Minimum On-the-node Data Security for the Next-generation Miniaturized Wireless Biomedical Devices

Vladimir Vakhter[1], Betul Soysal, Patrick Schaumont[1], and Ulkuhan Guler[1]
[1]Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, Worcester, USA
Email: vvvakhter@wpi.edu, betuls@ieee.org, pschaumont@wpi.edu, and uguler@wpi.edu

***Abstract*— As continuous health monitoring and treatment outside of the traditional clinical environment has become of interest to healthcare providers and governments, the manufacturers of miniaturized wireless biomedical devices have sought to facilitate this idea. Much research has been devoted to smart-and-connected health technologies of various form factors including injectables, implantables, ingestibles, and wearables. Such devices are constrained in physical size, power-consumption budget, storage capacity, and computing power. Yet, they handle sensitive, private information and require trust as they directly affect the health of the patient by means of stimulation and/or drug delivery. In this work, we discuss the role of security as a fundamental component of these devices. We propose a generic layered model to support lightweight and cost-effective implementation of data security and protection mechanisms against possible attacks.**

***Index Terms*—Security, biomedical applications, next-generation biomedical devices, injectables, implantables (IMD), ingestibles, wearables.**

I. Introduction

Wireless miniaturized biomedical devices have gained tremendous attention for remote health monitoring and treatment in recent years [1]–[3]. The demand for smart-and-connected health devices is expected to continue rising worldwide [4], as their contribution to the reduction of healthcare costs becomes more prominent. They are suited for outpatient use and can be deployed in a rural or low-resource environment. Because of their convenience, low-cost, and easy access, smart-and-connected health devices are thought to support the transformation from traditional reactive (symptom-based) medicine towards proactive healthcare [5], which will create even more demand [6].

While fully functional wireless miniaturized biomedical devices are regularly presented, they are still generally considered to be emerging devices. We distinguish four primary categories: i) injectables, injected into human tissue; ii) implantables, implanted inside the human body by means of surgery; iii) ingestibles, swallowed by a human like regular pills; iv) wearables, worn outside of the human body. Nowadays, various injectables, implantables, ingestibles, and wearables are proposed for smart drug delivery [7], [8], stimulation [9], [10], monitoring of vital signs (e.g., heart rate, blood pressure, blood oxygen saturation, pH, etc.) [11], [12], and bio electrical activity (e.g., bioimpedance, electrocardiogram, and electromyography) [13], [14].

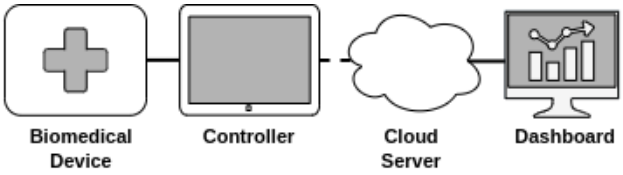

Fig. 1: A typical biomedical system (adopted from [18]).

Despite the significant achievements in device functionality, wireless miniaturized biomedical devices are extremely vulnerable to security threats [15]–[17]. While these devices bring considerable conveniences, they also produce various privacy and security risks [18]. Indeed, these devices collect and transmit sensitive private information and affect the human body by employing stimulation and drug delivery [15]–[17]. Yet, security of biomedical devices all too often is an afterthought. Instead, the traditional focus has been on features and functionality, rather than security. Accordingly, it may be observed that a large number of novel and even mature designs overlook proper protection mechanisms on the architectural level [7]–[13], [19].

In a typical next-generation biomedical system, demonstrated in Fig. 1, a biomedical device wirelessly (unilaterally/bilaterally) linked to an external controller (a smartphone/watch, a laptop, or a custom device) that may serve as a gateway and send the user data to a cloud server for processing, and then to a dashboard for informing the authorized users [18]. In most of the current solutions, protection mechanisms are known to be usually implemented by starting from the gateway [20]. Yet, the lack of security on the core of a biomedical device makes the whole system vulnerable. Therefore, security should be built into the design of biomedical devices [21] with a holistic approach.

