# Poster: Near Field Communication based Access Control for Wireless Medical Devices

Xiali Hei, Xiaojiang Du and Shan Lin
Department of Computer and Information Sciences
Temple University
19122 Philadelphia, USA
{xiali.hei, xjdu, shan.lin}@temple.edu

## ABSTRACT

Security of wireless medical devices is critical for patient safety because security attacks may directly hurt patients' health. In this paper, we design a novel access control scheme based on bi-channel and multi-factor authentication for wireless medical devices. Our scheme utilizes near field communication (NFC) to perform device pairing, which supports key exchange between a device and a reader in short communication range (<= 6cm) with bounded response time. To further defend against attacks when a malicious reader is placed within the device's communication range in crowded situations, we design a crowd detection algorithm using WiFi and user's smart phone to assist the key exchange. Our analyses and experiments show that our security schemes are effective and efficient.

## Categories and Subject Descriptors

J.3 [**Computer Applications**]: Life And Medical Sciences—*Medical information systems*

## General Terms

Security,Measurement,Human Factors

## Keywords

Response Time, Near Field Communication, Secure Pairing, Access Control, Medical Devices

## 1. INTRODUCTION

Security for wireless medical devices, such as cardiac defibrillators, insulin pumps, and various drug delivery systems, is critical for patient's safety [1]. Unfortunately, most of the existing wireless medical devices lack of sufficient security mechanisms to protect them from malicious attacks. There are a number of attacks from Satan adversary may launch on wireless medical devices [2] [3] [4] [6] [7].

Securing wireless medical devices is a challenging task due to their limited resources and the open environment. To address this problem, we propose integrating NFC with medical device. We implement secure pairing between a device and a reader over NFC, which allows a doctor's reader to share a key with a medical device with a very short distance. This pairing procedure is shown in Fig 1(a). If the medical device is not implantable, the device requests the patient to press a button to confirm. After sharing a key successfully, the reader and medical device can securely communicate with each other using their existing radios.

The key exchange procedure between a device and a reader over NFC is vulnerable to attacks if a malicious reader is within their communication range. Such attacks can be launched in crowded situations without causing users' attention. To address this problem, we design a crowd detection algorithm to alert users about insecure scenarios. This crowd detection algorithm is based on wireless device counting using users' smart phone. The basic procedure of this algorithm is shown in Fig 1(c). If the surrounding is not a crowded area, then the algorithm will notify the medical device. For implantable medical devices, other patient access patterns based control (PAPAC) scheme [4] is also used to defend against attacks.

## 2. DESIGN AND EXPERIMENTATION

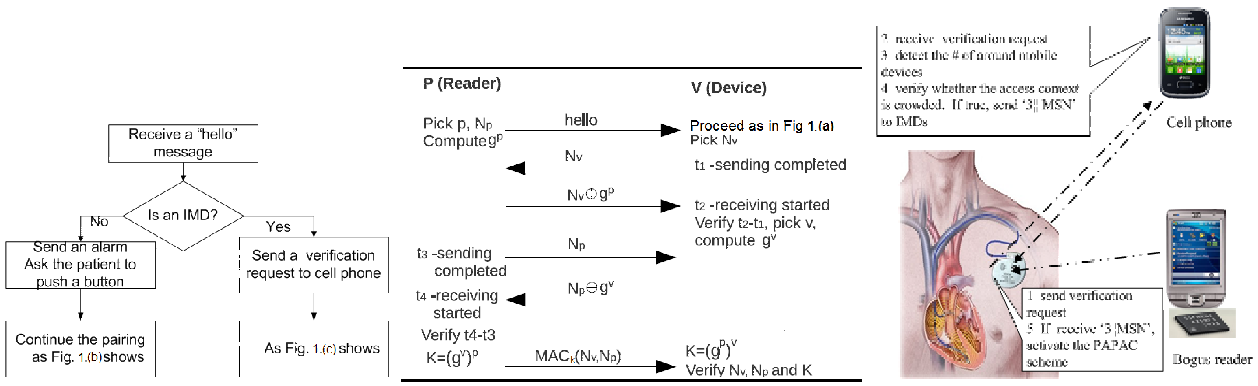
**NFC Communication Range.** We tested the transmission range using 2 NFC-enabled smart phones (with PN544 chips). Our experimental results showed that they can successfully exchange data within 5cm. The two devices can recognize each other at 6cm, however, they cannot successfully exchange data at 6cm. We also confirmed this when one cell phone is around 5mm-thickness pork.

**NFC Round Trip Time.** As NFC is a new wireless technology, we conducted experiments to measure the round trip time (RTT), which can help eliminate relay attacks. Specifically, we use the time difference between finishing sending the last bit of a request message and the receiving of the first bit of the response message, which also is called response time. We used two Android smart phones with NFC chips to test the typical response time. The time resolution in cell phone is 1ns when we call the system time. We programmed these two phones to send and reply to messages at data link layer. Figure 2(a) shows our experimental results over 50 runs. From it, we can see that average response time is $E$=0.258ms, and the standard deviation $D$=0.026ms. We choose $Th_t = E + 2D = 0.31ms$.

**The Device Pairing Protocol.** In our scheme, the access control is based on device pairing employing NFC. We design the distance bound pairing schemes based on the Diffie-Hellman key exchange protocol [5]. In Figure 1(b), $P$ and $V$ represent the reader and the medical device. We use the response time $t_2 - t_1$ to bound the distance between them. The sharing key is $(g^v)^p$ for later communication.

