Enabling Cybersecurity Mechanisms in a SmartPatch-Based Emergency Response System

Magdalena Kostoska*, Vladimir Trajkovik*,
Bojana Koteska*, Nevena Ackovska*, Fedor Lehocki†, Ana Madevska Bogdanova
* *Ss. Cyril and Methodius University,*
Faculty of Computer Science and Engineering
Skopje, North Macedonia
{magdalena.kostoska,vladimir.trajkovikj,bojana.koteska,nevena.ackovska,ana.madevska.bogdanova}@finki.ukim.mk
†*Faculty of Informatics and Information Technologies*
Bratislava, Slovakia
fedor.lehocki@stuba.sk

***Abstract*— This paper elaborates on the cybersecurity challenges of a healthcare system that includes a chest-patch (SmartPatch) sensor, used for the process management of massive victims' events. Integrating biosensors into emergency communication strategies requires mechanisms for achieving trustful communication.**

A use case of usage Bluetooth LE communication between SmartPatch and other device is presented in the paper, and presents the security challenges and potential solutions.

Keywords— Emergency Response System, Smart Patch, Cybersecurity Mechanisms

I. INTRODUCTION

The advancements in wireless sensor networks play a crucial role in the acquisition of vital function information from patients/victims in natural disasters/combat and ensuring secure data transfer to mobile platforms and healthcare cloud systems. These factors, in combination with artificial intelligence techniques, can be used for shortening the response time for the treatment of these urgent patients. By leveraging wireless sensor networks, first aid responders can gather real-time data on patients' vital functions, enabling timely and informed decision-making.

Managing victims after a mass injuries event, such as a terrorist attack or natural disaster, requires improvements in the rescuing procedures and the supporting systems, in order to reduce the number of potential casualties [1]. In our approach, we use a wearable monitoring system that uses an integrated wireless sensor SmartPatch (SP) for continuous measuring and recording of the victim's vital parameters.

II. SMART PATCH SYSTEM OVERVIEW

The Smart Patch sensor integrates three sensors that support each other – ECG, PPG and Laser induced graphene (LIG) [2] in order to gather the four vital parameters, needed to instantly estimate the hemostability of the patient– Heart rate (HR), Respiratory rate (RR), oxygen saturation (SPO2) and Blood pressure (BP). The Smart Patch System (SPS) can calculate the HR and RR, while the SPO2 and BP are estimated on the medic tablet in the medical vehicle while transporting the patient to the hospital, by using Artificial Intelligence models developed for the Android platform [3], [4]. The obtained four parameters and history are eventually transferred to the hospital server, providing the incoming patient's health status to the hospital before he/she arrives for treatment.

The primary concept behind the Smart Patch is to facilitate the notification and alerting of changes in the condition of an injured individual, particularly to a critical state, for immediate attention by on-site medical personnel. Additionally, it allows for continuous monitoring of the injured person's condition during transportation. This system also enable the medical personnel to assess the priority for medical treatment. SPS provides data transmission vie Bluetooth to the on-site medic tablet, as well as to the tablet in the medical vehicle and then by WiFi or mobile network to the central data repository. Fig. 1 depicts the data transferring process from the disaster site to the relevant stakeholder, for further victim's vital signs analytic.

III. SECURITY AND PRIVACY CHALLENGES

It is crucial to focus on addressing potential security vulnerabilities that could be used to exploit potential vulnerabilities of SPS.

Weak Authentication leading to potential Data Breaches [5]: If the system has weak authentication mechanisms, an attacker could potentially gain unauthorized access to the system, compromising the integrity and confidentiality of the health data. If unauthorized individuals gain access to the system or intercept the transmitted data, it can lead to the compromise of sensitive health information. Adequate measures must be in place to prevent and detect unauthorized access, and robust security controls should be implemented to protect against data breaches.

Interception of Wireless Communication [6]: If the wireless communication between the wearable sensors, mobile platforms, or healthcare cloud systems is not properly secured, an attacker could intercept and eavesdrop on the data transmission, potentially obtaining sensitive health information. Employing strong encryption, secure communication protocols, and authentication mechanisms

