Cybersecurity of Biomedical Capsules

Matthew Mao[1,2], Alperen Yasar[2], Qijun Liu[2], Professor David Starobinski[2], Professor Rabia Yazicigil[2]

Henry M. Gunn High School, 780 Arastradero Rd.[1], Boston University, Boston, MA 02215[2]

Introduction

- Biomedical research is expanding its inquiry into ingestible capsules
  - Travels through the G.I. tract
  - Sends (via wireless signals) chemical measurements taken in by microsensors

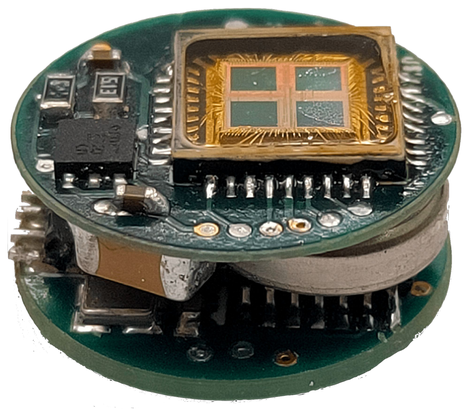

Figure 1: Biocapsule

- On the other end, a receiver will take in these wireless signals
  - Most likely a mobile phone
  - Medical professionals will be able to apply treatments to their patients as they see fit.
- Limited power of capsules due to their small size causes their communication to be susceptible to cyber attacks.

This poster will go over research into the possible cyber attacks and security implementations to prevent such attacks.

Tools

- ADALM PLUTO
  - Software defined radio capable of transmitting and receiving signals

Figure 2: ADALM PLUTO

- Universal Radio Hacker (URH)
  - Software responsible for controlling the ADALM PLUTO, telling it to transmit and receive.
  - Ability to edit signals and autodetect demodulation parameters
- RevEng
  - Reverse engineering CRC algorithms- we will get into what these are later

Doorbell Demonstration

- To familiarize ourselves with our tools, we conducted a replay attack on a doorbell system
- Setup: The doorbell system had two components:
  - Button transmitter
    - Transmits multiple signals (packets) when pressed
  - Ringer receiver
    - If there is a match with the expected signal, a "ring" sound will be played

Figure 3: Ringer (left), button (right)

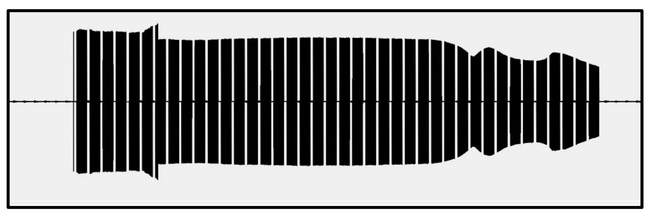

Figure 4: Recorded packets (signal v.s. time domain)

- By recording and playing back the signal sent by the button transmitter (using URH) at **433 MHz** (frequency given by the seller of the doorbell), we were able to make the receiver ring.

Biocapsule Attack

- Setup: Simulation using two CC1120 transceivers that used packet architectures identical to the biocapsule.
  - One transceiver acted as a receiver (mobile phone) while the other acted as the transmitter (capsule)
  - Each transceiver was controlled through a computer using SmartRF Studio 7

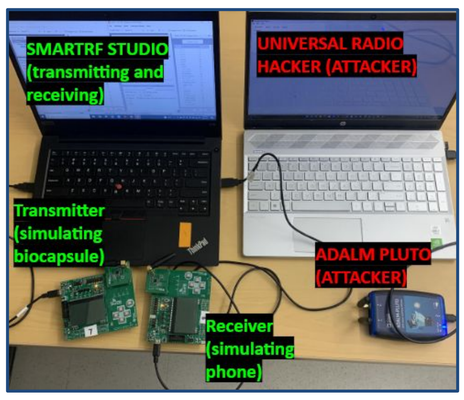

Figure 5: Setup diagram

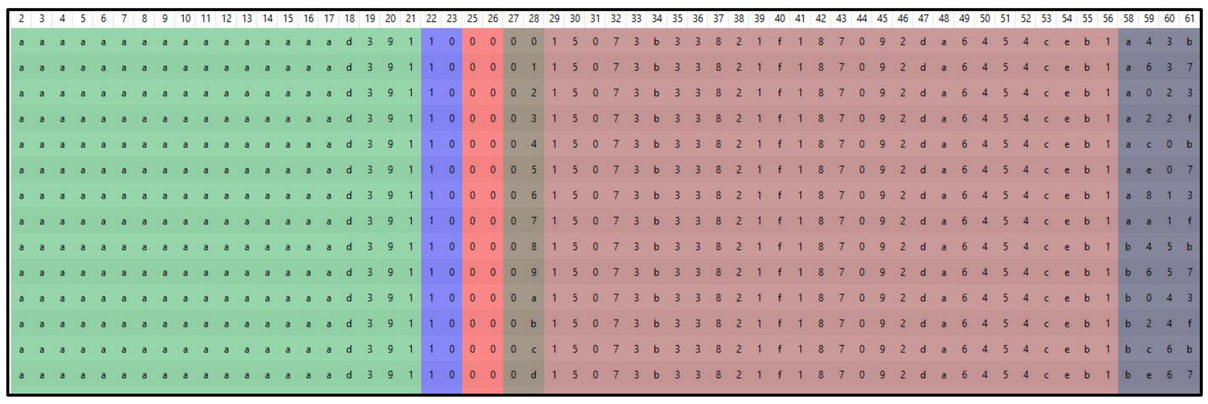

Figure 6: Labeled packets represented in hex (each color represents a different section)

