School of Engineering and Computing Sciences

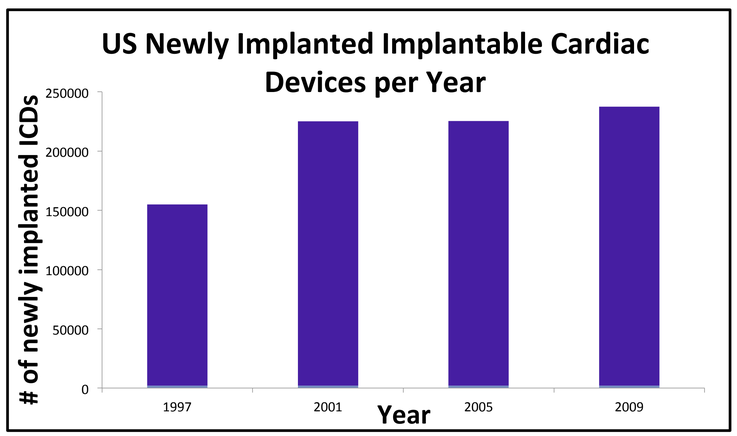
A Feasible IMD Communication Protocol: Security without Obscurity

NYIT Research Experience for Undergraduates (REU)
May 26 – July 30, 2015

REU fellow(s):, Jason Wang[1], Keyon Mohebzad[2], Luke Johnson[3], Faculty mentor: N. Sertac Artan[4],
Affiliation: [1]: University of North Carolina at Chapel Hill, [2]: University of Texas at Austin, [3]: Gonzaga University, [4]: School of Engineering and Computing Sciences, NYIT

Abstract

Our study analyzes the feasibility of secure communication in implantable medical devices (IMDs). We propose a dual-band authentication protocol that provides a high degree of privacy and authentication to the patient, while being easily used by utilizing current technology. Our proposal takes advantage of two of the communication technologies readily available in many smartphones (Bluetooth Low Energy (BLE) and Near Field Communication (NFC)) to integrate the convenience of wireless communications with the security of near field communications. By separating the standard communication medium (BLE) from the authentication medium (NFC), our protocol protects the IMD against resource depletion attacks and long range adversaries while allowing a usable communication distance. In order to perform authentication, we utilize pre-shared key distribution scheme that allows for protection from unprivileged adversaries and accountability to potentially malicious medical personnel. Our protocol compares favorably to the state-of-the-art security solutions for IMDs in the literature.



IMD Use and Growth

IMDs are a growing market that provide life critical medical measurements and actions depending on the device. The most common life critical medical devices are implantable cardiac devices (ICDs) such as pacemakers, and implantable automatic defibrillators. These devices growth is accounted for above in the world survey of ICDs by the International Cardiac Pacing and Electrophysiology Society. These numbers are not given at each year but by connecting reported data with a linear trend you can estimate a total number of over 8 million new implants since 1997 with a growing market each year. The communications of these implants need to be secured and while there are many solutions suggested the usability for the patient and doctor should remain critical to the design to ensure proper use.

IMD Design Constraints

- Life Span: Replacing the IMD or its battery requires surgery. Insuring a long life span in the patients body is critical to avoiding unnecessary procedures.
- Power Consumption: IMD batteries should last up to 10 years in normal use. This means that their power use must be minimized.
- Heat Dissipation: since these devices are contained entirely within the human body they must not damage the surrounding tissues via heating.
- Physical Size: these devices should be as small as possible in order to fit in the limited space available within the patient's body.

Comparison Table of Key Attributes in Different Protocols

Name of Solution	Emergency Data Access	Role-Based Authentication	External Device	Resource Efficient	Measurement privacy	Bearer privacy	Non-Drainable
[2] IMDShield	x		x	x	x	x	x
[3] MedMon	x		x	x	x	x	x
[4] IMDGuard	x		x	x	x	x	x
Our Proposal	x	x		x	x	x	x

Related Work

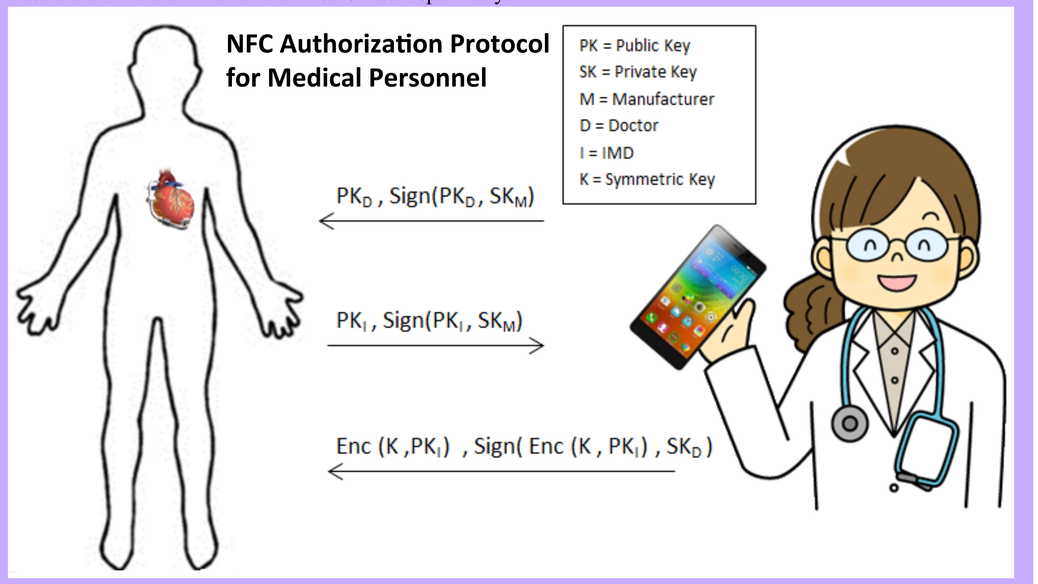
IMDShield[2] A device worn by the patient that jams all signals, by default. Only allows communication from an external device if the communication aligns with its own antidote signal.

