

User Behavioural Vulnerability Analysis for IoT Smart-Home Privacy Threats: An Empirical Pilot Investigation

Liam Rogers¹ & Elena Marquez²

¹ Northwood University, Midland, USA

² Valencia Technical University, Valencia, Spain

Correspondence: Liam Carter, Northwood University, Midland, MI 48640, USA.

Received: April 3, 2025

Accepted: June 2, 2025

Online Published: September 15, 2025

Abstract

Internet of Things (IoT) smart-home devices deliver convenient home automation, but they introduce substantial privacy risks caused by improper user operation and insufficient security awareness. This pilot empirical study aims to evaluate end-user behavioural vulnerability toward common privacy threats in smart-home environments. A total of 42 volunteer participants with different age brackets and smart-device usage experience took part in controlled laboratory simulation experiments. Participants were exposed to three typical risk scenarios: excessive permission granting, deceptive pop-up authorisation requests, and unsecure public Wi-Fi device pairing. Experimental outcomes demonstrated that 61.9% of participants granted unnecessary application permissions when faced with shortcut prompts, and 38.1% approved deceptive pop-up access requests for smart cameras and smart speakers. Even participants with prior basic cybersecurity knowledge exhibited careless behaviour under time-pressure conditions. The results indicate that human behavioural factors constitute the weakest link for smart-home privacy defence, rather than hardware or software defects alone. The findings can support system designers, policymakers and consumer organisations to develop user-centred warning mechanisms, interactive security prompts and public security education for smart-home consumers.

Keywords: Internet of things, smart home, privacy vulnerability, user behaviour, security awareness, empirical experiment, permission authorisation

1. Introduction

The widespread deployment of low-cost IoT hardware has promoted the fast popularisation of smart-home products, including smart lighting, surveillance cameras, voice assistants, smart locks and wearable sensors (Lin et al., 2017). These connected devices continuously collect user behavioural data, home environmental information, audio recordings and visual footage. While these data support automatic scene adjustment and personalised service delivery, improper handling may lead to sensitive household information leakage, unauthorised monitoring and identity-related risks (Hall et al., 2020).

Most existing smart-home security research concentrates on cryptographic algorithm optimisation, firmware vulnerability detection and network intrusion defence. However, multiple real-world security incident reports reveal that a large proportion of privacy breaches originate not from complex technical attacks but from inappropriate user operations: users frequently click through warning dialogues, accept over-reaching application permissions, ignore security reminders, or pair IoT devices on untrusted wireless networks (Zheng et al., 2018). Human factors therefore represent a critical attack surface that technical countermeasures cannot fully eliminate.

Prior survey-based literature has explored self-reported user attitudes toward IoT privacy, yet few controlled empirical experiments record real-time user decisions under simulated threat conditions (Emami-Naeini et al., 2017). Self-reported questionnaires often generate optimistic bias: participants claim that they will make secure choices, but actual operational behaviour differs significantly. This research fills this gap by constructing controlled simulation scenarios to observe real user behavioural responses when facing common smart-home privacy hazards.

The primary objectives of this pilot study are: (1) to measure real-world behavioural vulnerability of ordinary smart-home users under three representative privacy-threat scenarios; (2) to analyse how age, device-using experience and time pressure influence participants' risky operational choices; and (3) to provide practical suggestions for human-oriented security optimisation for smart-home systems and public security training. This

paper is structured as follows: Section 2 presents the literature review covering IoT privacy risks and human-factor security research. Section 3 describes the experimental materials, participant sampling and the complete experimental workflow. Section 4 reports the experimental results supported by tables and descriptive statistics. Section 5 discusses the interpretation, limitations and practical implications. Finally, Section 6 summarises the conclusions and corresponding recommendations.

