CyCon 2024: Over the Horizon
16th International Conference on Cyber Conflict
C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, D. Štrucl (Eds.)
2024 © NATO CCDCOE Publications, Tallinn

Resilience and Vulnerability of Consumer Wireless Devices to Cyber Attacks

Pēteris Paikens
Senior Researcher
Institute of Mathematics and Computer Science
University of Latvia
Riga, Latvia
peteris@ailab.lv

Krišjānis Nesenbergs
Researcher
Cyber-Physical Systems Laboratory
Institute of Electronics and Computer Science
Riga, Latvia
krisjanis.nesenbergs@edi.lv

Abstract: As consumer wireless devices, such as wearables, smartphones and Internet of Things devices become more and more intertwined in our everyday lives, the potential attack surface and the risks if such devices are compromised rise drastically.

Specifically, most of these devices use wireless communication, which uses a broad range of protocols—such as Wi-Fi, Bluetooth and Bluetooth Low Energy—and mesh protocols, such as Zigbee. While Wi-Fi security and vulnerabilities are widely researched and known due to their existing impact on office computing security, the vulnerabilities in Bluetooth and other protocols have received limited attention in the IT security industry because they have historically been hard to monetize for financially motivated threat actors, but these vulnerabilities are still relevant in espionage and cyber conflict. As the prevalence of such devices grows and the costs of equipment such as software-defined radios fall, these vulnerabilities and the related preventive measures need to be better understood.

In this paper we analyze these threats and provide a classification of vulnerabilities and relevant resilience approaches in consumer wireless devices, based on an analysis of the Common Vulnerabilities and Exposures (CVE) reports from 2023 in order to evaluate the risks posed by them to society both in peacetime and during conflicts with a cyber component.

Keywords: *wireless, Internet of Things (IoT), Bluetooth, vulnerabilities, Common Vulnerabilities and Exposures (CVE)*

1. INTRODUCTION*

The classical approach to information system security is primarily concerned with formally structured organizations and technologies [1], so informal activities and human factors are often neglected in practice, even though some related attack vectors, such as social engineering, are highly visible and thus well-known even if not well-understood [2]. This has led to the current situation, where there is a good understanding of the security of systems involving formally structured and well-understood technologies, such as Ethernet and Wi-Fi access points forming a network that is explicitly managed by an organization, while more flexible wireless communications where people are capable of moving devices, easily bringing new devices into the network and acting in less predictable ways with almost limitless potential ad-hoc configurations of devices are often perceived as inherently insecure [3]. Even though such a perception should logically motivate greater scrutiny of wireless communications and their security, the opposite is often true. A lot of myths at both ends of the spectrum—such as "wireless connections are always insecure" or "encrypted wireless connections are secure"—have permeated the common understanding, leading to radical approaches where either all wireless devices are disallowed, or wireless devices are not considered at all in the security threat models. This common lack of understanding usually leads to a wide attack surface, but the relative complexity of exploiting wireless communications has led to a lower number of well-known practical attacks, leading to a false sense of safety that does not withstand scrutiny in the face of more elaborate and capable state actors participating in cyber conflicts.

This has been slowly changing for more mature technologies, such as cell phone protocols [4]–[6] and Wi-Fi [7]–[9], where more control and understanding have been accumulated over the years. Still, the resilience of these technologies is highly reliant on minimizing the attack surface, which is still relatively easy when handling a limited diversity of organization-issued devices with a limited number of known wireless connections. Unfortunately, the advent of smaller, more energy-efficient Internet of Things (IoT) devices and the related differentiation in specialized needs for wireless communications has motivated device manufacturers to adopt new, less mature protocols that lack verified, secure implementation mechanisms.

The problem of IoT device security is even more severe in the consumer market, which has received much less attention in terms of security than devices purchased and maintained in the corporate and government domains. There is a sustained growth in the quantity and variety of cheap wireless consumer IoT devices entering the market and these devices accompany their users almost everywhere—in their homes and workplaces, during transit and in leisure time.

* This research was funded by the Latvian Council of Science project "Automated wireless security analysis of wearable devices" (WearSec), project No. lzp-2020/1-0395.