In this work, a theoretical model for the lightweight implementation of data security for the next-generation miniaturized wireless biomedical devices is proposed. The consequent sections are organized as follows. Section II provides background on security challenges in these devices. Afterwards, Section III describes the developed model. Finally, Section IV concludes the paper.

II. Security Challenges in the Next-generation Miniaturized Wireless Biomedical Devices

The injectable, implantable, ingestible, and wearable next-generation wireless biomedical devices are known to have

978-1-7281-8058-8/20/$31.00 ©2020 IEEE

highly reduced area, weight, power, storage, and computing capabilities [21]. These limitations also affect the security features that may be available for them. For example, constraints in area put a limit on the complexity of cryptographic algorithms that can be implemented. Constraints in power put a limit on the complexity of cryptographic computations, as well as communication bandwidth and range. The constraints in storage and in processing ability imply that only simple cryptographic algorithms can be supported [22]. As a result, the design of security protocols and algorithms cannot be done in isolation, but rather must take these resource limitations in mind [23]. For example, while asymmetric cryptography may be desirable [24], it may be too expensive for these devices. Hence, dedicated lightweight security mechanisms should be developed [22].

Simultaneously, these devices may be equipped with a wide range of sensors/actuators and employ various communication/power delivery schemes. All these interfaces may be thought as channels where the attacker can maliciously interact with the target [25]. For a typical wireless biomedical device, we identify five such channels. Three input channels include the control channel, the sensors' channel, and the power delivery channel. Two output channels entail the data channel and the actuators' channel. We will briefly elaborate these channels in terms of the most possible attacks.

The Control channel includes the commands received from an external controller. They may be passively eavesdropped and replayed to cause malfunctioning or denial of service (DoS) for the device, or used to analyze and disclose the patient's treatment. These signals may also be actively altered to harm the user. By exploiting the breaches in this channel, an attacker can elevate privileges to cause malfunctioning/DoS or repudiate malicious intervention. Pairing with a counterfeit controller may expose the device to any of the above threats.

The Sensors' channel spans the read out of physiological values from various sensors integrated in the device. This channel may be exposed to fault injection attacks, sensor's spoofing, physical destruction of a sensor, disturbing the interconnection of sensors, or altering sensor data, etc.

The Power Delivery channel reflects the way how the energy is delivered to, and harvested by the device. This channel may be exploited to perform side channel attacks, such as monitoring power consumption while a device performs secret key operations. Another possible attack scenario for this channel, in case of the use of the wireless power link, is exceeding the power limit to cause DoS.

The Data channel represents the sensitive and private user information transmitted by the device. These data may be eavesdropped and disclosed, or tampered with to false the input for treatment, etc.

The Actuators' channel represents different mechanisms that can be triggered to stimulate the user. In case of being exposed to physical attacks, they would harm the user because of malfunctioning or DoS.

Assuming that the rest elements of the system, shown in Fig. 1, are secured, an overall attacker's model for wireless biomedical devices may be depicted as in Fig. 2. Besides input/output (I/O) and physical attacks, other possible threats include memory attacks and hardware attacks, which reveals that these devices have many possible attack surfaces.

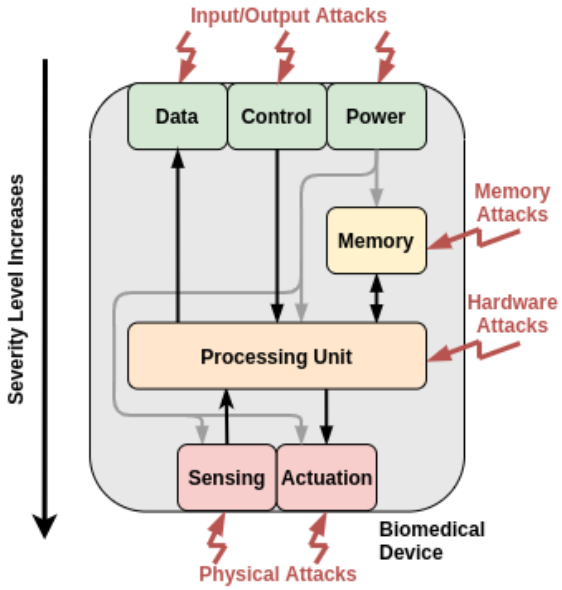

Fig. 2: Attacker's model for wireless biomedical devices (colors from green to red reflect the increase in the severity level of attacks).

