IoT Software Updates: User Perspectives in the Context of NIST IR 8259A

S. P. Veed, S. M. Daftary,
B. Singh, M. Rudra, S. Berhe
Computer Science and Engineering
University of the Pacific
Stockton, USA
s_parambatheveed@u.pacific.edu, sberhe@pacific.edu

M. Maynard
Data Independence LLC
Ellington, USA
marc@DataIndependenceNow.com

F. Khomh
Polytechnique Montreal
Montreal, Canada
foutse.khomh@polymtl.ca

***Abstract*—The quality of software update systems is critical for the performance, security, and functionality of IoT devices. Grounded in NIST IR 8259A standards, which emphasize secure updates, device integrity, and minimal disruption, this paper evaluates how these requirements align with user expectations and challenges. By examining the standard's technical requirements, the study identifies gaps where user feedback can inform improvements in update mechanisms. A survey of 52 participants provides feedback into user behaviors and concerns regarding software updates. Key challenges include performance degradation, dissatisfaction with interface changes, and inconsistent cross-platform experiences. Users prioritize security alongside performance and feature updates but express reservations about system slowdowns and time-intensive update processes. The findings highlight the need for secure, fast, and user-focused update systems that align with NIST standards. Proposed strategies include lightweight updates, context-aware notifications, and rigorous testing protocols to improve system reliability and user compliance.**

I. Introduction

Consumers increasingly rely on IoT products to manage critical aspects of daily life, including home safety, health, recreation, and personal convenience. However, the heterogeneous design and implementation practices of IoT devices—characterized by vendor-specific protocols, development approaches, and security frameworks—pose significant challenges to both IoT security and consumer usability. Software update systems serve as a critical mechanism for maintaining device performance, introducing new features, and addressing security vulnerabilities. Yet, user feedback reveals persistent issues such as system slowdowns, disruptive interface changes, and inconsistencies across platforms, which undermine the effectiveness of these systems [1].

Software updates are particularly challenging for IoT devices due to their inherent constraints. Limited connectivity, battery capacity, storage, and processing power often restrict the ability to deliver and install updates seamlessly. Moreover, physical access for manual updates or debugging is frequently impractical due to the distributed and embedded nature of IoT devices. Updates must also achieve a high level of reliability, as remote rollbacks are often infeasible, making error-free deployment crucial. These unique challenges further complicate the design and implementation of effective update mechanisms for IoT systems [2].

Updates have a particularly high impact on the user experience, influencing consumer trust and satisfaction. As outlined in NIST IR 8259A, secure and reliable software update mechanisms are essential for mitigating security vulnerabilities and ensuring device longevity. These guidelines highlight practices such as secure transmission, integrity verification, and user notification strategies that prioritize clarity and control. However, NIST IR 8259A primarily focuses on minimum security capabilities and does not comprehensively address system usability and functionality, which are also crucial to overall security. Aligning IoT update systems with these principles while considering usability aspects can significantly improve the user experience by minimizing disruption and maximizing security [3].

The goal of this paper is to evaluate user requirements for software updates and their subsequent impact on the technical requirements of update systems. By examining how user expectations influence the design and implementation of IoT update mechanisms, this research seeks to bridge the gap between consumer needs and technical feasibility. Specifically, we analyze the software update mechanisms mandated by IoT standards, including those outlined in NIST IR 8259A, from a user-centric perspective to assess their adequacy and impact. Additionally, we explore the limitations of NIST IR 8259A within the context of its intended purpose and propose directions for complementary standards that address usability concerns. Furthermore, we aim to provide actionable feedback on how these requirements can be addressed more granularly to improve their relevance and effectiveness [4].

Towards this objective, Section II presents related work on NIST IR 8259A requirements and user evaluation in the IoT context. In Section III, we review the requirements outlined in NIST IR 8259A and the survey structure. Next, Section IV

Workshop on Security and Privacy in Standardized IoT (SDIoTSec) 2025
24 February 2025, San Diego, CA, USA
ISBN 979-8-9919276-6-6
https://dx.doi.org/10.14722/sdiotsec.2025.23078
www.ndss-symposium.org

evaluates how well these requirements were addressed in the user feedback. Section V provides an analysis of the results, with concluding remarks in Section VI.

II. Related Work

The challenge of ensuring timely and effective software updates is critical for maintaining the security and functionality of systems. Mathur et al. (2018) conducted a survey quantifying users' beliefs about software updates, identifying factors such as perceived update costs, necessity, and risks that influence user compliance [5]. Their findings suggest that addressing these user concerns can improve update adoption rates. Similarly, Fagan et al. (2015) examined user perspectives on software update message design, finding that certain design features can lead to confusion and annoyance, thereby affecting user compliance [6]. They recommend designing update messages that are clear and minimize user disruption to improve adoption rates.