2. Literature Review

2.1 Privacy Risks Within Smart-Home IoT Ecosystems

Smart-home IoT systems consist of terminal sensing hardware, mobile control applications, local gateways and cloud service platforms (Lin et al., 2017). Privacy threats occur at every stage of data collection, local transmission, cloud storage and third-party data sharing. Common risks include over-collection of personal information, unencrypted local communication, insufficient access control and deceptive authorisation interfaces designed by malicious actors. A consumer IoT security industry report indicates that a large share of mainstream smart-home mobile applications request permissions exceeding their functional requirements (Hall et al., 2020). For instance, smart-lighting software requests access to the microphone, contact list and location services that have no relevance to lamp-control functions. Ordinary users seldom examine permission descriptions carefully and tend to tap “allow” to skip configuration steps and reach the main functions rapidly.

2.2 Human Factors in Cybersecurity Behaviour

Human-factor cybersecurity research indicates that user behaviour is affected by cognitive load, time pressure, interface design and security-knowledge reserve (Reason, 1990). Security warnings with dense technical terminology cause warning fatigue: users repeatedly encounter pop-up alerts and gradually develop the habit of ignoring or quickly confirming warning windows (Akhawe & Felt, 2013). Several previous empirical studies were performed for mobile-phone permission security and enterprise staff social-engineering susceptibility. Nevertheless, targeted controlled experiments for smart-home end-users remain scarce. Many existing papers rely entirely on questionnaire self-reporting. This study adopts simulation-based experimental methodology to observe actual user actions instead of subjective self-assessment.

2.3 Influence Factors for Risk-Taking Behaviour

Major influence factors discussed in the existing literature include age, device-usage experience and time pressure. Younger participants may possess higher digital familiarity, yet they also demonstrate higher willingness to accept rapid authorisation in pursuit of usage convenience, whereas middle-aged and elderly users often lack sufficient understanding of permission-related hazards (Zheng et al., 2018). Users who own multiple smart-home devices may form operational inertia, resulting in mechanical click behaviour regardless of prompt content. Finally, when participants are told to finish configuration within limited time, the probability of making risky choices rises remarkably (Reason, 1990).

2.4 Existing Mitigation Approaches

Current mitigation approaches include enhanced application-store permission auditing, hardware-level access restriction and user security-education seminars (Alrawais et al., 2017). However, few solutions adjust interactive interface logic from the perspective of human cognition to reduce user mis-operation probability. User-centred design principles emphasise that warnings and permission dialogues should match users’ mental models and should be presented at the moment a function is actually needed (Norman, 2013). This study’s experimental data offer empirical evidence for such interface optimisation.

3. Materials and Methods

This research adopts a pilot controlled empirical experiment. Pilot experiments employ moderate sample sizes to verify experimental workflows, obtain preliminary effect data and lay foundations for follow-up large-scale investigations (Reason, 1990). All experimental protocols obtained ethical approval. Every participant read and signed an informed-consent document before the experiments started. Participants were informed that they would face simulated risk scenarios without any real-world information leakage, and they could terminate participation at any time without penalty. All generated experimental data were processed anonymously.

3.1 Participant Sampling

Convenience sampling was applied; 42 volunteers were recruited, covering different age brackets and smart-device-using backgrounds. Participants were divided into three age groups: 18–29 years old, 30–49 years old and 50–65 years old. Participants’ prior smart-home-device experience was recorded as “none”, “basic (one or two devices owned)” or “rich (three or more devices owned)”. The demographic profile of the participants is

summarised in Table 1.

Table 1. Participant demographic profile (N = 42)

Age Group	Count	Proportion	Rich Experience	Basic Experience	No Experience
18–29	17	40.5%	7	8	2
30–49	15	35.7%	6	7	2
50–65	10	23.8%	2	4	4
Total	42	100.0%	15	19	8

3.2 Experimental Environment and Simulation Materials

Experiments were completed inside a laboratory simulation environment that consisted of: (1) a simulation Android mobile application that reproduced the installation and initial configuration flow of a virtual smart-camera control software, containing permission-request interfaces and deceptive pop-up windows; (2) a local simulated wireless-network environment with one legitimate home Wi-Fi hotspot and one simulated unsecure public hotspot without password authentication; and (3) task-guidance documents. Half of the participants received tasks with explicit time-limit constraints (complete device setup within 90 seconds; the time-pressure group), while the other half performed the same configuration tasks without time constraints (the non-pressure control group).