Being limited in available resources and having multiple attack surfaces, biomedical devices should employ protective mechanisms that do not put the patient safety at risk in emergency [22]. It means that while these devices, as all other devices, need the server-side authentication to ensure that all commands are authorized, the first responder must access the device even when the normal authentication method is no longer available in an emergency case scenario. Therefore, it is preferable to exclude the patient from the authentication schemes like the 2-factor protocol proposed in [26]. Such straightforward approaches as disregarding authentication and authorization in emergency seem to introduce many plausible threats. Therefore, because of this hardship, authentication in medical devices is still an open problem [22].

There are many other challenges for these devices. For instance, healthcare personnel must be able to detect and communicate with the secured device in various environments (different medical institutions, countries, etc.). Moreover, these devices should comply with different legal and administrative measures, e.g., the laws on cross-border data transfer [21]. All these issues complicate the problem of embedding security mechanisms into tiny wireless biomedical devices.

Taking into account the above limitations, it might be appropriate to talk about the trade-offs between security and other performance parameters of the system. While it is not a trivial task to keep balance between security towards power, area, and computation optimisations [27], biomedical devices should contain, at least, some basic guards against the most possible attacks. Moreover, if designers adhere to well-understood principles and practices, building secure devices is repeatable [24]. That is why it is so important for developers to be armed with a generic model which would help implementing lightweight data security mechanisms in their designs.

III. The Proposed Model for the Lightweight Implementation of Data Security

While a small number of lightweight schemes to implement security for biomedical devices, as in [28], have been proposed, most of the lately released miniaturized wireless biomedical devices, among which injectables [29], implantables [9], ingestibles [12], [30], and wearables [31], are found to be lack of protective mechanisms. Only a few of relatively more resource-rich wearables, like [14], have some security mechanisms on board.

In order to guard a device, it is important to identify its main assets, or the resources that must be kept secured. They may include user's personal data, therapies, etc. [32]. From the perspective of different stakeholders, various resources may be considered as the most valuable assets for a particular device. For miniaturized wireless biomedical devices, the manufacturer, the user, and the hospital appear to be the primal stakeholders. Focusing on different assets means that different security measures must be employed. Security is never free and may cause extra overhead (exceeding a tight power budget, increasing time delays or memory usage, etc.) [22]. However, ad-hoc security is insufficient for these devices.

Obviously, there are no generic countermeasures that would protect a device from all the classes of attacks [27]. In each particular case, threat modeling should be performed [33]. At the same time, the existence of a generic model for the lightweight implementation of data security would stand developers in good stead to start protecting their emerging designs of miniaturized wireless biomedical devices.

We propose to structure the lightweight implementation of data security in a three-layer model, shown in the Fig. 3, where the layers are formed as follows:

I) Layer 1 is the most basic layer which includes data integrity and mutual authentication. Two-way authentication implies that both the biomedical device and the controller (see Fig. 1) verify each other. So, only the commands/data received from authenticated parties are processed. Integrity is the property of data items that have not been altered in an unauthorized manner since they were created, transmitted, or stored [34].

II) Layer 2 includes the properties of layer 1 and the privacy of data. Privacy means the use of individually identifiable health information and the freedom from illegal gathering [34], [35].

III) Layer 3 includes the properties of both previous layers and the confidentiality of data. Confidentiality is a property that data are not made available or disclosed to unauthorized persons or processes [34].