The global consumer IoT device market in 2023 was evaluated at around $183 billion, with a long-term expected compound annual growth rate (CAGR) of about 5% per year. It is expected to reach $192.4 billion in 2024 and will more than double in less than 15 years [10], making it comparable to the global computer peripherals market, which was worth $470.95 billion in 2022 with an expected CAGR of 6.5% [11]. This is exacerbated by the proliferation and expected rapid growth of wearable smart devices (devices with smart functionality that are worn or carried on the person of the user)—the wearables market was worth $61.30 billion in 2022, with an expected CAGR of 14.6% [12]—due to the increased privacy and surveillance risks of such devices.

Many people currently carry around not only a smartphone but multiple smart embedded or IoT devices with wireless connection capabilities. If a malicious actor takes control of such devices, they can create a variety of security risks—they can serve as Trojan horses into secure infrastructure [13]; become sources of distributed denial-of-service (DDoS) attacks [14], [15]; allow the extraction of secret information leading to industrial espionage [16], political espionage [17] and extortion [18]; and could also potentially hold malware from advanced persistent threats or state actors [19]. There are also the privacy and surveillance risks of tracking or fingerprinting specific devices using their wireless communications [20], [21]. The straightforward solution of just having a policy to remove every wearable consumer device is feasible only in highly controlled environments, and even in this case, there may be issues with devices like medical implants that have similar risks but cannot be removed or sometimes even detected [22]. These risks and the lack of social resilience in case they should be abused on a large scale in cyber warfare motivate the work done in this paper, where we analyze and classify the vulnerabilities and threats of devices to provide a basis for mitigating them in the future.

2. WIRELESS DEVICES AND PROTOCOLS

To explore and classify the threats to consumers, we first have to identify the specific protocols of interest that are used by the consumer wireless devices.

The most widespread wireless protocols in consumer devices are Bluetooth Classic (BT) and Bluetooth Low Energy (BLE), with more than 7 billion devices shipped in 2023 that have one of these protocols enabled [23]. BT has a wide range of applications in audio devices, mobile devices, and certain IoT and Smart Home technologies.

BT is a highly complex set of protocols with support for many different (and contradictory) use cases. Most devices do not need its full capabilities and only

implement some parts of the BT protocol standards. The current certification and testing practices of manufacturers mostly concern reliability in the face of noise or accidental transmission errors, with limited testing for resilience to malicious inputs. In the last few years, multiple critical vulnerabilities in popular BT chipsets have been identified, confirming these gaps in security practices [24]. This situation is made worse by the fact that BLE modules, SoCs (systems on a chip) and devices commonly persist with the same designs for many years without providing upgrade options [25].

A competing proprietary protocol usually used for consumer sportswear is the Adaptive Network Topology (ANT) protocol (and its low-power version, ANT+) by Garmin. This protocol is currently known to be in use in more than 1,000 consumer products, including multiple Samsung mobile phones [26]. ANT is a multicast protocol meant for personal area networks, and thus has some optimizations, such as tree topology, that allow faster, low-energy data rates from wearable sensors than comparable BLE solutions. It uses adaptive isochronous transmission to allow many devices to communicate concurrently without interference, while BLE uses scatternets and broadcasting for the same effect.

Another well-known wireless communication technology available in many consumer devices is radio-frequency identification (RFID) and the family of connected protocols. RFID technology involves tags that are usually passive (although not always) and active readers. Many of the tags can be made read-only, but more and more tags are also "active" in order to improve security through rotating keys and have the option to program them wirelessly. There are multiple RFID technologies based on the frequencies used—low frequency, high frequency (also known as near-field communication or NFC) and ultra-high frequency.

In addition to these mostly well-known technologies, there are several other IoT-related wireless communication protocols mostly made for specific tasks. A group of technologies for long-range IoT communication called low-power wide-area networks includes such protocols as LoRaWAN and Sigfox. LoRaWAN is a point-to-multipoint networking protocol that uses LoRa's physical modulation scheme and hardware [27]. For closer distances or local area networks, Z-wave and Zigbee are frequently used and have interesting security implications [28]. Zigbee is a family of protocols with the standard number IEEE 802.15.4 that is used mostly for home automation and is capable of very low-power communication. Z-wave is also mostly used for home automation, but due to its lower frequency range of about 800–900 MHz, it is capable of much longer-range transmissions and there are more than 4,000 different products in the market that use this protocol. For even closer-range or personal area networking in IoT, one of the most-used technologies is 6LoWPAN [29], which is meant for IPv6 networking over low-power wireless personal area networks and thus can work on

top of IEEE 802.15.4 protocols. Finally, there are several other lesser-known personal area network protocols, some even meant for body area networks, which are all joined under the IEEE 802.15 protocol family.

