Chapter 11
Cyber Security and Confidentiality Concerns with Implants

Abstract Many lifesaving implantable devices are equipped with wireless technology. This technology enables remote device checks and relieves patients from recurrent consultant visits. But this convenience is associated with unforeseen hazards. These hazards are the security and privacy of data. The labor needed to defend patients from exploits of stealing or nastiness gains more significance. This is especially so with increasing use of wireless telecommunication facilities and the services of global computer network or Internet by implanted devices. The susceptibilities of medical devices are of two types, viz., control or privacy susceptibilities. In control susceptibilities, an unauthorized person acquires control of device operation. The unlicensed person reprograms the device without the patients' knowledge to disable its therapeutic services. In privacy susceptibilities, confidential patient data are disclosed to an unsanctioned party. Both vulnerabilities are detrimental to patient's health outcome. Both are avoidable by incorporating well-thought-out measures in device design.

Keywords Security • Confidentiality • Privacy • Encryption • Cryptography • Jamming • Hijacking • Insulin pump • ICD • Biosensor • Shield

11.1 Introduction

Security is freedom from risk or danger from adversaries. Security should be clearly differentiated from safety, a somewhat similar term that is often confused with security. Safety is concerned with design errors or system failures. Security of data means that its storage and transference are protected. Cyber security or information technology security is the organization of preventive know-hows, procedures, and rehearses. This body is devised for protecting computers, nettings, software packages, and information from unapproved access, change, or destruction. Cyber security of a system along with its reliability constitutes its trustworthiness.

Confidentiality or privacy is freedom from observation, disturbance, and interference by others. Confidentiality of data implies its accessibility by and availability to authorized personnel only. They may access it either for viewing or using the same.

V.K. Khanna, *Implantable Medical Electronics*,
DOI 10.1007/978-3-319-25448-7_11

11.2 Apprehensions of Patients Receiving Implants

Apprehensions of defiance of cyber security and confidentiality are not unreasonable. These anxieties arise because many implantable electronic devices contain computing and communication modules. Wireless and Internet connectivity is an intrinsic feature of these devices (Fig. 11.1). As we are aware, the malicious incidents of invasion of computers by viruses are frequently heard. Hacking of accounts or theft of laptops is common too. Therefore, it is plausible that any unauthorized person can take liberty to gain control of an implant. The evil person can go the extent of crippling its functioning. Exposure of a patient's vital data may also tempt a person with mala fide

Fig. 11.1 Wireless body area network

intensions to deliberately make changes in data that are harmful to the patient. By hacking, a person may operate the drug delivery pump of a patient to administer lethal doses of drugs. A wicked person may gain control over a defibrillator and impart an unnecessary high-voltage electric shock to the patient's heart. Therefore, such trepidations in the minds of patients and doctors need to be dispelled. They can only be allayed by building defensive mechanisms to thwart threats. Additional impregnable features have to be introduced into the systems to make them secure and private.

11.3 Security Requirements

Medical implants should ensure continued, reliable service through secure communication and functionality. Following are the main requirements that need to be fulfilled [1]:

1. Device-existence privacy: No one except the authorized personnel should be able to detect that a patient has an implanted device.
2. Device-type privacy: If someone knows that a patient has an implanted device, the type of device should not be disclosed.
3. Specific device ID privacy: No unauthorized person should be able to track any individual device.
4. Data integrity: Access to the private details of a patient such as name, diagnostic/therapeutic parameters, and other stored data should be invincible to unauthorized people.

Security requirements vary from device to device. In devices like cochlear implants, malfunctioning poses less risks to human life. So, they are deemed to be less life-threatening. Hence, user identification and data validation may be adequate. But for devices such as pacemakers and insulin pumps, any security contravention may endanger the life of the patient. So, elaborate security features must be built into the device. Rigorous testing and verification of these features must be done prior to marketing to avoid any remote chances of security violation.

11.4 Causes of Security Breaches

Probable reasons are either deliberate or unintentional [2].

11.4.1 Deliberate Breaches

Causes could be jealousy against competitors, e.g., for damaging the reputation of a firm; seeking financial advantages by accessing private data; sabotage by a dissatisfied employee or customer; and a terrorist attack.

11.4.2 Unintentional Breaches

Causes include inadvertent collateral damage spawned by a virus, worm, or other malicious software. The software might have been designed to disrupt other computers but invaded the medical network also. This may occur during updating software of medical devices through the Internet. Although updating is aimed at improving the device functionality, it also provides a portal for software contamination.