The hardware requirements for the aforementioned layers are discussed below. Secure wireless biomedical devices contain a hardware-based root of trust [24] that ensures authenticity and enables secure identification. The on-chip root of trust may be available in the form of (i) a unique ID/secret key stored in a one-time programmable memory (OTP) like e-fuses/antifuses [23], and (ii) physically unclonable functions (PUFs) [36]. These hardware primitives result in static (random, but stable and repeatable corressponding to input challenges) entropy. In terms of dynamic on-the-fly entropy generation, true random number generators (TRNGs) [37] are used to produce session keys, nonces, initialization vectors, and seeds for pseudo-random number generators (PRNGs) [23]. Some examples of available lightweight two-way authentication schemes for the electronic health systems may be found in [38].

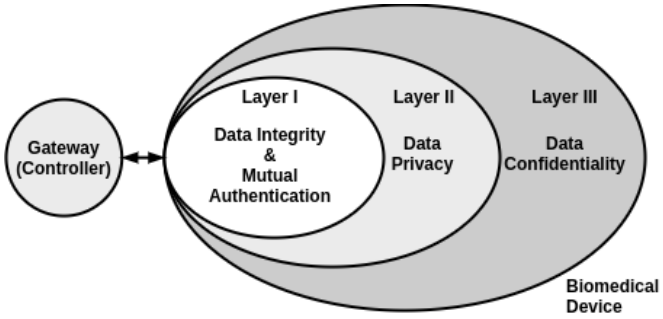

Fig. 3: Three-layer model for the lightweight implementation of data security.

The data monitored and exchanged by miniaturized wireless biomedical devices needs to be protected in terms of integrity. In order to ensure physical integrity, various types of circuit level sensors (e.g., light, temperature, power, or clock sensors, etc.) may be added to the design [27]. If a chip ID/secret key is stored in an OTP, layout obfuscation techniques, as in [39], may be applied to circumvent physical attacks, such as optical readout and layout scanning [23].

The privacy layer has to ensure that medical devices take adequate precaution to protect the privacy and anonymity of their users as it is required by such regulatory acts as the HIPAA Privacy Rule [35]. This reflects indirectly onto the complexity of security protocols. For example, all protocol exchanges must be unique through the use of randomness. Public identifiers must be obfuscated or hidden through encryption and/or randomization. This complicates the use of public identifiers such as those used in preshared-key designs [26]. Instead, to guarantee untraceability, identities must be systematically rotated [40]. Another aspect of privacy is that the medical-device data may not be revealed to an untrusted server even when it is desirable to have server-side computations on that data; the recent discussion on COVID-19 contact tracing is a good example of this tension between privacy and public health [41]. This indicates the potential of novel privacy-friendly solutions based on homomorphic computing or multi-party computation.

The confidentiality of the plaintexts is typically implemented with authenticated encryption with associated data (AEAD) primitives that also ensure the integrity of the ciphertexts [42], and with light-weight cryptographic protocol frameworks such as STROBE [43] and BLINKER [44].

IV. Conclusion

In this paper, we have proposed a generic model for the lightweight implementation of data security for the next-generation miniaturized wireless biomedical devices. This model contains three layers. The first layer involves the data integrity and mutual authentication. The next layer, built on

top of the above one, includes the data privacy. The last layer, while contains the properties of both previous layers, also introduces the data confidentiality. To mitigate and prevent attacks, the next-generation wireless biomedical devices should be equipped with protection mechanisms providing, at least, basic security properties. Yet each particular device requires performing a separate threat modelling, the existing general-purpose threat models seem to be hardly applied for these devices. Our dedicated model aims to bridge this gap and appears to be a good basic step towards embedding security in these emerging designs.

REFERENCES

[1] C. J. Bettinger, "Advances in materials and structures for ingestible electromechanical medical devices," *Angewandte Chemie International Edition*, vol. 57, no. 52, pp. 16 946–16 958, 2018.

[2] H. C. Koydemir and A. Ozcan, "Wearable and implantable sensors for biomedical applications," *Annual Review of Analytical Chemistry*, vol. 11, pp. 127–146, 2018.

[3] J. Dunn, R. Runge, and M. Snyder, "Wearables and the medical revolution," *Personalized medicine*, vol. 15, no. 5, pp. 429–448, 2018.