MedMon[3] Monitors communications within the network and jams communication when a threat is perceived by the behavioral anomaly detection system.

IMDGuard[4] Communicates with the IMD using proximity as a security measure and does the long range communication and security computation.

Proposed Protocol

In our protocol there are two bands: The data communication band and the authorization band. At first a user must use the authorization band to authenticate their identity and exchange a symmetric key in order to use the data communication band and the devices functionality. Within the authorization band are two separate protocols for user authentication and each has distinct device access attached to which authentication method is used. The first is a time based protocol that is for patients' use; the second is a pre shared key system intended for easy use by medical personnel. We decided on Bluetooth Low Energy and Near Field Communication for the data communication and the authorization bands respectively.



Data Communication

- BLE is preferable because it has out of band authentication as a built-in feature
- Also built-in to BLE is AES-CBC 128 which is a form of authenticated encryption that makes determining sender identification quick and low resource.
- BLE (also called Bluetooth Smart) is widely implemented in smartphones today, available with NFC in most high end devices.

Authorization

Patients authorizing with the time based protocol need to present their device (and exchange partial keys) to the IMD a number of times over a period of time. This allows for users to gain access to their device while still preventing unwanted parties from gaining access.

Doctors will be issued keys by the manufacturer an d then use that source of verification to send a symmetric key via NFC. This option allows for quick access in the office or in an emergency situation.

Time Based Authorization

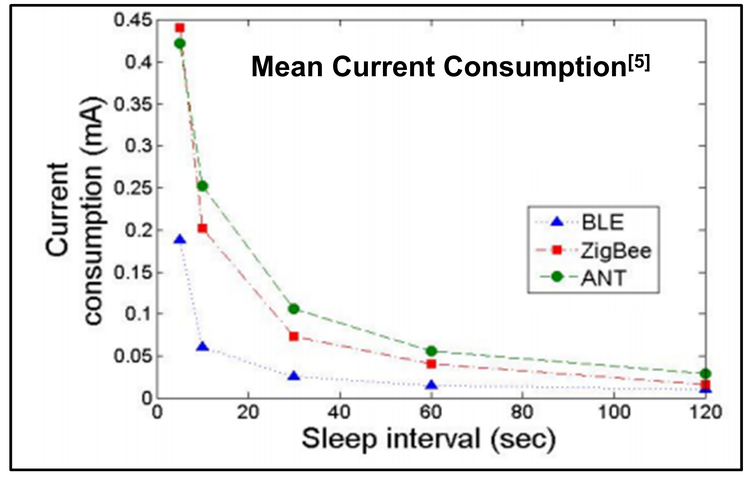
The phone sends the IMD a partial key and the IMD stores that key. When the second partial key is sent is receive by the IMD it is XORed with the stored key and then stored in its place. This results in a final key that requires all partial keys in order to be recovered.

```
1100111010001100  Partial Key 1
1010011010100011  Partial Key 2
----------------------------------XOR
0110100000101111  Intermediate Key 1
1110001010111010  Partial Key 3
----------------------------------XOR
1000101010010101  Intermediate Key 2
0001010010111010  Partial Key 4
----------------------------------XOR
1001111000101111  Final Shared Key
```

By spreading the partial keys out across an extended period of time the authenticating party must maintain a close physical proximity to the IMD and therefore the patient. If the authenticating party is an adversary they would have to act suspiciously in order to gain access to any functionality of the device. This method only allows access to the most basic services including reading the devices measurements. Other information about the patient, doctor, or other non-critical identifying information would require authorization using the other protocol.

Power Efficiency

- BLE only decreases the longevity of the battery life (compared to no wireless communication) by 5.54%
- The BLE communication protocol is optimized for burst communications (maximized sleep interval) rather than continuous communication.
- The IMD will utilize passive NFC which means that it will receive both power and data through NFC without costing anything from the battery
- Supplying the power for authentication through NFC also makes this protocol immune to resource depletion attacks



Acknowledgement

This project is funded by National Science Foundation Grant No.1263283 and by New York Institute of Technology.

References

[1] Halperin, Daniel, Tadayoshi Kohno, Thomas S. Heydt-Benjamin, Kevin Fu, and William H. Maisel. "Security and privacy for implantable medical devices."*Pervasive Computing, IEEE* 7, no. 1 (2008): 30-39.
[2] Gollakota, Shyamnath, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. "They can hear your heartbeats: non-invasive security for implantable medical devices." *ACM SIGCOMM Computer Communication Review* 41, no. 4 (2011): 2-13.
[3] Zhang, Meng, Anand Raghunathan, and Niraj K. Jha. "MedMon: Securing medical devices through wireless monitoring and anomaly detection."*Biomedical Circuits and Systems, IEEE Transactions on* 7, no. 6 (2013): 871-881.
[4] Xu, Fengyuan, Zhengrui Qin, Chiu C. Tan, Baosheng Wang, and Qun Li. "IMDGuard: Securing implantable medical devices with the external wearable guardian." *INFOCOM, 2011 Proceedings IEEE* (2011): 1862-1870.
[5] Dementyev, Artem, Steve Hodges, Stephen Taylor, and Johan Smith. "Power consumption analysis of Bluetooth Low Energy, ZigBee and ANT sensor nodes in a cyclic sleep scenario." In *Wireless Symposium (IWS), 2013 IEEE International*, pp. 1-4. IEEE, 2013.