Wayne Burleson · Sandro Carrara
Editors

Security and Privacy for Implantable Medical Devices

Springer

Security and Privacy for Implantable Medical Devices

Wayne Burleson • Sandro Carrara
Editors

Security and Privacy for Implantable Medical Devices

Springer

Editors
Wayne Burleson
Department of Electrical and Computer Engineering
University of Massachusetts
Amherst, MA, USA

Sandro Carrara
École Polytechnique Fédérale de Lausanne
Lausanne, Switzerland

ISBN 978-1-4614-1673-9 ISBN 978-1-4614-1674-6 (eBook)
DOI 10.1007/978-1-4614-1674-6
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2013948851

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Contents

Chapter 1
Introduction

Wayne Burleson and Sandro Carrara

Implantable medical devices (IMDs) have advanced considerably in the last few decades, promising unprecedented access to the human body to gather personal health data anywhere and any time. Widely deployed devices such as pacemakers and insulin pumps already provide enormous health benefits. Cochlear and ocular implants use advanced microelectronics and novel powering schemes for vastly improved hearing and vision. Biosensors address disease by drug and biomarker detection with myriad applications, ranging from cancer therapies and infectious disease detection to genome analysis, promising to improve health, increase safety, and reduce the cost of diagnostics.

However, the security and privacy of these devices and their data have still not been adequately addressed. The low cost and lightweight nature of the devices makes implementation of standard information security and cryptography challenging and motivates novel approaches that are customized to constraints and threat models. Wireless interfaces are perhaps the most obvious vulnerability; however, device counterfeiting and data fraud are also realistic threats. The most disturbing concerns arise in systems where drug (e.g., insulin pumps) or electric therapies (e.g., pacemakers) can be maliciously modified to deliver lethal results. But the security and privacy of personal health data and genomics information motivate discussions about data ownership and fundamental human privacy rights.

Most recently, the development of new biosensors has allowed blood tests to be performed in the body that previously required blood sampling, incurring costs, compromising safety, and causing inconvenience for patient and physician. Furthermore, the fact that lab tests can be performed anywhere and any time allows

W. Burleson (✉)
Department of Electrical and Computer Engineering, University of Massachusetts,
309C Knowles Engineering Building, Amherst 01003, USA
e-mail: Burleson@ecs.umass.edu

S. Carrara
École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland
e-mail: Sandro.Carrara@epfl.ch

W. Burleson and S. Carrara (eds.), *Security and Privacy for Implantable Medical Devices*,
DOI 10.1007/978-1-4614-1674-6_1,

unprecedented exposure of the body and personal health information. Personalized health solutions can be used to tackle difficult problems in cancer and other therapies. Responses to drugs and drug interactions can be monitored on a much finer-grained level than before.

However, the increased reliance on these technologies, especially in the case of potentially life-saving therapies, can introduce difficult tradeoffs in reliability and security. Personal health information that was once restricted to the confines of a medical laboratory and physician could now potentially be accessible to various unauthorized parties.

Wireless Access to Implantable Devices: A Double-Edged Sword

Wireless connectivity at various scales provides numerous benefits with respect to implantable medical devices (IMDs). The ability to communicate with an implanted device allows data to be transferred both up and down as well as download of control information and software updates. Fortunately, most data transfer rates from IMDs are quite slow and the out-of-body radio can be located quite close, removing many concerns about power levels and eavesdropping. Recent examples where the external radio is on a bandage [1] just millimeters from a subcutaneous implant [2] pose issues that are relatively easy to solve in terms of wireless communication system design by drawing upon recent techniques in radio-frequency identification (RFID), (NFC), and inductive coupling. More challenging are deeply implanted devices that must cross significant amounts of human tissue before leaving the body. Examples include deep brain implants, deep heart implants, and fetal monitors [3].

If the external radio is on the body (Fig. 1.1), this can either tie into or form the basis of a body area network (BAN). BANs have been proposed for a wide range of applications, and a good survey on them can be found in [4]. The IEEE recently announced a new standard for BANs (the IEEE 802.15.6) that emphasizes ultra-low-power devices.

