Securing Wireless Ingestible Medical Devices (Final Report)

Rabia Yazicigil Kirby (PI), David Starobinski (Co-PI), Alperen Yasar (RA)

I. Introduction

Ingestible medical devices (IMD) can provide continuous remote monitoring with respect to conventional healthcare technologies while ensuring a more comfortable diagnostic process for the patient. However, as in other intelligent wearable or implantable devices, physical layer security of the chip and reliability of the communication scheme is critical for patients privacy and health [1]. A breach in security may result in a wrong diagnosis, leak of monitored data or even a lethal action against the patient [2].

In this project, we investigated several attack schemes, their possible outcomes and countermeasures. Initially, we conducted research to uncover attacks on a variety of applications and communication schemes (cf. Section II). Later on, we focused on a case study of securing a threshold-crossing based bio-engineered sensor [3], [4], as shown in Fig. 6 (cf. Section III). We report on our publications and future plans in Section IV.

II. Threat Models

The only way to build secure wireless ingestible medical devices is to understand the underlying vulnerabilities that attackers can exploit in the physical layer and analyze these vulnerabilities using security metrics.

A. Classification

Attack schemes can be classified in two groups as non-invasive and invasive methods. Non-invasive methods include attacks that do not require the attacker to damage the packaging of the chip, or make irreversible changes on it. A non-invasive attack can focus on the communication system to alter, capture or block the transmitted data. The attacker can try to communicate with the chip to request data or send a command. Another non-invasive method includes side-channel attacks, which tries to obtain data or bypass the security by monitoring or altering voltage levels, power consumption or EM radiation.

Invasive methods requires the attacker to have a hold of the chip and make an irreversible damage on it. These methods are effective in forensics where attacker tries to obtain some information, such as the cryptographic key, after the chip has been used. If chips do not have a unique identification system, attacker can invasively investigate one chip to perform an attack on the target chip. Invasive methods might require additional equipment such as EM analyzer or microscope, which makes it a more expensive approach than non-invasive methods.

B. Non-Invasive Methods

In this section, possible non-invasive attack schemes on a chip having a two-way communication protocol and an authentication system are investigated. One vulnerability of ingestible devices comes from its low-power nature. Since these devices rely on very small batteries or power harvesting, an attacker can take advantage of this. In the following methods, consequences of this situation will be considered.

1) Communication Attacks: These attacks focuses on capturing, altering or blocking the communication between the transmitter and receiver. The attack might be either passive or active. Passive attacks are the type where attacker eavesdrops without taking any action to alter or block the communication. These attacks can be used to gather information or store the transmitted data to process at a later time. Whereas active attacks aims to change or block the transmitted data, or target one of the devices to prevent it from functioning properly.

Common attack methods such as spoofing, Man-In-The-Middle (MITM) or Denial of Service (DoS) can be effective in IMD applications that has a duplex communication protocol. Spoofing can be defined as disguising as an authorized node to communicate with another node in the system. MITM or DoS typically require the attacker to use spoofing. Once disguised as the authorized server, an attacker can request data from, or send malicious commands to IMD.

In MITM attack, attacker uses spoofing to get in between the transmitter and receiver node, creating a link that goes through itself. This way, attacker can receive data from the server and send it to IMD (or vice versa) with or without altering the data depending on whether it is a passive or active attack. Since the receiver believes it receives data from an authorized node, detection is difficult especially in the passive case.

DoS is an attack type that might be very effective against IMD due to their low-power budget. Since they typically run on small batteries, a repeated data request would make the chip to use its RF front-end block frequently, which would deplete its battery. Since the output power of the IMD transmitter is low, the signal going to the server can be jammed fairly easy. An attack could include selective jamming that blocks the uplink from IMD while keeping the downlink. This would make the authorized server repeatedly request data from the IMD since the last transmission is blocked, which would cause depleting its battery faster.

2) Side-Channel Attacks: Side-channel attacks gathers additional information about the processes running on the chip

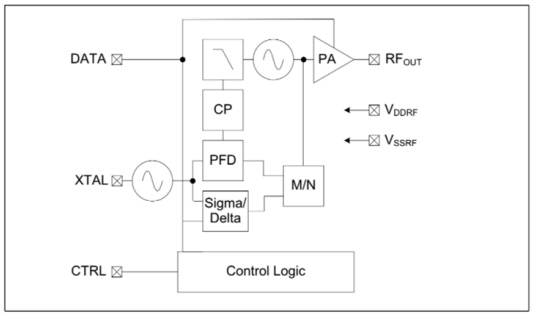

Fig. 1. PIC12 RF Front-End [3], [4]

