Chapter 2
Related Work

2.1 Introduction

In the past several years, many research groups have dedicated themselves to security issues of IMDs. For example, Kevin Fu's group at University of Massachusetts Amherst and Fei Hu's group at University of Alabama have been working in this field for several years. There is a new conference called HealthSec Workshop that is held in conjunction with the USENIX Security Symposium. This field has attracted more and more attentions from various people, including recognitions by computer security specialists, patients, medical personnel, medical device manufactures and government regulatory agencies such as the Food and Drug Administration (FDA).

2.2 Related Work on IMD Security

There are a lot of solutions proposed to address the security issues on IMDs during normal (non-emergency) situations. Some literature propose the use of an additional external device, such as an access token [19] or a physical communications cloaking device [20]. However, these external devices may be stolen, lost, or misplaced by the patient. In addition, these devices can disclose the patient's status. Certificate-based approaches [21] require the IMD reader to be able to access the Internet, and in addition a global authority is needed to maintain certificates. The certificate-based approaches have two drawbacks: First, a reader may not always have online access. Second, it is costly to maintain a global certification authority. In [16], the authors propose allowing IMDs to emit an alert signal (sound, vibrations, etc.) when it is engaging an interaction. However, this approach may not work in noisy environments or area with barriers, and may consume excessive battery power. Some papers (e.g., [22, 23] and [24]) propose schemes that deny long distance wireless interactions with an IMD unless the proximity of the IMD is verified. For example, the secure telemetric link solution in [22] proposes the use of a physical backdoor to verify if

X. Hei and X. Du, *Security for Wireless Implantable Medical Devices*,
SpringerBriefs in Computer Science, DOI: 10.1007/978-1-4614-7153-0_2,

the reader is acceptably close to the IMD. Access control based schemes on close-range communication is very intuitive, however, it is not secure against an attacker that uses special equipments (e.g., high-gain antennas), and it cannot prevent the resource depletion attacks. The authors in [24] propose a new IMD access control scheme based on ultrasonic distance bounding. The authors of paper [25] proposes using zero power (harvested RF energy) authentication, zero power notification, and sensible security of patients to protect the IMD. Our paper [11] proposes utilizing patient's IMD access pattern and designs a novel Support Vector Machine (SVM) based scheme to address the RD attacks. With the assistance of the patient's cell phone, the scheme [11] is very effective in non-emergency cases. In addition, we [26] propose utilizing a patient's biometric information to perform authentication during emergency situations. Other literature [27] proposes a wearable device called "the shield," designed to jam any incoming signals to the medical device. It doesn't require any modification to equipment the patient already has, and it is small enough that it can be easily removed for medical procedures. The built-in alarm beeps or vibrates to alert a patient or care giver of an incoming attack. This solution does not require cryptographic mechanisms and is directly applicable to IMDs that are already implanted. Using a USB device (which is used to upload the data to the web-based Carelink system) purchased from eBay, Radcliffe [9] was able to track data transmitted from the computer and control the insulin pump's operations. He found that by intercepting wireless signals sent between the sensor device and the display device on his BG monitors, he could cause them to display inaccurate readings. However, he needs to know the serial number in advance, which can be harvested using existing technology. McAfee's Barnaby Jack could furtively deliver fatal doses to diabetic patients, even the entire reservoir of insulin-300u. With software and a special and custom-built antenna designed by Jack, he can locate and seize control of any device, i.e. instruct the insulin pump to perform all manner of commands within 300 feet, even when he doesn't know the serial number. Also he can just scan for any devices in the vicinity and they will respond with the serial number of the device. Other literature [28] discusses possible attacks on wireless insulin pumps and proposes using a traditional cryptographic approach (rolling code) combined with body-coupled communication to secure device communications. Our group focus on how to detect the malicious increment of insulin dosage, how to build the audit schemes on different IMDs from different manufacturers, and how to decrypt the special communication protocols of IMD system.

