
aracne

GERARDO **IOVANE**, SALVATORE **VILLANO**

RED TEAM CYBERSECURITY LECTURES

SMARTWATCHBASED CYBERATTACK: THEORY, STRATEGIC FOUNDATIONS AND ALGORITHMS

aracne

ISBN
979-12-218-2524-4

PRIMA EDIZIONE
ROMA 19 FERBBRAIO 2025

Table of Contents

Part I

Introduction

In an era of seamless integration of technology, smartwatches have quickly become an indispensable tool, bridging the gap between convenience, connectivity, and performance. Originally positioned as companions for communication and fitness tracking, these devices have undergone significant transformation and now offer a rich array of capabilities. Along with this development comes a hidden complexity, a latent duality that introduces novel cybersecurity vulnerabilities and offensive capabilities. This thesis explores the offensive cybersecurity potential of smartwatches, focusing on their potential to be used for active cyber intrusion and persistence in the consumer and enterprise space.

This exploration is especially relevant as wearable technology becomes more pervasive in the workplace, further blurring the boundary between personal and professional devices, which in turn increases the attack surface of organizational networks. Smartwatches represent a special instance of this evolving risk landscape, primarily because of their size, resource limitations, and utilization of companion apps that can offer an unexpected attack vector. Consequently, attackers are provided with avenues for intrusion that may be less visible compared to attacks against other device classes, potentially circumventing established security protocols. Moreover, within the larger scope of IoT growth, with expected estimates exceeding 75 billion connected devices by 2025, in-depth analysis of smartwatch-specific offensive techniques and the development of targeted mitigation strategies are paramount for the construction of effective IoT security architectures.

The aim of this thesis is to characterize and analyse the offensive cybersecurity potential of smartwatches by describing how these devices can be actively utilized as attack platforms, rather than simply being passive attack endpoints. The analysis includes attack chains and walkthroughs for Wear OS and watchOS, detailing attack surfaces that can be exploited to perform reconnaissance, deliver payloads, execute malicious code, and prevent forensic analysis. Emphasis is placed on companion app ecosystems and the implications for Bluetooth Low Energy (BLE) communication, with specific attention paid to the use of prox-

imity-based reconnaissance and covert communication using BLE. The results of the analysis can be leveraged by red team professionals, cybersecurity analysts, and researchers to develop relevant attack scenarios, countermeasures, and defences in both the consumer and enterprise spaces.

This exploration relies on multiple approaches, including theoretical modelling, reverse engineering of companion apps, and practical evaluation of code execution on devices. The structure begins with the establishment of the technical foundations through a discussion of smartwatch hardware and architecture, followed by the operating system and wireless protocols. Subsequently, a threat model for smartwatches is developed, leading to the formulation and execution of feasibility tests for various attack vectors. Hardware and software-based attacks are then presented, followed by a comprehensive examination of the communication protocol attacks possible with Bluetooth, BLE, and NFC channels. These attack vectors are further explored in a section focused on persistent intrusion. Lastly, the BYOD risk associated with smartwatches in the enterprise is presented and defended with recommendations for defensive architecture implementation.

The security research on wearables has predominantly focused on data privacy, security of wearable health-tracking devices, and user authentication methods. Literature often points to vulnerabilities such as the ones present in Bluetooth and BLE, companion app infrastructures, and update processes of the wearables firmware. However, little research has been carried out that brings together theoretical analysis with detailed practical exploitation scenarios that focus on complete offensive attack chains and how technical and organizational vulnerabilities in wearable devices can be utilized for cybercrime. This thesis attempts to close that research gap by presenting concrete exploitation scenarios with an emphasis on offensive approaches and analysis of weaknesses present in smartwatch companion apps.

