforts over the years in **understanding contextual factors for smart home security and privacy**. Driven by our observations, we will highlight future research opportunities in **building context-aware smart home systems**. Our talk will include three major themes as below.

What are the contextual factors related to smart home security and privacy? We discovered that the security and privacy issues of smart homes are influenced by multiple social, technical, environmental, temporal, and informational factors that interact with each other. For example, attitudes and preferences regarding security and privacy can shift depending on social relationships (e.g., parents vs. children) [1], the device's location (e.g., indoor vs. outdoor camera) [1, 2], the trustworthiness of the device and its manufacturer (e.g., big tech vs. unheard companies), and different phases in the adoption journey of smart home products. We will also highlight several recent influences on the security and privacy context, including the integration of artificial intelligence and the evolving beliefs about the geo-political impact on smart home supply chain.

How can researchers capture contextual factors from different perspectives? We have employed various research methods, such as user surveys [1, 2], content analysis [3, 4], and framework building [5], to understand contextual factors of smart home security and privacy. From different perspectives, these research methods form a thorough pipeline for identifying challenges in creating a context-aware and user-centric smart home system and generating design recommendations.

User surveys are used to probe smart home users directly and quantify contextual factors from a user's perspective. Through proper survey design and statistical analysis, we can decouple the contextual factors muddled in users' decision-making process. For example, our work showed that users have different levels of trust in long-term residents in the same household when access to smart home data is permitted without explicit consent. Unlike family members, users' trust in roommates only extends to smart home devices in the common areas, such as the living room [2].

Content analysis of online security and privacy information allows us to non-intrusively understand contextual factors from a community's viewpoint and manufacturers' perspective. For instance, we investigated how contextual factors drive smart home users' collaborative exploration of security and privacy issues in real life [3] and studied the consistency of privacy communication in smart home marketing [4].

Framework building maps the learned contextual factors to security and privacy requirements of the actual system design, informing smart home designers. For example, studies have suggested that children's usage of certain smart home devices should only be done supervised, which requires the system to recognize users' ages and proximity to the device. Our framework helps smart home designers optimize system design according to the sensors appropriate for this task, given their unique privacy implications [5].

The talk will further discuss the applicability of these methods and evaluate their pros and cons, including the potential biases.

How can we build better smart home systems that are context-aware and user-centric? To conclude the talk and stimulate further discussion, we will present several research opportunities stemming from our work. First, a system that recognizes nuances in users' attitudes and contexts is also inevitable to make mistakes, either due to a user's wrongdoing or a faulty sensor reading. More research is needed to address faults in configuring and enacting security and privacy policies for an automated smart home. Second, when multiple parties are involved in one system, conflicts are bound to happen. What is required for conflict resolution under social pressures and how a system could support it requires more studies from both a user's and a system's standpoint. Further, opportunities remain to offer users consistent and persistent security and privacy support throughout the life cycle of a smart home product, including less-studied scenarios like ownership transferal or device removal. These directions call for a joint effort by experts in different areas, including security and privacy, mobile systems, and human-computer interaction.

REFERENCES

[1] Weijia He, Roshni Padhi, Jordan Ofek, Maximilian Golla, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *USENIX Security Symposium*, 2018.

[2] Weijia He, Nathan Reitinger, Atheer Almogbil, Yi-Shyuan Chiang, Timothy J. Pierson, and David Kotz. Contextualizing Interpersonal Data Sharing in Smart Homes. In *Proceedings on Privacy Enhancing Technologies*, 2024.

[3] Jingjie Li, Kaiwen Sun, Brittany Skye Huff, Anna Marie Bierley, Younghyun Kim, Florian Schaub, and Kassem Fawaz. "It's up to the Consumer to be Smart": Understanding the Security and Privacy Attitudes of Smart Home Users on Reddit. In *IEEE Symposium on Security and Privacy*, 2023.

[4] Kaiwen Sun, Jingjie Li, Yixin Zou, Jenny Radesky, Christopher Brooks, and Florian Schaub. Unfulfilled Promises of Child Safety and Privacy: Portrayals and Use of Children in Smart Home Marketing. In *ACM Conference on Computer Supported Cooperative Work*, 2024.

[5] Weijia He, Valerie Zhao, Olivia Morkved, Sabeeka Siddiqui, Earlence Fernandes, Josiah Hester, and Blase Ur. SoK: Context Sensing for Access Control in the Adversarial Home IoT. In *IEEE European Symposium on Security and Privacy*, 2021.