Poster: DarkWrt: Towards Building a Dataset of Potentially Unwanted Functions in IoT Devices

Daichi Uezono*, Junnosuke Kushibiki*, Takayuki Sasaki*, Satoshi Hara*‡,
Yury Zhauniarovich†, Carlos H. Gañán†*, Michel van Eeten†*, Katsunari Yoshioka*
*Yokohama National University, †Delft University of Technology, ‡FUJISOFT

***Abstract*—IoT device firmware may contain hidden mechanisms that allow unauthorized access or functionality, posing serious security risks. Developing effective countermeasures against these potentially unwanted functions requires datasets that reflect real-world implementation patterns. However, most existing research focuses on package repositories, limiting their applicability to embedded devices. In this study, we systematically investigated potentially unwanted functions in IoT devices by analyzing 23 cases across various network devices. Our analysis showed that manufacturers and OSS developers employed methods such as hardcoding and system configuration file modifications. We classified these cases based on triggers (authentication bypass, undisclosed service, undisclosed command, and time) and capabilities (privilege escalation, data breach, configuration change, and kill switch). To support further research, we developed DarkWrt, a dataset for evaluating detection techniques of potentially unwanted functions. Based on OpenWrt, DarkWrt implements various examples of these functions and will be made available to the research community.**

I. Introduction

IoT devices have become increasingly prevalent in our daily lives, but their security implications remain a serious concern. The complex supply chains involved in IoT device manufacturing and development create numerous opportunities for various stakeholders to covertly embed unwanted functionalities, making security assurance particularly challenging. Of particular interest are intentionally embedded capabilities that enable unauthorized access or functionality beyond device specifications. We define these intentionally embedded, undesired capabilities as “potentially unwanted functions.”

To develop effective countermeasures, a comprehensive dataset of implementation patterns is essential. However, the existing dataset [2] focuses mainly on package repositories, limiting its relevance to embedded devices. Moreover, while a previous study [1] has investigated potentially unwanted functions in IoT devices, creating an effective dataset requires a detailed analysis of their implementation, particularly the triggering mechanisms and capabilities.

To address this issue, we conducted a systematic investigation of potentially unwanted functions in IoT devices. Specifically, we analyzed 23 cases across various device types, including routers, NAS, firewalls, VPN gateways, network cameras, and VoIP devices. Our investigation methodology involved keyword searches using Google search engine and the Japan Vulnerability Notes (JVN) database. By systematically searching through diverse sources including security advisories, vulnerability reports, vendor notifications, and news articles in multiple languages, we achieved reasonably comprehensive coverage of documented cases. The analysis revealed common implementation patterns by manufacturers and OSS developers, such as hardcoding and embedding functions in system configuration files. We classified these cases based on their triggers (authentication bypass, undisclosed service, undisclosed command, and time) and capabilities (privilege escalation, data breach, configuration change, and kill switch).

Based on the results of our systematic analysis, we developed DarkWrt, a modified version of the OpenWrt Linux distribution for embedded routers, embedding potentially unwanted functions in it. DarkWrt includes hidden authentication accounts, hard-coded credentials, privilege escalation, data breaches, configuration changes, kill switches, and trace removal capabilities. It can be used to develop and evaluate detection techniques for potentially unwanted functions.

II. Taxonomy of Potentially Unwanted Functions

Our taxonomy emerged from analyzing potentially unwanted functions found in IoT devices. While a previous study [1] classifies these functions into Special credentials, Hidden functionality, and Unintended network activity, this classification lacks the granularity needed for creating comprehensive test datasets. Based on our systematic investigation of 23 real-world cases, we developed a classification framework based on two aspects: triggers and capabilities. Through iterative refinement, we established mutually exclusive categories that provide comprehensive coverage of the observed cases. Specifically, we classify the triggers of potentially unwanted functions into four categories: authentication bypass, undisclosed service, undisclosed command, and time. Similarly, we categorize their capabilities into four types: privilege escalation, data breach, configuration change, and kill switch.

III. Survey of Potentially Unwanted Functions

We organize the investigated cases from two perspectives: triggers and capabilities. Our analysis includes the actors who embedded these functions, their implementation and concealment methods, and the resulting impacts. We investigated cases through keyword searches (e.g., vulnerability, potentially unwanted function, backdoor, kill switch, data breach, and configuration change) using Google search engine and

TABLE I
LIST OF INVESTIGATED POTENTIALLY UNWANTED FUNCTIONS

Triggers: AB: Authentication Bypass, US: Undisclosed Service, UC: Undisclosed Command, TI: Time

Capabilities: PE: Privilege Escalation, DB: Data Breach, CC: Configuration Change, KS: Kill Switch

