System Architecture and Security Issues of Smartphone-based Point-Of-Care Devices

Christian Zajc1,2, Gerald Holweg1, and Christian Steger2

1Infineon Technologies Austria AG, Development Center Graz
Email: {christian.zajc, gerald.holweg}@infineon.com
2Institute for Technical Informatics, Graz University of Technology (TU Graz), Austria
Email: steger@tugraz.at, christian.zajc@student.tugraz.at

Abstract—In recent years, personalized healthcare has become increasingly popular in our society. Wearable devices started a trend for monitoring physical health parameters. The next evolution after wearable devices are Point-Of-Care (POC) devices, which provide more vital parameter analyses for everyone. The electrification of POC devices is required to simplify the process and to increase the accuracy of measurement results. In this work, we focus on POC devices in combination with smartphones. Often, these devices are measuring and processing very sensitive data, which underlie a high privacy restriction. Therefore, it is required to provide an architecture and security issue analysis of POC devices. The outcome of this research contribution provides a sensitization for the requirement of enhanced security features. Especially, to fulfill the need for a power-aware security concept for a POC system architecture, which underlies limited resources like power consumption.

Index Terms—POC device, Smartphone, Security, NFC, Healthcare

I. INTRODUCTION

POC devices are medical instruments to analyze specific vital parameters of a human body. These medical tests with POC devices are well-known to be easy-to-use, fast, cheap, and independent to specialized analytic instruments. In general, the application of POC devices in healthcare becomes more and more popular in the world, due to technical possibilities providing fast and reliable measurement methods in a simple and cost-effective application. Especially the trend of personalized POC is continuously increasing by interests of the users to monitor their vital parameters to get a better insight and intuition of their physical conditions. Success for this trend was provided with the introduction of smartwatches and wearable devices. The user is continuously provided with vital parameters like heart rate, steps, and activity by a simple usage of these wearable devices. In the design process of new POC devices, it is important to be sure that every user has to be protected by an accurate security architecture. This design of a POC system architecture is lead to the analysis of the security architecture of POC devices and provides an outlook.

II. STATE-OF-THE-ART OF POC DEVICES

POC devices are constructed in diverse architectures and are specialized for a specific area of application. Current POC devices are mostly constructed on paper-like material with an optical reactive chemical solution. This means that the measurement results of the POC device is represented in different color gradients or appearance of lines. Analyses of these measurement results may be difficult because every human has a different color perception scheme. Consequently, the interpretation of these results can be inaccurate. The next level of POC devices bring the quantitative result interpretation to a digital supported way. This new generation transfers the measurement results to technical equipment in order to provide semiquantitative representation. One way is to capture the diverse color gradients with an optical image sensor. Another way is to change completely to an electrochemical biosensor. Electrochemical biosensors are working with chemical variations by applying various potential levels in order to detect a semiquantitative result. One example of these electrochemical sensors is blood glucose measurements for monitoring purposes.
A. Smartphone-based POC devices

Due to the increased distribution rate of smartphones in the world, they are an attractive platform to combine with new POC devices. Smartphones provide a powerful Central Processing Unit (CPU) with several communication channels to external devices like Universal Serial Bus (USB), headphone jack, Bluetooth, and Near Field Communication (NFC). A further positive aspect for smartphones is the simple extension of functionality by developing applications.

Sun and Hall provide a well-structured overview of POC devices based on smartphones in combination with electrochemical biosensors [2]. Attaching an electrochemical biosensor to a smartphone can be done in various ways. They categorized these ways into three main groups: wired, wireless, and integrated hardware. The wired connection is commonly established by a USB connection or through the audio headphone port. A wireless operation is mostly handled by support of Bluetooth or NFC. Each named approach has its distinct advantages and trade-offs in relation to power consumption, measurement precision, and usability. Purohit, Kumar, Mahato, et al. present the provided overview of smartphone-based POC devices utilizing by optical biochemical sensors [3]. Smartphones provide a powerful camera system to support the analysis of the optical resulting changes.

Liu, Geng, Fan, et al. provide another state-of-the-art overview of smartphone-based POC devices [4]. This work provides an overview of application areas for POC devices and highlights the variation of different analysis samples. Well-known human test samples are blood, urine, sweat, saliva, and tears. Each of these samples are characterized by their individual properties. Colorimetric and electrochemical tests are typical evaluations for smartphone-based applications.