Wireless connectivity also provides capabilities for directly updating electronic health records (EHRs) [5]. One of the main concerns about EHRs has been the cost and accuracy of manual data entry [6]. By directly entering data from implantable devices, some of these concerns may be reduced. In addition, wireless capabilities facilitate the concept of a personal health record (PHR) or portfolio (PHP) [7], which extends the EHR to a record that is under the control of the patient. This addresses many concerns about individual civil liberties and privacy rights.

If the external radio is not on the body, the wireless communication problem is significantly more challenging and additional vulnerabilities arise. However, this scenario is quite attractive because it avoids the inconvenience of the patients having to wear a device, possibly losing the device, and keeping it powered. Instead, a wall-powered base station, similar to a Wi-Fi router, can be used to communicate

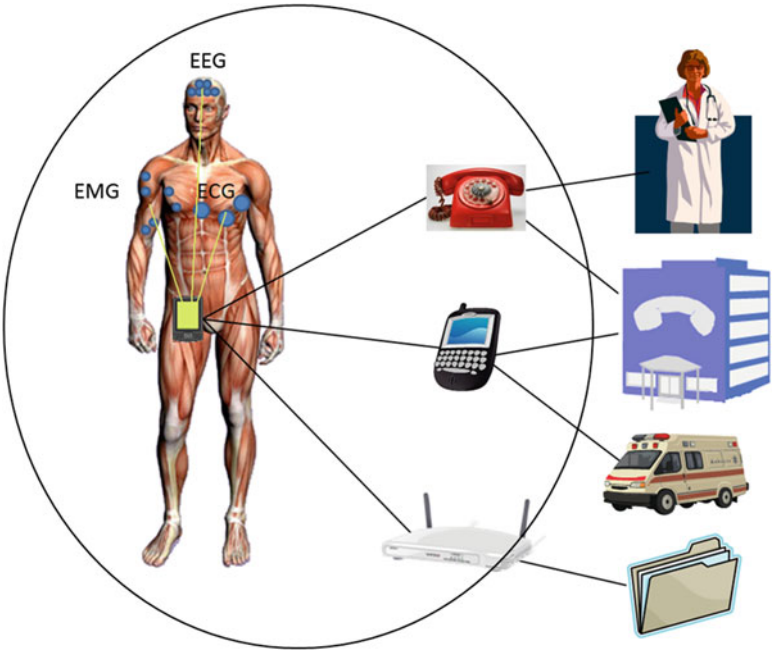

Fig. 1.1 A body area network (BAN) connects various sensors to a wearable router/hub that communicates wirelessly with other networks for medical, emergency, and record-keeping purposes (Courtesy of CSEM/Switzerland)

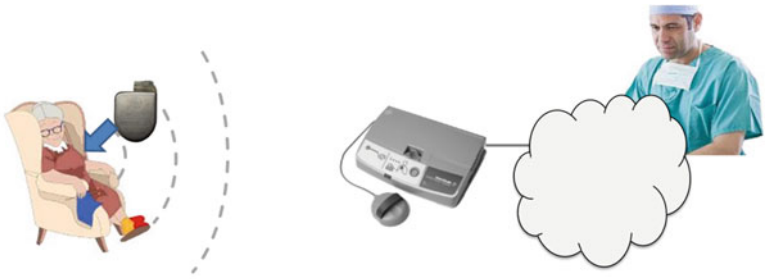

Fig. 1.2 Remote access to implantable pacemaker and cardiac monitor (Courtesy of Golkatta (MIT))

with the implanted device and then directly tie into the cellular or fixed network and then to the Internet (Fig. 1.2). A recent US study suggests that physician access to medical devices through remote monitoring can offer a reduction in hospital visits by 40 % and cost per visit by US$1,800 [8].