11.5 Types of Adversaries

An adversary is an opponent, enemy, competitor, or combatant. Adversaries are characterized in accordance with their objectives, capabilities, and resources at their hands (Table 11.1). Security designers assess the different threats in terms of definite criteria. The criteria laid out include their values and the efforts applied by adversaries to gain access to the implanted device.

Secret, purposeful real-time interception of a phone call, videoconference, or other private messages, and listening to their conversation without consent fall under eavesdropping. A passive eavesdropper can capture data but does not disturb or modify it. An active adversary is one endowed with augmented capabilities to compromise with the data. This adversary indulges in erroneous controlling actions. An oscilloscope, software radio, directional antenna, etc., may be used in these actions [3]. Such an adversary may produce RF traffic for blocking signals. By such blocking, the signals are prevented from performing their assigned tasks. Blocking of wireless communication called jamming may be continuous. Continuous jamming is characterized by a nonstop signal of a fixed power. Jamming may be periodic. Periodic jamming is marked by pulsating action to damage a packet if hit. Jamming can also be reactive. In reactive jamming, the decisions are based on the present and past channel states. Another damaging capability involves binary analysis. This analysis is done for disassembling the software of the device. The intention is to know its operation. Then the same knowledge is used with malevolence. An adversary possessing an external device constructed for use with the implant could undesirably use the device for wicked intents, e.g., for disabling therapies [1].

Table 11.1 Passive and active adversaries

Sl. No.	Passive adversary	Active adversary
1.	One with limited facilities who violates privacy of data without any interference. This could be a person listening to radio communication from an implanted device	One with advanced resources. This person is not only capable of receiving the radio signals from an implanted device but also able to modify the operation of the device in an unfriendly manner.
2.	Less dangerous	More dangerous because this adversary can acquire control of the device. He/she can guide it to erroneous life-threatening therapies

11.6 Design Principles for Implant Security

Designers should keep security in mind from the very beginning [4]. The ideas of security in computers and computer networks do not represent a new field. The already proven concepts have to be applied to implants according to the particular application. If security is imbibed after the system has been built, unexpected failure forms may be encountered. Thus security is a preplan rather than an addendum. Security is an essential or integral component of both the product and the manufacturing company. The organization and the management should enforce procedures to prevent leakage of vital information that may lead to flaws. One tactic that assists in tackling the confrontation of the implant designers with dreadful intentions goes by the name of "the principle of defense in depth." This principle recommends multiple tiers or layers to toughen security. The chosen measures embody the broad field covering from corporal security and admission controllers to security of the network.

If the system design is simple, it can be readily understood. Therefore, different likely routes to be adopted by the adversaries can be preconceived. Such a preconception enables provision of suitable mechanisms to ward off the dangers. A difficult design may make it too complex for the designer to foresee the weak links.

A source code is the initial program written in a programming language. It is readable by humans. It is later translated into a machine language. This translation gives it a form called the machine code with binary 1s and 0s for execution by the computer. Therefore, designers of implants should use standard source codes. These standard source codes have proved their worth over time. New untested codes need not be followed. Further, designers should not rest assured that the source code is too difficult to understand. They should always remember that it can be deciphered by someone to create nuisance.

Any information that is to be kept under the veil of secrecy is classified as sensitive data. It should be disclosed only to commissioned parties. Cryptography deals with techniques of information hiding and verification. It aims at protecting communication from adversaries. One form of cryptography is called encryption. It converts the given data known as *plaintext* into a form termed *ciphertext*. It does so, for example, through substitution of numbers by letters using an algorithm. In cryptography, a cipher is an algorithm for encryption or decryption. Only legitimate persons are able to read the encrypted data. For reading the data, a secret key is given. This key is actually an algorithm that unwraps or undoes the encryption. For safeguarding against threats, cryptographic building blocks are combined to construct a cryptosystem.

Encryption is the transformation of data from its original native format called the plain text format into a format known as the cipher text format. This format is not easily comprehensible to people that do not have official clearance or approval to do so. Decryption is the reverse process. It involves reverting encrypted data back into its original native format. This enables it to be unreservedly understood by common people.

Designers should use regular cryptographic building blocks in place of impromptu designs. Customary ciphers and security protocols must be used. But cryptographic keys must be carefully protected. The vast expertise of the cryptographic community is gainfully utilized by taking recourse to cryptosystems that have undergone scrutiny by professionals. Cryptographic specialists with years of experience must be employed. Building homemade encryption or key management systems is disastrous. Moreover, use of algorithms that have been broken long ago is precarious. Encryption technology leveraging new algorithms should be utilized.