3. SURVEY OF VULNERABILITIES

The cases listed in the introduction and survey papers [30]–[32] show a variety of threats to organizations and individuals. However, we wanted to contrast them with an analysis of the technical vulnerabilities reported for relevant wireless devices, based on the public MITRE Common Vulnerabilities and Exposures (CVE) list [33].

A. Selection of CVE Reports

In this paper, we review vulnerabilities initially reported throughout 2023, selecting all entries with a 2023 ID as of January 8, 2024,[1] that match specific keywords, analyzing each report to identify relevant aspects and classifying them according to their properties.

The following keywords were used for the initial selection: *IoT, Bluetooth, BLE, BT, ANT, ANT+, LoRa, LoRaWAN, Zigbee, Z-wave, NFC, RFID, 6LoWPAN, IEEE, 802.15, 802.15.1, wireless* and *wearable*. Based on this, a total of 216 vulnerability reports were identified.

Next, these vulnerability reports were analyzed for relevance to the scope of this paper. In a few cases, the keyword search results included unrelated products whose descriptions mentioned the search terms by coincidence or vulnerabilities in software packages that would not be used on the relevant devices but rather on the servers or desktop computers used to manage them. For wireless vulnerabilities, we focused on risks to consumer devices that do not overlap with computers and corporate devices. This excluded Wi-Fi routers, repeaters, access points and Wi-Fi chipset vulnerabilities, because they have been well-studied elsewhere and because of their widespread use in sensitive commercial networks. We excluded vulnerabilities in Windows drivers, but we did consider Linux and Android vulnerabilities as relevant, because those platforms are used not only for computers and smartphones but are also widely used by manufacturers as a basis for many other types of consumer devices. Out of the initial 216 CVE reports we analyzed, 163 were determined to describe vulnerabilities applicable to consumer wireless devices.

B. Analysis and Classification

A limitation of CVE reports is that many of them reflect fixes for bugs with potential

1 As there is a delay between initial CVE report and the public disclosure, at the time of publication will be more vulnerabilities with 2023 IDs, for example, https://www.cve.org/CVERecord?id=CVE-2023-5253 was published at 2024-01-15 after the data collection and analysis.

vulnerabilities that may not be exploitable in real attacks, and none of the reviewed CVEs asserted that these vulnerabilities have been actually exploited "in the wild."

Furthermore, the CVE reports use the Common Vulnerability Scoring System (CVSS) standard to quantify the severity of the vulnerability. While this standard is very useful as a universal qualitative metric, the categories used are designed in the context of "mainstream" vulnerabilities in software running on networked computers, but the physical aspects of wireless protocols and the specifics of consumer wearable and IoT devices require a more targeted approach. For example, CVSS vector "adjacent" (AV:A) is used both for vulnerabilities that require the attacker to simply be in physical range for the wireless connection to function and for vulnerabilities that apply only to previously paired devices, which is a substantial difference with respect to the risk of practical exploitation.

However, the CVE records include links to technical advisories that often are sufficient to manually determine the relevant properties of the vulnerability. Where the technical aspects of the vulnerability were not sufficiently detailed, we made reasonable conservative assumptions to interpret them. Where the CVE did not specify whether a software bug in processing some wireless protocol data could be triggered by a remote attacker or only from the local side, we assume that such data could be delivered remotely.

4. VULNERABILITY CLASSIFICATION

Due to the focus on consumer devices and the potential applications to cyber conflict, we consider it relevant to separate different aspects of classification—the impact, limitations of the attack vector and cause of the problem—instead of reusing existing threat taxonomies.

A. Classification According to Impact

From the perspective of risk analysis, the primary grouping of vulnerabilities is with respect to their potential impact for exploitation and the capabilities that they could offer an attacker, with the relative frequency of these groups shown in Table I.

TABLE I: NUMBER OF CVES ACCORDING TO VULNERABILITY IMPACT

Impact category	Number of CVEs
Information disclosure	53
Denial of service	32
Elevation of privilege	29
Device takeover	42
Unclear	7

1) Information Disclosure

The lowest impact vulnerabilities are those that leak some information that should not be normally accessible. The actual information may vary from a few bytes following some buffer—which might not be useful or dangerous in any way—to capabilities to read arbitrary data from protected system memory that could include encryption keys or other credentials.

