

# Preface

The objective of this book is to help readers learn more about the security and safety issues in the area of implantable medical devices (IMDs). This book takes the view that security concerns are critical in IMDs because there is the potential that a patient may be directly harmed without warning or notice. In this book, we present two plausible solutions for normal cases and emergency cases. We hope these solutions will inspire readers to propose better solutions. In addition, we review a number of current works published within the last five years. Furthermore, we discuss many future works at the end of this book, and we hope it will be helpful for researchers who are interested in this field.

In this book, we provide an overview of new security attacks, challenges, defense strategies, design issues, modeling, and performance evaluation in wireless IMDs. We mainly discuss two methods to perform access control for IMDs. One scheme is pattern-based, and the other is biometric-based.

Solutions in the book are for IMDs. This reflects both the restrictions and the specific properties of IMDs. However, we feel that it should not be difficult for researchers of other medical devices to find or construct similar solutions of their own. While studying corresponding security defenses, the readers will also learn the methodologies and tools of designing security schemes, modeling, security analysis, and performance evaluation, thus keeping pace with the fast-moving field of wireless security research.

July 2012

Xiali Hei  
Xiaojiang Du



<http://www.springer.com/978-1-4614-7152-3>

Security for Wireless Implantable Medical Devices

Hei, X.; Du, X.

2013, XI, 45 p. 13 illus., Softcover

ISBN: 978-1-4614-7152-3