979-8-3503-0329-2/23/$31.00 ©2023 IEEE

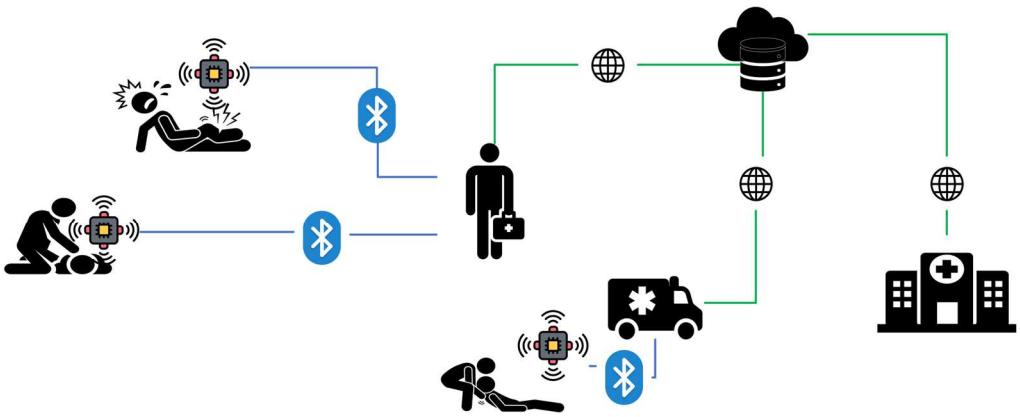

Fig. 1. Smart Patch System overview.

helps mitigate these risks and ensures the confidentiality and integrity of the transmitted data.

Privacy Concerns [7]: Privacy is a major consideration when handling health data. Collecting and storing sensitive personal health information raises concerns about the potential misuse or unauthorized disclosure of such data. Proper de-identification techniques and privacy-preserving measures should be implemented to protect individuals' privacy, ensuring that their identities cannot be linked to the collected data without appropriate authorization.

Compliance with Regulations [8]: Healthcare data is subject to various regulations, such as HIPAA, GDPR, or local data protection laws. Ensuring compliance with these regulations presents a challenge as the system must adhere to strict data protection and privacy requirements. Compliance efforts include implementing proper security measures, obtaining necessary consent, and providing individuals with control over their data.

Security of Healthcare Cloud Systems [9]: The security of the healthcare cloud systems used to store the collected data is critical. These systems may be targeted by cyberattacks, and the compromise of the cloud infrastructure can lead to unauthorized access or disclosure of sensitive health data. Robust security controls, regular audits, and adherence to industry best practices are necessary to secure the cloud infrastructure and protect the data stored within it.

IV. Bluetooth LE Security Options and Challenges

Bluetooth Low Energy (LE), also known as Bluetooth Smart, is a wireless communication technology designed for short-range communication between devices. It is widely used in various applications, including fitness trackers, smartwatches, medical devices, and home automation. Bluetooth LE security is crucial to protect the privacy and integrity of data exchanged between devices. Here are key aspects of Bluetooth LE security:

A. Pairing and Bonding

Pairing: This is the process of establishing a secure connection between two devices. Bluetooth LE devices use different pairing methods, including Just Works, Passkey Entry, Numeric Comparison, and Out of Band (OOB). The chosen method depends on the device's capabilities and the security requirements.

Bonding: After successful pairing, devices may go through a bonding process where they exchange and store security information. Bonding enables devices to recognize each other in subsequent connections without repeating the pairing process. Security Modes

Bluetooth LE supports two security modes: Security Mode 1 (no security) and Security Mode 2 (authenticated pairing with encryption). Security Mode 2 provides a higher level of security by ensuring that devices authenticate each other and encrypt data during communication.

B. Encryption

Bluetooth LE uses the Advanced Encryption Standard (AES) for data encryption. When devices establish a secure connection, they negotiate encryption keys to protect the confidentiality of data transmitted between them.

C. Privacy Features

Bluetooth LE includes features to enhance user privacy. For example, devices can use random addresses during advertising to prevent tracking of a device's unique address over time.

D. Secure Connections

Bluetooth LE 4.2 introduced the concept of "Secure Connections," which enhances the security of the pairing process. It uses Elliptic Curve Diffie-Hellman (ECDH) key exchange to establish a secure connection with forward secrecy.

E. Key Management

Proper key management is crucial for Bluetooth LE security. Devices must securely store and manage keys used for encryption and authentication. Keys should be protected against unauthorized access.

F. Firmware Updates

Security vulnerabilities may be discovered over time, and manufacturers need to provide firmware updates to address these issues. Ensuring that devices can receive and apply updates securely is essential for long-term security.

G. Device Authentication

Bluetooth LE supports device authentication to ensure that devices connecting to each other are legitimate. This is achieved through the pairing process, which may involve passkeys, numeric comparisons, or other methods.

H. Security Best Practices

Manufacturers and developers should follow best practices for secure implementation. This includes regularly updating firmware, using secure communication protocols, validating user inputs, and implementing proper access controls.