The organization of the thesis starts in Chapter 2 with a discussion of the smartwatch security architecture: hardware, operating systems, and wireless communication. Chapter 3 covers the threat model used in this work for the smartwatch attack surfaces, along with an overview of the adversary capabilities. In Chapter 4 the hardware and software attacks, along with the wireless protocol vulnerabilities (Bluetooth, BLE, NFC), will be presented. After covering the introduction mechanisms used on the smartwatches, the persistence mechanisms that allow adversaries to maintain access to a smartwatch are described in Chapter 5. Then, in Chapter 6, the impact of smartwatch-enabled attacks and security of a corporate network will be investigated in the context of BYOD programs, along with de-

fensive recommendations for risk mitigation. Finally, the thesis presents a conclusion containing a discussion of the key findings, reflection on the original question as to whether smartwatches can be used offensively in cybersecurity, and recommendations for future work.

1. Smartwatch Security Architecture Fundamentals

Understanding the foundation of the smartwatch security architecture is the basis for both vulnerability recognition and defence. In the following, the hardware components, the system, and its communication protocols are the core for analysing the security of the smartwatch in the greater context of this entire work.

1.1. Hardware Components and System Design

Exploring the basic hardware components of smartwatches is crucial to understanding their security. We will investigate the processors, memory, sensors, and batteries that can affect the device's susceptibility to potential attacks. Understanding these areas as a part of the overall cybersecurity landscape is key for developing effective and smart security protection strategies for the whole system.

1.1.1. Processing Units and Memory Constraints

Processing units and memory limitations in smartwatches represent fundamental challenges to the security of these devices. Smartwatches utilize energy-efficient microcontrollers or system-on-chip (SoC) architecture that emphasize power efficiency and low thermal output to support compactness and improve battery longevity. While this architecture prolongs battery life, it severely restricts the complexity of security functions executable on smartwatches. Performing operations like continuous encryption, malware scanning, or behavioural anomaly detection exceed the processing capabilities of smartwatches, creating a loophole exploited by attackers. Specially crafted malware that remains lightweight and conservative of hardware resources bypasses system restrictions designed to trigger elevated computational and memory usage (Fawle & LeBlanc, 2024; Tiwari & Srivastava, 2025). Moreover, smartwatches generally lack advanced hardware security functions like cryptographic accelerators or secure enclaves for the efficient processing of cryptographic and authentication operations (Fawle & LeBlanc, 2024).

The lack of hardware isolation can cause runtime payload injection, bypass of secure memory regions, and side-channel attacks. Such weaknesses have been empirically documented for certain smartwatch models deployed in enterprise BYOD scenarios (Shin et al., 2018). This is further exacerbated by the fact that manufacturers make security compromises to prioritize user experience and real-time sensor response. The unprotected data streams are consequently susceptible to interception and manipulation by attackers (Huynh et al., 2018). Furthermore, the small RAM and storage on smartwatches severely constrain the implementation of complex security solutions such as resident anti-malware, system forensics, or intrusion detection. Attackers, in contrast, design malware obfuscation strategies to reduce memory consumption and thereby overcome these limitations to remain stealthy within the limited resources of smartwatches. Additionally, the simpler memory designs in smartwatches can be targeted for advanced intrusion techniques such as memory scanning bypass tactics employed by attackers (Fawle & LeBlanc, 2024; Shin et al., 2018). The limited memory also affects process and memory isolation, increasing the risks of privilege escalation. An attacker can exploit vulnerabilities in buffer boundary protection and memory management to inject and execute arbitrary code at a higher privileged level in these cases, resulting in an intrusion leading to root-level access to all system resources (Shin et al., 2018). Moreover, inadequate isolation of user and application data, coupled with a lack of encrypted storage, exposes the entire system and all installed applications to leakage or manipulation in cases of process compromise (Fawle & LeBlanc, 2024).

The processing and memory constraints also limit the applicability of update strategies in smartwatches. The inability to deploy security updates quickly results in an attack window for adversaries to exploit existing software vulnerabilities (Tiwari & Srivastava, 2025). Compromised smartwatches that lack timely updates may then become sources for further attacks, spreading vulnerabilities to other interconnected systems. The heterogeneous nature of the smartwatch market, characterized by vendors employing proprietary hardware, firmware, and updating schemes, complicates patch distribution and management. As a result, known vulnerabilities can persist for a longer duration on certain models. Attackers are able to take advantage of such weaknesses and craft attacks against specific manufacturers across entire generations of devices, especially in the BYOD enterprise context where varying smartwatch models are often intermixed (Fawle & LeBlanc, 2024).

