2022-10-13

Live demonstration: cyber attack against an ingestible medical device

Live Demonstration: Cyber Attack Against an Ingestible Medical Device

Alperen Yasar[1], Qijun Liu[2], Matthew Mao[3], David Starobinski[4], Rabia Tugce Yazicigil[5]
Department of Electrical and Computer Engineering
Boston University, Boston, MA
{ayasar[1],liuq[2],mzmao[3],staro[4],rty[5]}@bu.edu

I. Introduction

Intelligent and compact healthcare systems are gaining interest, potentially changing medical monitoring and treatment procedures. Ingestible medical devices (IMD) inside a swallowable pill can transform unpleasant and immobile operations like endoscopy into a remote process. These devices raise a concern for security, where its absence can result in a lethal attack [1]. Some attacks have been shown on medical devices, such as insulin pumps and cardiac defibrillators [2]. A typical challenge for securing an IMD is its resource-constrained design. IMDs have to be small in size to make them swallowable, which limits the battery size. This obliges the device to run on ultra-low power, targeting hours of measurement and data transmission on a small battery. Considering that, it is generally not feasible to have calculation-intensive encryption or a separate cryptography core on the device. However, the security of an IMD is crucial as a breach can cause leakage of confidential data or a wrong diagnosis.

This work demonstrates an attack on a threshold-crossing based bio-engineered sensor shown in Fig. 1 [3], [4]. 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.

II. Demonstration & Visitor Experience

To demonstrate the feasibility of the attack, the adversarial setup (Fig. 1) 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.

The demonstration, using the setup shown in Fig. 1, includes step-by-step reverse engineering, letting the visitors experience the unfolding of the attack through the eyes of an adversary. Using an open-source software for SDRs called Universal Radio Hacker [5], 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

Fig. 1. Attack Demonstration Setup

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.

Acknowledgments

This research was partially supported by the NSF under grant EECS-2128517, Catalyst Foundation (to R. T. Yazicigil, Q. Liu), Leona M. and Harry B. Helmsley Charitable Trust (3239 to R. T. Yazicigil, Q. Liu), and funds from the Center for Information & Systems Engineering and the College of Engineering at Boston University.

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] 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.