A perilous practice of database encryption relates to the storage of the key used for encrypting the data or the authentication credential. In this practice, the key is stored in the same database along with the encrypted data. Such key storage should never be done. Indeed, the management of encryption key must be kept unconnected with the database that was used for storing the data encrypted with that key. Encryption keys are better protected by the hardware. Then the encryption key does not at any time quit the device. Hence, unlawful personnel or data thieves are neither able to retrieve the key nor the cryptographic functions and operations in which the keys are used. To reiterate, encryption places a high burden on a network and its users. However, data encryption is not difficult. But allowance of access to protected files for ratified users while keeping unwanted people away is complicated.

Similar to the security practices followed for one's own devices, any devices from third parties must also prove their capability of safeguarding before acceptance. Any encryption claims must be validated prior to use.

Threat modeling is concerned with studies of the different kinds of possible threats to security and their behavioral pattern to build suitable threat models. These models can be used to devise countermeasures for the expected menace.

Prima facie policy planning appears to fall outside the domain of device designers. But the long series of changes in the life of a device developing into a product and preventive regulatory surroundings have made policy a design-time issue. Implanted devices are pushed into market after undergoing validation tests. Supposing that new security threats are discovered after launch of a product, it becomes the responsibility of manufacturers to plan for any changes such as software updates. These changes are normally done in a clinical environment. Permitting updating in an unrestricted or poorly verified setting may cause security problems. During policy formulation, the regulatory environment under which the devices are placed in their market lifetimes must also be considered. Fresh clearance is required for significant updates to devices that are already in the market. Thus, it is essential that the designers should tackle with foresight the likely future threats. They should solve such problems at the design time itself. As threat modeling helps to plan for future complications, designers can advocate for security statements and policies at the company level. These considerations imply that policy planning must be kept in view at the design stage of a product. The above ideas are presented in a concise form in Table 11.2

Table 11.2 Extension of fundamental security ideas to implantable devices

Sl. No.	Idea	Explanation
1.	Integration of security from creation	Security should be built in the system during its construction. It should not be stuffed after the system is completed
2.	Simplicity of security designs	Simple security systems are easy to understand. Then the possibilities of attacks can be argued. Necessary retaliatory methods are suggested and readily put into effect
3.	Adoption of industry-standard source code techniques	Designers must refrain from using nonstandard source codes. This self-enforced restraint is necessary because their ruggedness is not guaranteed
4.	Non-reliance on obscurity	Obscurity is not an assurance for security. It should always be presumed that someone may break open the source code and cause havoc
5.	Encryption of sensitive data	Encryption is an unsurpassed method to avert the appalling inconveniencies with stolen data. If the data is encrypted, nothing useful is taken even if experienced hackers penetrate a system. To bestow the uppermost ranks of security, encryption should be invariably supplemented with proper management of the key
6.	Use of standard cryptographic building blocks	Carefully deliberated and established building blocks must only be used. New technology-based algorithms must be applied, wherever applicable. Old algorithms that are already broken must be avoided
7.	Authentication of third-party devices	Third-party device vendors must prove their cryptographic claims
8.	Modeling of threats	Threats should be prioritized. The most appealing targets for attackers must be identified and defended against. This must be followed by less frail targets

11.7 Expository Examples of Security Breach Possibilities

Several researchers have conducted mock drills of penetrating through the security of commercial implantable devices. Some interesting examples of such studies are presented here.

11.7.1 Hijacking an Open-Loop Procedure: The Insulin Infusion Pump

The insulin pump arrangement is an open-loop procedure. In this system, a patient varies the pump settings, as per requirement. The system has both implanted and external components. A subcutaneous glucose sensor is used for measuring the instantaneous glucose concentration in the blood. The measured concentration is wirelessly transmitted to the external control. Based on this measurement, a wirelessly coupled insulin infusion pump subcutaneously delivers insulin to the patient. This pump

works under the supervisory control of the patient. The patient reads the display on a wireless remote control for necessary information. Then he/she alters the pump settings through this remote control. It is this remote control interface carrying the patient glucose level and control information that is open to security threats.