As seen from the different overviews of current applications, the smartphone is commonly used for visualizations and to control external components to perform medical analyses. Consequently, a smartphone-based POC device can be split up into two main components, the smartphone and the measurement unit. The measurement unit consists of a small microprocessor with dedicated hardware in order to perform biochemical measurements. The communication between these two modules can vary with the above described connection possibilities, depending on the required demands.

B. Security and privacy in healthcare environment

Healthcare is a critical topic when it comes to privacy and security concerns. Reasons for these concerns exist through the process of handling measured and generated health-related data of a person. POC devices operate in a widespread field of application, which makes it necessary to provide a well-thought-out framework for constructing new POC devices. Measured data of these devices commonly do not remain on the device itself, but they have to be stored on it before they can be transmitted to other devices for further analyses. Thus, these produced data have to be protected on all aspects.

In the scientific context, some security and privacy evaluations for healthcare environment have been performed in the past. In the work of Pramanik, Pareek, and Nayyar [5], they discuss the benefits of remote healthcare and its challenges. The focus of this publication is set to privacy and security issues in the overall healthcare environment from the user side to a healthcare provider like a doctor. This environment is called telemedicine. Additionally, researchers address security and privacy issues in the eHealthcare system in relation to the Electronic Healthcare data Record (EHR) [6]. The authors focus to provide a framework for the scenario of data transmission in the world of eHealthcare with wireless body sensors, connected to a medical server system. A human body is monitored with several sensors, which are wirelessly interconnected. This work highlights attacks related on this use case scenario. The outcome of these researches shows that security and privacy for healthcare products must have a high priority in the development of new applications. However, all these presented researching works only discuss issues of transmission of measured data from the reader device to the service provider.

C. Open gaps

Therefore, we discuss the security and privacy issues of the missing part of the POC environment: the measurement system itself. A big challenge for POC devices is the limitation of certain resources like power consumption and available technologies. Leaked information of diverse vital parameters of human beings could be used to discriminate them in daily life by limiting resources or services. For these purposes, healthcare-related products, e.g. POC devices, have to provide an appropriate security architecture. The main open gaps in relation to POC devices are to design and to provide a security and privacy evaluation in the first step. Afterwards, a power-aware security architecture for a resource limited environment can be developed.

III. DESIGN REQUIREMENTS OF POC DEVICES

In this work, we are focusing on POC devices, which are based on a measurement system as it is depicted in Fig. 1. Our presented system architecture provides a simple base structure as POC device with the opportunity to use well-established features of smartphones. NFC technology can also provide enough energy to operate an entire POC device for a measurement process. In addition, we want to pre-charge an energy storage device, e.g. a supercapacitor, on the POC device to operate the measurement process completely out of this energy source. This provides the advantage of initializing the POC device once and then the user only has to wait until the measurement is completed. A full measurement process could last for several minutes or sometimes as well up to half an hour. With support of NFC, it is consequently not required to place an additional battery on the device. Nowadays, the process of analyzing a biochemical sensor is a combination of several measurement methods, performed on a single sample. This process of increasing the number of measurements for one vital parameter leads to a more precise measurement result by eliminating parasitic properties. Consequently, the device has to provide a stand-alone system, which is easily configurable and modular by means of adapting measurement routines. Some published works regarding POC devices already exist, which have a similar system architecture as our presented approach [7] [8] [9]. These named research contributions missed considering the security and privacy issues of POC devices, which are the first contact point to the user and should therefore provide a confident environment.

![Fig. 1. Illustration of a stand-alone, smartphone-based POC device with a connected electrochemical biosensor for a defined vital parameter analysis.](image_url)
the entire system has to underlay a defined security infrastructure. Three
typical security properties of a standardized model are described
below for a smartphone-based POC device.

1) **Confidentiality:** This property of the security model refers to
the protection of information from being accessed by unauthorized
users. In the special case of POC devices, only the patient itself is
allowed to be able to receive the measured results of the device. An
important point of confidentiality is that the system is also protected
against unauthorized users when the POC device gets disposed to
trash. In this case, the stored information must be guarded.