V. Use Case: Bluetooth LE Data Transfer from SmartPatch to Medic Tablet

In the SPS environment the first data transfer, and potential security vulnerability happens when the data is transferred from the SmartPatch to the medic tablet. The SmartPatch is built around MAX32630 ultra-low consumption microcontroller with 2MB flash memory and 512kB RAM memory. Its single core is Arm Cortex M4 with FPU running at 96MHz. For communication with the tablet, Bluetooth module PAN1780AT is used. It supports BT v5.0+ standard with LE LR modes. It is connected to the microcontroller over the serial line and is controlled by AT commands.

Given the physical environment and number of patches and medics available on-site, it is not always feasible to have predefined list of available devices (either patches or tablets). In this scenario several security vulnerabilities should be addressed. This is even more important given the scenarios where SPS is used - mass casualty event, especially if it is targeted attack (i.e. terrorist attack). In this scenario it is possible the SPS system to be misused (i.e. attacked) to increase the number of casualties.

The potential use case vulnerabilities include:

Eavesdropping - Attackers might attempt to intercept and monitor Bluetooth LE communications to gather sensitive information. Encryption mechanisms are in place to prevent this, but vulnerabilities in implementations or weak key management could be exploited. To mitigate this vulnerability the Smart Patch system plans to use AES encryption and possibly use secure pairing methods.

Man-in-the-Middle (MITM) Attacks - MITM attacks involve an attacker intercepting and possibly altering communication between two parties. Bluetooth LE uses pairing and encryption to mitigate MITM attacks, but vulnerabilities in these processes can be exploited. Regarding the pairing process, good practice to mitigate this attack is to use secure pairing methods such as Numeric Comparison or Passkey Entry during the pairing process. The Smart Patch system plans to address this issue in the next iteration.

This methods, along with AES encryption, secure key storage, secure key exchange protocols and the rest of the recommendations can mitigates in addressing Key Management Issues. This vulnerability includes weaknesses in the generation, storage, or handling of encryption keys can expose Bluetooth LE connections to attacks. If keys are compromised, an attacker can decrypt communication and potentially gain unauthorized access to devices.

BlueBorne is a set of vulnerabilities affecting various Bluetooth implementations, including Bluetooth LE. The specifics of BlueBorne vulnerabilities may vary across different devices and implementations, but the general threat is the potential for remote code execution and unauthorized access through Bluetooth connections. Keeping devices updated with the latest security patches is a fundamental step in mitigating the risks associated with BlueBorne and similar security threats.

Device Spoofing presents vulnerability where attackers might attempt to impersonate a legitimate device to gain access to a Bluetooth LE network. Proper authentication and employment of secure pairing methods during the pairing process is crucial to prevent device spoofing. This vulnerability also includes Weaknesses in Pairing Methods. The security of Bluetooth LE connections heavily depends on the chosen pairing method. If devices use weak or easily guessable passkeys, PINs, or lack proper authentication, it can lead to vulnerabilities. Methods like Numeric Comparison, Passkey Entry, or Out of Band (OOB) authentication involve user interaction and confirmation, making it harder for an attacker to spoof a device.

Replay Attacks - In a replay attack, an attacker intercepts and later retransmits data to mimic a legitimate communication. Bluetooth LE uses nonces and timestamps to mitigate replay attacks, but vulnerabilities in these mechanisms could be exploited. This attacks can be mitigated also by implementing session tokens (that are unique to each session), rolling codes (use of codes that change with each communication session), sequence numbers or counters in the data packets etc. The Smart Patch system currently uses counters in the data packages.

BlueSnarfing and Bluejacking - BlueSnarfing involves the unauthorized access and extraction of information from a Bluetooth-enabled device. Bluejacking involves sending unsolicited messages to a Bluetooth device. While these attacks are more common in classic Bluetooth, they can still occur in Bluetooth LE if not properly secured.

VI. SPS Medic Application Interface

Considering the human factors alongside cybersecurity techniques promotes both security and usability. Thus, it is essential to create a user-centric approach where cybersecurity measures are implemented in a way that minimizes disruption to users' workflows and did not impede their ability to perform their tasks efficiently. In SPS, we are implementing a userfriendly interface, clear instructions, and intuitive processes that enable users to navigate the system securely and easily (see Fig. 2).

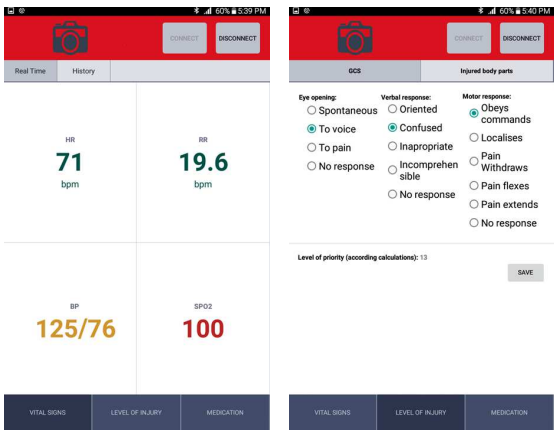

Fig. 2. SPS Interface [10].