Demonstration of security infringement was done by Li et al. [5, 6] on the wireless communication link of a commercially available blood glucose measurement and delivery system. To launch the attack, the frequency of the radio link was found online in the public domain from Federal Communications Commission (FCC) as 915 MHz. By intercepting the radio signal, the modulation scheme was decided as on/off keying. For data reception by the insulin pump, a code of 6 digits in hexadecimal code must be entered by the user. These digits constituting the personal identification number of the device were stamped on the backside of the glucose meter or its remote control accessory. The data packets between the remote control and the glucose meter were intercepted. After synchronizing the sequence of binary zeroes and ones, it was ascertained that the communication packet contained 80 information bits whose roles are explained below: the first 4 bits, device type; next 36 bits, device PIN; next 12 bits, information bits; next 12 bits, counter bits, repeating after 256 reckons; succeeding 12 bits, random cyclic redundancy check (CRC) bits; and final 4 bits, 0101. The counter was found to be an 8-bit counter. The device PIN was found to be transmitted without encryption. After conducting several trials, the CRC parameters were determined. Regarding replay attacks, the defense methodology was that the system did not accept any packet if the counter had the same value as the preceding packet. Hence, two packets are intercepted and transmitted in an alternating fashion for acceptance by the system. After discovering the packet format and CRC parameters, it was possible to design a valid packet. This designed packet will be acceptable to the insulin pump. It will enable full control of the operation of the pump to fall in the illegitimate hands of the attacker.

Both passive and active mode attacks were brought into the realms of possibility. One could imitate and pose as an empowered user to fool around with the device controls. For carrying out these manipulations, one could use easily available tools such as Universal Software Radio Peripheral (USRP). The USRP provides an inexpensive hardware platform for software radio. It enables the users worldwide to undertake wide-ranging applications in research, academics, and industry. Without knowing the device PIN, it was possible to successfully launch three types of attacks:

1. System privacy attacks: Eavesdropping on the communication channel could be done. The attacker can decode information about the device type, its PIN, and medical status of the patient.
2. System integrity attacks: In a replay attack, the attacker acquires the control of the pump by alternative transmission of two succeeding packets. The attacker can report an erroneous glucose reading to it. This reading would cause operation of the system in a malfunctioned manner.
3. System availability attacks: The attacker jams the communication channel. Then the attacker makes certain that either remote control ceases to work or no data is transmitted.

By knowing the device PIN, the following kinds of attacks could be launched: (1) stoppage of insulin infusion inside the body, in which the blood glucose level of the patient is elevated; (2) restart of a stopped pump, in which the pump would push insulin into the patient's body; or (3) release of an indiscriminate dose of insulin into the body. Thus misconfiguring of the pump could be done leading to erratic behavior. Such incorrect response through wireless forgery can cause heavy insulin pumping during hyperglycemia. It may cause insulin stoppage during hypoglycemia. These disturbances could result in a serious risk to patient's life.

In this open-loop system, the user is a part of the loop. The threats target the user. Such a system comes under the subfield of usable security. It aims at building a secure user interface design. Users must be given unambiguous indications regarding the status of the device. They must be provided with tools to take informed security decisions. They must also be educated about the potential security risks to the devices which they are using.

Two solutions were also proposed for countering the attacks: (1) Rolling code technique: In this technique, the same PIN is not sent always. In lieu of the same PIN being sent, a rolling code encoder is firmly rooted in the remote control. Another encoder is embedded in the insulin pump. Such an arrangement is more difficult to break. An encryption key is shared between the rolling code and the remote control. The data sent are encrypted. Also, the rolling code keeps changing every time. Hence, PIN extraction is a hard nut to crack. (2) Body-coupled communication: Here, there is no communication through the air medium. Instead, communication takes place through the patient's body. Thus, the communication is effected in the restricted region nearby the patient's body. Therefore, there is less likelihood of eavesdropping. Persons in close vicinity of the patient can, however, do this, but they may get caught. A bonus advantage is the lower power consumption by the communication system. The power consumption is low because the system works over a shorter range.

11.7.2 Security Analysis of a Closed-Loop System: The Implantable Cardioverter Defibrillator

The ICD extends the capabilities of a pacemaker by delivering a large shock to the patient to arrest an unsustainable heart rhythm. Unlike the insulin pump, the ICD is a closed-loop system. In this system, the sensing of an abnormal rhythm prompts the actuation. Using simple software and radio tools, researchers could record the communicative messages between the ICD and a programming console used in clinics [3, 7]. Patient data was revealed easily. It was found that the signals were not coded in any way against undesired access. There was no evidence of encryption. Replaying the translated commands, it was possible to control or immobilize the ICD action. A sequence of radio transmissions were found to keep the ICD in highly active mode. The packets were transmitted regularly for an indefinite period. Enormous power was thus drained out. By employing this type of gimmick, it is possible to prematurely exhaust the battery of an implanted device.