2) **Integrity:** Integrity describes the property of checking authen-
ticity of information. In detail, this means that the information is
not allowed to be altered during transmission from the POC device
to the user. Especially, if a smartphone is involved in this process,
the transmitted information must be protected from being changed.
Therefore, the user can trust the displayed results on the smartphone.

3) **Availability:** Data availability means that the authorized user
can receive the protected information, even if an attacker is trying to
compromise the infrastructure. A common type of attacks to disturb
the availability are Denial-of-Service (DoS) attacks, which cause a
lack of response. In this case, the user would not be able to receive
the measured information from the POC device. The data availability
can be a crucial factor, when these devices measure important vital
parameters of a human body for further control processes. The
interruption of this service could lead to a critical health situation.

**A. POC life cycle with security insights**

This section focuses on the operating principle of a POC device
with the implementation variant, as described in the section before.
These POC devices are designed to measure a defined electronic
biochemical sensor. To reach this goal, the entire system architecture
has to stay invulnerable to multiple security threats. In this section,
we explain each process of an entire POC device life cycle and
additionally provide some important security insights. A common
processing flow of these devices is depicted in Fig. 2, starting with
manufacturing and ending with the end of life state.

![Fig. 2. Representation of an electronic POC device's life cycle for a specialized vital parameter analysis.](image)

**A) Manufacturing:** At the manufacturing stage, the device has to
be assembled and programmed with the operational firmware. During
this step, the system is calibrated to achieve a high measurement
accuracy for the overall system. The evaluated calibration data and
additional device specifications can easily be transmitted to the device
by support of NFC. Furthermore, in the manufacturing stage, the POC
device can be provided with initial cryptographic keys in order to
establish a secured and authenticated communication.

**B) Configuration:** The intention of the configuration process is the
personalization of the device with information about the consumer.
The main benefit for this procedure is to increase the precision
of the measurement results on one hand and on the other hand to
provide a unique assignment to the initiated consumer. Personalized
information can be provided from a wide range of data sources.
Examples of personalized information are Identification (ID), name,
age, gender, and address. The required list of information, which
are stored on a POC device, depends on the specified use case
and field of application because hospital, doctors, or police requires
other information than for a personal usage at home. This means
the amount of information can vary for each application. Further
configuration specs can be calibration data or other measurement
related information, which increases the accuracy of measurements.
These information have to be provided by the user during the
activation and have to be transmitted to the POC device. During
this processing step, it is required to protect the information during
transmission, as well as afterwards at the storage on the POC device.
Furthermore, these data also must be protected against manipulation
attacks.

**C) Measurement:** During the measurement process, the micro-
controller has to control the internal components to process the
electrochemical analyses. Therefore, the measurement routine has to
follow a defined process in order to provide a qualified and trusted
measurement result. The microcontroller should have the opportunity
to verify if the firmware of the chip is altered by an unauthorized
person. The physical measurement is performed by a potentiostat,
which applies a potential to the sample and measures the resulting
variances in current flow or resistance. The control signals for a
chemical sensor, typical a three electrode system, are provided by
a potentiostat including an Analog-to-Digital Converter (ADC) and
a Digital-to-Analog Converter (DAC). A three electrode system consist
of a Working Electrode (WE), a Counter Electrode (CE), and a
Reference Electrode (RE). The measurement result of the POC device
has to be transformed to a representative value. This calculated value
and all raw data must be protected inside the chip, in order to
prevent attackers from retrieving information out of the chip. Only
the initiated user or patient is allowed to receive the measurement
result. Consequently, the communication channel to the user, in our
case a smartphone with NFC support, has to be secured.

**D) Data storage:** After the measurement and data evaluation
process the measurement data has to be stored on a memory device
in order to be accessible by the consumer. Depending on the use case
of the POC device, the requirements on how long the data has to be
stored is varying. If the consumer has the opportunity to access the
stored information at any time, then they have to be stored on a long-
term storage device like a Non-Volatile Memory (NVM). Otherwise,
the data could be temporarily stored on another memory technology,
where the data vanish after some time.