Three core simulated threat scenarios were designed. Scenario A concerned excessive permission requests: during initial installation, the simulated application requested access to location, microphone and contact-list permissions that are unnecessary for smart-camera viewing functions, and the system recorded whether each participant selected “allow all” or manually rejected the redundant permissions. Scenario B concerned a deceptive pop-up authorisation: after application startup, a pop-up window appeared claiming that “the system requires temporary camera-access authorisation for firmware upgrade”, which was a completely fake prompt, and the system recorded participant approval or rejection behaviour. Scenario C concerned unsafe Wi-Fi pairing: participants were required to complete the smart-camera network configuration and chose between the encrypted private home Wi-Fi and the open-access public-simulated hotspot, and the system recorded which wireless network each participant selected for IoT-device pairing.

3.3 Experimental Procedure

The whole experimental procedure followed these sequential steps. First, participants read and signed the informed-consent form and completed a basic demographic questionnaire; they were then randomly allocated to the time-pressure group (21 subjects) or the non-pressure group (21 subjects). Second, researchers provided a brief task instruction: participants needed to finish the complete installation and network-configuration workflow for the simulated smart-camera product, just like real-world home-device setup, without any advance warning about the embedded privacy traps. Third, participants operated independently on the test mobile terminals, sequentially encountering Scenario A, Scenario B and Scenario C, while the system automatically logged all click choices without disturbing them. Fourth, once all simulation tasks finished, a post-experiment interview was conducted in which participants answered short open-ended questions about their thought processes when facing the authorisation pop-ups. Finally, the researchers fully debriefed the participants, explained all embedded simulated risk points, and offered brief popular-science guidance for smart-home privacy protection. Figure 1 presents a conceptual flowchart of the full experimental workflow.