In contrast to open-loop systems where the user interface is the weakest link in the chain, in the closed-loop system, the biggest challenge is the automated decision-making. To avoid security violations, some manufacturers allocate secret keys to their devices before deploying them. If any such pre-distributed key becomes compromised during deployment, every device with that key must be updated. A viable option is to let customers generate their own keys before using the devices. The issue of key compromising is done away with. But a way to install the key on a device without user interface must be found. Halperin et al. [7] put forward a credible method employing transcutaneous acoustic coupling to exchange the key material. Audio alerts or beep warnings are used for communication with a system without a user interface.

RF interface is not the only unsafe zone. Analog sensors responsive to electromagnetic interference (EMI) serve as unrestrained admission points into an otherwise guarded system. These sensors allow an attacker to influence sensor readings. The amended sensed data appears directly at the application layer of the device. It thus dodges usual security apparatuses and gives the assailant some chances of governing the system. Foo Kune et al. [8] showed that in open air, preconceived, conscious electromagnetic interference under 10 W could hold back pacing. It could provoke shocks for defibrillation at interspaces up to 1–2 m on ICDs. Then the sensing leads along with the medical devices were submerged in a brackish bath for closer approximation to conditions inside the human body. In this case, the distance for the similar trial lessened to <5 cm. Sometimes the attacker cannot match the wavelength of the EMI signal with the length of the sensing leads. Nevertheless, an increase in power of EMI transmission can induce signals in millivolt range at the sensing leads of the implantable device. Therefore, sensed time-dependent voltages are prone to contamination by analog signal injection through EMI. Moreover, sensing in ICDs is done in the subkilohertz band. Due to this reason, filters in this frequency range cannot be used. In addition, coaxial design is prevented by mechanical constraints on the sensing leads. These issues make EMI more embarrassing to the implanted device. To combat the EMI, a suggested defense strategy is to detect the spurious sensor input. This detection is done by checking its consistency with the refractory period of the heart tissue.

11.7.3 Security and Privacy of Implantable Biosensors Used for Data Acquisition

Biosensors span a broad category of signals and techniques for processing signals. They cover a range of data rates, from the low-data-rate glucose sensors to the high-data-rate optical imaging devices [3]. These biosensors can detect biomarkers for various diseases. They can also measure pH, temperature, and other parameters. They communicate wirelessly through the tissue to supply the information to the external monitoring systems. Many of these sensors are also powered wirelessly. The security concerns associated with these sensors are different from those discussed above. The data acquired by these sensors are used for actuating therapeutic

devices or drug delivery systems. Therefore, confidentiality of these data must be strictly guarded to avoid their unethical use.

The main concern with implanted biosensors is that their wireless transmissions are small in information content and take place at less frequent intervals as opposed to the continuous transmissions of other devices. These small, infrequent transmissions are more difficult to protect. A sensor might require a few minutes to accomplish its assignment. After completion of task, it delivers only few bytes of data. Cautious usage of cipher is essential in case the plaintext data from the sensor acquire only a small number of dissimilar denominations. There is only a little intrinsic redundancy in the small quantity of data. So, error correction must be done.

Sometimes, small biosensors are injected into a patient (Fig. 11.2). They are powered inductively through a bandage-like external patch on the skin to relay the sensed data outside. When a biosensor is paired with a patch, different risks arise. In view of the short transmission range around a few millimeters for a subcutaneous biosensor, eavesdropping may be difficult. However, a fraud through caricature of either the clinical reader or patch is a likely possibility. If a patient is unconscious, the patch can sometimes be easily detached and swapped with a fraud one. Likewise, a deceitful sensor can feed wrong information to a dependable patch. Proper cryptographic mechanisms should make sure that all the components involved in the treatment are well authenticated.

Implanted biosensors with stringent space and energy restrictions pose special difficulties in protecting against security and privacy attacks. The imposed restrictions make routine encryptions unusable. New cryptosystems for energy-constrained implanted devices offer a ray of hope. Notwithstanding, the available algorithms for these devices are very few as opposed to general-purpose solutions, which are of little help.