Product	Triggers				Capabilities				Embedded by	Notes
	AB	US	UC	TI	PE	DB	CC	KS		(Embedding/Concealment Methods)
LG Mobile Wi-Fi Router	✓				✓	✓			–	–
Jetstream/Wavlink Routers	✓	✓	✓		✓	✓			FW Vendor	Hardcoded, Scripts in bin directory
Dahua Router	✓				✓	✓			Device Vendor	–
Netis Router		✓			✓				Device Vendor	Hardcoded
D-Link Router	✓	✓	✓		✓		✓		Device Vendor	Hardcoded, Port listening
Sercomm FW Router		✓			✓				FW Vendor	Port listening
TP-Link Router			✓		✓	✓	✓	✓	Device Vendor	Hidden HTTP request implementation
Uniway Router			✓					✓	–	Embedded in component files
Trendnet Webcam			✓			✓			Device Vendor	–
Xiongmai Camera		✓	✓		✓		✓		Device Vendor	–
ADUPS FW Smartphones				✓		✓			FW Vendor	Embedded in FW update system
Samsung Smartphone			✓			✓	✓		Device Vendor	–
Qihoo360 Smartwatch			✓			✓			FW Vendor	Embedded in apps and packages
Harman AMX Products	✓		✓		✓	✓			Device Vendor	Hardcoded
Huawei Devices	✓				✓				Device Vendor	Hardcoded
Dbltek VoIP Devices	✓				✓				Device Vendor	Embedded in Telnet management interface
Seagate HDD		✓			✓				Device Vendor	Undocumented Telnet functionality
Western Digital NAS	✓		✓		✓	✓			–	Hardcoded
Zyxel Devices	✓				✓				Device Vendor	Hardcoded, Hidden in user interface
ASML EUV Equipment								✓	Device Vendor	–
ScreenOS	✓	✓			✓	✓			–	Hardcoded
XZ Utils	✓				✓				OSS Developer	Disguised as legitimate commit
SSH Decorator			✓		✓	✓			–	Disguised as library update

*Note: FW stands for firmware.

vulnerability information database. Table I summarizes the investigated cases.

IV. DARKWRT: DATASET OF POTENTIALLY UNWANTED FUNCTIONS

To facilitate research on detecting potentially unwanted functions in IoT devices, we created DarkWrt by modifying OpenWrt, an open-source Linux distribution for routers. Unlike datasets that only provide source code or binaries, DarkWrt can be deployed as a fully functional router, enabling both static and dynamic analysis. DarkWrt implements the following potentially unwanted functions:

- Hidden accounts for WebUI and SSH authentication
- Hard-coded credentials
- Privilege escalation capabilities (root group account addition, password-less sudo execution)
- Data breach functions (packet sniffing, time-triggered data transfer, configuration information retrieval)
- Configuration modification features (port-based Telnet backdoor, firewall settings manipulation)
- Kill switch (denial-of-service capabilities)
- Trace removal function

In our preliminary evaluation, a security-knowledgeable student examined functions in DarkWrt. Through static and dynamic analysis, they discovered basic functions like hidden accounts, but failed to detect sophisticated implementations such as obfuscation. This demonstrates DarkWrt's utility in evaluating detection approaches.

DarkWrt will be available to researchers upon request. We plan to continuously update the dataset with new implementations to establish it as a benchmark for potentially unwanted function detection research.

V. CONCLUSION AND FUTURE WORK

We investigated potentially unwanted functions and classified them by their triggers and capabilities. Using this classification, we developed DarkWrt – a dataset that implements the identified patterns.

To expand the dataset beyond our limited resources, we propose a two-phase collaborative approach involving security experts: (1) simulated attackers embed potentially unwanted functions into the firmware, and (2) separate experts analyze the firmware. Through iterative cycles of this embedding–detection process, we aim to build a comprehensive knowledge base. We are currently conducting pilot trials within our laboratory to validate this approach.

ACKNOWLEDGEMENT

This work was supported by JST [K Program] Japan Grant Number [JPMJKP24K2].

REFERENCES

[1] Soheil Hashemi and Mani Zarei. Internet of things backdoors: Resource management issues, security challenges, and detection methods. *Transactions on Emerging Telecommunications Technologies*, 32(2):e4142, 2021.

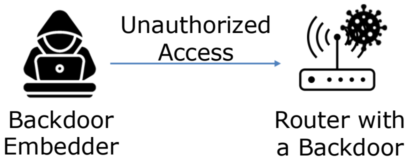
[2] Marc Ohm et al. Backstabber's knife collection: A review of open source software supply chain attacks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 2020.

Poster: DarkWrt: Towards Building a Dataset of Potentially Unwanted Functions in IoT Devices

Daichi Uezono[1], Junnosuke Kushibiki[1], Takayuki Sasaki[1], Satoshi Hara[1,3],
Yury Zhauniarovich[2], Carlos H. Ganan[2,1], Michel van Eeten[2,1], Katsunari Yoshioka[1]
[1]Yokohama National University, [2]Delft University of Technology, [3]FUJISOFT

1 Introduction

It has been reported that potentially unwanted functions, such as data exfiltration and backdoor capabilities, have been covertly embedded in IoT devices through the complex software supply chain.