2) Denial of Service

Denial-of-service vulnerabilities are limited to temporary disruption of device activities, denying use of devices or disrupting a service. While this does theoretically present a risk, the motivation for potential attackers is limited, as the wireless attacks are limited by range, and only in very niche cases are these devices used in critical scenarios where a temporary disruption of the device would cause significant damage or present a significant gain for the attacker.

Conceptually, IoT devices may have denial-of-service vulnerabilities that allow the attacker to permanently disrupt device operations, which can either require a "factory reset" operation that might not be easily accessible to the operator, restoring the firmware to a known good state or in some cases even "bricking" the device because the chips cannot be restored to normal operation. However, none of the reviewed 2023 CVEs reported a capability for permanent damage.

3) Elevation of Privilege

Many vulnerabilities grant the attacker the capability to do something that they should not have permission to do, such as breaking the operating system user account restrictions model or gaining access to restricted hardware features. Locally exploitable vulnerabilities can present a practical risk in conjunction with another vulnerability that provides arbitrary code execution in a restricted application context. They are also relevant for platforms that enable downloading untrusted third-party applications

or plugins with the expectation that they will be executed within a restricted sandbox environment, but such a vulnerability may enable to break this containment.

4) Device Takeover

The most dangerous group of vulnerabilities are those with the potential to enable the attacker to take control of the device's behavior, either through its own capabilities or by obtaining remote code execution, effectively permitting the takeover of the consumer wireless device. In the context of cyber conflict, this permits the use of these devices for espionage, theft of confidential data and other intelligence operations. We abstain from adopting the widely accepted term "remote code execution" in this context, as a vulnerability may enable attacker-controlled code execution from a different component on the same physical system, not something that is actually remote. Also, there are vulnerabilities that allow the attacker to take over control of the key functions of the device (for example, remotely altering the strength of electrostimulation in a medical device, as in CVE-2023-26979, or opening a smart lock, as in CVE-2023-34625) without necessarily having the ability to execute arbitrary code on the device.

B. Classification According to the Limitations of the Vulnerability

For consumer wireless devices, the two key aspects are the requirement for physical proximity and the requirement for specific conditions (often, the device being paired with the attacking device, which may require user interaction to put the device in pairing mode or approve the connection) for the vulnerability to be exploitable. The riskiest class of vulnerabilities are those that can be exploited remotely over the internet, usually through an exploitable online service, unless the device is directly accessible with a publicly routable IP address. However, in this paper, we focus on vulnerabilities through direct wireless connections, which are grouped as shown in Table II.

TABLE II: NUMBER OF CVES ACCORDING TO ACCESS VECTOR LIMITATIONS

Access vector	Number of CVEs
Remote	63
Remote for a paired device	32
Local	82
Unclear	6

1) Exploitable Locally

Multiple reported vulnerabilities were flaws in the interaction between multiple system components (i.e. the operating system and a Bluetooth controller), so exploitation is possible only if another part of the system is malicious or compromised—this is generally not applicable for remote attackers who do not have physical access, unless combined with another vulnerability. We do not consider risks of backdoored malicious devices or vulnerabilities that require destructive physical access, since in that case the device could be replaced with a malicious equivalent even if the device model does not have any specific vulnerabilities. However, there is also a large group of local vulnerabilities that circumvent the various sandboxing and permission mechanisms on platforms that allow third-party applications to be run (e.g. Android) but expect their capabilities to be limited. Exploitation of those vulnerabilities may allow a seemingly benign application downloaded from an application store to elevate privileges and use the device for malicious purposes, such as surveillance.

2) Exploitable Remotely over the Air in Specific Conditions

Many wireless vulnerabilities require specific conditions that are unlikely to occur in the real world and cannot be easily caused by the attacker. They are still relevant, as they indicate bugs that should be fixed and may become more easily exploitable in conjunction with other vulnerabilities (e.g. a pairing-mode-only vulnerability can be enabled by a different vulnerability that breaks the existing connection, forcing the device to enter pairing mode), but on their own, they do not imply a risk for the device user. However, evaluating this difference for reported CVEs was difficult, as not all security bulletins provided sufficient information about the preconditions to access the vulnerability.

