Exploring Hardware Vulnerabilities in Smartwatch Security: A Comprehensive Study

Mr. Raihan Patel [1, *], Dr. Harshal Arolkar [2]
[1, 2] Faculty of Computer Applications & Information Technology, GLS University, India
Email: [1] raihan.patel@glsuniversity.ac.in, [2] Harshal.arolkar@glsuniversity.ac.in
*Corresponding Author

Abstract—**Smartwatches have gained widespread adoption across the world. In today's day and age, the smartwatches comes with the integration of advanced sensors as well as computing and connectivity modules that provides users with convenience, but at the same time, they also increase the level of security problems associated with such complex systems. This paper focuses on hardware related flaws and vulnerabilities a typical smartwatch may come with which can lead to compromised device performance, loss of user data privacy, as well as breach of integrity. Building on case studies, the study classifies and describes hardware vulnerabilities into different severity ratings. The findings are intended to be useful to researchers, developers and individuals to diagnose critical hardware weaknesses and help create a strong hardware security measure.**

Keywords—Smartwatch, Hardware Vulnerabilities, IoT Security Challenges, Cybersecurity in Wearables.

I. INTRODUCTION

Smartwatches are a crucial part of lifestyle for many people. They offer many functionalities that range from health monitoring to communication, and they integrate very well with smartwatches as well [1]. However, this rapid adoption has made many adversaries interested in smartwatches as well, particularly in terms of hardware vulnerabilities [3]. Unlike software vulnerabilities that can often be patched post deployment, hardware vulnerabilities are near to impossible to fix post-deployment as they are part of the physical design [2].

The security risks associated with smartwatch hardware is critical due to its impact on privacy of user and data integrity. Common areas for such vulnerabilities to be present in smartwatch hardware includes areas such as design flaws, improper manufacturing process and untested firmware updates [4]. For instance, Side-channel attack uses physical characteristics such as power consumption to get into sensitive data, that highlights the requirement for robust hardware defenses [4]. Such vulnerabilities not only compromise personal information of the user but also impact the trustworthiness of wearable technology in many sectors, especially in healthcare and finance.

Weak security mechanisms used in firmware updates can cause much worse conditions to the smartwatches. Ineffective update process may also create opportunities to have the malicious firmware installed that will damage the integrity of the device [5]. Knowing such hardware level issues will help improve the security and privacy of users who increasingly rely on smartwatches to monitor their health and lifestyle.

II. OBJECTIVE

This research aims to consolidate and analyze hardware-layer vulnerabilities present in typical smartwatches, gathering the discussion in peer-reviewed studies, various advisories released by the vendors and documented case analysis. The research specifically aims to:

- Define taxonomy for vulnerabilities in hardware of smartwatch – covering side-channel attacks in sensor, insecure boot chains, physical extraction paths, and wireless-interface related hardware implementation flaws, to provide a consistent view for analysis and comparison [6].
- Documenting real-world evidence for each class in the taxonomy by linking to public proof of concepts, advisories, CVEs and attack studies that targeted wearables [1][5][6].
- Assess impact and severity at the hardware boundary, distinguishing attacks that can bypass software detection from those that primarily decrease reliability [6].
- Map attacks to affected components and to smartwatch examples, which include formal CVE records such as Huawei Children Smart Watch authentication bypass and platform advisories [8][9].
- Synthesize mitigation guidance for manufacturers and practitioners – cover various sections such as firmware update design, debug-port lockdown, sensor-based access control, anomaly detection mechanism for motion and NFC misuse, and proper BLE testing. This will address all the attacks discussed in the literature and advisories [6].
- Highlight research gaps such as limited public data on real-world exploits in wearables, and the need for standardized suite that is specifically designed for smartwatches and propose directions for security benchmarking [5][6].

Received: 23-9-2025
Revised: 28-12-2025
Published: 31-12-2025

III. METHODOLOGY

To achieve the objective of the study, both qualitative and quantitative research has been carried out. It aims to capture both the breadth and depth of the security issues that exist in the various platforms of smartwatches.