- First step was to record multiple packets at **915 MHz** from the transceiver responsible for transmitting data.
  - URH demodulated signal (FSK) using its auto detect capabilities
  - We deconstructed the packet into its multiple sections (see figure 6) using pattern recognition techniques

- Next, we had to reverse engineer the CRC.
  - CRC's are meant to check for errors within a packet (not security).
    - Data must match correct CRC checksum
  - However, attackers do not have access to the parameters used for a CRC calculation. Luckily, the RevEng algorithm takes care of this.
    - Solution was a brute force script that eliminates bytes from the front of the packet and ran result on RevEng's program

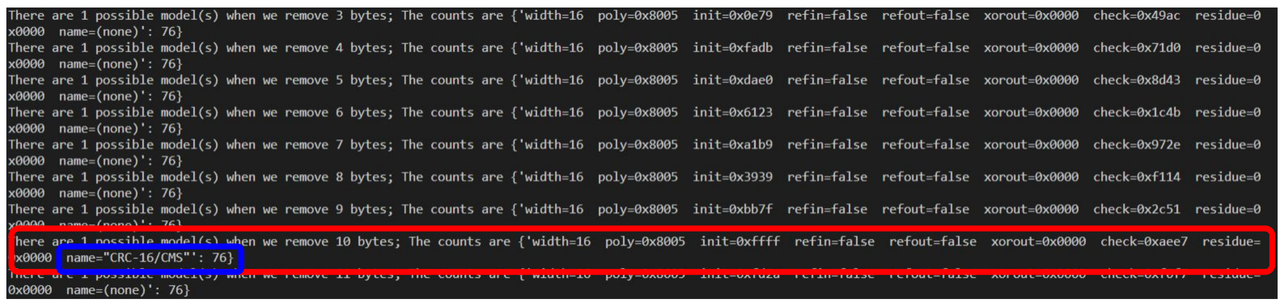

Figure 7: Output of brute force algorithm. It is clear that removing 10 bytes is the only option that gives us a known CRC.

- Finding the location of data allows attackers to eavesdrop on their victims (invasion of privacy)
- False data injection attack
  - After recording a signal from the biocapsule, an attacker could potentially change the data section and update the CRC accordingly (to prevent the false packet from being thrown out for error detection)
  - Jamming the capsule's signal using a significantly more powerful signal from the PLUTO while sending the edited one, attackers would be able to trick the receiver into taking in the false information
  - Exposes victim to false therapies inducing physical harm

Conclusion

- Attacks are imminent for capsules when the hacker is able to understand the packet architecture.
  - We can potentially introduce lightweight encryption algorithms into our system
    - RC6 is one algorithm that we have looked into
  - Without access to the key, attackers would be left with an incohesive string of encrypted characters
    - Packet breakdown will be impossible
  - Still vulnerable to brute force attacks, but it would take lifetimes to reach the correct key

References

Q. Liu, A. Riaz, T. Zirtiloglu, M. E. Inda, M. Jimenez, Y. Lai, C. Steiger, E. Diamond, G. Traverso, T. Lu, A. Chandrakasan, P. Nadeau, and R. T. Yazicigil, "Zero-crossing-based bio-engineered sensor," in 2021 IEEE Custom Integrated Circuits Conference (CICC), 2021, pp. 1–2.

M. Inda, M. Jimenez, Q. Liu, N. Phan, J. Ahn, C. Steiger, A. Wentworth, A. Riaz, T. Zirtiloglu, K. Wong, K. Ishida, N. Fabian, J. Jenkins, J. Kuosmanen, W. Madani, R. McNally, Y. Lai, A. Hayward, M. Mimee, P. Nadeau, A. Chandrakasan, G. Traverso, R. Yazicigil, and T. Lu, "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

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

A. Yasar, Q. Liu, M. Mao, D. Starobinski, and R. T. Yazicigil, "Live Demonstration: Cyber Attack Against an Ingestible Medical Device," Biomedical Circuits and Systems Conference, 2022. (Under Review)

Acknowledgements

- Special thanks to Alperen Yasar and Qijun Liu for working closely with me and answering my questions.
- I would also like to thank Professor Yazicigil and Professor Starobinski for helping us when we became stuck on software issues.