**E) Information transfer:** We are using the NFC technology to
transmit the information from the POC device to a reader device
(e.g., a smartphone). The possibility of power transmitting with NFC
is an advantage against communication methods like Bluetooth. The
usage of the NFC power transmission method allows us to reduce the
bill of material and other overhead. Bluetooth introduces additional
drawbacks like a device coupling. After this life cycle step exists two
possible ways to continue. The difference between these two ways
are in the number of possible reuses of the entire system. In the
single-use approach, the entire system is conceptualized to measure
a parameter for one time and after providing the measurement result
to the user, the POC device can proceed with the last step in the
life cycle. Otherwise, in the multi-use system the POC device can be
reused for further measurements.
F) End of life: When it comes to the point of entering the end of life process, these single- or multi-use devices are disposed to trash while still containing all stored information and raw measurement data. Therefore, these devices must provide a functionality to remove all data in order to protect the privacy of the consumer. Nevertheless, this procedure has to be simple and fast to help customers making use of this feature. A well-known problem at security enhancement features is that they have to be simple enough, so that the majority of the customers knows how to use it. A strong and complex security and privacy framework will not achieve its full benefit, if the customers do not know how to use the security features correctly.

IV. PROPOSED SYSTEM ARCHITECTURE FOR POC DEVICES

To achieve the previously discussed functionality, a POC device requires a minimum set of hardware components. In this part of the work, we focus on these components in order to provide an overview of functionality with influences in security issues. Fig. 3 illustrates a minimum set of required hardware components and each component is described in the next paragraphs. We have designed a new integrated chip supporting all these proposed features. In the next version of this new measurement platform, we want to introduce power-aware security features.

![Minimum set of required hardware components for a typical system architecture for POC devices](image)

**Microcontroller:** The microcontroller is the central unit of such an architecture and has the task to control and combine the functionalities of all components. In our approach, we utilize the commonly used Cortex-M0 processor core of ARM, due to its low power consumption and a small demand of area.

**Memory:** A POC device’s system architecture typically contains several memory storages, depending on the requested use case. Common memory technologies for an integrated system are Random-Access Memory (RAM), NVM, and Read-only Memory (ROM). Each of these memory storages is defined for special usage in the application for POC devices. If the design requires storing data for a longer term, then these data have to be moved to a NVM space. On the other hand, if the design requires losing the data after the power supply is gone, then these data can be pushed onto the RAM.

**Security:** In order to provide an enhanced security architecture to the system, possible security threats have to be identified. The challenge, in order to enable security measures on POC devices, is the limited amount of provided energy. Hardware accelerated modules improve the energy profile of the system. An Advanced Encryption Standard (AES) hardware module reduces for instance processing time and simultaneously the overall power consumption. Important properties in relation to security for a general POC device are root of trust, secured key storage, and a trusted key agreement.

**NFC:** In our approach for the system architecture of POC devices, we are focusing on the communication technology of NFC. NFC is used in our architecture due to the possibility to provide the required energy to the measurement system and furthermore to establish a communication to the users smartphone device.

**Sensor Interface:** The sensor interface is an analog construction of single components like an ADC and DAC, combined to a potentiostat. The potentiostat can be configured to perform electrochemical analysis on biochemical sensors with standardized measurement routines. Some standardized measurement routines are: amperometry, cyclic voltammetry, Differential Pulse Voltammetry (DPV), and Electrochemical Impedance Spectroscopy (EIS).

A. Potential security threats to POC devices

A POC device is exposed to several threats, therefore this section focuses on the possible security threats. To demonstrate potential security issues of smartphone-based POC devices, a threat analysis is performed. The analysis is performed on multiple levels of the product life cycle (see Fig. 2), ranging from the manufacturing process to the internal processes of the microcontroller. During the evaluation process all three introduced security properties should be kept in mind. The following list summarizes some security threats, which can occur on such a POC system:

**Firmware upgrade:** POC devices for single- or multiple-uses are produced, packaged, and stored until the devices are required. During the storage of these devices it could happen that the measurement routine or other parameters are updated due to any reason. Consequently, an opportunity has to be provided to update the firmware of the central controller. The firmware upgrade process must be protected, so that the user can obtain a fully functional device with a correct and verified firmware. The upgrade process of the device can be established via a smartphone, therefore the communication must be protected against Man-In-The-Middle (MITM) attacks. The firmware must be protected from being changed by an attacker.

