Poster: An Analysis of IoT Device Manufacturer's Security Advice to Users Through Companion Apps

Ryota Honda*, Junnosuke Kushibiki*, Takayuki Sasaki*, Simon Parkin†*,
Carlos H. Gañán†*, Michel van Eeten†*, Katsunari Yoshioka*
*Yokohama National University, †Delft University of Technology

Abstract—**Device manuals, management web interfaces, and companion apps associated with IoT devices are typical communication channels for informing users about security risks, such as vulnerable firmware, and their countermeasures. Among these channels, management web interfaces and companion apps have the advantage of dynamically providing information based on device status and user interactions, potentially motivating users to take action compared to static channels such as device manuals. However, research on how effectively manufacturers utilize these channels to deliver such information remains limited. Large-scale studies of management web interfaces are challenging due to the need for physical devices. Therefore, this study focuses on companion apps for IoT devices that are available in app stores. We analyzed resource files from Android apps to examine the messages displayed to users. The analysis included 41 apps from 33 manufacturers of routers, NAS devices, printers, and network cameras. Of the 24 apps for devices without auto-update functionality, 13 failed to provide messages encouraging firmware updates.**

I. Introduction

The rise of cyber-attacks targeting IoT devices has highlighted the critical need for effective risk management by users. To address security vulnerabilities resulting from user inappropriate use, research institutions and government agencies are providing security advice to device users [1], [2]. IoT manufacturers also provide security-related information through various channels, including device manuals, websites, configuration interfaces, and companion apps. Compared to third-party notifications, manufacturer-provided security advice is considered more effective because it can be delivered directly during device setup and use. Specifically, user interfaces, such as web interfaces and companion apps, can deliver essential security information during device setup and configuration.

Research on the state of notifications and information provision by device manufacturers has revealed that some manuals of devices with Telnet and FTP capability fail to mention the use of such unencrypted communication protocols or the associated risks [3]. Furthermore, an analysis of IoT device manuals and support pages indicated that they lack sufficient information about the security features of the devices [4]. In contrast, although some studies have examined companion apps, none have focused on the security advice they provide, leaving the full scope of such advice unclear. Additionally, since companion app analysis does not require physical devices, it enables large-scale studies to be conducted.

This study analyzes companion apps and the risk messages displayed by the apps to understand how device manufacturers communicate risk through these apps. We collected publicly available companion apps for home IoT devices from the Google Play Store. From these, we extracted messages from 41 apps with Japanese data in their resource files, identified security notification messages, and evaluated their content.

II. Research questions

This research addresses the following questions to assess and enhance the effectiveness of security advice in companion apps for IoT devices, with the goal of encouraging users to adopt countermeasures:

RQ1. What security risks and countermeasures are communicated to users in companion apps for IoT devices?

RQ2. What security advice do IoT manufacturers provide through apps when devices require users to take security actions?

III. Method

Collection of companion apps. We collected companion apps for routers, printers, network cameras, and NAS devices from the Google Play Store. Specifically, we selected apps with XML resource files in Japanese. As each manufacturer typically provides a single app supporting multiple products, we collected 41 apps from 33 manufacturers. Specifically, we collected 11 apps for routers, 9 for NAS, 11 for printers, and 10 for network cameras.

Analysis of security advice in companion apps. We decompiled each app and extracted the resource files in the `values`, `values-ja`, and `values-ja-rJP` subdirectories within the `res` directory. Next, we manually investigated the text strings in the resource files to determine what security advice was given for each category of router, NAS, printer, and network camera.

We then examined security advice associated with firmware updates, initial password changes, and password formats, which are common security recommendations for IoT devices. Specifically, we classified the security advice based on the clarity of the description of the security risk and the clarity of the statement recommending measures to address the security risk (Table I).

Furthermore, if the initial password is unique for each device, users are not required to proactively change the password. Therefore, we investigated the initial passwords of IoT devices.

TABLE I
LIST OF EVALUATION ITEMS AND CRITERIA

Evaluation item	Evaluation level	Evaluation criteria
Explanation of security risks	●	The description clearly explains the security risks that may arise if the countermeasures are not implemented. The explanation includes keywords clearly related to security, such as “security” or “safety.”
	◐	The description is unclear whether it refers to actual security risks. The description includes keywords that might be related to security, such as “bug” or “stability.”
	○	The description does not provide any explanation of security risks.
Recommendation of measures	●	The description clearly recommends countermeasures or explicitly states that countermeasures are necessary. Alternatively, it uses imperative language to instruct the user to take action.
	◐	The description includes methods to mitigate risks but lacks recommendations or a statement of necessity.
	○	The description does not mention any countermeasures.