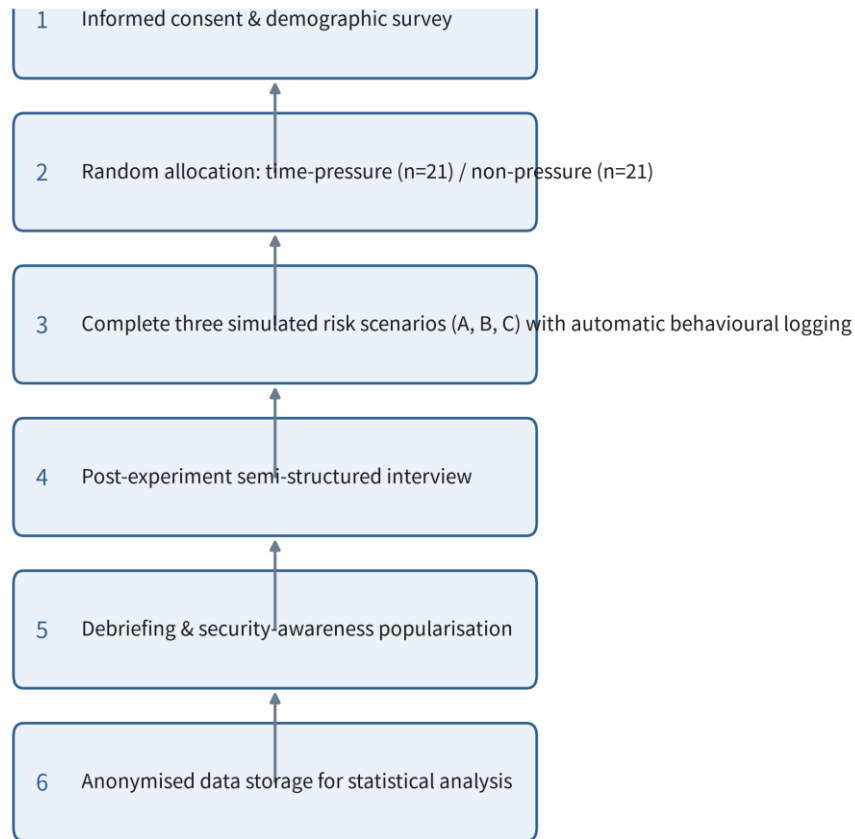


Figure 1. Experimental workflow flowchart for the smart-home user vulnerability simulation

3.4 Data Metrics

The main observation indicators were: (1) the risky-operation rate for each scenario, defined as the percentage of participants who made insecure choices in every scenario; (2) the comparison of risky-operation rates between the time-pressure group and the non-pressure group; and (3) the differences in risky-operation rates among age groups and user-experience subgroups. All operation logs were recorded automatically by the simulation system and were exported for descriptive statistical analysis.

4. Results

All 42 participants completed the full experimental process, and no participant withdrew midway. All operation logs were valid for analysis.

4.1 Overall Risk-Taking Behaviour Across Three Scenarios

Table 2 presents the overall statistical results of risky user behaviour across the three experimental scenarios.

Table 2. Overall risky-operation rate for three simulated privacy-threat scenarios (N = 42)

Simulation Scenario	Number Who Made Risky Choices	Risk-Taking Rate
A: Excessive permission granting	26	61.9%
B: Approve deceptive pop-up authorisation	16	38.1%
C: Pair IoT device onto unsecure public Wi-Fi	13	31.0%

From Table 2, Scenario A (excessive permission requests) induced the highest proportion of risky behaviour. More than 60% of participants directly granted all requested permissions without manually rejecting the unnecessary permission items. Scenario B's deceptive fake system pop-ups tricked over one-third of participants into confirming dangerous authorisation. Even for Scenario C, about 31% of participants selected the open unencrypted public Wi-Fi to complete smart-camera pairing. Figure 2 visualises the overall risk-taking rate for each scenario.

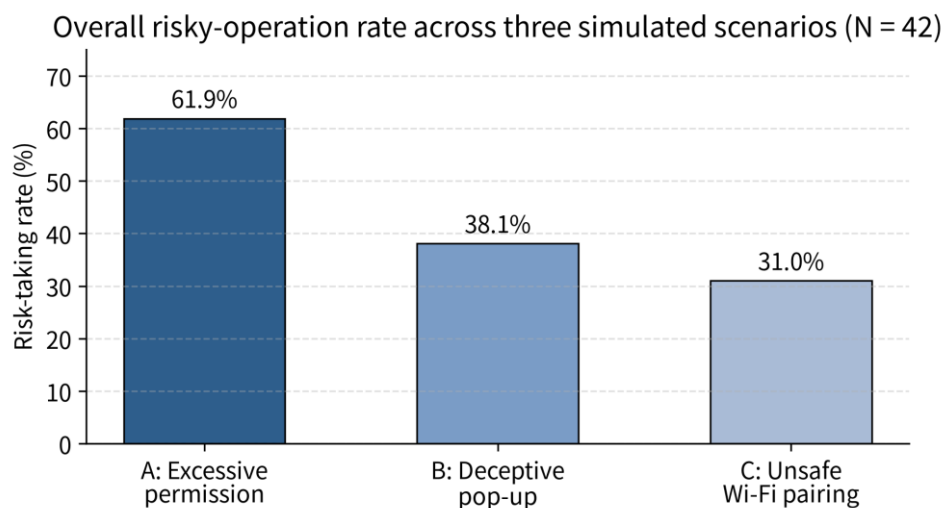


Figure 2. Overall risky-operation rate across the three simulated scenarios

4.2 Impacts of Time Pressure

Table 3 contrasts the risky-operation rates between the time-pressure experimental subgroup and the non-pressure control subgroup.