The work is largely based on articles from CVE reports, security reports from respective smartwatch manufacturers and white papers containing information about known vulnerabilities and their consequences. It assists in categorizing the known security threats in smartwatches, to make it easier to discuss them. In this study, exploitability and user exposure procedures are coupled with impact to analyze the risk level of certain vulnerabilities.

IV. RESULTS

The smartwatches can also be exploited through their complex hardware. Such threats tend to be directed at the hardware parts or sensor devices essential to the functioning of the devices. Here, we have discussed different hardware related vulnerabilities that may be faced in smartwatches.

1. Unsecured Interfaces: Every smartwatch requires some form of port that can be used to charge the device or interact with other devices. Such physical ports of the smartwatches can get compromised if proper security measures are not in place to protect it.
2. Sensor Spoofing: Maliciously tweaking sensors (e.g., GPS, heart rate) to produce incorrect data hence compromising the usability of health and fitness tracking.
3. Side-Channel Attacks: Taking advantage of the hardware to obtain information that may be necessary without a direct way of getting it, like using power analysis or electromagnetic emanations.
4. Fault Injection: Specifically, attempting to physically tamper with a piece of hardware to subvert its security mechanisms; or to otherwise disrupt its correct functioning.
5. Screen Capture Vulnerabilities: Products that contain hardware vulnerabilities that permit capturing of their screens or monitoring without the user's approval.
6. Microphone Eavesdropping: Use of computer hardware bugs to switch on/off any type of microphone with a view of eaves dropping.
7. Camera Exploits: Public access to the camera of smartwatch thus enabling visual monitoring of the public.
8. Physical Data Extraction: Copying data from the device storage using hardware mechanisms.
9. NFC Exploits: Attacks that entail using NFC features of smartwatch to get to the data or to start transactions without the owner's consent.
10. Wearable-Specific DoS Attacks: Software vulnerabilities that allow hackers to take advantage of design flaws within the actual hardware of the targeted system to sap all its battery life or completely shut it down.

These are forms of hardware attacks indicate that there is an essential requirement for physical security layers in the smartwatch development and production processes. It is imperative to provide solutions to these problems so that user information can be protected, and functionality of various devices can be secured. Table 1 given below discusses some of the examples of the said vulnerabilities getting exploited in the real world in the order of occurrence from 2024 to 2021.

V. DISCUSSION

The results above indicate that hardware weaknesses in smartwatches present severe risks, but the level of evidence varies sharply by category. The sweyntooth campaign revealed implementation flaws in BLE stacks used numerous chipsets found in majority wearables. These flaws enable denial-of-service, deadlocks and in many cases bypass of security states. This work was published at USENIX ATC with public POCs and was subsequently reflected in multiple advisories (e.g., CISA and vendor notices), indicating that smartwatches using those chipsets are vulnerable to exposure until patched [2][6][13].

Beyond side-channels and radio-stack defects, firmware authenticity and boot-chain security are central to hardware security because bypass on this level can permanently expose the higher-layers. While smartwatch specific public case studies are limited, standards such as NIST SP 800-193 and IETF SUIT RFC 9019 provides a trustworthy update architecture that is suitable for devices like smartwatches [10][11].

The device-specific evidence base is growing but is still very limited in public records. For example, CVE-202248395 provides details related to an authentication bypass on the Huawei Children Smart Watch (Simba-AL00). Although this issue includes both application and hardware-proximate input i.e., microphone/voice pipeline, It illustrates that smartwatch vulnerabilities are receiving formal CVE numbers and coordinated vendor response [9] [12].

By contracts, few categories in our results like unsecured physical/debug interfaces, sensor spoofing for physiological or GPS manipulation, fault injection, screen/camera hardware capture, NFC relay/charge attacks, and wearable specific energy-drain DoS are largely not researched in the publicly documented smartwatch literature. There are many demonstrations in IoT and mobile contexts (e.g., EM/power side-channels, NFC relays, physical extraction) and well reported issues in children's smartwatches that shows the high risk associated with the system, but smartwatch-specific, peer reviewed hardware exploit write-ups are missing. This asymmetry suggests the field is under-measured rather than safe [14] [15] [16].

For manufacturers, short-term priorities include:

- Sensor-path hardening, rate-limiting, permissions and signal obfuscation for motion sensors.