3) Exploitable Remotely over the Air at Any Time

The final and most dangerous class of vulnerabilities are those that can be exploited over the air, using the applicable wireless protocols that require some physical proximity, but are not restricted by the need for the vulnerable device to be in a specific unusual mode or configuration.

C. Classification According to the Cause of Vulnerability

It is also relevant to group vulnerabilities according to what type of problem created it, as that determines the applicable ways to eliminate or at least detect such flaws. The CVEs often (but not always) have some technical information about the nature of the flaw, and during our analysis, we attempted to map these causes to Common Weakness Enumeration (CWE) [34] IDs as maintained by MITRE and group these causes as shown in Table III.

TABLE III: NUMBER OF CVES ACCORDING TO CAUSE OF THE VULNERABILITY

Cause of the vulnerability	Number of CVEs
Memory safety	105
Improper access control	32
Cryptography flaws	14
Unspecified	12

1) Memory Safety

The most common cause of the reviewed vulnerabilities was various types of memory safety issues—buffer overflows and different types of out-of-bounds access. Within this category, we saw CVEs with various issues grouped under CWE 119 (Improper Restriction of Operations within the Bounds of a Memory Buffer), such as:

- CWE 120: Buffer Copy without Checking Size of Input ("Classic Buffer Overflow")
- CWE 125: Out-of-bounds Read
- CWE 126 Buffer Over-read
- CWE 787: Out-of-bounds Write
- CWE 824: Access of Uninitialized Pointer
- CWE 416: Use After Free

We also saw memory issues following CWE 190 (Integer Overflow) or CWE 129 (Improper Validation of Array Index).

All of these are classic software engineering issues that have been largely mitigated in desktop software through decades of investment in tooling, training and engineering policies, but as this data illustrates, they are the currently dominant challenge in consumer device cybersecurity. While it is practically inevitable that not all software is perfect and some bugs will be present, the dominance of these types of issues can be prevented (though at a cost) by the organizations developing the software.

2) Improper Access Control

In this category, we grouped various issues relating to mistakes in verifying the authorization for specific actions or, in some cases, the total lack of any verification. This refers to CWE 284 (Improper Access Control) and its subgroups, such as:

- CWE 862: Missing Authorization
- CWE 306: Missing Authentication for Critical Function
- CWE 648: Incorrect Use of Privileged APIs
- CWE 346: Origin Validation Error
- CWE 20: Improper Input Validation
- CWE 441: Unintended Proxy or Intermediary ("Confused Deputy")

In this category we also included multiple bounds-checking errors if they resulted not in a memory safety issue but triggered a business logic flaw, circumventing some restrictions.

These mistakes are especially relevant when the platform is expected to run untrusted third-party code, such as downloaded apps, and the application programming interface (API) design needs to ensure that security restrictions are enforced for potentially malicious apps.

3) Cryptography Flaws

The final relevant group of vulnerability causes were various flaws relating to the design or implementation of cryptography, or the lack of any cryptography mechanism where one would be reasonably required to prevent the attack. Weaknesses in this group observed in our analysis include:

- CWE 321: Use of Hard-coded Cryptographic Key
- CWE 294: Authentication Bypass by Capture-replay
- CWE 347: Improper Verification of Cryptographic Signature

There was also a set of attacks ("BLUFFS," Bluetooth Forward and Future Secrecy [35]) targeting the cryptographic fundamentals of Bluetooth session encryption keys.

5. RISKS AND RESILIENCE

The vulnerability analysis in the previous section shows that there is an abundance of low-hanging fruit—relatively unsophisticated vulnerabilities caused by well-known risk factors—so attacks are likely not limited by attacker capabilities or the security of the systems but rather by the lack of attacker motivation. A relevant factor affecting motivation is the effect that a successful attacker can hope to achieve, since for many vulnerabilities the impact is limited only to denial of service (19%) or information disclosure (32%). But as 26% of the reported vulnerabilities do show a potential for device takeover, motivation should not be a prohibitive obstacle. Therefore, apparently, the main relevant restriction that leads to the low level of observed attacks is the

requirement for physical proximity, which makes it hard to perform mass attacks. This limitation makes these vulnerabilities relevant only to attackers who intend to target a specific person or a limited number of people located relatively close to the attacker. The proximity requirement also acts as a deterrent by making it clear to a potential attacker that they might be identified and penalized for any malicious acts.