Wireless powering is another advantage of wireless access to subcutaneous IMDs (Fig. 1.3). Although numerous possibilities have been proposed for energy

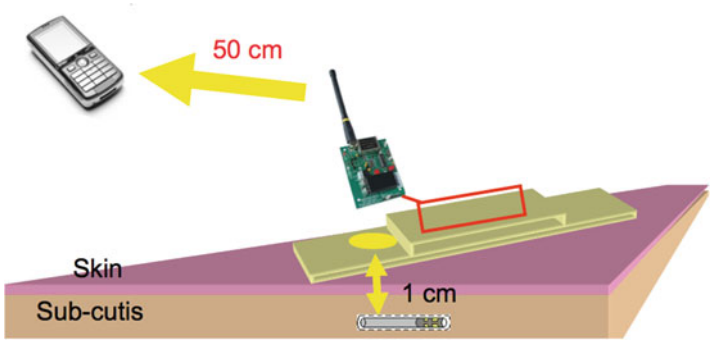

Fig. 1.3 Fully implantable medical devices may be powered by patches located on top of the skin, and these electronic patches may be wirelessly connected to a smartphone via a Bluetooth link

harvesting within the body, including thermal gradients, electrochemical techniques, and vibration harvesting, most are not considered sufficiently mature or reliable for medical applications [9]. Batteries have their own problems, including size, weight, cost, and toxicity. Most rechargeable batteries have safety risks, which limit their application in implantable devices. Recent problems with lithium-ion batteries in various applications will only continue to hinder their public acceptance for safety-critical applications like medical devices. A major reason for pacemaker replacement surgery is simply due to the lifetime of the battery (approximately 7–10 years), so any reduction in power consumption can translate to reduced surgery. Wireless powering over a short range, similar to RFID and smart-card technology, is very promising for providing up to milliwatts of power to the implantable device. Recent research [10] has shown that optimal powering frequencies in GHz range allow very small millimeter-sized antennas on implantable devices. We have demonstrated novel antennas for remote powering from patches applied to the skin directly above a subcutaneous device that allow MHz frequencies, too, for millimeter-sized antennas on implantable devices [1]. The close proximity and ease of alignment allow highly efficient energy transfer.

The Promise of Implantable Medical Devices

This book will show that IMDs are not limited to biosensors. Chapter 5 shows a quite different case of IMDs, and numerous other IMDs are on the drawing boards. Therefore, a taxonomy of IMDs can be defined by several dimensions:

- Physical location/depth, procedure, lifetime;
- Sensing/actuating functions (sense, deliver drugs or stimulus, grow tissue!);
- Computational capabilities;
- Data storage (both volatile and non-volatile);

- Communication: bandwidth, up-link, down-link, interdevice positioning system (IPS), distance to reader, noise;
- Energy requirements (memory, communication, computation), powering, harvesting, storage (battery or capacitive);
- Vulnerabilities: security functions (access control, authentication, encryption);
- Reliability and failure modes.

Of course, IMDs may be formalized in the abstract, as a general concept. However, the aim of this book is more to provide an introduction to the field of IMDs and to related fields in security and privacy. Therefore, we will introduce here the notion of the promise of biosensors by considering some key examples the details of which will be presented and discussed in more depth in Chaps. 2, 3, and 5. Thus, here we briefly touch on a few example devices, from those already on the market to those from the literature at the cutting edge and state of the art in medical implants.

Modern medicine is currently facing new challenges. One in particular is of importance for this book: *the personalization of pharmacological therapies offered to patients*. This new challenge is now trying to address the main problem in pharmacological therapy: when a group of patients is treated with exactly the same pharmacological compound, the result is usually different in terms of patient responses (for more details, see the introduction in Chap. 4). The market already tried once to solve this problem with a new chip based on microarray technology and capable of clustering patients into different groups [11]. The aim was to cluster patients in order to forecast their behaviors in terms of their response to the same therapy. However, this approach has been not very successful. The reason is not related to the chip performance but to the nature of genetics. Patients are different not only at the level of gene expression. They are also different from each other at the level of gene regulation, epigenetics, and daily variations in their metabolism. Therefore, daily monitoring of their metabolism is strictly required if the new approach of therapy personalization hopes to succeed.

