SNAPPY TITLE GOES HERE

A Dissertation
Submitted to
the Temple University Graduate Board

---

in Partial Fulfillment
of the Requirements for the Degree
DOCTOR OF PHILOSOPHY

---

by
Christian Radcliffe Ward
May / August / December, 20XX

Examining Committee Members:

Dr. Your Advisor , Advisor, Dept. of Electrial and Computer Engineering
Dr. Member One, Dept. of Z and X
Dr. Member Two, Dept. of Z and X
Dr. Member Three, Dept. of Z and X
Dr. Member Four, External Reader, Dept. of Z and X

ABSTRACT

ACKNOWLEDGEMENTS

This book could not have been written without Dr. Xiaojiang Du, who encouraged and challenged me through my academic program. He never accepted less than my best efforts. Thank you. What is written in this book are materials that I found in my papers. A special thanks to the authors mentioned in the bibliography page. I would like to acknowledge and extend my heartfelt gratitude to another advisor of mine –Dr. Shan Lin. Most especially to my family, friends and my son, Peiheng Ni. Words alone cannot express what I owe them for their encouragement and whose patient love enabled me to complete this book. A special thanks to Jie Wu for comments on my editing. The book was developed from ideas originally published in the Globecom 2010, Infocom 2011 and As always it was editor Xuemin (Sherman) Shen who provided the shelter conditions under which the work could take place: thanks to him for this and many other things.

Words.

TABLE OF CONTENTS

LIST OF FIGURES

Figure

LIST OF TABLES

Table

CHAPTER 1

INTRODUCTION

Securing IMDs is a very challenging task due to their very limiting resource constraints in terms of energy supply, processing power, storage space, etc. An IMD is implanted in a patient's body and is expected to operate for several months or years. Typical IMDs are powered by a non-rechargeable battery, and replacement of the battery requires surgery. Re-charging an IMD via an external RF electromagnetic source causes thermal effects in body tissues and thus is not recommended. Unlike general medical sensors that may use AA-type or renewable (e.g., solar) batteries, an IMD typically uses silver vanadium oxide batteries and therefore is very vulnerable to the Resource Depletion (RD) attacks Hei et al. (2010). The RD attacks include a number of attacks that try to consume as much energy as possible, such as Denial of Service (DoS) attacks and forced authentication attacks (discussed later). These kinds of attacks can be easily launched but are difficult to defend against. A number of literatures Malasri & Wang (2009), Juels (2006), Raymond & Midkiff (2008), Raymond (2006), Halperin et al. (2008) have studied DoS attacks on wireless sensor networks. Raymond and Midkiff Raymond & Midkiff (2008) provide a survey of DoS attacks against sensor networks. However, the security schemes designed for sensor networks cannot be directly applied to IMDs, because IMDs have much less available resources than typical sensor nodes. For example, a Mica2 mote sensor has 128KB programmable memory and 512K data memory "Mica2 mote sensor" (n.d.), while an IMD may have less than 10KB memory. Furthermore, it is much easier to replace

the battery for a sensor node than for an IMD. Hence, special light-weight security schemes need to be designed for IMDs. Another difference between sensor nodes and IMDs is that an IMD is implanted in a patient's body and directly involves a human (the patient). Hence, effective security schemes for IMDs may utilize the human in their design.

During emergencies, a patient (say Bob) may be unconscious and cannot provide his credentials (such as a token or a key) to the medical personnel, nor can he show his ID or inform medical personnel about his medical information. In addition, neither device-based schemes nor family-based schemes Sun et al. (2011) can be used if the patient has an emergency outside his home country. In this case, the safety of patients outweighs the security and privacy concerns of IMDs. A good access control scheme should satisfy security, privacy and safety requirements.

CHAPTER 2

LITERATURE REVIEW

CHAPTER 3

A UNIFIED SECURE FRAMEWORK FOR WIRELESS MEDICAL DEVICES USING PATIENT'S CELL PHONE

CHAPTER 4

NEAR FIELD COMMUNICATION BASED ACCESS CONTROL FOR WIRELESS MEDICAL DEVICES

CHAPTER 5

A PATIENT ACCESS PATTERN BASED ACCESS CONTROL SCHEME

CHAPTER 6

PATIENT INFUSION PATTERN BASED ACCESS CONTROL SCHEMES FOR WIRELESS INSULIN PUMP SYSTEM

CHAPTER 7

BIOMETRICS BASED TWO-LEVEL SECURE ACCESS CONTROL FOR IMPLANTABLE MEDICAL DEVICES DURING EMERGENCIES

CHAPTER 8

CONCLUSION

BIBLIOGRAPHY

Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T., & Maisel, W. H. (2008, Jan.-Mar.). Security and privacy for implantable medical devices. *IEEE Pervasive Computing*, *7*, 30-39.

Hei, X., Du, X., Wu, J., & Hu, F. (2010). Defending resource depletion attacks on implantable medical devices. In *Proc. of the ieee globecom 2010* (p. 1-5).

Juels, A. (2006, Feburary). Rfid security and privacy: a research survey. *IEEE JSAC*, *24*, 381-394.

Malasri, K., & Wang, L. (2009, July). Securing wireless implantable devices for healthcare: ideas and challenges. *IEEE Communications*, *47*, 74-80.

Mica2 mote sensor. (n.d.).

Raymond, D. (2006). Effects of denial of sleep attacks on wireless sensor network mac protocols. In *Proc. of the 7th ann. ieee systems, man, and cybernetics, information assurance workshop* (p. 297-304).

Raymond, D., & Midkiff, S. (2008, Jan.-Mar.). Denial-of-service in wireless sensor networks: attacks and defenses. *IEEE Pervasive Computering*, *7*, 74-81.

Sun, J., Zhu, X., Zhang, C., & Fang, Y. (2011). Hcpp: Cryptography based secure ehr system for patient privacy and emergency healthcare. In *Proc. of icdcs'11* (p. 373-382).

APPENDIX A

Appendix A