A. Threat Model

With that in mind, the main threat model relevant for these vulnerabilities of consumer wireless devices to cyber attacks is a sophisticated attacker, possibly a state-sponsored actor, who intends to attack existing vulnerable consumer devices in the target country with the goal of either disrupting civilian life or specifically targeted espionage.

The other threat model is targeted attacks for personal reasons, especially within the context of domestic disputes and violence, which is an established motivation for the abuse of technology [36], and one where the attacker's goals explicitly include surveillance and control of IoT devices, rather than fraud or other forms of monetization.

It is important to note that the threats in this model are largely speculative, because while the risks and vulnerabilities are there, the motivation for such attacks is limited, as there are not many options to exploit them for financial gain or perform them at a large scale due to the physical proximity requirement. The IoT exploits in the wild mentioned in the reports of major security vendors are limited to compromised IoT devices becoming part of botnets and being used to attack other systems that attackers consider valuable via DDoS [37], [38], once again demonstrating the industry focus on protecting corporate networks and commercial services.

B. Resilience

The list of reported vulnerabilities in consumer wireless devices is dominated by memory safety issues—buffer overflows, out-of-bounds access, use after free—even more than in the case of desktop software. However, the development practices applied to embedded systems seem to lag behind other domains of software development, and the situation will likely improve with diligent application of the same best practices: a thorough review of static analysis tools and compiler features to identify potential risks in C or C++ source code, and gradual switch in from C/C++ to memory-safe systems programming languages such as Rust or Golang. Also, fuzzing is a powerful approach to discovering implementation flaws and vulnerabilities, as demonstrated by projects such as Frankenstein [39], BrakTooth [24] and SweynTooth [40], and it can be used in integration testing to identify deviations and undocumented features [41] in parts from third-party vendors. Some of the CVE reports analyzed in this paper noted that the issues had been discovered in this manner.

Of course, that will only be applied by the device manufacturers if they have sufficient motivation to do so. For consumers and society in general, resilience relies on measures such as third-party penetration testing during procurement of devices with potentially risky applications, or a liability shift toward making device manufacturers financially responsible for consequences of security flaws, which may motivate them to invest in measures to reduce vulnerabilities.

6. CONCLUSION

We observe that the published vulnerability data overrepresents issues in general-purpose computer systems, as opposed to non-computer devices whose installed base is far larger. We also observe that most of the reported vulnerabilities are for platforms or software development kits, but not for specific devices or products.

To us, the fact that relatively few registered CVE records apply to consumer or IoT devices is not reassuring. Given the relatively large number of relevant wireless security flaws identified in major software platform projects such as Android, Linux kernel and Zephyr project, and the relatively low level of investment in and attention to security of non-computer consumer devices, we would expect that the multitude of custom proprietary systems would also have a comparable or higher number of flaws. However, the lack of reported CVEs indicates that for most IoT products and companies making them, vulnerabilities are either unidentified or identified outside of public view, and any devices are likely to be vulnerable without the general public knowing.

Similarly, the issues reported with a specific software platform would apply to many different products using that platform. However, there is often no simple way to identify specific devices that use that version of the platform and may be vulnerable. Therefore, the reports are useful for device manufacturers if they properly track their software dependencies, but not for the general public protecting itself. Some manufacturers[2] report affected *chipsets*, but it is not easy for consumers to identify which chipsets are used in their devices and whether they are affected, leading to inaction due to the inability to determine which threats are applicable to specific devices.

The events of 2023 have once more demonstrated the interest of advanced actors in achieving surveillance and spyware goals using highly sophisticated malware such as TriangleDB [42] or Pegasus [43] that exploit multiple iOS zero-day vulnerabilities and were detected only years after their first attacks. Due to substantial investment by Apple and Google, it is technically much more difficult to exploit smartphones than

2 For example, Qualcomm, https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2023-bulletin.html.

various consumer wireless devices, in which the CVEs we reviewed often represented the low-hanging fruit of basic vulnerabilities.

While we are happy to see that the detected vulnerabilities were fixed proactively before they were exploited in the wild, this does provoke an important question: Have there really been no sophisticated attacks on these devices, or are we just not able to detect them?

REFERENCES

[1] I. V. Koskosas and N. Asimopoulos, "Information system security goals," *International Journal of Advanced Science and Technology*, vol. 27, pp. 15–26, 2011.