In fact, that approach is already in place for diabetic patients. As amply shown in Chap. 2, glucose control is the cornerstone of diabetes mellitus (DM) treatment. Continuous glucose monitoring systems provide a dynamic assessment of shifting blood glucose concentrations and facilitate the making of optimal treatment decisions for diabetic patients. These systems contribute to the management of glycemic control and personalize insulin administration. Such an approach permits the narrowing of daily glucose fluctuations in blood while decreasing the incidence of hypoglycemic phenomena. This aspect is of key importance because improved glycemic control has proven beneficial to patients – and to the healthcare economy – by reducing the frequency and severity of associated complications. Glycemic control is now also gaining importance in intensive care units. It significantly improves both mortality and morbidity but requires frequent (often hourly) and accurate glucose testing. Therefore, a new generation of intravenous glucose systems are presently under development in key biosensor companies [12], such as A. Menarini Diagnostics, whose technologists contributed Chap. 2 of this book.

Another improvement in the human telemetry of glucose monitoring is the possibility of having remote access to data gathered by the measurement system. As shown in Chap. 3, wireless potentiostats are now being developed and commercialized for use in the development of implantable electrochemical biosensors for the monitoring of physiological markers in a wide range of pathologies. Chapter 3 presents an example of those developments by discussing the merits and drawbacks of a novel implantable biotransducer, the dual responsive MDEA 5037 of ABTECH Scientific [13]. The chapter refers to a series of laboratory tests that have shown positive assays on the device performance. For implantable amperometric biosensors, this system fulfills the desired functionality in the most efficient way possible, also giving due consideration to size, power management, telemetry capabilities, and signal processing. Therefore, it holds good promise for future devices in the market for metabolite telemetry.

Of course, in attempting to develop a monitoring system that can follow human metabolism over time, we are confronted with two main issues: providing the right specificity and the right sensitivity. Chapter 4 of this book provides a general overview on the possibility of developing devices that not only assure glycemia monitoring but also monitoring of glucose, lactate, adenosine triphosphate (ATP), bilirubin, and many other substances that are strictly related to several well-known human diseases. The chapter also presents a series of technological approaches that have been used in recent years in the successful development of a fully implantable subcutaneous implant that assures the metabolism monitoring of humans and addresses issues concerning the biocompatibility of those kinds of implants [15].

Problem of Specificity

When planning the development of an implantable device capable of detecting several molecules related to human metabolism, it is necessary to be able to identify the proper probes that can provide specific recognition of each single target metabolite. Chapter 4 of this book deals with specific recognition and discusses several possibilities: antibodies, oxidases, hexokinases, and cytochromes. Antibodies are the first molecules to consider when referring to specific molecular recognition. However, they are not very suitable for continuous monitoring for the following reason. When a sensing surface is fabricated based on an antibody, the obtained sensor is an immune sensor capable of sensing antigens (the target molecules of an antibody); meanwhile they are trapped by the antibodies that had previously been immobilized on the surface. Of course, the senseing is “continuous” but it applies only until the surface is fully saturated. Once all the antibodies have stuck to the antigen, they are no longer able to monitor other antigens arriving at the sensing surface. Thus, the surface is the sensing is continuous. Instead, enzymes are proteins too with the capability of true continuous monitoring because they are biological catalysts that are free to work on other substrates (the target molecules of an enzyme) immediately after participating in the previous reaction. Thus, enzymes

are always prepared to deal with new incoming substrates at the sensing surface. Hence, the surface is constantly ready to detect new target molecules. Chapter 4 introduces three types of possible enzymes for continuous monitoring: oxidases, which are usually used to detect glucose (the glycemic blood level), lactate, cholesterol, and many other endogenous metabolites; hexokinases, usually used to detect endogenous molecules that do not have a corresponding oxidase (the chapter presents the case of the ATP); and cytochromes, which have been proposed for the detection of several commonly used drug compounds and which were recently successfully introduced for continuous monitoring in personalized therapy [15].