Table 11.3 gives a comparative depiction of the security precariousness of open- and closed-loop and implanted biosensor systems and the obliteration of the Achilles' heels.

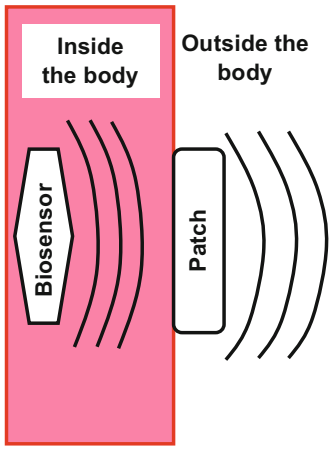

Fig. 11.2 Biosensor injected into a patient and powered via inductive coupling by a patch, which sends the received data to a physician

Table 11.3 Security challenges posed by different systems

Sl. No.	Feature	Type of system		
		Open-loop systems	Closed-loop systems	Implanted biosensor systems
1.	Example	Insulin pump	Implanted cardioverter defibrillator	Subcutaneous glucose sensor
2.	Risky situations	User interface	RF interface violation and EMI contamination	Impersonation and fraudulent practices
3.	Suggested remedies	Rolling codes, body-coupled communication	Secret keys, detection of fake sensor input	Cryptography

11.8 Conflict of Security with Safety, Efficiency, and Usability

There is an obvious antagonism between patient security and safety [Li]. Tighter and stricter security norms may sometimes hinder the provision of required medical attendance to the patient. This may be especially so in emergency situations when the patient is incapacitated and needs urgent attention. Then if the doctor is unable to adjust the device parameters, valuable time is lost. Clearly, authentication mechanisms should be context-aware and flexible. The reason is that during an emergency when a patient is unconscious, he/she cannot cooperate with the doctor to provide password for the device.

Cryptographic solutions must be as undemanding and frivolous as conceivable, in terms of both calculation time and storage requirements. Otherwise, the power and storage space will be drained quickly. Thus, there is a rivalry between security and efficiency.

Usability becomes difficult as security increases. Operation by omitting some manual steps simplifies usage but weakens the security. Long-distance usage over wireless enhances usability by monitoring the patients at home, instead of the clinic. At the same time, there is increased risk of meddling by eavesdroppers.

11.9 Negative Aspects of Security Scheme

The need of authentication of the user to start the operation of a device strengthens its security. But let us imagine an emergency situation when the patient is unconscious. The attending doctor may not be able to reprogram the device according to patient's condition. In such cases, the built-in authentication or encryption

Table 11.4 Incompatible scenario

Sl. No.	Situation	Security	Usability
1.	Medical emergency	Requires the proper certification of the user for altering its functionality to provide the required emergency treatment	Authentication process may render it impossible to provide treatment if the patient is unconscious. Treatment cannot be given in the absence of a programming device with the shared secret
2.	Energy drainage	Heavy-weight encryption unduly loads the power supply. It exhausts the battery prematurely and necessitates battery replacement	Energy consumption by the encryption must not overburden the normal availability of the device for the intended use
3.	Cost	Costly encryption may make the large-scale deployment of subcutaneous biosensors prohibitively impractical	Encryption costs must be a proportionately reasonable fraction of the price of implantable device

algorithms act as a hindrance to the doctor in providing immediate medical care. Hence, the patient may be denied the valuable service required in a critical situation.

Elaborate encryption schemes unduly load the power source. A lot of power is drained. The implant should primarily prove its worth in medical treatment. Therefore, heavy-duty encryption schemes may be a boon to security. But they may act as a burden on the battery causing it to run out fast. This calls for a balancing of cyber security and confidentiality with safety and utility of the device [7]. Safety means that the implant should be more beneficial than harmful. Utility implies its usefulness to patients and doctors. Please see Table 11.4 for a side-by-side delineation of security and usability.

11.10 Protection Without Device Modification

Several patients have already received implants. If any security measures are to be adopted, the question arises how they will be incorporated in devices which are already implanted in patients. It is not easy to surgically remove and recall such devices. Therefore, an alternative approach is logical. In this scheme, the responsibility of protection is assigned to a personal base station. This base station will serve as a jammer of implant messages for others, thus preventing their decoding efforts [9]. But for the genuine users, this jamming action is ineffective. Thus it is a jammer-cum-receiver. The base station is a shield against illegitimate users (Fig. 11.3).