Further, many existing smartwatches also exhibit poor over-the-air (OTA) updating schemes and have inadequate storage to sustain frequent, full updates of the operating system and applications. Therefore, in these circumstances, the software vulnerability attack

window for attackers tends to be increased (Tiwari & Srivastava, 2025). The lack of a unified update strategy or mechanism across manufacturers and device models provides a sustained period for attackers to maintain a foothold on vulnerable devices even after security patches have been issued (Tiwari & Srivastava, 2025).

The prioritization of processing speed and minimized latency impacts the ability to validate sensor input data. To enable timely performance of applications dependent on sensors, vendors often implement design choices to allow sensor values that may not have integrity-checking mechanisms or that are not validated before they are utilized (Huynh et al., 2018). Prior studies have shown how attackers can manipulate sensors to produce incorrect physiological output values, evade integrity checks, and conduct subsequent network-based intrusion attacks (Huynh et al., 2018). These forged biometric or behavioural data can also undermine gesture-based authentication mechanisms and health-tracking or fitness applications on the smartwatch. Therefore, the integrity of applications depending on the reliability of physiological sensors must be maintained in order to ensure user privacy and enterprise information security. When unvalidated and forged, physiological data are utilized to breach boundaries between applications, all application-level data, including sensitive enterprise information, are put at risk (Siboni et al., 2018).

Limitations of computing and memory resources can also allow attackers to implant persistent stealthy malware. Minimalist malware designed for smartwatches can survive a reboot and evade forensics countermeasures by wiping artifacts from volatile memory and relying on other anti-forensics strategies. Moreover, it may be extremely challenging to detect such malicious software on wearable devices in certain use cases due to the fact that enterprise environments may not contain forensics tools capable of processing memory dumps and logs on these novel computing platforms (Siboni et al., 2018). Additionally, an attacker can load malicious files from outside the local system only at specific times based on criteria such as time of day or geographic region. By selectively loading malicious payload components during such scenarios, the attacker can make it increasingly difficult to reconstruct and identify how the system became compromised and by which attacker (Shin et al., 2018). To further avoid suspicion, the attacker can also disable or erase logs and logs databases.

Tamper-proof audit logging and event storage mechanisms are currently lacking in most wearable devices, preventing post-incident verification of device integrity and compromising the ability to perform audit reviews, in general (Shin et al., 2018). As the quantity of log data to be retained for audit requirements can quickly exceed the maximum memory and storage size of the wearable device, most vendors do not choose to implement robust log and event tracing mechanisms in order to conserve hardware resources. This also allows attackers to operate for a longer duration without detection, as malicious activities remain less traceable and are more difficult to correlate for intrusion analysis. Furthermore, anti-forensics tactics, such as selective deletion of certain event categories or log entries from volatile memory, can also be applied by attackers to mask traces of malicious activities, ensuring they cannot be identified by forensic investigators with a memory dump after system restart (Siboni et al., 2018).

In conclusion, the architectural characteristics of smartwatches associated with limited computing and memory resources yield a variety of security and forensic implications for BYOD enterprise scenarios. This resource limitation is responsible for the difficulty of implementing stringent security features, increases the attack surface and the opportunity for attacks to establish persistence, and significantly delays patch rollout.

1.1.2. Sensor Integration and Data Collection

The integration of multiple sensors in smartwatches facilitates the collection of continuous streams of sensitive physiological and behavioural data; sensors such as accelerometers, gyroscopes, heart rate monitors, and microphones are included in this integration. While beneficial user-centric applications can be supported by this extensive data collection, significant security and privacy risks are posed when access by malicious actors is gained. According to research, the exfiltration of highly personal information, including health metrics, movement patterns, and behavioural habits, can be achieved through compromised firmware or rogue applications by exploiting sensor data (Terzidis et al., 2023; Siboni et al., 2018). Enterprise environments, especially those operating under Bring Your Own Device (BYOD) policies, see these risks amplified, where the intersection of personal and corporate data results in heightened exposure. As an illustration, organizational privacy can

be undermined and compliance challenges with data protection regulations created through unauthorized access to location data within corporate facilities, meeting audio, or even employee routines. Therefore, a critical concern emerges as the lack of robust safeguards for data access permissions and dynamic monitoring mechanisms within smartwatch ecosystems.