TABLE II
SECURITY ADVICE FOUND IN COMPANION APPS

Device category	Security advice
Router	Importance of firmware updates, Importance of initial password changes, Password format, Risk of port forwarding, Risk of enabling DMZ, Risk of turning the security functions off, Recommendation to disable guest logins, Risk of accepting untrusted certificate
Printer	Importance of firmware updates, Importance of initial password changes, Password format, Risk of accepting untrusted certificate, Risk of using unsecured communication
Network camera	Importance of firmware updates, Importance of initial password changes, Password format, Risk of using unencrypted networks, Benefit of two-step authentication, Risk of third-party products
NAS	Importance of firmware update, Importance of initial password changes, Password format, Risk of accepting untrusted certificate, Risk of third-party products

TABLE III
INVESTIGATION RESULT OF SECURITY ADVICE

Risk explanation	●(Clear)			◖ (Unclear)			○(No desc.)			Total
Recommendation of measures	●	◖	○	●	◖	○	●	◖	○	
Firmware update	6	1*	0	4	2*	0	1	8*	2*	24
Initial password change	1	1†	0	0	0	0	2	0	6†	10
Password format	5	0	0	0	0	0	19	0	4‡	28

* 13 apps do not include messages recommending updates
† 7 apps did not include messages suggesting password changes
‡ 4 apps have no messages addressing the risks of using simple passwords or recommending countermeasures

Similarly, if firmware auto-update is enabled by default, users are relieved from performing update tasks themselves. Thus, we also examined the default settings for firmware auto-updates.

IV. RESULTS

Answer to RQ1. Through analysis of the resource files, we identified security advice across all device categories, including recommendations on updating firmware, changing the default password, and password formats. Additional security advice was also found within each IoT device category. A summary of these recommendations is provided in Table II.

Answer to RQ2. Table III presents the evaluation results for risk descriptions and recommended measures, with a focus on apps that require users to take security actions. Among the 24 apps capable of updating firmware but lacking an automatic update feature, 13 did not include messages recommending updates. Additionally, for 4 out of 28 apps that support device password updates, we found no messages addressing the risks of using simple passwords or recommending countermeasures. In the case of devices with a common initial password requiring user updates, 7 out of 10 apps with password update functions did not include messages suggesting password changes. Overall, many apps provide either risk explanations or user measure recommendations, but not both.

V. CONCLUSION AND FUTURE WORK

We investigated the security advice displayed in apps bundled with IoT devices and found the following: the explanation of security risks related to password formats is insufficient, many devices that require an initial password change do not provide such an explanation, and some devices lack adequate information about firmware updates. Therefore, improvements are needed for the explanation of security risks across various devices.

The survey was conducted in Japanese. However, because the resource files contain one-to-one mappings of strings across languages, and no discrepancies in evaluation results were found between Japanese and English, we expect that an equivalent survey in English would yield similar results.

The survey did not assess when security advice is presented to users. In future work, we aim to explore this by conducting actual user study with people actively using the devices. Additionally, we intend to examine security advice delivered through alternative channels, such as device manuals and web interfaces.

ACKNOWLEDGMENT

This paper is based on results obtained from a project, JPNP24003, commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

REFERENCES

[1] C. Utz, M. Michels, M. Degeling, N. Marnau, and B. Stock, “Comparing large-scale privacy and security notifications,” in *PETS 2023*, July 2023.

[2] T. Sasaki, T. Inazawa, Y. Yamaguchi, S. Parkin, M. v. Eeten, K. Yoshioka, and T. Matsumoto, “Am i infected? lessons from operating a large-scale iot security diagnostic service,” in *34th USENIX Security Symposium*, 2025. To appear. Preprint available as arXiv:2501.07326.

[3] Takayuki Sasaki et al,, “Who left the door open? investigating the causes of exposed iot devices in an academic network,” *IEEE S&P 2024*, 2024.

[4] S. D. J. John M Blythe, Nissy Sombatruang, “What security features and crime prevention advice is communicated in consumer iot device manuals and support pages?,” *Journal of Cybersecurity, Volume 5, Issue 1*, 2019.