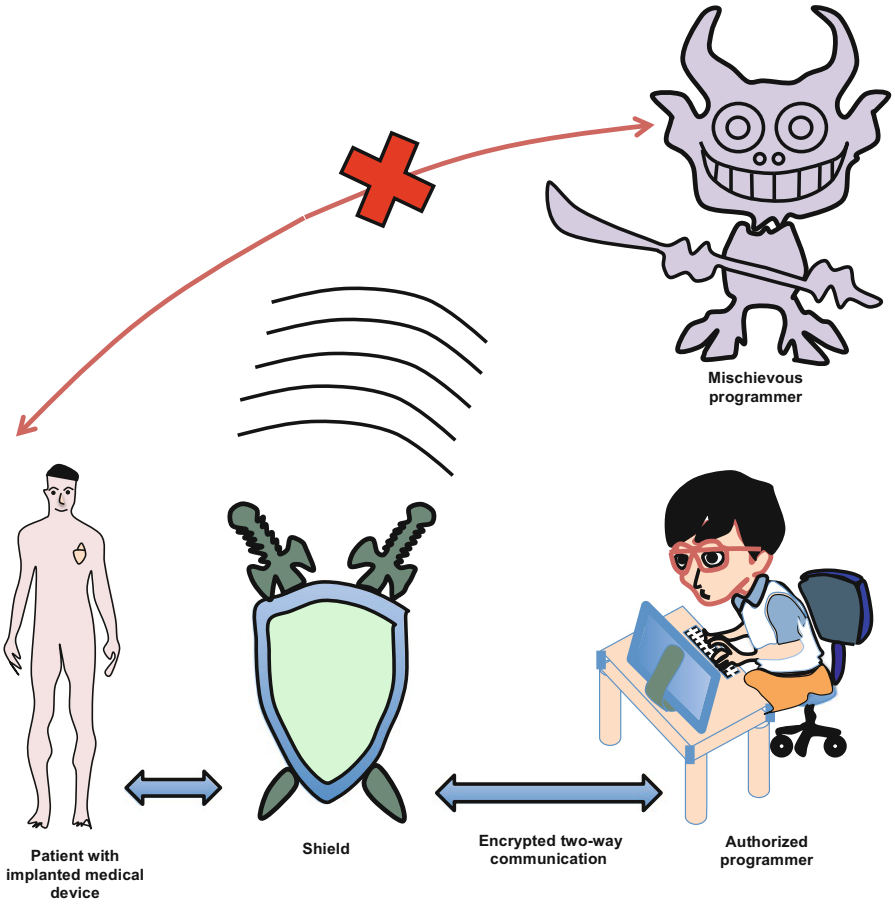

Fig. 11.3 Protection of a medical implant without modification by inserting a shield, which paralyses any straight interfacing or interaction with the implant, whereas a ratified person is able to establish a secure channel with the implant through the shield

11.11 Discussion and Conclusions

Ubiquitous health monitoring (UHM) through wireless body area networks (WBANs) provides e-healthcare for in-home monitoring and diagnosis. It frees the patients from frequently visiting hospitals [10]. It is more important in countries with shortage of medical infrastructure. Its relevance increases especially during natural disasters and calamities, when several precious human lives can be saved.

Many available devices have shown weakness and defenselessness against attacks. Security and privacy protection of patient information mandates the deployment of various techniques. They are essential both during transmission and storage in the network. They are applied carefully in accordance with the degree of risk

resulting from the data tampering to the patient for the particular medical implant. In addition, the associated power constraints must be considered.

Cryptography is not a cure for all security risks. Many questions still remain unsolved. Some of these unresolved questions are: If an implantable device uses encryption of data, how is the necessary key distributed? Who should distribute the key? How does an implantable device distinguish between external agents that are allowed to communicate with it benignly and those that may interact wickedly? Since security of some implantable devices needs to be disabled for emergency healthcare, how to protect these devices under nonemergency circumstances? Should a device raise hue and cry as an audible alarm during an attack?

Review Exercises

11.1 What is the difference between security and safety? Define cyber security. What does privacy of data mean?

11.2 "A logical fear irks the minds of patients that cyber security and confidentiality of implantable medical devices can be contravened." Do you agree with this statement? If yes, please explain why?

11.3 State the four principal security requirements that must be fulfilled for implantable medical devices. Do cochlear implants and cardiac pacemakers present the same security risk?

11.4 How do you classify the causes of security breaches? Give examples of each class.

11.5 What is an adversary? Into how many groups will you place the different adversaries for implantable devices? Which type of adversary is most dangerous?