Longitudinal datasets result from the continuous nature of sensor data collection; should these be exfiltrated, adversaries are provided with an avenue to comprehensively profile users. Not only is individual privacy breached through insights into heart rate variability, arrhythmias, or other health indicators, but also the targeting of individuals or groups based on inferred vulnerabilities is enabled for adversaries (Terzidis et al., 2023). Furthermore, detailed behavioural profiles, potentially for use in targeted cyberattacks or coercive tactics, can be yielded when this data is cross-referenced with location and activity patterns. In professional environments, where sensitive data, personal habits, and work details intertwine, these risks are amplified, creating a multifaceted threat landscape. Often relying on user consent models, current privacy frameworks struggle in addressing these compounded risks, which results in gaps that adversaries can exploit.

An additional vector for attackers to maintain persistent and unauthorized access to sensors is presented through firmware-level compromises. User consent mechanisms and permission checks can be bypassed through privileged access at this level, which facilitates continuous harvesting of sensor data (Siboni et al., 2018). Concerns beyond immediate privacy are implied through such attacks, with firmware-level control enabling prolonged surveillance without detection. Additionally, complete device replacement or specialized forensic intervention to restore integrity is often required to remediate the highly privileged nature of firmware compromises, making it particularly challenging. The potential for advanced persistent threat scenarios is exemplified through this persistent access model, which could target consumers and enterprises alike, resulting in long-term exploitation of sensitive data. It is further illustrated through empirical studies that malicious applications can covertly leverage smartwatch sensors to harvest data without user notification. Transparency gaps and user awareness are exploited by these applications, subverting consent-based frameworks designed to safeguard wearable privacy (Terzidis et al., 2023). As an example, unauthorized collection of data without triggering visible alerts is enabled when attackers tamper with APIs that manage sensor functionality. Therefore, insufficiencies in current

application-layer defences are highlighted through this weakness, and questions are raised about the effectiveness of app marketplace vetting procedures. A deeper scrutiny of sensor-related API usage, in addition to a shift toward real-time monitoring architectures capable of identifying misuse, is required to address these vulnerabilities.

A more accurate picture of user behaviours and physiological states can be created when attackers combine data streams from multiple sensors for corroboration because of the versatility of smartwatch sensors. Surveillance and misuse scope can be further enhanced when, for example, accelerometer and gyroscope data are leveraged in tandem to map movement patterns with high precision (Terzidis et al., 2023). Risks of unauthorized profiling and data exploitation can be amplified through such corroborative techniques, particularly when employed by adversaries with access to analytics tools. Improved access control and dynamic policy enforcement are urgently needed to counter this multi-sensor exploitation, even though sensor fusion can enhance legitimate applications.

Another significant vulnerability, introduced through side-channel attacks, is found in the capability of smartwatch motion sensors to capture wrist and hand movements. It is demonstrated through research that motion sensor data can be exploited for keystroke inference, with high success rates in reconstructing typed input such as passwords or confidential messages (Maiti et al., 2016). Adversaries are able to infer typed content with alarming accuracy based on even subtle wrist movements during keyboard use near a smartwatch; this includes 100% success in detecting left or right keypresses and 93.75% accuracy for reconstructing longer words (Maiti et al., 2016), as revealed through studies. Therefore, the limitations of current permission models are highlighted; these are ill-equipped to counter the passive and ambient nature of side-channel data generation. Furthermore, these attacks are made accessible even to relatively unsophisticated attackers through their practicality, which is based on commodity hardware and standard APIs, increasing the prevalence of such threats.