[2] X. Luo, R. Brody, A. Seazzu, and S. Burd, "Social engineering: The neglected human factor for information security management," *Information Resources Management Journal (IRMJ)*, vol. 24, no. 3, pp. 1–8, 2011.

[3] M. B. Schmidt, "Development and analysis of a model for assessing perceived security threats and characteristics of innovating for wireless networks," Ph.D. dissertation, Mississippi State University, USA, 2006.

[4] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes", *Journal of Network and Computer Applications*, vol. 101, pp. 55–82, 2018.

[5] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Transactions on Communications*, vol. 64, no. 3, pp. 1204–1219, 2016.

[6] R. Odarchenko, V. Gnatyuk, S. Gnatyuk, and A. Abakumova, "Security key indicators assessment for modern cellular networks," in *2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC)*.

[7] H. Peng, "WIFI network information security analysis research," in *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*.

[8] G. Sagers, B. Hosack, R. Rowley, D. Twitchell, and R. Nagaraj, "Where's the security in WiFi? An argument for industry awareness," in *2015 48th Hawaii International Conference on System Sciences*.

[9] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, W. H. Robinson and W. Alexis, "Securing commercial WiFi-based UAVs from common security attacks," in *MILCOM 2016 – 2016 IEEE Military Communications Conference*.

[10] Grand View Research. "Consumer IoT – Worldwide." Statista. Accessed: Jan. 5, 2024. [Online]. Available: https://www.statista.com/outlook/tmo/internet-of-things/consumer-iot/worldwide

[11] "Global computer peripherals market size by devices (input devices, output devices), by connectivity (wired, wireless), by end user (commercial, residential), by geographic scope and forecast." Verified Market Research. Accessed: Jan. 5, 2024. [Online]. Available: https://www.verifiedmarketresearch.com/product/computer-peripherals-market/

[12] "Wearable technology market size, share & trends analysis report by product (head & eyewear, wristwear), by application (consumer electronics, healthcare), by region (Asia Pacific, Europe), and segment forecasts, 2023–2030." Grand View Research. Accessed: Jan. 5, 2024. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/wearable-technology-market

[13] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in internet of things and wearable devices," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 99–109, 2015.

[14] R. Khader and D. Eleyan, "Survey of DoS/DDoS attacks in IoT," *Sustainable Engineering and Innovation*, vol. 3, no. 1, pp. 23–28, 2021.

[15] K. Doshi, Y. Yilmaz, and S. Uludag, "Timely detection and mitigation of stealthy DDoS attacks via IoT networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2164–2176, 2021.

[16] O. D'Mello, M. Gelin, F. B. Khelil, R. E. Surek, and H. Chi, "Wearable IoT security and privacy: A review from technology and policy perspective," in *Future Network Systems and Security: 4th International Conference (FNSS)*, Paris, 2018.