Jenkins et al. (2024) investigated the patching behaviors of system administrators, revealing that dedicated testing environments are not as prevalent as assumed and that system administrators employ various problem-solving behaviors when encountering troublesome patches [7]. This highlights the complexity of patch management in organizational settings. Vaniea et al. (2016) explored user experiences with software updates, identifying that users often avoid updates due to concerns about undesirable changes and unclear benefits [8]. They suggest better communication of update benefits to increase user acceptance.

While these studies provide valuable feedback into user behaviors and perceptions of software updates, they largely focus on general-purpose computing systems or enterprise environments. In contrast, our work centers on the unique challenges and constraints associated with IoT devices, as governed by standards such as NIST IR 8259A. Unlike traditional systems, IoT devices are characterized by limited connectivity, battery life, storage, and processing power, which impose significant restrictions on update mechanisms. Additionally, IoT devices often lack physical access for manual updates or debugging, and remote rollback is frequently infeasible, making error-free updates critical.

III. Methodology

This study evaluates the requirements for software updates as outlined, focusing on their alignment with user expectations and technical constraints. The NIST guidelines emphasize secure update mechanisms, including secure transmission, integrity verification, and minimal disruption during updates. These principles form the basis for analyzing user feedback and identifying gaps in the current implementation of IoT update systems.

A. Evaluation of NIST IR 8259A Requirements

The evaluation of NIST requirements involved a detailed review of the standard's prescribed practices for secure and reliable software updates. Key elements analyzed include:

- **Secure Transmission**: Ensuring that updates are delivered through encrypted channels to prevent unauthorized interception.
- **Integrity Verification**: Guaranteeing that updates are applied only if their integrity is confirmed, preventing corrupted or malicious updates.
- **Minimal Disruption**: Designing updates to minimize user impact, considering IoT-specific constraints like limited resources and lack of physical access.

The analysis compared these technical requirements with user-reported challenges and expectations derived from the survey data.

B. Survey Design and Implementation

To capture user perspectives, a survey was conducted with 52 participants, including college students, professionals, and academic staff. The survey included both quantitative and qualitative questions designed to evaluate user experiences and expectations regarding software updates. Participants were recruited through university mailing lists and professional networks. The analysis revealed a tendency among participants to focus on smartphones rather than traditional IoT devices, highlighting a common association of mobile devices with IoT ecosystems. This finding underscores the importance of clarifying how user perspectives on smartphones translate to broader IoT systems, given their distinct operational constraints and functionalities.

C. Survey Questions

The survey was structured around the following key themes:

- **Frequency of Updates**: Participants were asked how often they applied software updates, with options ranging from *immediately upon release* to *rarely or never*.
- **Motivations for Updating**: Participants identified primary reasons for applying updates, such as security, performance improvements, or new features.
- **Barriers to Updating**: Respondents described obstacles to timely updates, including system slowdowns, time constraints, and concerns about changes to the user interface.
- **Preferences for Notifications**: Participants expressed their preferences for notification styles, such as pop-up alerts, scheduled reminders, or silent updates.

D. Data Analysis

Quantitative data were analyzed to identify trends in user behavior and update preferences. Qualitative responses were coded thematically to extract feedback on user concerns and expectations. These findings were then mapped to NIST IR 8259A requirements to assess their adequacy in addressing real-world constraints and user needs.

IV. Results

This section presents the findings from the survey conducted to evaluate user feedback on IoT software updates [1]. The results are divided into quantitative and qualitative analyses, highlighting user behaviors, motivations, and concerns [9].

[1] Survey Result: https://github.com/SE4CPS/SDIoTSec25

TABLE I
QUANTITATIVE RESULTS FROM USER SURVEY

Survey Question	**Percentage**
Frequency of updates (when prompted)	60.0%
Users prioritizing safety as a motivator	56.0%
Users citing performance as a motivator	48.0%
Preference for security updates over feature updates	62.0%
Users concerned about update size	34.0%
Preference for minimally disruptive notifications	72.0%
Preference for automatic updates	65.0%

A. Quantitative Results

Table I summarizes the key quantitative findings from the survey of 52 participants. The data reveals trends in update behaviors, preferences, and barriers.

The majority of participants (60%) reported applying updates only when prompted by system notifications, indicating a reactive approach. Security (56%) and performance improvements (48%) were the primary motivators for installing updates. When asked to prioritize security versus non-security updates, 62% of users indicated a preference for security updates, emphasizing their importance for maintaining device integrity. Concerns about update size (34%) and disruptions to functionality or interface were also frequently mentioned. Notably, 72% of users preferred minimally intrusive notifications, and 65% supported automatic updates to reduce manual effort.