VII. Conclusion

Addressing these security and privacy challenges requires a comprehensive and proactive approach that includes implementing robust security controls, ensuring compliance with regulations, maintaining privacy-preserving measures, conducting regular security assessments, and staying updated on emerging threats and best practices in the field of data security and privacy.

In the context of the SmartPatch System (SPS) environment, several potential security vulnerabilities are identified, particularly during the data transfer from the SmartPatch to the medic tablet. The SmartPatch utilizes a microcontroller, Bluetooth module, and associated technologies for communication. Given the dynamic nature of the environment and potential scenarios like mass casualty events, security vulnerabilities need to be addressed comprehensively.

In conclusion, addressing the security vulnerabilities in the SmartPatch System involves a multi-faceted approach. The planned mitigation measures encompass encryption, secure pairing, key management, software updates, and specific strategies tailored to counter each identified threat. This comprehensive approach aims to enhance the overall security of Bluetooth LE communications in the dynamic and potentially challenging environment of the SmartPatch System.

We have promoted active participation from users in providing feedback and reporting any security concerns or vulnerabilities they may encounter. This collaborative approach allowed for continuous improvement of the system's security while ensuring that user perspectives are considered. At the same time, this approach ensures that security measures do not impede the functionality or usability of the system, according to the established urgent medical procedures.

Acknowledgment

This paper has been written thanks to the support of the "Smart Patch for Life Support Systems" - NATO project G5825 SP4LIFE and by the National project BIOX of the Faculty of Computer Science and Engineering, at Ss. Cyril and Methodius University in Skopje.

References

[1] L. Posthuma, C. Downey, M. Visscher, D. Ghazali, M. Joshi, H. Ashrafian, S. Khan, A. Darzi, J. Goldstone, and B. Preckel, "Remote wireless vital signs monitoring on the ward for early detection of deteriorating patients: A case series," *International Journal of Nursing Studies*, vol. 104, p. 103515, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0020748919303220.

[2] T. Vicenti´ c,´ M. Raslji˘ c´ Rafajilovic,´ S. D. Ilic,´ B. Koteska, A. Madevska Bogdanova, I. A. Pasti, F. Lehocki, and M. Spasenovi˘ c,´ "Laser-induced graphene for heartbeat monitoring with heartpy analysis," *Sensors*, vol. 22, no. 17, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/17/6326.

[3] I. Kuzmanov, A. M. Bogdanova, M. Kostoska, and N. Ackovska, "Fast cuffless blood pressure classification with ecg and ppg signals using cnnlstm models in emergency medicine," in *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, 2022, pp. 362–367.

[4] B. Koteska, H. Mitrova, A. M. Bogdanova, and F. Lehocki, "Machine learning based spo2 prediction from ppg signal's characteristics features," in *2022 IEEE International Symposium on Medical Measurements and Applications (MeMeA)*, 2022, pp. 1–6.

[5] A. McLeod and D. Dolezel, "Cyber-analytics: Modeling factors associated with healthcare data breaches," *Decision Support Systems*, vol. 108, pp. 57–68, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167923618300368

[6] L. A. Tawalbeh, H. Tawalbeh, H. Song, and Y. Jararweh, "Intrusion and attacks over mobile networks and cloud health systems," in *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2017, pp. 13–17.

[7] A. Dimitrievski, E. Zdravevski, P. Lameski, and V. Trajkovik, "Addressing privacy and security in connected health with fog computing," in *Proceedings of the 5th EAI International Conference on Smart Objects and Technologies for Social Good*, ser. GoodTechs '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 255–260. [Online]. Available: https://doi.org/10.1145/3342428.3342654

[8] D. Mohammed, R. Mariani, and S. Mohammed, "Cybersecurity challenges and compliance issues within the u.s. healthcare sector," *International journal of business and social research*, vol. 5, pp. 55–66, 2015.

[9] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, "ehealth cloud security challenges: A survey," *Journal of Healthcare Engineering*, vol. 2019, 2019.

[10] M. Kostoska, M. Simjanoska, B. Koteska, and A. M. Bogdanova, "Real-time smart advisory health system," in *Proceedings of the 8th International Conference on Web Intelligence, Mining and Semantics*, ser. WIMS '18. New York, NY, USA: Association for Computing Machinery, 2018. [Online]. Available: https://doi.org/10.1145/3227609.3227686