[17] D. Carstens, J. Mahlman, J. Miller, and M. Shaffer, “Mobile device espionage,” Association for Industry, Engineering and Management Systems (AIEMS), 2019.
[18] J. Ibarra, H. Jahankhani, and S. Kendzierskyj, “Cyber-physical attacks and the value of healthcare data: Facing an era of cyber extortion and organised crime,” *Blockchain and Clinical Trial: Securing Patient Data*, pp. 115–137, 2019.
[19] F. Blow, Y.-H. Hu, and M. Hoppa, “A study on vulnerabilities and threats to wearable devices,” *Journal of the Colloquium for Information Systems Security Education*, vol. 7, no. 1, 2020.
[20] Q. Xu, R. Zheng, W. Saad, and Z. Han, “Device fingerprinting in wireless networks: Challenges and opportunities,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 94–104, 2015.
[21] B. Blumbergs, Ē. Dobelis, P. Paikens, K. Nesenbergs, K. Solovjovs, and A. Rušiņš, “WearSec: Towards automated security evaluation of wireless wearable devices,” in *Nordic Conference on Secure IT Systems*, Reykjavik, 2022.
[22] Y. Kim, W. Lee, A. Raghunathan, V. Raghunathan, and N. K. Jha, “Reliability and security of implantable and wearable medical devices,” in *Implantable Biomedical Microsystems*, S. Bhunia, S. J. A. Majerus, and M. Sawan, Eds., Elsevier, 2015, pp. 167–199.
[23] M. Powell. “2023 Bluetooth Market Update.” Bluetooth. Accessed: Jan. 2, 2024. [Online]. Available: https://www.bluetooth.com/2023-market-update/
[24] M. E. Garbelini, V. Bedi, S. Chattopadhyay, S. Sun, and E. Kurniawan, “BrakTooth: Causing havoc on Bluetooth Link Manager via directed fuzzing,” in *31st USENIX Security Symposium (USENIX Security 22)*, Boston, 2022.
[25] M. Cäsar, T. Pawelke, J. Steffan, and G. Terhorst, “A survey on Bluetooth Low Energy security and privacy,” *Computer Networks*, vol. 205, 2022.
[26] Garmin Canada Inc. “ANT+ Directory.” Ant. Accessed: Feb. 12, 2024. [Online]. Available: https://www.thisisant.com/directory/filter/2316/~/~/~/
[27] M. A. Ertürk, M. A. Aydın, M. T. Büyükakkaşlar, and H. Evirgen, “A survey on LoRaWAN architecture, protocol and technologies,” *Future Internet*, vol. 11, no. 10, 2019.
[28] C. W. Badenhop, S. R. Graham, B. W. Ramsey, B. E. Mullins, and L. O. Mailloux, “The Z-Wave routing protocol and its security implications,” *Computers & Security*, vol. 68, pp. 112–129, 2017.
[29] G. Mulligan, “The 6LoWPAN architecture,” in *Proceedings of the 4th Workshop on Embedded Networked Sensors*, 2007.
[30] A. Barua, M. A. Al Alamin, M. S. Hossain, and E. Hossain, “Security and privacy threats for Bluetooth Low Energy in IoT and wearable devices: A comprehensive survey,” *IEEE Open Journal of the Communications Society*, vol. 3, pp. 251–281, 2022.
[31] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.
[32] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A survey on IoT security: Application areas, security threats, and solution architectures,” *IEEE Access*, vol. 7, 2019.
[33] “CVE database search.” MITRE. Accessed: Jan. 2, 2024. [Online]. Available: https://cve.mitre.org/
[34] “Common Weakness Enumeration (CWE).” MITRE. 2023. Accessed: Jan. 5, 2024. [Online]. Available: https://cwe.mitre.org/index.html
[35] D. Antonioli, “BLUFFS: Bluetooth forward and future secrecy attacks and defenses,” in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, Copenhagen, 2023.
[36] J. Slupska and L. M. Tanczer, “Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the Internet of Things,” in *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, J. Bailey, A. Flynn, and N. Henry, Eds., Emerald Publishing Limited, 2021, pp. 663–688.
[37] E. Altares, J. Salvio, and R. Tay. “FortiGuard Labs threat research – 2022 IoT threat review.” Fortinet. Accessed: Jan. 5, 2024. [Online]. Available: https://www.fortinet.com/blog/threat-research/2022-iot-threat-review
[38] Check Point Research. “The tipping point: Exploring the surge in IoT cyberattacks globally.” Check Point. Apr. 11, 2023. Accessed: Jan. 8, 2024. [Online]. Available: https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the-education-sector/
[39] J. Ruge, J. Classen, F. Gringoli, and M. Hollick, “Frankenstein: Advanced wireless fuzzing to exploit new Bluetooth escalation targets,” in *29th USENIX Security Symposium (USENIX Security 20)*, 2020.
[40] M. E. Garbelini, C. Wang, S. Chattopadhyay, S. Sumei, and E. Kurniawan, “SweynTooth: Unleashing mayhem over Bluetooth Low Energy,” in *2020 USENIX Annual Technical Conference (USENIX ATC 20)*, 2020.

[41] J. Classen and M. Hollick, “Inside job: Diagnosing Bluetooth lower layers using off-the-shelf devices,” in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019.
[42] I. Kuznetsov, V. Pashkov, L. Bezvershenko, and G. Kucherin. “Operation Triangulation: iOS devices targeted with previously unknown malware.” Kaspersky. Jun. 1, 2023. Accessed: Jan. 5, 2024. [Online]. Available: https://securelist.com/trng-2023/
[43] K. Hawkinson. “Apple warns Russian journalists their phones may be targets of a state-sponsored attack.” Business Insider. Sep. 16, 2023. Accessed: Jan. 5, 2024. [Online]. Available: https://www.businessinsider.com/apple-russia-journalists-pegasus-spyware-putin-ukraine-war-2023-9