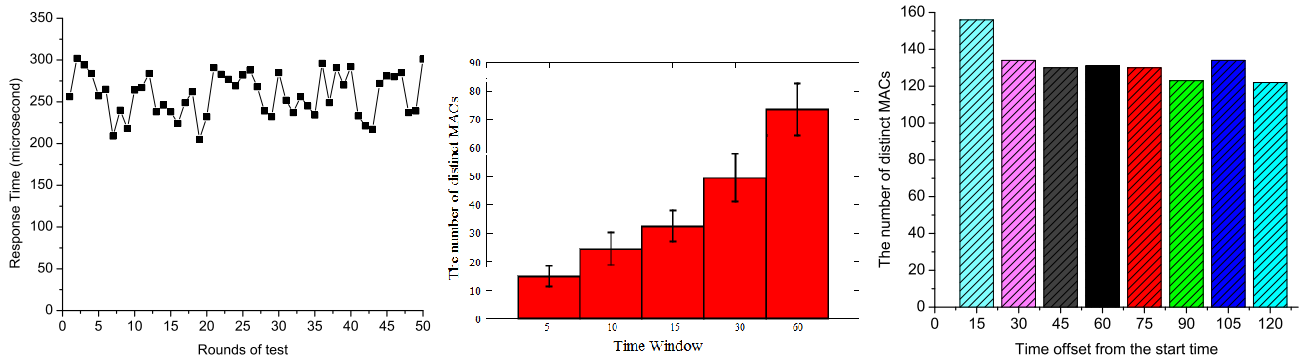
**PAPAC Scheme.** The light-weight PAPAC security scheme can be used to protect wireless medical devices from attackers who are extremely close to the patient. PAPAC utilizes the patient's IMD access patterns and the patient's cell phone. It modeled the normal IMD access pattern using five kinds of IMD access data: reader action type, time interval of the same reader action, location, time,


*MobiHoc'14,* August 11–14, 2014, Philadelphia, PA, USA.
ACM 978-1-4503-2620-9/14/08.
http://dx.doi.org/10.1145/2632951.2635944 .




(a) Workflow of a device (b) The device pairing protocol (c) Access control scheme for IMDs

**Figure 1: The main process**




(a) Response time test results (b) The mean and standard variance for each time window of testing example 1 (c) Test examples 2

**Figure 2: Test results**

and day type (weekday or weekend). The patient's cell phone stores these data and runs a classification algorithm. When contacted by a reader, the IMD first sends a short *Verification* request message to the patient's cell phone. The cell phone then runs the classification algorithm and makes the following decisions: (1) if the algorithm indicates that this is a normal access, it sends a *Continue* command to the IMD, signaling the IMD that it may continue communication with the reader (i.e., performing standard authentication); (2) if the algorithm indicates that this is an attack, it sends a *Block* command to the IMD; and the IMD will enter sleep mode.

**Detecting Crowded Situations.** When a patient is in a crowded situation, hackers may use their mobile devices to attack the patient's wireless medical device. Our crowd detection is to roughly evaluate the number of mobile devices around a patient. Specifically, wireless radio on user's cell phone can observe the active MAC addresses and their corresponding received signal strengths of each probe request of each mobile device. Then we count the number of distinct active MAC addresses with strong signals within a short period. We denote $\Delta$ as the time window and determine the value of $\Delta$ by analyzing experimental results.

We conducted experiments to test our crowded area detection scheme by using the Samsung Galaxy Nexus phone with an Alpha360 WiFi adapter. We programmed the Android phone to collect the number of different MACs it can sense over different time windows: 5sec, 10sec, 15sec, 30sec, 60sec, 90sec and 120sec.

We recorded that there were 32 different persons in the train when we sat down until we left for the next station. Figure 2(b) shows the mean and standard variance of the number of distinct MAC addresses for each time window $\Delta$. We can see that when $\Delta$=15sec, the mean of it is close to 32 and the ratio between it and the standard variance of it is the least. So we choose $\Delta$=15sec for later analysis. Figure 2(c) shows one test example in crowded area. From experiments, we chose the -38dBm as the threshold of signal strength. The difference between the number of distinct MAC addresses detected by our algorithm and the number of persons around us during the experiments is the error. The mean and standard variance of the error rates are 5.70% and 4.73%, respectively. This shows the test result is close to our observations. Since we only need a rough evaluation on the number of mobile devices around the patient, the result is reliable enough.

## Acknowledgment

This work was supported in part by the US NSF under grants CNS-0963578, CNS-1022552, CNS-1065444, IIS-1231680, CNS-1239108, and CNS-1035715.

## 3. REFERENCES

[1] W. H. Maisel, "Safety issues involving medical devices," in J. of the American Medical Association, vol. 294, Aug. 2005, pp. 955-958.

[2] K. Fu, "Inside risks: reducing risks of implantable medical devices," in Commun. of the ACM, vol. 52, June 2009, pp. 25-27.

[3] D. F. Kune et al., "Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors", in Proc. of the 34th Annual IEEE Symposium on Security and Privacy. May 2013.

[4] X. Hei et al., "Defending resource depletion attacks on implantable medical devices," in Proc. of the IEEE GLOBECOM'10, 2010, pp. 1-5.

[5] W. Diffie and M. Hellman, "New directions in cryptography". in IEEE Trans. on Information Theory, vol. 22, no. 6, 1976, pp. 644-54.

[6] X. Hei, X. Du, S. Lin, and I. Lee, "PIPAC: Patient Infusion Pattern based Access Control Scheme for Wireless Insulin Pump System", in Proc. of IEEE INFOCOM'13, Turin, Apr. 2013.

[7] X. Hei and X. Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies," in Proc. of IEEE INFOCOM'11, 2011, pp. 346-350.