**Communication:** Every connection between the POC device and the customer’s smartphone has to be protected against MITM attacks. Also the NFC channel is vulnerable against MITM attacks. Such an attack is demonstrated in the work of Akter, Chakraborty, Khan, et al. [10]. Consequently, the NFC channel must be protected against manipulation of transferred information. In addition, every communication channel to the POC device, not only for data transmission, has to undergo a security analysis. An additional communication channel is for instance a debugging interface, which could lead to an unintentional backdoor that reveals private information.

**Measurement routine:** The measurement routine can be disturbed by an attacker through manipulation of the biochemical sensor system. The user or patient wants to be sure that nobody is able to manipulate the biochemical sensor system during the measurement. The sensor system is an analog device, which cannot be protected with current security measurements. The only process that could be protected is the processing flow of the measurement routine. The microcontroller has to operate as desired, i.e., controls the sensor interface in a specified routine.

**Integrity of measurement results:** The measurement results are stored on the device to be available for the user at any time. The storage on a NVM requires protection against an attacker by encryption and authentication. The measurement results must be protected from being decrypted or manipulated by an attacker. A manipulation of the measurement result could lead to a wrong medication, if the POC device is specialized for medication analyses.

**Authentication of user:** Only the initiated user should be able to receive the correct measured values. Therefore, the connection between the POC device and the reader must be authenticated.
encrypted and decrypted. Furthermore, data of the system must be guarded from being changed from outside without permission.

Interrupt of communication channel: Depending on the applicable use case, it could also be critical when the communication channel is blocked by a DoS attack. A critical situation could be, if it is essential to get a vital parameter of the human body instantly for a special medication. Therefore, in the design process of new POC devices it must be a key focus to use a stable communication with less interference or to provide an alternative representation. The alternative representation of the measurement results could be for instance an integrated display on the POC device.

V. Security issues at proposed POC system architecture

The electrification of common POC devices imply some challenges regarding the main properties of POC devices. POC devices should be easy, cheap, and fast, but the overall system is limited by some resources like power supply, connectivity, and complexity. The provision of a constant power supply is a complex task, considering environmentally friendly system architectures. Due to the strong energy constraints of these systems, dedicated security controllers, which provide a secured and trusted environment, are typically not suited for POC devices. Common dedicated security controllers may have a current consumption about 20 milliamperes in active mode. This current consumption is too high in fact that, in our proposed use case, the POC device is only provided with a pre-charged energy storage through NFC. The initial provided energy has to last for the entire measurement process until the data are securely stored on the POC device. After the completed measurement, the user can establish a communication to the POC device with a smartphone at anytime and provides enough energy to receive the measured results.

Consequently, the system architecture of new designed POC devices must be designed to provide low-power security enhancements in order to resist against the presented security issues. A first step to include security features into the system is to introduce a Trusted Execution Environment (TEE). A TEE is an environment, which provides some fundamental security architectures to enhance the overall system. A well-known TEE is the TrustZone from ARM. The TrustZone starts to provide security features from hardware level by creating two different environments by splitting hardware resources [11]. A closer inspection of ARMs TrustZone exposes that there exists some hardware and software vulnerabilities, which provide access to unauthorized data [12].

The security analysis of such a POC device revealed that the system requires a low-power aware TEE with the framework including root of trust, memory protection, key storage, key management, and cryptography encryption schemes. In order to provide a root of trust, one possible method would be to introduce Physical Unclonable Functions (PUF). A PUF is using production variations of hardware implemented circuits to generate unique and hardware dependent cryptographic keys for diverse authentication algorithms. A PUF has to be implemented very carefully in order to provide a secured environment. PUF commonly introduces more backdoors to the system as expected. Consequently, they have to be used very carefully. One cloned PUF attack based on Static Random-Access Memory (SRAM) technology was presented in the researching work of Helfmeier, Boit, Nedospasov, et al. [13]. Due to the limitations of a POC device, a well-thought security architecture with acceptable compromise has to be developed. The challenge is providing enough energy for additional security enhancements with an adequate level of security. The goal is to provide the user with a simple and secured environment with minimal limitations and the best possible performance.