An Analysis of IoT Device Manufacturer's Security Advice to Users Through Companion Apps

Ryota Honda*, Junnosuke Kushibiki*, Takayuki Sasaki*, Simon Parkin†,
Carlos H. Gañán†,*, Michel van Eeten†,*, Katsunari Yoshioka*

*Yokohama National University, †Delft University of Technology

1. Motivation

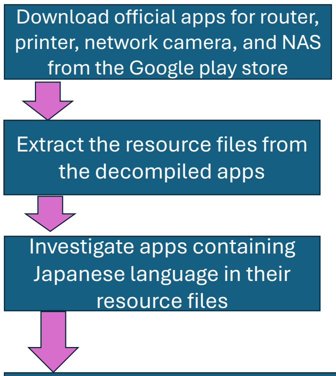
- Manufacturers provide security advice through device manuals, web interfaces, and companion apps to assist users in managing their devices.
- The effectiveness of this advice remains unclear, and the delivery methods are not well-studied.
- Given the lack of research on companion apps as a delivery channel, our study focuses on this particular method.

2. Research Questions

RQ1: What security risks and countermeasures are communicated to users in companion apps for IoT devices?

RQ2: What security advice do IoT manufacturers provide through apps when devices require users to take security actions?

3. Method



Download official apps for router, printer, network camera, and NAS from the Google play store

Extract the resource files from the decompiled apps

Investigate apps containing Japanese language in their resource files

Researchers manually examine the security advice in the resource files to assess:

- The types of security risks and countermeasures presented
- Any variations in the security advice provided.

An example of a resource file

```
<resources>
  <string name="example">This is an
  example</string>
</resources>
```

Selection of companion

Device category	#Manufacturers	#Apps
Router	11	11
Printer	11	11
Network camera	10	10
NAS	7	9
Total	33	41

Note: The survey was conducted in Japanese. However, because the resource files contain one-to-one mappings of strings across languages, we expect that an equivalent survey in English would yield similar results.

4. Security advice in companion apps

Companion apps of across all device categories include advice of

- Importance of firmware updates
- Importance pf initial password changes
- Password format

Other security advices

Device category	Other security advices
Router	Risk of port forwarding, enable DMZ, turning the security functions off and accepting untrusted certificate Recommendation to disable guest logins
Printer	Risk of accepting untrusted certificate and using unsecured communication
Network camera	Risk of using unencrypted networks, Risk of third-party products. Benefit of two-Step authentication
NAS	Risk of accepting untrusted certificate, Risk of third-party applications

5. Evaluation of security advice

We evaluated the security advice related to firmware updates, initial password changes, and password formats.

Evaluation item	Evaluation level	Evaluation criteria
Explanation of security risks	●	The description clearly explains the security risks that may arise if the countermeasures are not implemented. The explanation includes keywords clearly related to security, such as "security" or "safety."
	◐	The description is unclear whether it refers to actual security risks. The description includes keywords that might be related to security, such as "bug'' or "stability."
	○	The description does not provide any explanation of security risks.
Recommendation of measures	●	The description clearly recommends countermeasures or explicitly states that countermeasures are necessary.
	◐	The description includes methods to mitigate risks but lacks recommendations or a statement of necessity.
	○	The description does not mention any countermeasures.

6. Evaluation result

- Apps of 11 devices lack adequate information about firmware updates
- Apps of 8 devices that require an initial password change do not provide such an explanation
- The explanation of security risks related to password formats is insufficient in apps of 23 devices

Details of App Evaluation Results

Risk Description	●(Clear)			◐(Unclear)			○(No desc.)			
Recommendation	●	◐	○	●	◐	○	●	◐	○	Total
Firmware update	6	1	0	4	2	0	1	8	2	24
Initial password change	1	1	0	0	0	0	2	0	6	10
Password format	5	0	0	0	0	0	19	0	4	28

7. Conclusion

- Answer to RQ1: We identified security advice across all device categories, including recommendations on updating firmware, changing the default password, and password formats. Additional security advice was also found within each IoT device category.
- Answer to RQ2: Some apps provide no advice on measures, despite the user's need to take action. Improvements are needed for the security advice about security risks and measures across various devices.

8. Future work

- The survey did not examine the timing of when security advice is displayed to users. We plan to address this aspect in future work, including conducting dynamic analysis of app behavior.
- We also plan to investigate security advice delivered through other channels, such as device manuals and web interfaces.

This poster is based on results obtained from a project, JPNP24003, commissioned by the New Energy and Industrial Technology Development Organization (NEDO).