[4] Business Insider, "Iot healthcare in 2020: Companies, devices, use cases and market stats," 2020, last accessed 29 March 2020. [Online]. Available: https://www.businessinsider.com/iot-healthcare

[5] A. Kiourti and K. S. Nikita, "A review of in-body biotelemetry devices: Implantables, ingestibles, and injectables," *IEEE Transactions on Biomedical Engineering*, vol. 64, no. 7, pp. 1422–1430, 2017.

[6] Deloitte, "2020 us and global health care outlook," 2020, last accessed 23 April 2020. [Online]. Available: https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/global-health-care-sector-outlook.html#

[7] B. Yan et al., "Battery-free implantable insulin micropump operating at transcutaneously radio frequency-transmittable power," *Medical Devices & Sensors*, vol. 2, no. 5-6, p. e10055, 2019.

[8] X. Guo et al., "A novel and reproducible release mechanism for a drug-delivery system in the gastrointestinal tract," *Biomedical microdevices*, vol. 21, no. 1, p. 25, 2019.

[9] J. Charthad et al., "A mm-Sized Wireless Implantable Device for Electrical Stimulation of Peripheral Nerves," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 12, no. 2, pp. 257–270, 2018.

[10] B. C. Johnson et al., "Stimdust: A 6.5mm3, wireless ultrasonic peripheral nerve stimulator with 82% peak chip efficiency," in *2018 IEEE Custom Integrated Circuits Conference (CICC)*, 2018, pp. 1–4.

[11] H. Jiang et al., "A Sub-1μW Multiparameter Injectable BioMote for Continuous Alcohol Monitoring," in *2018 IEEE Custom Integrated Circuits Conference (CICC)*, 2018, pp. 1–4.

[12] M. Mimee et al., "An ingestible bacterial-electronic system to monitor gastrointestinal health," *Science*, vol. 360, no. 6391, pp. 915–918, 2018.

[13] M. Li, W. Xiong, and Y. Li, "Wearable measurement of ecg signals based on smart clothing," *International Journal of Telemedicine and Applications*, vol. 2020, 2020.

[14] S. Song et al., "A 769 w battery-powered single-chip soc with ble for multi-modal vital sign monitoring health patches," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 13, no. 6, pp. 1506–1517, 2019.

[15] W. Sun et al., "Security and privacy in the medical internet of things: a review," *Security and Communication Networks*, vol. 2018, 2018.

[16] B. Alexander, S. Haseeb, and A. Baranchuk, "Are implanted electronic devices hackable?" *Trends in cardiovascular medicine*, vol. 29, no. 8, pp. 476–480, 2019.

[17] D. Kotz et al., "Privacy and security in mobile health: a research agenda," *Computer*, vol. 49, no. 6, pp. 22–30, 2016.

[18] G. Selimis, "A healthy approach to medical security," *electronics europe News*, pp. 30–31, January 2020.

[19] Y. Jia et al., "A trimodal wireless implantable neural interface system-on-chip," in *2020 International Solid-State Circuits Conference (ISSCC), Session 26 / Biomedical Innovations*, February 2020, pp. 414–415.

[20] S. Tuli et al., "Next generation technologies for smart healthcare: Challenges, vision, model, trends and future directions," *Internet Technology Letters*, p. e145, 2019.

[21] P. A. Williams and V. McCauley, "Always connected: The security challenges of the healthcare internet of things," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. IEEE, 2016, pp. 30–35.

[22] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *Journal of biomedical informatics*, vol. 55, pp. 272–289, 2015.

[23] M. Alioto and S. Taneja, "Enabling ubiquitous hardware security via energy-efficient primitives and systems : (invited paper)," in *2019 IEEE Custom Integrated Circuits Conference (CICC)*, 2019, pp. 1–8.

[24] G. Hunt, G. Letey, and E. Nightingale, "The seven properties of highly secure devices," *tech. report MSR-TR-2017-16*, 2017.