11.6 It is said that the planning for security of implantable device should commence from the very beginning. Give your arguments in support of this assertion.

11.7 Why should the security system be simple? How does it help you?

11.8 What is a source code? Why may happen if the designers of implantable devices use nonstandard source codes?

11.9 What is cryptography? What do you understand by encryption and decryption of data? Explain the terms: "plain text" and "cipher text".

11.10 Why is it said that building homemade encryption can cause havoc? Give reasons.

11.11 Why should the encryption key be stored in a different database than the one used for storing the encrypted data?

11.12 What is threat modeling? How does it help in providing security to implantable devices?

(continued)

(continued)

11.13 Why is policy planning considered to be a job of the implantable device designer? Give arguments justifying your answer.

11.14 Explain the working of an insulin pump system for diabetes relief. How was a passive attack on this system demonstrated? How was it possible to launch an active attack on this system?

11.15 What is the most attractive target for the attacker in an open-loop system? What is usable security?

11.16 What is rolling code technique for security of a device? What makes the PIN difficult to crack when the rolling code is used?

11.17 What is meant by body-coupled communication? How does it help in protecting against eavesdropping?

11.18 How was the possibility of security violation of an ICD demonstrated? How can an attacker deplete the battery of an ICD very fast, inflicting suffering on the ICD patient?

11.19 What is the weakest link in the closed-loop system? How does distribution of secret keys prevent security breaches in a closed-loop system? Highlight some problems associated with the keys.

11.20 What kind of attacks can be done through intentional EMI? How can EMI disturb the operation of an ICD? Suggest a suitable remedy to counteract the EMI menace.

11.21 Bring out the main worries of implantable device designers regarding the security of implanted biosensors. Emphasize the differences between these security concerns with those normally faced with implantable devices. Suggest the necessary remedial steps.

11.22 Explain by giving examples on how the severity of security measures falls in the way of providing efficient treatment to the patients and hence conclude that a balance needs to be struck between the security and utilization of implantable devices.

11.23 A large number of patients today are getting benefitted by different types of devices implanted in their bodies. If therefore a new security scheme is launched, it may not be applicable to these patients. How can such patients be protected against security threats? Suggest a scheme applicable to such patients.

References

1. Daniluk K, Niewiadomska-Szynkiewicz E (2012) Energy efficient security in implantable medical devices. In: Proceedings of the federated conference on computer science and information systems, 9–12 Sep, Wroclaw, pp 773–778
2. Maisel WH, Kohno T (2010) Improving the security and privacy of implantable medical devices. N Engl J Med 362(13):1164–1166

3. Burleson W, Clark SS, Ransford B (2012) Design challenges for secure implantable medical devices. In: 49th ACM/EDAC/IEEE Design automation conference (DAC), 3–7 June, San Francisco, CA, pp 12–17
4. Ransford R, Clark SS, Foo Kune D et al (2014) Chapter 7: Design challenges for secure implantable medical devices. In: Burleson W, Carrara S (eds) Security and privacy for implantable medical devices. Springer Science + Business Media, New York, pp 157–173
5. Li C, Raghunathan A, Jha NK (2011) Hijacking an insulin pump: security attacks and defenses for a diabetes therapy system. In: 13th International conference on e-health networking, applications and services. Columbia, MO 13–15 June, pp 150–156
6. Li C, Zhang M, Raghunathan A et al (2014) Chapter 8: Attacking and defending a diabetes therapy system. In: Burleson W, Carrara S (eds) Security and privacy for implantable medical devices. Springer Science + Business Media, New York, pp 175–193
7. Halperin D, Kohno T, Heydt-Benjamin TS et al (2008) Security and privacy for implantable medical devices. Pervas Comput 7(1):30–39
8. Foo Kune D, Backes J, Clarke SS et al (2013) Ghost talk: mitigating EMI signal rejection attacks against analog sensors. In: Proceedings of the 34th IEEE annual symposium on security and privacy, Berkley, CA, 19–22 May, pp 145–159. doi:10.1109/SP.2013.20
9. Gollakota S, Hassanieh H, Ransford B et al. (2011) They can hear your heartbeats: non-invasive security for implantable medical devices. In: SIGCOMM'11, August 15–19, Toronto, 12 p
10. Li M, Lou W, Ren K (2010) Wireless data security and privacy in wireless body area networks. IEEE Wireless Comm Mag 17(1):51–58