B. Qualitative Results

The qualitative analysis of open-ended survey responses revealed recurring themes regarding user experiences and expectations:

C. Qualitative Results from User Survey

The following key themes emerged from the qualitative analysis of user feedback:

- **Security vs. Non-Security Updates**: A strong preference for security updates emerged among users. One respondent highlighted the necessity of such updates, stating, *"For important safety updates, automatic updates would be better,"* emphasizing the role of automation in maintaining device integrity. Another added, *"Overall security, avoiding zero-day concerns,"* underlining the importance of addressing critical vulnerabilities promptly.
- **Concerns About Disruption**: Many users expressed concerns about system instability or changed functionality post-update. A participant remarked, *"I hesitate to update because new versions often change features I rely on, making them harder to use."* Another added, *"Sometimes the phone/app is slower because of faults in the update."*
- **Resource Constraints**: Resource limitations, especially on older devices, were frequently cited. One user explained, *"My device slows down significantly after updates, and I run out of space quickly."* Another noted that updates *Might take up extra storage.*
- **Notification Preferences**: Respondents highlighted the need for user-friendly notifications. As one participant suggested, *"I'd like updates to occur at night, with a summary of changes provided afterward."*
- **Trust in Stability**: Past issues with bugs and performance led to hesitation among users. One comment was, *"After some updates, my phone slowed down and even started overheating occasionally."* Similarly, three users noted that *"Yes, I have after installing updates sometimes phone hangs-up and reduces the speed and sometimes it heats up"* and *"Some bugs and sometimes existing features have not worked properly"* and *"I've seen updates cause compatibility problems with other software, leading to crashes or unexpected errors. Sometimes, performance drops occur, especially on older systems, where new features might be too demanding."*
- **Scheduling and Timing of Updates**: Flexible scheduling emerged as a critical factor. One respondent noted, *"I prefer updates to happen when I'm not actively using my device. It's frustrating when an update disrupts my workflow unexpectedly."* Similarly, another user noted *"Not important, I rather control the timing of updates."*
- **Clarity in Update Descriptions**: Users emphasized the importance of clear descriptions. A participant remarked, *"If I know exactly what's changing or improving, I'm more likely to install the update immediately."*

D. Key Observations

The survey results indicate that while users value safety, performance, and feature improvements, their concerns about disruption, resource constraints, and stability remain significant barriers. Notably, most, if not all, participants referred to smartphone-related updates, which are often integral to IoT ecosystems. Security updates are viewed as critical, with users prioritizing them over feature updates. The need for flexible scheduling and transparent communication about update content emerged as important factors influencing user compliance. This feedback underscores the necessity of designing update mechanisms that prioritize transparency, efficiency, and user control to address user hesitations effectively.

V. DISCUSSION

The findings from this study provide valuable user-centric feedback that can complement the technical requirements outlined in the NIST IR 8259A IoT standard for software updates. By integrating user preferences and behaviors, these results help bridge the gap between technical feasibility and real-world usability, improving the effectiveness of IoT update mechanisms.

A. Security vs. Non-Security Updates

NIST IR 8259A emphasizes the importance of secure and reliable update mechanisms to address vulnerabilities in

IoT devices. Our findings reveal that users prioritize security updates over feature updates, viewing them as critical for maintaining device integrity. However, this preference is accompanied by hesitations about update stability and performance impacts. Incorporating clear distinctions between security-critical and optional feature updates into the update design could improve user trust and compliance, aligning with the NIST emphasis on secure and reliable operations.

B. Minimizing Disruption and Improving Stability

IoT devices are often resource-constrained, with limited storage, battery life, and processing power. These constraints exacerbate user concerns about performance degradation and system instability after updates. While NIST IR 8259A emphasizes minimal disruption during updates, our results suggest that users require more tangible assurances, such as flexible scheduling options and detailed change logs. These features can help mitigate perceived risks, ensuring updates are delivered seamlessly without impacting device functionality.

C. Lightweight Updates for Resource-Constrained Devices

A significant concern identified in this study was the impact of updates on resource-constrained devices, particularly in terms of storage and processing power. Lightweight updates, which minimize download size and installation time, are essential for IoT devices with limited resources. Incremental updates, which only deliver changes to the existing software rather than a full replacement, can further reduce the resource burden. These strategies align with the NIST emphasis on ensuring updates are compatible with diverse IoT environments and maintaining device usability. Additionally, clear communication about update size and resource requirements can improve user confidence and compliance, particularly in bandwidth-constrained or battery-sensitive scenarios.