Problem of Sensitivity

Generic amperometric sensors respond to increases in the amount of molecular concentration by an increase in currents. However, all sensors typically become blind below a certain concentration. The minimum amount of molecules that return the first slightest increase of current in a sensor is usually called the *detection limit*. Of course, the detection limit is a crucial parameter for identifying the working technology considering our goals. In fact, if the detection limit of a sensor does not fit within the physiological or pharmacological ranges of the molecules we would like to detect, we completely lose the possibility of addressing the medical application of our sensor. Chapter 4 also presents and discusses in detail how to use nanomaterials to improve the sensitivity of electrochemical sensors and, thus, how to decrease their detection limits in order to optimally use these kinds of sensors in the most important biomedical applications of IMDs. The nanotechnology proposed in Chap. 4 consists mainly of carbon nanotubes that have been successfully employed to enhance the sensor properties of both endogenous (e.g., glucose [16]) and exogenous metabolites (e.g., anticancer and anti-inflammatory drugs [17]).

Another Kind of Medical Implant

Part I of this book, "The Promise of IMDs," closes with a completely different kind of IMD: Chap. 5 refers to the possibility of developing IMDs that provide in vivo bioreactors. This kind of IMD addresses the human aspiration of creating our own tissue and organ substitutes. The last approach proposed for that purpose involved harvesting cells from the human organism (so-called stem cells) and expanding them in vitro before seeding them onto a biodegradable scaffold shaped according to the contour of the tissue to be replaced. The cell-scaffold construct is usually

cultured in an in vitro bioreactor that tries to mimic the in vivo regenerative niche. Although successful in some cases (the typical successful example is that of corneal cells), the approach has several disadvantages and technical obstacles inherent in the conventional tissue-engineering process. Therefore, a new approach has emerged involving the design of in vivo bioreactors. These completely new kinds of IMD are mainly implanted engineered tissues supported by an intrascaffold flow of medium created by an extracorporeal portable pump system for in situ tissue and organ regeneration. This design combines the traditionally separated in vitro three-dimensional cell-scaffold culture system and the in vivo regenerative processes associated with engineered tissue while treating recipients as bioreactors for tissue-engineered prostheses. Of course, it is very easy to imagine that marketing such an innovative technology would require automated systems also capable of hosting all the required fluidics [18] and carriers [19], as well as new monitoring sensors, in order to precisely control the tissue regeneration.

Security in Implantable Medical Devices

The second part of this book provides an introduction to security issues related to IMDs. Security is defined as the protection of a device, system, or data from a malicious (and usually human) adversary [20]. This should be distinguished from safety, where problems arise due to design errors, system failures, or random acts. However, IMD security is more complex than information security because it involves a physical system and humans as both producers and consumers of data. The relatively new discipline of security engineering [21] has much to offer in addressing this issue and provides a systematic approach. The methods of security engineering involve identifying the following aspects:

– Assets
– Vulnerabilities
– Threats
– Defenses

Defenses can be further divided into:

- Policies
- Mechanisms
- Enforcement

Security engineering is a challenging problem that is compounded by a variety of myths that include the following:

– Security is binary
– Standards are infallible
– Penetration testing and security consultants can ensure security

These problems arise primarily due to the fact that the adversary is human and attacks continue to evolve and improve to avoid new defenses. An escalating game of cat and mouse ensues. The adversary has the advantage by only needing to find a single point of weakness, while the defender must ensure that all possible attacks are defended. The multilayered nature of embedded computing systems further exacerbates the problem, and it is in fact between layers where many attacks succeed. This is due to the limitations of models and abstractions that were often designed without security in mind. Hardware-based attacks are an example, where information leaks through power and timing side channels not envisioned at the time of design [22].

Security guru and blogger Bruce Schneier [23] reminds us that:

> Any person can invent a security system so clever that he or she can't imagine a way of breaking it.

Schneier criticizes security approaches that only try to prevent intrusion, instead arguing that it is more important to design systems to fail well. This has become a standard approach in large-scale cybersecurity, including military and financial systems, where a certain amount of intrusion is assumed and the objectives are containment and resiliency. These arguments can be extended to medical systems, where the ultimate assets are human life and safety.