2.3 Related Work on Biometrics

Biometric recognition, or biometrics, refers to the automatic identification of a person based on his/her anatomical (e.g., fingerprint, iris) or behavioral (e.g., signature) characteristics or traits [29]. This method of identification offers several advantages over traditional methods involving ID cards (tokens) or PIN numbers (passwords) for various reasons: (i) the person to be identified is required to be physically present at

the point-of-identification; (ii) identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased integration of computers and Internet into our everyday lives, it is necessary to protect sensitive and personal data. Biometric techniques can potentially prevent unauthorized access to ATMs, cellular phones, laptops, and computer networks. Unlike biometric traits, PINs or passwords may be forgotten, and credentials like passports and driver's licenses may be forged, stolen, or lost. As a result, biometric systems are being deployed to enhance security and reduce financial fraud. Various biometric traits are being used for real-time recognition, the most popular being face, iris and fingerprint. However, there are biometric systems that are based on more than one biometric trait such as retinal scan, voice, signature and hand geometry together to attain higher security and to handle failure to enroll situations for some users. Such systems are called multi-modal biometric systems.

The basic idea of biometric cryptosystems [30] is either binding the cryptographic key with biometric templates (i.e., codes) or generating a key directly from the template. Therefore, biometric cryptosystems can be classified into two types: key binding and key generation.

Key binding schemes need additional credentials. Key generation schemes generate some public information to assist in verification. In fingerprint recognition, there is a term named helper data—which is public information about the biometric template, and it is used to deal with the fuzziness of biometric signals during the verification phase. The public information is supposed to reveal no important information about the biometric template while at the same time it is useful in the verification phase. The three most common biometric cryptosystem schemes are: fuzzy commitment [31], fuzzy vault [32] and fuzzy extractor [33].

Fuzzy Commitment Biometric data storage must be used as less as possible, because it is not easy to cancel or revoke them when biometric templates are compromised or stolen. Juels and Wattenberg propose a biometric system in [31]. Their method is called Fuzzy commitment because a cryptographic key is decommitted using biometric data. Here, fuzziness means that a value is sufficiently close to the original to extract the committed value. However, this scheme has some shortcomings because it is based on infeasible assumptions.

Fuzzy Vault Scheme Juels and Sudan propose Fuzzy vault schemes in [32], which can be considered as an extension of the fuzzy commitment schemes. They employ a Reed-Solomon code and evaluate the codeword using a polynomial over a set of points. One practical implementation of the fuzzy vault is in the form of a secure smart-card, as proposed in [34].

In [35], the authors show that hardening the fuzzy vault scheme with a password enhances its security and provides revocability and protection against cross-matching across different biometric systems. There are fuzzy vault implementations based on a user's face [36] and hand-written signature [37]. Moreover, two important schemes based on the key binding model are proposed in (see [33, 38]). The first scheme uses the fuzzy vault scheme to bind a secret with iris images, while the second one proposes a fuzzy extractor, according to the definitions of Dodis et al. [33].

Fuzzy vault schemes have some limitations: (1) If the same biometric data is used to construct different vaults with different polynomials and chaff points, the genuine points can be easily identified by correlating the abscissa values from the fuzzy vaults of different systems. (2) The set of chaff points is bigger than the set of genuine points and an attacker may be able to substitute some points of the chaff-point set. In this way the attacker and the original user can be identified with the same fuzzy vault. (3) The non-uniformity of biometric features makes it possible to identify the genuine set from the set of chaff points by using a statistical analysis. Chang and Li have analyzed this problem in [39].

Fuzzy Extractor Scheme A Fuzzy extractor scheme is a biometric tool whose purpose is to authenticate a user using their own biometric template as a key. It works by extracting a uniformly random string S from a biometric template B in a way that is noise-tolerant. This means that if the biometric template changes to B' but remains close, the string S can still be reproduced exactly. To help the reproduction of S, the first time the fuzzy extractor is used, i.e., in the enrollment phase, it outputs a helper string H that can be made public safely without decreasing the security of S.

The role of each variable is described in the following: S is the encryption or authentication key and H is the public data stored in the database whose function is to recover S. The user's biometric template acts as the key to recover S. The fuzzy extractor process can be considered as a pair of efficient randomized procedures: Generate (Gen) and Reproduce (Rep). The correctness of the whole procedure depends on the differences between B and B'. A basic tool needed in the development of a fuzzy extractor is a secure sketch. It allows the precise reconstruction of a noisy input. On input B a procedure outputs a sketch C. Then, given C and a value B' close to B, it is possible to recover B. The sketch is secure in the sense that it does not reveal much information about B even if C is known. Thus, it is possible to store C.

2.4 Summary

Security on wireless medical devices is a relatively new research field, which is far from being well exploited. Most of the current solutions have many limitations and cannot be widely applied. Therefore, better solutions are needed. This field has also received attentions from many academic scientists and industry specialists, and it is expected to grow in the future.

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