Table 1 – Attacks Related to Hardware Vulnerabilities in Smartwatches

No.	Vul.	P.D.	A.D.	A.S.	L.I.	S.R.	Ref.
1	Wearable-Specific DoS Attacks	08/10/2024	Allow attackers to cause a Denial of Service	Fire-Boltt Artillery Smartwatch (NJ-R6E-10.3)	Watch not functioning	H	CVE-202446539
2	Fault Injection	26/09/2023	The attack prevents the device from locking	Apple Watch Ultra	Unauthorized access of the device	M	CVE-202340418
3	Physical Data Extraction	23/06/2023	An attacker with physical access to a locked Apple Watch may be able to view user photos or contacts via accessibility features.	Apple Watches	Sensitive Data Leakage	M	CVE-202332417
4	Sensor Spoofing	27/02/2023	Successful exploitation of this vulnerability may cause the access control function of specific applications to fail.	Huawei Children Smartwatch (SimbaAl00)	Malfunction of Watch	M	CVE-202248305
5	Microphone Eavesdropping	20/12/2022	Successful exploitation of this vulnerability may cause unavailability of the camera and microphone.	Huawei Smartwatches	Microphone inaccessible	M	CVE-202246313
6	Camera Exploits	20/12/2022	Successful exploitation of this vulnerability may cause unavailability of the camera and microphone.	Huawei Smartwatches	Camera inaccessible	M	CVE-202246313
7	Screen Capture Vulnerabilities	26/05/2022	An app may be able to capture a user's screen.	Any Apple Watch running WatchOS 8.5 or older	Sensitive Data Leakage	M	CVE-202226726
8	Side-Channel Attacks	08/03/2022	Allows attacker to access password information of connected WiFiAp in the log	Galaxy Watches	Password Leakage	L	CVE-202225827
9	NFC Exploits	08/12/2021	Improper check or handling of exception conditions vulnerability in Samsung Pay allows attacker to use NFC without user recognition.	All Samsung Smartwatches	Financial Loss	M	CVE-202125525
10	Unsecured Interfaces	11/06/2021	Allows attacker with log permissions to leak Wi-Fi password connected to the user smartphone within log	Galaxy Watches	Password Leakage	M	CVE-202125420

Vul. – Vulnerabilities , P.D. – Published Date , A.D. – Attack Description , A.S. – Affected Smartwatches , L.I. – Loss Incurred , S.R. –Severity Rating , Ref. – References , C – Critical , H – High , M – Medium , L – Low

- Aggressive BLE stack testing against campaigns like Sweyntooth.
- Robust update aligned with SP 800-193 and SUIT (e.g., authenticated updates, rollback protection, measured boot, recovery).

For researchers, systematic validations of gaps on representative smartwatch platforms is needed. Furthermore, researchers may carry-out controlled attempts at debug-port exploitation, inertial/PPG/GPS spoofing with ground-truth evaluation, fault injection feasibility studies on wearable SOCs and NFC relay experiments designed with ethical safeguards. These studies should produce reproducible artifacts to accelerate vendor remediation and ecosystem learning [6] [10] [11].

At last, better transparency and coordinated disclosure would greatly improve the evidence base. Smartphone platforms regularly publish detailed documentations; however, smartwatch vendors do not follow the same path. Wider publication of advisories/CVEs and cross-vendor test suites would enable proper tracking of hardware risks in wearables and support independent replication.

VI. CONCLUSION

This paper has identified the severe hardware threats that remain in smartwatch ecosystems. Weaknesses like insecure interfaces, vulnerability to sensors and firmwarelevel vulnerabilities, the findings prove not to be theoretical but are increasingly being confirmed by real-world example attacks such as SweynTooth BLE SoC flaws and side-channel keystroke inference attacks. These weaknesses demonstrate that even though wearable technology is quickly being adopted, the underlying hardware security position of smartwatches is typically weaker than that of smartphones and IoT hubs .