Table 3. Risk-taking rate comparison: time-pressure group versus non-pressure group

Simulation Scenario	Risk Rate (Time-Pressure, n = 21)	Risk Rate (Non-Pressure, n = 21)
A: Excessive permission granting	80.9%	42.9%
B: Deceptive pop-up approval	57.1%	19.0%
C: Unsafe Wi-Fi pairing	42.9%	19.0%

Across all three scenarios, participants under time-limit pressure displayed substantially higher vulnerability to privacy risks. Even users who would make relatively secure decisions when they have sufficient time tend to adopt quick-click strategies under time constraints, ignoring potential privacy hazards.

4.3 Behaviour Differences Among Age Groups

Figure 3 presents the risk-taking rate distribution across the three age groups under the three simulation scenarios. The 50–65 age bracket shows the highest risky-choice proportion in Scenario A and Scenario B, whereas the 18–29 group still presents high risk-taking rates under time-pressure conditions despite higher digital familiarity.

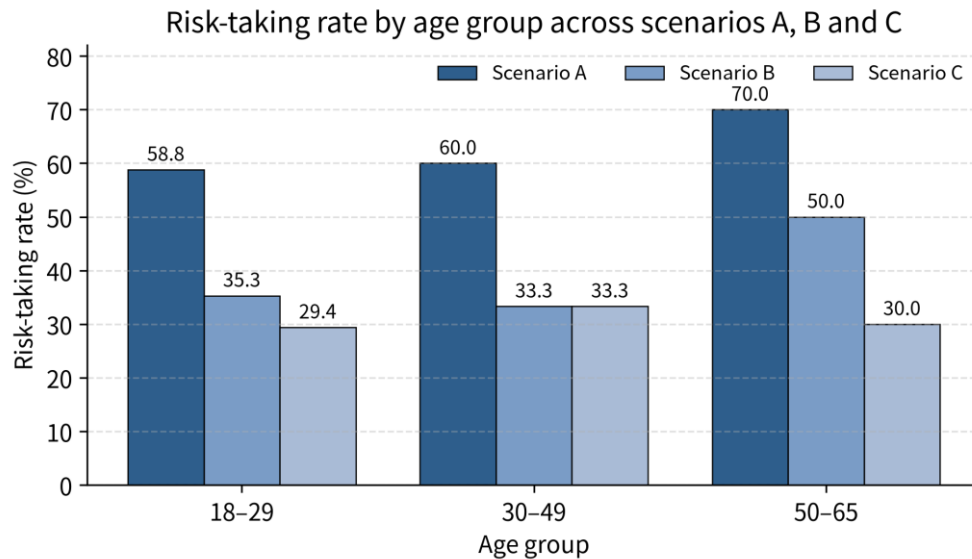


Figure 3. Risk-taking rate by age group across scenarios A, B and C

4.4 Relationship Between Smart-Home Usage Experience and Risk Behaviour

Participants with rich smart-home-device experience did not exhibit obviously safer behavioural patterns. Many participants with long-term device-usage habits formed mechanical operational inertia: they habitually clicked “allow” for various authorisation dialogues regardless of prompt-content details. Some participants mentioned in post-experiment interviews: “I always click allow to get through setup steps quickly; I never read permission text carefully.”

5. Discussion

The empirical pilot-study results demonstrate that smart-home user privacy vulnerability is widespread. Risky behaviour is not limited to older users lacking digital literacy; even young participants with rich digital-device experience make insecure decisions under time-pressure conditions. This observation aligns with previous human-factor cybersecurity theories about warning fatigue and cognitive-load effects (Akhawe & Felt, 2013; Reason, 1990).

The highest risk-taking rate appeared in Scenario A (excessive permission granting). This finding confirms that permission-request interfaces represent a critical weak point for smart-home privacy defence. Most users treat permission pop-ups as obstacles preventing them from using application functions rather than as important security reminders. Deceptive pop-up windows that imitate system-update prompts also achieve high deception-success rates because users tend to trust text carrying “firmware update” and “system maintenance” wording.