Respected security and cryptography expert Ari Juels [24] proposes the following tenets:

- Security should be designed in rather than added on. The example of the Internet illustrates this rather painfully.
- Open design: Public scrutiny usually breeds stronger systems than private finger crossing. Openness has long been a cardinal rule of cryptography and a pillar of secure system design. Similarly, responsible disclosure of vulnerabilities holds the technology industry to high standards and brings vital education to the community.
- Security should be designed holistically because piecewise solutions inevitably leave gaps at their boundaries.

These points will be expanded in Chaps. 7 and 8, which were written by leading security experts. Chapter 7 emphasizes the challenges associated with securing IMDs. The chapter presents some standard recommendations for sound security design and applies them to three classes of IMDs. Chapter 8 focuses on the wireless aspect of IMDs and their interface with BANs. Several attacks are shown and countermeasures proposed. Although by no means exhaustive, the novel attacks illustrate in detail the complexity and ingenuity that characterize modern threat scenarios. The reader is encouraged to expand on these two chapters by envisioning more sophisticated threats and the wide range of issues that must be considered in security engineering.

References

1. Jacopo Olivo, Sandro Carrara, and Giovanni De Micheli, *A study of Multi-Layer Spiral Inductors for Remote Powering of Implantable Sensors*, IEEE Transaction of Biomedical Circuits and Systems, 2013, in press
2. Sandro Carrara, Andrea Cavallini, Sara Ghoreishizadeh, Jacopo Olivo, Giovanni De Micheli, Developing Highly-Integrated Subcutaneous Biochips for Remote Monitoring of Human Metabolism, IEEE Sensors conference 2012, Taipei, Taiwan, October 28–31, 2012, p. 271–274
3. Benjamin Cotté, Cyril Lafon, Catherine Dehollain, and Jean-yves Chapelon. Theoretical Study for Safe and Efficient Energy Transfer to Deeply Implanted Devices Using Ultrasound. IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control, vol. 59, no. 8, August 2012
4. Gyselinckx, B., Van Hoof, C.; Ryckaert, J.; Yazicioglu, R.F.; Fiorini, P.; Leonov, V., "Human++: Autonomous Wireless Sensors for Body Area Networks," IEEE 2005 Custom Integrated Circuits Conference, pp. 13–19
5. Bruce Moulton, Zenon Chaczko, Mark Karatovic, Updating Electronic Health Records with Information from Sensor Systems: Considerations Relating To Standards and Architecture Arising From the Development of a Prototype System, Journal of Convergence Information Technology Volume 4, Number 4, December 2009, pp. 21–26
6. S. Kliff, Why electronic health records failed? washingtonpost.com, Jan 11, 2013
7. http://personalhealthportfolio.wordpress.com/
8. Wayne Burleson, Design Challenges for Secure Implantable Medical Devices, seminar published at http://www.cs.ru.nl/ifip-wg11.2/events/Slides-seminar2012/Burleson.pdf
9. Jacopo Olivo, Sandro Carrara, Giovanni De Micheli, *Energy Harvesting and Remote Powering for Implantable Biosensors*, IEEE Sensors Journal, 11(2011), 1573–1586
10. A. Poon, S. O'Driscoll, and T.Meng, "Optimal Operating Frequency in Wireless Power Transmission for Implantable Devices," Proceedings of the 29th Annual International Conference of the IEEE EMBS, pp.5673–5678, 2007
11. De Leon, J., Susce, M., Murray-Carmichael, E., The AmpliChip CYP450 genotyping test: Integrating a new clinical tool,Mol. Diagn. Ther. 10 (2006), 135–151
12. Valgimigli, F. Lucarelli, C. Scuffi, S. Morandi, and I. Sposato, "Eval- uating the clinical accuracy of GlucoMenDay: A novel microdialysis- based continuous glucose monitor," *J. Diabetes Sci. Technol.,* vol. 4, no. 5, pp. 1182–1192, 2010
13. Rahman, A.R.A., G. Justin, and A. Guiseppi-Elie, *Towards an implantable biochip for glucose and lactate monitoring using microdisc electrode arrays (MDEAs).* Biomedical Microdevices, 2009. **11**(1): p. 75–85
14. Sandro Carrara, Sara Seyedeh Ghoreishizadeh, Jacopo Olivo, Irene Taurino, Camilla Baj-Rossi, Andrea Cavallini, Maaike Op de Beeck, Catherine Dehollain, Wayne Burleson, Francis Gabriel Moussy, Anthony Guiseppi-Elie, Giovanni De Micheli, *Fully Integrated Biochip Platforms for Advanced Healthcare*, Sensors 12(2012) 11013–11060
15. Camilla Baj-Rossi, Giovanni De Micheli, Sandro Carrara, Continuous monitoring of a drug in real-time by a cytochrome P450-based electrochemical sensor, Biosensors and Bioelectronics, 2013, submitted
16. Guiseppi-Elie, A.; Lei, C.; Baughman, R.H. Direct electron transfer to glucose oxidase using carbon nanotubes. *Nanotechnology* **2002**, *13,* 559–564
17. Sandro Carrara, Andrea Cavallini, Victor Erokhin, Giovanni De Micheli, *Multi-panel drugs detection in human serum for personalized therapy*, Biosensors and Bioelectronics, 26 (2011) 3914–3919
18. Tan Q, Hillinger S,van Blitterswijk CA, Weer W. Intra-scaffold continuous medium flow combines chondrocyte seeding and culture systems for tissue engineered trachea construction. Interact Cardiovasc Thorac Surg. 2009 Jan;8(1):27–30