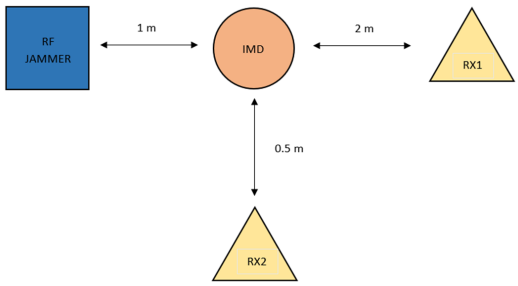

Fig. 2. Jamming Test Setup

TABLE I
JAMMING RESULTS

Distance [m]	Power [dBm]	Correct	Lost	CRC Error
0.5	-30	10	0	0
0.5	-20	10	0	0
0.5	-10	2	3	5
0.5	0	0	8	2
0.5	10	0	10	0
2	-30	10	0	0
2	-20	0	10	0
2	-10	0	10	0
2	0	0	10	0
2	10	0	10	0

or data, or bypass some of the protocols such as authentication. Methods include investigating EM wave radiation, power consumption or decreasing supply voltage to increase delays and bypassing functionalities. Prevention of these attacks require both physical and procedural design choices. For instance, using an encoding that balances number of 0's and 1's would make it harder to get information by monitoring the power consumption. A cyber-security company, Fox IT, showed cracking an AES-256 in five minutes from a distance of one meter. This emphasizes that just being cryptographically secure is not enough for hardware security.

C. Invasive Methods

Invasive methods requires tampering of the device such as removing its packaging to reverse engineer the design under a microscope. These methods are effective in some side-channel attacks like optical radiation investigation. Once the package is removed, UV light can be used to flip the memory bits, potentially deactivating security protocols. Typically these attacks require special equipment which might be costly.

III. Threshold-Crossing-Based Bio-Engineered Sensor

This section focuses on possible attacks and measures to be taken for a specific Ingestible Medical Device shown in Fig. 6. This device, designed by PI Yazicigil and her collaborators at MIT [3], [4], uses a PIC12 microcontroller for data transmission. This device is chosen due to its low power and miniaturized form factor with limited hardware resources. However, due to same reasons, this microcontroller does not have a receiver as part of its RF front end as shown in Fig. 1. This limits the communication protocols that can be used and prevents the chip to detect surrounding devices, making it difficult to detect attacks.

A. Denial-of-Service

A Denial-of-Service (DoS) attack by jamming is performed on the device using a test setup as shown in Fig. 2. An RF wave generator is used as the jammer to produce a sine wave with carrier frequency same as the IMD. As shown in Table. I, since the output power of the PIC12 transmitter is considerably low, it is possible to jam the device that is 0.5 meters apart with a signal at -10 dBm power. Whereas for the device that is 2 meters away, -20 dBm is enough for jamming. IMD is not capable of detecting the attack since it has no receiver and even if the server detects, it cannot notify the IMD. Potentially this can go on throughout the time that the IMD stays in the body, blocking every communication attempt. The problem arises because the chip is operating under a very tight power budget while the attacker has no power limit.

By choosing a jamming power level such that it will be strong enough to jam the signal from the IMD to receiver but will not block the signal from a secondary stronger transmitter (attacker) can result in a false data injection as shown in Fig. 3. Since there is no authentication protocol implemented, this did not require attacker to do spoofing. The packet format can be seen in Fig. 5. This device periodically takes a measurement and sends data every 70 seconds. If the attacker sends the board ID that is being jammed, and sends data in correct time-stamp, it can disguise as the IMD as shown in Fig. 4. By varying the time interval between transmissions according to a secret pseudorandom pattern recognized by the transmitter and receiver, it would be harder for the attacker to send data at the correct time stamp. This way, if the timing of the received signal does not obey the pattern, the server would know there is an adversary in the system and discard the received data.

For a system that has only receiver such as automobile or garage keys, rolling codes provide a level of security that can be applied to our current IMD. For this scheme, transmitter and receiver should agree on a secret sequence of codes. Each time transmitter sends a data, it will append the next code in the sequence to be verified by the receiver. If the code is

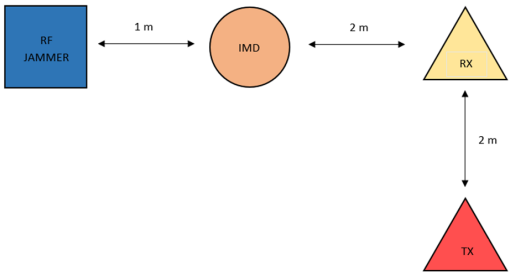

Fig. 3. False Data Injection Test Setup
Red triangle represents the attacker and yellow represents the authorized receiver

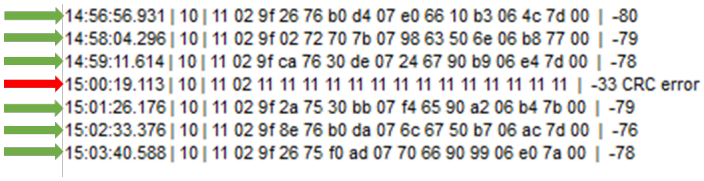

Fig. 4. False Data Injection Results

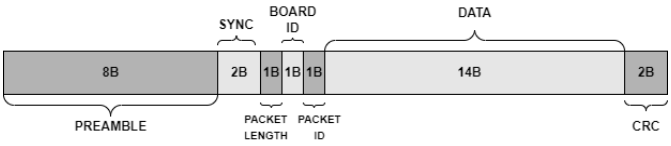

Fig. 5. Packet Format

valid, the receiver will accept the data and change the code to the next one in the sequence. The receiver will keep a range of valid codes in case a transmitted packet is lost and the transmitter still update its code to the next code.