Time pressure significantly amplifies user vulnerability. In real-life situations, consumers often want to finish new-device setup as quickly as possible; therefore, laboratory results under time-pressure conditions are closer to real-world household usage contexts. It is insufficient to merely improve technical encryption and firmware security; human cognitive factors must be incorporated during product interface design (Norman, 2013).

5.1 Practical Implications

Several practical suggestions can be derived from the experimental findings. First, application-interface optimisation should avoid displaying dense permission-description text and should separate truly necessary permissions from non-essential ones, delaying non-critical permission requests until the moment functions actually need them instead of requesting all permissions upon first-time installation. Second, anti-deception

design for pop-up windows should adopt unique visual styles for system-level warning dialogues that malicious third-party applications cannot replicate, thereby reducing the success probability of fake deceptive pop-ups. Third, consumer-guidance materials should emphasise risk scenarios such as permission granting and Wi-Fi selection for IoT-device pairing rather than only introducing complex technical knowledge, because short vivid case explanations are more effective than lengthy text descriptions. Fourth, smart-home product regulatory specifications should require manufacturers to strictly limit the permission requests of companion mobile applications and to ban the behaviour of applying for function-irrelevant permissions.

5.2 Study Limitations

This research is a pilot study with a limited sample size ($N = 42$). Participants were recruited through convenience sampling, so the sample cannot fully represent the whole general population. Experiments were performed inside controlled laboratory environments, and user behaviours in real-family surroundings may show slight differences. Further follow-up research will expand the sample scale and add field investigation in real household settings. In addition, this study focuses on behavioural observation; future work can introduce more psychological-scale measurements to explore the underlying cognitive mechanisms.

6. Conclusion and Recommendations

This pilot empirical research investigated user behavioural privacy vulnerability within simulated smart-home IoT scenarios. According to the experimental outcomes, 61.9% of participants granted excessive unnecessary permissions, 38.1% approved deceptive fake authorisation pop-ups, and 31.0% selected unsecure public Wi-Fi for smart-device pairing. Time pressure greatly increases the risky-operation probability, and vulnerable behaviours exist across all age groups and experience levels. Human operational behaviour therefore constitutes a non-ignorable weak link for smart-home privacy protection. Pure technical defence measures cannot offset the risks caused by user mis-operation, and combined efforts from product designers, regulatory authorities and consumer-education organisations are required.

6.1 Recommendations

Based on the findings, the following recommendations are proposed. Smart-home application developers should reconstruct the permission-request interaction logic, minimise over-reaching permission requests and separate essential and non-essential authorisation items. Mobile operating-system vendors should strengthen the visual differentiation mechanisms of genuine system pop-ups against counterfeit application pop-ups. Consumer security-awareness education should adopt scenario-based popular-science content that focuses on permission checking and IoT-device network-selection guidance. Finally, follow-up large-scale empirical studies are needed to further verify behavioural patterns among broader user groups.

References

- Akhawe, D., & Felt, A. P. (2013). Alice in warningland: A large-scale field study of browser security warning effectiveness. In *Proceedings of the 22nd USENIX Security Symposium*. USENIX Association.
- Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing*, 21(2), 34-42.
- Emami-Naeini, P., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F., & Sadeh, N. (2017). Privacy expectations and preferences in an IoT world. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association.
- Hall, F., Maglaras, L., Aivaliotis, T., Xagoraris, L., & Kantzavelou, I. (2020). Smart homes: Security challenges and privacy concerns. *arXiv*. Retrieved from <https://arxiv.org/abs/2010.15394>
- Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4(5), 1125-1142.
- Norman, D. A. (2013). *The design of everyday things* (Revised ed.). Basic Books.
- Reason, J. (1990). *Human error*. Cambridge University Press.
- Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. In *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), Article 85.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).