19. Tan Q, El-Badry A, Contaldo C, Steiner R, Hillinger S, Welti M, Spahn D, Higuera G, van Blitterswjik C, Luo QQ, Weder W. The effect of perfluorocarbon-based artificial oxygen carriers on tissue-engineered trachea. Tissue Eng. 2009 Sep;15(9):2471–80
20. Matt Bishop, Computer Security: Art and Science, Addison-Wesley Publisher, December 2002
21. R. Anderson, Security Engineering, Wiley, 2010, available free on-line (http://www.cl.cam.ac.uk/~rja14/book.html)
22. C. Kocher, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, Online, (available free on-line http://www.cryptography.com/resources/ whitepapers/TimingAttacks.pdf)
23. http://www.schneier.com/
24. Ari Juels, personal communication, 2008.

Part I

Chapter 2
Blood Glucose Monitoring Systems

Francesco Valgimigli, Fabrizio Mastrantonio, and Fausto Lucarelli

Background and Content of This Chapter

Glucose control is the cornerstone of diabetes mellitus (DM) treatment. Although self-monitoring of blood glucose (SMBG) still remains the best procedure in clinical practise, continuous glucose monitoring systems (CGMSs) provide a dynamic assessment of shifting blood glucose concentrations and facilitate the making of optimal treatment decisions for the diabetic patient. As such, CGM systems could contribute to a paradigm shift in the management of glycaemic control, making insulin administration more personalised. Such an approach makes it possible to narrow the daily glucose fluctuations in blood whilst decreasing the incidence of hypoglycaemic phenomena. This aspect is of paramount importance because improved glycaemic control has been shown to be beneficial to patients – and to the healthcare industry– by reducing the frequency and severity of associated complications [55]. Moreover, tight glycaemic control (TGC) in acutely ill hospitalised patients significantly improves both mortality and morbidity but requires frequent (often hourly) and accurate glucose testing [32, 33]. To meet the specific needs of intensive care units ICUs, specifically designed glucose hospital meters are already commercially available whilst a new generation of intravascular CGM systems is presently under development and clinical testing.

The aim of this document is to review the principles underlying the use of electrochemical glucose biosensors for monitoring the blood glucose level in diabetic patients.

The introductory section provides descriptions of blood, general features of the enzymatic systems and basic carbohydrate chemistry. The concept of the biosensor is introduced while focusing on the enzymes that represent the heart of essentially all commercially available glucosensors: glucose oxidase (GOD) and glucose dehydrogenases (GDHs).