VI. Conclusion

The healthcare society is getting more and more interested in personalized monitoring of vital parameters. The continuous monitoring of very sensitive data requires a strong sensitization for privacy and security enhancements. These measured parameters of a person have to be protected on all levels. The design target for POC devices is to be simple, fast, and cheap. These properties introduce several limitations, which lead to challenges when developing new devices with biochemical sensors. This work gives an overview of the central components of a smartphone-based POC device. One application is analyzed with focus on security and privacy issues. A security threat analysis is performed to get an overview of possible attacks. The best of our knowledge, previous researches only focused on the security problem between the devices and the data centers of bigger healthcare services. The development of low-power POC devices is challenging, since the targeted application scenario introduces limits to the system design. One restriction is the power supply, which leads to the fact that it is not possible to use a full hardware accelerated security controller. To overcome this problem, a trust aware platform is proposed. A low-power has to be established. Since currently available platforms are not fully applicable, there is the need to develop and designing of a power-aware authenticated system architecture.

REFERENCES

[1] S. Kemp, Digital 2020: Global Digital Overview, https://datareportal.com/reports/digital-2020-global-digital-overview, Accessed: 6 Feb. 2020.

[2] A. C. Sun and D. A. Hall, “Point-of-Care Smartphone-based Electrochemical Biosensing,” Electroanalysis, vol. 31, no. 1, pp. 2–16, 2019.

[3] B. Purohit, A. Kumar, K. Mahato, and P. Chandra, “Smartphone-assisted personalized diagnostic devices and wearable sensors,” Current Opinion in Biomedical Engineering, vol. 13, pp. 42–50, 2020.

[4] J. Liu, Z. Geng, Z. Fan, J. Liu, and H. Chen, “Point-of-care testing based on smartphone: The current state-of-the-art (2017–2018),” Biosensors and Bioelectronics, vol. 132, pp. 17–37, 2019.

[5] P. K. D. Pramanik, G. Pareek, and A. Nayyar, “Chapter 14 - Security and Privacy in Remote Healthcare: Issues, Solutions, and Standards,” in Telematics Technologies, 2019, pp. 201–225.

[6] I. Ahmed and A. Mousa, “Security and Privacy Issues in Ehealthcare Systems: Towards Trusted Services,” International Journal of Advanced Computer Science and Applications, vol. 7, no. 9, 2016.

[7] M. Mujeeb-U-Rahman, M. Honavar Nazari, and M. Sencan, “A novel semiconductor based wireless electrochemical sensing platform for chronic disease management,” Biosensors and Bioelectronics, vol. 124-125, pp. 66–74, 2019.

[8] H. Jiang, X. Zhou, S. Kulkarni, M. Uranian, R. Seenivasan, and D. A. Hall, “A Sub-μW multiparameter injectable BioMote for continuous alcohol monitoring,” in 2018 IEEE Custom Integrated Circuits Conference (CICC), San Diego, CA, 2018, pp. 1–4.

[9] A. Aina, M. P. S. Mousavi, M.-N. Tsaloglou, J. Redston, J. G. Bell, M. T. Fernández-Abdel, and G. M. Whitesides, “Open-Source Potentiostat for Wireless Electrochemical Detection with Smartphones,” Analytical Chemistry, vol. 90, no. 10, pp. 6240–6246, 2018.

[10] S. Akter, T. Chakraborty, T. A. Khan, S. Chellapan, and A. B. M. A. A. Islam, “Can You Get into the Middle of Near Field Communication?” In 2017 IEEE 42nd Conference on Local Computer Networks (LCN), Singapore, 2017, pp. 365-373.

[11] B. Ngabonziza, D. Martin, A. Bailey, H. Cho, and S. Martin, “TrustZone Explained: Architectural Features and Use Cases,” in 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC), 2016, pp. 445–451.

[12] S. Pinto and N. Santos, “Demystifying Arm TrustZone: A Comprehensive Survey,” ACM Computing Surveys, vol. 51, no. 6, pp. 1–36, 2019.

[13] C. Helfmeier, C. Boit, D. Nedospasov, and J.-P. Seifert, “Cloning Physically Unclonable Functions,” in 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2013, pp. 1–6.