The risk associated with side-channel attacks is exacerbated in enterprise settings, where sensitive communications and credentials are frequently entered. Application-layer defences and traditional security systems are bypassed through the passive nature of these attacks, in addition to their reliance on standard sensor outputs, which further complicates threat mitigation. The need for enhanced sensor data monitoring and filtering mechanisms, which are capable of identifying anomalous data usage patterns, is emphasized through the findings. Advancements in both hardware and software defences are necessitated to address

this emerging challenge, since current detection systems fall short in preventing such exploits.

The threat landscape is further exacerbated through poor administrative practices such as insecure default configurations, in addition to sensor-specific risks. A significant percentage of wearable devices, including smartwatches, are deployed with default or hard-coded credentials (Jiang et al., 2020), as revealed through studies. Therefore, remote attackers are allowed to gain unauthorized access to sensor data arrays, extract sensitive information, and manipulate device behaviour. Adversaries can, for instance, feed false readings to health monitors or create fake activity logs, undermining both device functionality and user trust. Potential entry points for wider network compromise in enterprise environments are also served through smartwatches with weak credentials. The need for mandatory operational controls and stricter device onboarding protocols is underscored through the lack of enforced credential management and automated audits, which exposes systemic vulnerabilities.

Smartwatches can be transformed into covert attack tools through malicious applications, further exploiting sensor integration. Compromised devices can, for instance, function as rogue wireless access points or data exfiltration tools, intercepting sensitive data such as print jobs or meeting audio, which is then leaked outside monitored networks (Siboni et al., 2018). Unauthorized communication channels that evade network security measures can also be established by attackers, leveraging inadequately secured sensor APIs to silently harvest and transmit data. The trust placed in wearable devices is exploited through such attacks, particularly in enterprise scenarios where app behaviour scrutiny may be lacking. The urgent need for real-time anomaly detection in enterprise infrastructures is emphasized through the persistence of these threats, even after attempted remediation, which highlights the insufficiencies in mobile device management and security frameworks.

An alarming trend is represented through the integration of artificial intelligence into offensive strategies, from an advanced adversarial perspective. Context-aware techniques, such as keystroke inference and behavioural profiling, can be refined through AI-augmented attacks, increasing the stealth and precision of their methods (Adi et al., 2022). Detection models can additionally be evaded when attackers leverage adversarial AI techniques, such as data poisoning or input manipulation. An escalating arms race between

offensive and defensive applications of AI results, with defensive efforts deploying machine learning-based anomaly detection remaining vulnerable to these evasion tactics. The feasibility of model-stealing attacks, where attackers replicate defensive AI models to craft malware optimized for evasion (Adi et al., 2022), is further demonstrated through empirical evidence. Therefore, robust retraining approaches, explainable AI methods, and continual updates to defensive architectures are required to counter the evolving sophistication of AI-driven threats.

In summary, a complex security landscape, characterized by privacy vulnerabilities, advanced exploitation techniques, and insufficient defences, is presented through sensor integration in smartwatches. Urgent attention is necessitated to safeguard both individual and enterprise environments through the continuous collection and potential misuse of sensor data, combined with adversaries' growing technological capabilities. Innovation in hardware design, security frameworks, and policy enforcement is required to address this multifaceted challenge, and to ensure the secure integration of wearables into modern ecosystems.

1.1.3. Power Management Systems

Energy efficiency is prioritized by the design of power management systems in smartwatches, which inherently gives rise to security vulnerabilities through the limitation of capabilities to maintain continuous monitoring and protection against malicious activities. Battery life is extended by strategies such as dynamic voltage scaling and aggressive sleep states through the management of active processing and wireless communication. These intended reductions in activity, however, create temporal blind spots wherein real-time security measures are suspended. Malicious processes can be executed by attackers without detection during these intervals. The effectiveness of runtime security protocols is undermined by such blind spots, as adversaries are able to time their operations to exploit the system's reduced vigilance. Trade-offs in wearable design are highlighted through these vulnerabilities, where the threshold for adversarial access and stealthy operations is inadvertently lowered when battery life is optimized (Fawle & LeBlanc, 2024).