2 Definition of Potentially Unwanted Functions

- We define vulnerabilities that possess "**intentionality**" and "**unacceptability**" as potentially unwanted functions.
- **Intentionality**: Mechanisms deliberately introduced by developers or manufacturers, rather than accidental flaws.
- **Unacceptability**: Mechanisms that are not socially acceptable due to their potential to cause harm to individuals, organizations, or society.

3 Taxonomy of Potentially Unwanted Functions

To systematically categorize reported cases of potentially unwanted functions, we developed a classification framework based on two key aspects: **triggers** and **capabilities**.

- We aimed for comprehensive coverage of all known cases, ensuring that each trigger or capability was uniquely classified without overlap.
- Through iterative refinement, these categories were established to effectively classify our collected cases.

Trigger-based Classification

Authentication Bypass	Undisclosed Command
Undisclosed Service	Time

Capability-based Classification

Privilege Escalation	Data Breach
Configuration Change	Kill Switch

4 Survey of Potentially Unwanted Functions

- Our investigation methodology involved using Google search engine and vulnerability information database to identify cases through keyword searches (e.g., "vulnerability," "potentially unwanted function," "IoT," "backdoor," "kill switch," "information leakage," and "configuration change").
- For each identified case, we investigated the triggers and capabilities involved. Additionally, we analyzed the actors who embedded these functions, along with their implementation and concealment methods.

List of potentially unwanted functions investigated

AB: Authentication Bypass
US: Undisclosed Service
UC: Undisclosed Command
TI: Time

PE: Privilege Escalation
DB: Data Breach
CC: Configuration Change
KS: Kill Switch

Product	Trigger				Capability				Embedder	Notes
	AB	US	UC	TI	PE	DB	CC	KS		
LG Mobile Wi-Fi Router	✓				✓	✓			-	-
Jetstream, Wavlink Routers	✓	✓	✓		✓	✓			FW Manufacturer	Hardcoded, Scripts in bin directory
Dahua Router	✓				✓	✓			Device Manufacturer	-
Netis Router		✓			✓				Device Manufacturer	Hardcoded
D-Link Router	✓	✓	✓		✓		✓		Device Manufacturer	Hardcoded, Port listening
Sercomm FW Router		✓			✓				FW Manufacturer	Port listening
TP-Link Router			✓		✓	✓	✓	✓	Device Manufacturer	Hidden HTTP request implementation
Uniway Router			✓					✓	-	Embedded in component files
Trendnet Webcam			✓			✓			Device Manufacturer	-
Xiongmai Camera		✓	✓		✓		✓		Device Manufacturer	-
ADUPS FW Smartphone				✓		✓			FW Manufacturer	Embedded in FW update system
Samsung Smartphone			✓			✓	✓		Device Manufacturer	-
Qihoo360 Smart Watch			✓			✓			FW Manufacturer	Embedded in apps and packages
Harman AMX Product	✓		✓		✓	✓			Device Manufacturer	Hardcoded
Huawei Device	✓				✓				Device Manufacturer	Hardcoded
Dbltek VoIP Device	✓				✓				Device Manufacturer	Embedded in Telnet management interface
Seagate HDD		✓			✓				Device Manufacturer	Undocumented Telnet functionality
Western Digital NAS	✓		✓		✓	✓			-	Hardcoded
Zyxel Device	✓				✓				Device Manufacturer	Hardcoded, Hidden in user interface
ASML EUV Equipment								✓	Device Manufacturer	-
ScreenOS	✓	✓			✓	✓			-	Hardcoded
XZ Utils	✓				✓				OSS Developer	Disguised as legitimate commit
SSH Decorator			✓		✓	✓			-	Disguised as library update

5 DarkWrt: Dataset of Potentially Unwanted Functions

- DarkWrt is a dataset of potentially unwanted functions created by modifying OpenWrt, a widely used open-source router firmware.
- Since our investigation found no publicly available source code implementations of these functions, we implemented them ourselves based on our classification.
- By implementing DarkWrt as a fully functional router firmware rather than just providing code or binaries, DarkWrt enables both static analysis and dynamic analysis.

Privilege Escalation	•Hidden accounts in WebUI and SSH •Modification of the authentication mechanism •Function to add an account to the root group •Function to enable SUDO usage without a password
Data Breach	•Packet sniffing function •Configuration information retrieval function •Data exfiltration function
Configuration Change	•Function to activate Telnet •Function to modify firewall configuration
Kill Switch	•Denial of service function
Trace Erasure	•Function to remove the added functions

6 Future Work

- The primary challenge is expanding the dataset, which is difficult to achieve with our resources alone.
- To address this, we propose a two-phase collaborative approach: security experts first act as attackers to implement potentially unwanted functions, followed by separate experts analyzing the modified firmware. Through iterative cycles of this process, we aim to build a comprehensive knowledge base.
- We are currently conducting trials of this approach in our laboratory.

[Acknowledgement] This work was supported by JST [K Program] Japan Grant Number [JPMJKP24K2].