D. Transparent and Context-Aware Notification Systems

The NIST standard highlights the importance of notifying users about updates in a secure and accessible manner. Our findings underscore the need for adaptive notification strategies that align with user preferences, such as scheduled reminders or nighttime installations. Transparent communication about update content, including the purpose, expected benefits, and potential risks, can further encourage compliance. By integrating user-preferred notification styles, IoT standards can better cater to diverse user contexts while maintaining security priorities.

E. User Control and Automatic Updates

While automatic updates are a practical solution for ensuring timely security patches, our findings reveal mixed user preferences. While some users appreciate the convenience of automatic updates, others emphasize the need for control over timing and content. This duality suggests that IoT update mechanisms should provide configurable settings, allowing users to balance automation with manual control. Such flexibility can support diverse user preferences while adhering to the NIST guideline of maintaining user awareness during updates.

F. Contributions to IoT Standards

The integration of user perspectives into IoT update standards offers several benefits:

- Aligning technical requirements with real-world user constraints, such as resource limitations and usability concerns.
- Improving compliance rates by addressing user priorities, including security, performance, and flexibility in update mechanisms.
- Improving transparency and trust through clear communication about update purposes and expected outcomes.
- Incorporating lightweight updates to reduce the burden on resource-constrained IoT devices and environments.

By incorporating these findings, IoT standards like NIST IR 8259A can achieve greater relevance and effectiveness, ensuring that update mechanisms meet both technical and experiential needs.

G. Future Directions

This study highlights the importance of understanding user perspectives in the design of IoT update mechanisms. Future work could explore:

- The impact of lightweight and incremental updates on compliance and user satisfaction.
- Contextual differences in update behaviors and preferences.
- Real-world testing of user-centered update designs in diverse IoT environments.

These directions will further improve the usability and adoption of IoT standards in software update systems.

VI. Conclusion

Software updates are essential for maintaining the security, functionality, and longevity of IoT devices, as emphasized in NIST IR 8259A. However, the unique constraints of IoT devices, such as limited resources, reliance on remote management, and the critical need for reliability, present challenges that cannot be addressed by technical standards alone. This study underscores the value of integrating user feedback into the design of update mechanisms, revealing that while users prioritize security updates, they often hesitate due to concerns about stability, resource impact, and usability.

Key findings from this research highlight the importance of lightweight updates, transparent communication about update content, and flexible scheduling to improve user compliance and satisfaction. These user-centered improvements can help bridge the gap between technical feasibility and real-world usability, ensuring that updates meet both security needs and user expectations. By incorporating user perspectives, IoT update systems can foster greater trust and adoption, aligning with the overarching goals of NIST standards. Future work should expand these findings through diverse user studies and real-world testing to refine and optimize update practices for IoT ecosystems.

REFERENCES

[1] M. Nordahl, A. Åkesson, B. A. Johnsson, G. Hedin, and B. Magnusson, "Software component update for iot systems," in *2024 11th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pp. 124–131, 2024.

[2] S. El Jaouhari and E. Bouvet, "Secure firmware over-the-air updates for iot: Survey, challenges, and discussions," *Internet of Things*, vol. 18, p. 100508, 2022.

[3] M. Fagan, M. Fagan, K. N. Megas, K. Scarfone, and M. Smith, *Foundational cybersecurity activities for IoT device manufacturers*. US Department of Commerce, National Institute of Standards and Technology, 2020.

[4] I. Mugarza, J. L. Flores, and J. L. Montero, "Security issues and software updates management in the industrial internet of things (iiot) era," *Sensors*, vol. 20, no. 24, 2020.

[5] A. Mathur and M. Chetty, "Understanding software update behavior via surveying user perceptions and practices." https://arxiv.org/pdf/1805.04594, 2018. [Accessed 08-09-2024].

[6] M. Fagan, M. M. H. Khan, and R. Buck, "A study of users' experiences and beliefs about software update messages," *Computers in Human Behavior*, vol. 51, pp. 504–519, 2015.

[7] A. D. G. Jenkins, L. Liu, M. K. Wolters, and K. Vaniea, "Not as easy as just update: Survey of system administrators and patching behaviours," in *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, (New York, NY, USA), Association for Computing Machinery, 2024.

[8] K. Vaniea and Y. Rashidi, "Tales of software updates: The process of updating software," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2016.

[9] Anonymous, "User feedback survey on software updates." https://docs.google.com/spreadsheets/d/1eYwnCIetIa4YOFkRJ119jJlmOnrQVdFSIuUkm1i8vUg/edit?usp=sharing, 2024. [Accessed 12-12-2024].