The maintenance of robust security during low-power operating modes is proving to be exceptionally challenging due to the intrinsic compromises that are required by wearable systems. Critical background processes, inclusive of intrusion detection and response mechanisms, are simultaneously suspended through frequent transitions into sleep or deep idle states, which are designed to conserve energy. These regular intervals can be exploited by attackers, who synchronize their operations to coincide with these states, allowing for the exploitation of delayed detection and response mechanisms. Threats that are persistent or unauthorized actions, as a result, can remain hidden within the typical activity cycles of the device. The tension between energy efficiency and comprehensive security integration in modern smartwatch design is underscored through this cyclical vulnerability (Fawle & LeBlanc, 2024).

The manipulation of power management logic, with the goal of actively disrupting device functionality and masking malicious intent, is possible for attackers. The programming of excessive sleep-wake cycles, through the exploitation of sensor events or system alarms, is one such example. This forces devices into rapid oscillation between low- and high-power states, leading to scenarios involving battery degradation or denial-of-service. The smartwatch's operation is disrupted through such tactics, while malicious resource usage is blended into the expected energy consumption patterns concurrently. Detection becomes exceedingly difficult for users and forensic analysis tools alike, due to the alignment of this activity with normal device behaviour. Another layer of vulnerability, inherent in the design of power-conscious systems, is revealed through this method of resource exploitation (Terzidis et al., 2023; Siboni et al., 2018).

Another dimension of exploitation is presented through improperly secured power management interfaces, most notably when attackers manipulate sensor-driven wake-up signals. Devices are deliberately kept awake or initiated into specific behaviours on demand by adversaries through the spoofing of accelerometer, gyroscope, or heart rate monitor inputs. This capability enables attackers to sustain unauthorized access or coordinate attacks during periods of low attention, such as nighttime or while the device is charging. Robust authentication mechanisms for sensor-driven actions are emphasized due to such vulnerabilities, in addition to the ongoing challenges surrounding the securing of low-power states within wearable ecosystems (Siboni et al., 2018).

Power-saving features also pose a significant risk, since they affect the timely deployment of critical updates and real-time security monitoring. Transitions into low-power states may

cause devices in sleep mode to miss notifications for important security patches or fail to complete downloads. These delays create exploitable windows for adversaries to target unpatched vulnerabilities, thereby extending the lifecycle of known risks. This weakness is further amplified through the compounding issue of fragmented manufacturer support, which leaves many devices inconsistently protected against evolving threats. This dynamic demonstrates how power management, while essential for device usability, inadvertently increases long-term security risks (Tileria et al., 2020).

The necessity for lightweight security features is dictated through the inherent energy constraints that are found in smartwatches, which often limits the implementation of advanced routines, for example full-disk encryption or machine-learning-driven anomaly detection. Attackers are becoming increasingly adept at crafting resource-efficient malware, which allows them to exploit these simplified security measures in order to maintain stealthy, persistent compromises. Enterprise environments are particularly concerning in this context, where BYOD policies permit the integration of personal smartwatches into sensitive networks. Malware designed for minimal resource consumption is able to infiltrate such environments, posing a persistent threat to organizational privacy and data security. The urgent need to reevaluate the balance between energy efficiency and effective security measures is emphasized through these risks (Siboni et al., 2018).

The deployment of robust cryptographic processes is significantly constrained further by limited energy resources. Battery life is often preserved through the sacrifice of computationally intensive routines, like continuous cryptographic validation. Communication channels, particularly those using Bluetooth Low Energy (BLE) protocols, are left either weakly protected or completely unsecured as a result. Attackers target these channels using interception, spoofing, and man-in-the-middle tactics, taking advantage of the absence of advanced cryptographic defences. The critical need for energy-efficient yet secure encryption technologies tailored to wearable devices is highlighted through this limitation (Fawle & LeBlanc, 2024).

Another obstacle to forensic readiness is posed by the inability to sustain continuous security analytics or maintain persistent logs during low-power states. Attacks staged during these intervals leave minimal traces, thereby complicating post-compromise investigations and root-cause identification. Attackers are able to obscure their tracks further, thereby minimizing the likelihood of detection, as memory and event logs fail to capture critical evidence. The necessity for strategically integrated security models, capable of operating