[25] J. Di and S. Smith, "A hardware threat modeling concept for trustable integrated circuits," in *2007 IEEE Region 5 Technical Conference*. IEEE, 2007, pp. 354–357.

[26] S. Maji et al., "A low-power dual-factor authentication unit for secure implantable devices," in *2020 IEEE Custom Integrated Circuits Conference (CICC)*, 2020, pp. 1–4.

[27] I. Verbauwhede, *The Cyber Security Body of Knowledge*. University of Bristol, 2019, ch. Hardware Security, version 1.0. [Online]. Available: https://www.cybok.org/

[28] S. Ghoreishizadeh et al., "A lightweight cryptographic system for implantable biosensors," in *2014 IEEE biomedical circuits and systems conference (BioCAS) Proceedings*. IEEE, 2014, pp. 472–475.

[29] Y. Zhang et al., "Battery-free, lightweight, injectable microsystem for in vivo wireless pharmacology and optogenetics," *Proceedings of the National Academy of Sciences*, vol. 116, no. 43, pp. 21 427–21 437, 2019.

[30] R. Fontana et al., "An innovative wireless endoscopic capsule with spherical shape," *IEEE transactions on biomedical circuits and systems*, vol. 11, no. 1, pp. 143–152, 2016.

[31] I. Costanzo, D. Sen, and U. Guler, "An integrated readout circuit for a transcutaneous oxygen sensing wearable device," in *2020 IEEE Custom Integrated Circuits Conference (CICC)*. IEEE, 2020, pp. 1–4.

[32] P. Torr, "Demystifying the threat modeling process," *IEEE Security & Privacy*, vol. 3, no. 5, pp. 66–70, 2005.

[33] N. Shevchenko et al., "Threat modeling: a summary of available methods," *no. July*, 2018.

[34] The National Institute of Standards and Technology (NIST), "Glossary," 2020, last accessed 20 April 2020. [Online]. Available: https://csrc.nist.gov/glossary

[35] U.S. Department of Health Human Services, "The HIPAA Privacy Rule," 2002, last accessed 17 March 2020. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

[36] Green IC, "Physically unclonable function database (pufdb)," 2020, last accessed 24 April 2020. [Online]. Available: http://www.green-ic.org/pufdb

[37] Ü. Güler and G. Dündar, "Modeling cmos ring oscillator performance as a randomness source," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 3, pp. 712–724, 2013.

[38] S. Aghili et al., "Laco: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in iot," *Future Generation Computer Systems*, vol. 96, pp. 410–424, 2019.

[39] X. Wang et al., "Secure and low-overhead circuit obfuscation technique with multiplexers," in *2016 International Great Lakes Symposium on VLSI (GLSVLSI)*. IEEE, 2016, pp. 133–136.

[40] A. Aysu et al., "End-to-end design of a puf-based privacy preserving authentication protocol," in *Cryptographic Hardware and Embedded Systems - CHES 2015 - Proceedings*, ser. Lecture Notes in Computer Science, vol. 9293. Springer, 2015, pp. 556–576. [Online]. Available: https://doi.org/10.1007/978-3-662-48324-4_28

[41] L. Ferretti et al., "Quantifying sars-cov-2 transmission suggests epidemic control with digital contact tracing," *medRxiv*, 2020. [Online]. Available: https://www.medrxiv.org/content/early/2020/03/31/2020.03.08.20032946

[42] The National Institute of Standards and Technology (NIST), "Lightweight cryptography," 2020, last accessed 24 April 2020. [Online]. Available: https://csrc.nist.gov/Projects/Lightweight-Cryptography

[43] M. Hamburg, "The strobe protocol framework." *IACR Cryptology ePrint Archive*, vol. 2017, p. 3, 2017. [Online]. Available: https://eprint.iacr.org/2017/003.pdf

[44] M.-J. O. Saarinen, "Beyond modes: Building a secure record protocol from a cryptographic sponge permutation," in *Cryptographers' Track at the RSA Conference*. Springer, 2014, pp. 270–285. [Online]. Available: https://eprint.iacr.org/2013/772.pdf