Lane Gramling
EECS 700
Reading 23

Summary - Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

This paper focuses on auditing the security performance of modern implantable defibrillators. In their work, the authors show how the pacemakers under study operate communicate in cleartext, as well as other vulnerabilities that allow a potential adversary to eavesdrop, alter settings, or exploit these vulnerabilities in other malicious ways. Additionally, defense techniques are proposed which are built around the idea of providing security benefits without consuming power in the device. In this paper, it is worth noting that the authors make clear that attack methods and other key pieces of information are intentionally omitted from the paper, so as to prevent this work from becoming a step-by-step guide for attacking ICDs.

Contributions

Initially, the paper provides a rundown of how ICDs operate on a hardware level, and how they wirelessly communicate with a device to allow for programmability, settings adjustments, and other functions. This knowledge allows for the first major piece of work contributed in this paper, which is how to intercept ICD communications. By using a recording oscilloscope and a universal software radio peripheral, it is shown that RF transmissions from the device are able to be identified. From the saved RF traces, and through some clever techniques to determine the modulation schemes for symbol and bit representations, the researchers showed that by using the proper analysis, the radio information can be reconstructed into the higher level information it represents. By doing this, it revealed that communications are unencrypted. After making these discoveries, the authors show that software can be written to perform these computations on the emitted RF signal to enable real-time eavesdropping. By doing this, the authors show that private patient records (Name, DOB, IDs, History, etc.) can be eavesdropped upon and stolen. Additionally, they were able to intercept telemetry broadcasting the patient's EKG reading.

Moving ahead from this, the paper also provides a number of examples of active attacks using a commodity software radio. Among these, the authors explain that they were able to perform a number of malicious attacks: disclosing both patient and cardiac data, changing the record for the patient's name, setting the device's clock, changing therapy responses to cardiac events, inducing fibrillation, forcing increased power consumption, and others.

The last key component of the paper is an enumeration of three zero-power defenses proposed to give a foundation for preventing these types of attacks from occurring in future models. The first of these is a notification system which uses a piezoelectric device to emit a chirping noise upon receiving a sequence of requests from an RFID reader, which constitutes a potential security-sensitive event. The second of these is a simple modification to the protocol adding a challenge-response scheme allowing devices to be authenticated upon attempts to communicate with the ICD. Finally, the last defense proposal is the usage of a symmetric cryptographic key exchange using a device held to the ICD, which provides both communication security and patient awareness due to the need to carry out the task.

Limitations

This paper provides a fairly through penetration into the ICD's communications and shows a number of ways this ability can be exploited. Additionally, it is fairly well-balanced, providing valuable input both on the offensive and defensive sides of ICD security. One limitation specifically expressed in the paper is that the researchers did not fully reverse-engineer the communication protocol, uncertain of what information is being transferred in portions of the packets, although noting that this information would likely not contribute additionally towards their goal of acquiring private data. Another limitation is the hardware and physical requirements for some of these attacks to be carried out. These attacks could prove very difficult to carry out in the wild due to the nature of the hardware necessary for intercepting and decoding the ICD's communications, thus lacking viability. Additionally, each defense method required extra hardware to be added to the device or handled by a person. Hardware additions are certainly easier said than done when dealing with the need to implant the device inside a body, and when that device serves functions critical to a patient's survival.

Future Work

In terms of future work, the defense proposals explained in the paper provide a good foundation for further inquiry into ICD security mechanisms. Given this, it could prove beneficial to establish a standard for operational and communications security in implantable medical devices, in addition to a protocol for robustly auditing the security of such systems. Since these devices usually have the patient's life placed directly in its hands, it seems obvious that it is critically important to have a clearly defined standard to follow for ensuring the device's secure operation and resistance to tampering.