A research gap was also identified in the discussion. In empirical study, some threat (e.g., sensor-based leakage, Bluetooth firmware bugs) is well-documented, whereas others (e.g., fault injection, physical data extraction, NFC relay attack) are not studied in specifics of the smartwatch environment. Such imbalance is not denying risks but denying systematic research. Therefore, the gaps between the academic researchers and industry stakeholders need to be addressed by filling them with peer-reviewed experiments that can be replicated.

In a pragmatic view, to maintain the integrity of the firmware and increase the speed of the hardware-related vulnerability patches the manufacturers will need to give significant attention to firmware resilience structures (e.g., NIST SP 800-193) and secure update processes (e.g., IETF SUIT RFC 9019). Meanwhile, transparency through coordinated disclosure and broader CVE reporting will play a critical role in enhancing trust and facilitating a proactive security culture into the smartwatch industry.

Finally, this paper concludes that smartwatch hardware acquisition is not a luxury but is at the core of protecting sensitive personal information like biometric signals, location, and communications. The paper notes the urgent necessity of a comprehensive security approach, such as integrating hardware, firmware and user-level protection, to ensure smartwatches are resistant to current and future hardware-related threats.

REFERENCES

[1] Fereidooni, H., Classen, J., Spink, T., Patras, P., Miettinen, M., Sadeghi, A.-R., & Hollick, M. (2017). Breaking fitness records without moving: Reverse engineering and spoofing Fitbit. Proceedings on Privacy Enhancing Technologies, 2017(4), 153– 173.

[2] Maiti, A., Jadliwala, M., He, J., & Bilogrevic, I. (2015). (Smart)Watch your taps: Side-channel keystroke inference attacks using smartwatches. 2015 IEEE Conference on Communications and Network Security, 207–212.

[3] Spreitzer, R., & Mangard, S. (2016). Systematic classification of side-channel attacks. Proceedings of the IEEE, communication surveys, and tutorials.

[4] Wu, Y. (2024). A study of firmware update vulnerabilities. USENIX Security Symposium.

[5] Liu, X., Zhou, Z., Diao, W., Li, Z., Liu, K., Zhang, K., & Wang, X. (2015). When good becomes evil: Keystroke inference with smartwatch. In Proceedings of the 2015 ACM Conference on Computer and Communications Security (CCS) (pp. 1273–1285) **6.**

[6] Garbelini, M. E., Tippenhauer, N. O., & Ooi, W. T. (2020). SweynTooth: Unleashing mayhem over Bluetooth Low Energy. In USENIX ATC '20

[7] CISA. (2020). ICS-ALERT-20-063-01: SweynTooth vulnerabilities. U.S. Cybersecurity and Infrastructure Security Agency

[8] NIST NVD. (2023). CVE-2022-48305: Identity authentication bypass—Huawei Children Smart Watch (Simba-AL00). National Vulnerability Database

[9] Huawei PSIRT. (2023). HWPSIRT-2022-18770: Identity authentication bypass in Huawei Children Smart Watch. Vendor advisory

[10] IETF. (2021, April). RFC 9019: A firmware update architecture for Internet of Things. https://datatracker.ietf.org/doc/rfc9019/

[11] NIST. (2018). SP 800-193: Platform firmware resiliency guidelines. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

[12] NIST NVD. (2023, February 27). CVE-2022-48305: Identity authentication bypass—Huawei Children Smart Watch (SimbaAL00). https://nvd.nist.gov/vuln/detail/CVE-2022-48305

[13] WIRED. (2015, July 9). Wearing a smartwatch could give hackers your PIN (report on smartwatch motion-sensor keystroke inference research). https://www.wired.com/story/smartwatchtyping-spying

[14] WIRED. (2020, October 23). Kids' smartwatches are a security nightmare despite years of warnings (survey of vulnerabilities across brands/models). https://www.wired.com/story/kidsmartwatch-security-vulnerabilities

[15] Sayakkara, A., Le, T., & Leckie, C. (2019). A survey of electromagnetic side-channel attacks and their applicability to digital forensics. Digital Investigation, 29, 94–110. https://www.sciencedirect.com/science/article/abs/pii/S1742287618303840

[16] Liptak, C., & Batina, L. (2022). Power analysis side-channel attacks and defenses. National Science Foundation public access repository. https://par.nsf.gov/servlets/purl/10409966