F. Valgimigli (✉) • F. Mastrantonio • F. Lucarelli
A. Menarini Diagnostics, Florence, Italy
e-mail: fvalgimigli@menarini.it; fmastrantonio@menarini.it; flucarelli@menarini.it

W. Burleson and S. Carrara (eds.), *Security and Privacy for Implantable Medical Devices*,
DOI 10.1007/978-1-4614-1674-6_2,

The working principles of the so-called mediator-less and mediator-based electrochemical glucosensors are then described. Special emphasis is given to those factors – both physical (environmental) and (bio) chemical – that affect the accuracy and precision of blood glucose quantisation.

The mechanism by which the most common endogenous or exogenous compounds interfere is discussed in relation to which element of the glucosensor architecture (i.e. electrode, mediator or enzyme) is directly involved.

The final sections discuss continuous glucose monitoring in terms of its purposes, technologies, target population, accuracy, clinical-indication outcomes and problems. In this context, the most promising advancements in CGMSs, such as methods for non-invasive continuous monitoring and fully implantable biosensors, are reported. The commercial advent of the aforementioned technologies will enable diabetic patients to use CGMSs more routinely than ever before.

Introduction

Diabetes mellitus is a worldwide public threat and is expected to become one of the major healthcare challenges in the new millennium. Recently compiled data by the World Health Organization (WHO) shows that worldwide approximately 180 million people have diabetes and that this number may double by the year 2025. This metabolic disorder results from an insulin lack (T1DM) or deficiency (T2DM) that causes blood glucose concentrations to reach levels that are higher than the normal range of 80–120 mg/dL (4.4–6.6 mM) [1]. More specifically, in Type 1 diabetes (T1DM) the pancreas fails to produce insulin, which is essential for survival. This form of diabetes develops most frequently in children and adolescents but is being increasingly diagnosed later in life. In contrast, Type 2 diabetes (T2DM) results from the body's inability to respond properly to the action of insulin produced by the pancreas. T2DM is much more common than T1DM and accounts for around 90% of all diabetes cases worldwide. It occurs most frequently in adults but is being noted increasingly in adolescents as well. Certain genetic markers have been shown to increase the risk of developing T1DM. T2DM is strongly familiar, but it is only recently that some genes have been consistently associated with increased risk for developing Type 2 diabetes in certain populations. Both types of diabetes are complex diseases caused by mutations in more than one gene as well as by environmental factors. It is worth pointing out that the last 20 years have seen an explosive increase in diabetes globally linked to, among other factors, the emergence of obesity (diabesity). Diabetes has been recognised as the fourth leading cause of death and disability in the world. The disease is always associated, in the medium to long term, with the occurrence of multi-organ complications such as diabetic retinopathy, nephropathy, and neuropathy, mostly related to lifestyle, treatment and poor glycaemic metabolism control. The American Diabetes Association (ADA) Guidelines recommend a close monitoring of the blood glucose in order to prevent,

Fig. 2.1 Examples of glucometers for diabetes self-testing

reduce or delay the onset of such complications. Accordingly, millions of diabetics test their blood glucose levels daily, making glucose the most commonly measured analyte. The most important support to this practice is represented by commercial *glucometers* (e.g. Fig. 2.1), low-cost yet highly specific and sensitive analytical devices.

The tremendous economic burden associated with the management of diabetes, along with the challenge of providing such reliable and tight glycaemic control, has thus led to a considerable amount of research and innovative detection strategies [1, 2].

Definitions

Whole Blood, Blood Serum and Blood Plasma

Blood is the specialised bodily fluid that delivers all necessary substances (i.e. nutrients and oxygen) to the body's cells and transports the waste products away. Whole blood is composed of *blood cells* suspended in a liquid called *blood plasma* (Fig. 2.2).

Blood Cells

The blood cells present in blood are mainly red blood cells (also called RBCs or erythrocytes), white blood cells (leukocytes) and thrombocytes. One microlitre of blood typically contains the following substances:

(I) 4.7–6.1 million (male) or 4.2–5.4 million (female) erythrocytes. The RBCs contain haemoglobin, an iron-containing protein that reversibly binds oxygen, facilitating its transport throughout the body. RBCs are also marked by glycoproteins, which define the different blood types. The proportion of blood occupied by RBCs is referred to as the haematocrit, and is normally approximately 45%.