One vulnerability of these rolling codes is brute-force attacks where the attacker sends data repeatedly to find the correct code. However, this can be improved by implementing rolling codes together with a time-varying communication scheme. Even if the attacker knows the time sequence, brute forcing the rolling code, while obeying the timing pattern would take too much time, making it impractical.

B. Forensics

Next type of attack is forensics which focuses on gathering information from the chip after it was used and disposed. In the current state of the device, the data is not being stored on the chip, making it impossible to recover measurement data in forensics. However, if the attacker passively captures the communication between the IMD and the server, the forensic analysis can be performed to retrieve the encryption key and decipher previously captured packets.

To prevent unauthorized reading of the chip memory, PIC12 microcontrollers come with a security flag called data protection bit and code protection bit. When these configurations are enabled, the chip returns all 0's when someone tries to read the memory. However, these flags are designed as active low making it vulnerable to externally switching the bit to 1 by UV light exposure. This attack has been demonstrated by a white-cap hacker nicknamed bunnie on PIC18 microcontroller. Once the packaging is removed, transistors forming the memory for the security flags can be identified with the metal shields built on them for protection. However, it is possible to bypass this by tilting the device 45° angle and exposing to UV light as demonstrated by the white-cap hacker. Even though parts of the data memory is also affected by this UV light exposure, it is possible to retrieve most of the data.

C. System Demonstration

We demonstrated an attack against our threshold-crossing based bio-engineered sensor shown in Fig. 6 [3], [4]. The live demonstration manuscript was published at the IEEE Biomedical Circuits and Systems Conference (BioCAS 2022) [5]. This diagnostic device periodically performs measurements inside the patient's body through its photodiodes, and transmits the data to the server wirelessly. It currently has no data encryption due to the lack of computational power. This makes it possible for an attacker to sniff the data and perform a false data injection. The attack is demonstrated using a software defined radio (SDR) and a host computer, without requiring any additional custom hardware. It is assumed that the attacker has no prior knowledge about the communication protocol and has to reverse engineer it. To demonstrate the feasibility of the attack, the adversarial setup (Fig. 6) includes only off-the-shelf hardware and open-source software. The ADALM-PLUTO is chosen as the SDR due to its low price ($172) and transceiver capabilities.

Using an open-source software for SDRs called Universal Radio Hacker [6], the frequency spectrum is analyzed to determine the carrier frequency of the transmission. After capturing multiple signals over time and comparing them, it is possible to reverse engineer the modulation scheme and packet contents, including the preamble, sync, packet/device ID, and data. Once these are known, the attacker can impersonate the IMD to transmit false data. The goal of this demonstration is to assess the security vulnerabilities of IMDs and emphasize the importance of developing countermeasures against these attacks. It aims at encouraging biomedical system designers to embed security in their resource-constrained systems, which is crucial for the health and safety of patients.

IV. Publication and Future Funding Plans

A. Publications

We presented an attack against the threshold-crossing based bio-engineered sensor shown in Fig. 6 as a live demonstration at the IEEE Biomedical Circuits and Systems Conference (BioCAS 2022) [5]. As of Spring 2023, we are currently

Fig. 6. Attack Demonstration Setup [5]

writing an invited journal article to IEEE Open Journal of the Solid-State Circuits Society focusing on wireless security for resource-constrained devices such as biosensors. This work will also become part of Alperen's Ph.D. dissertation.

B. Funding Plans

We plan to follow up with proposals to industry and federal agencies. For instance, we envision that the NSF Secure and Trustworthy Cyberspace (SaTC) program would be a good match, and plan to submit a proposal during FY 2023-2024.

REFERENCES

[1] V. Vakhter, B. Soysal, P. Schaumont, and U. Guler, "Threat modeling and risk analysis for miniaturized wireless biomedical devices," *IEEE Internet of Things Journal*, 2022.

[2] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services*, 2011, pp. 150–156.

[3] M. Inda *et al.*, "Ingestible capsule for detecting labile inflammatory biomarkers in situ," *bioRxiv*, 2022. [Online]. Available: https://www.biorxiv.org/content/early/2022/02/16/2022.02.16.480562

[4] Q. Liu *et al.*, "A Threshold-Based Bioluminescence Detector With a CMOS-Integrated Photodiode Array in 65 nm for a Multi-Diagnostic Ingestible Capsule," *IEEE Journal of Solid-State Circuits*, pp. 1–14, 2022.

[5] A. Yasar, Q. Liu, M. Mao, D. Starobinski, and R. T. Yazicigil, "Live demonstration: Cyber attack against an ingestible medical device," in *2022 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, 2022, pp. 250–250.

[6] J. Pohl and A. Noack, "Universal radio hacker: A suite for analyzing and attacking stateful wireless protocols," in *12th USENIX Workshop on Offensive Technologies (WOOT 18)*, 2018.