Interconnected, Secured and Authenticated Medical Devices

Matteo Cagnazzo[1] Markus Hertlein[2] and Norbert Pohlmann[1]

[1] Institute for Internet-Security, Gelsenkirchen, Germany
{Cognazzo | Pohlmann}@internet-sicherheit.de,
WWW: www.internet-sicherheit.de
[2] XignSys GmbH, Gelsenkirchen, Germany
hertlein@xignsys.com
WWW: www.xignsys.com

Abstract. The following paper introduces a secure and efficient application concept that is capable of authenticating and accessing smart medical devices. The concept is based on two already developed applications. It describes the used technologies and discusses the outcome and potential downfalls of the idea.

Keywords: Security, Authentication, Medical Devices, Communication, Internet Of Things

1 Preliminaries

Modern smart medical devices (SMD) are often connected to the internet or intranet, for example a hospital network, and therefore need authentication to offer services to an authenticating entitity. The reasons why connectivity need to be added are diverse for example the components are used for telemetry. The confidentiality, availability and integrity requirements for authentication and transmission mechanisms are also important. The mechanisms should be secure, easy to use and reasonable fast so the user has no waiting time and the application becomes tactile and tangible. If we consider nowadays common mechanisms to authenticate against a service or a device the most used technique is to use username and password based approaches. These are prone to manifold attack vectors for example *Brute Force-*, *Dictionary-*, *Rainbow Table* and *Keylogging-Attacks* [3]. Since users tend to use unsafe passwords or the same password for multiple services, attacks on and over the internet become more and more profitable [9]. But not just users are tending to use unsafe passwords, vendors and manufacturers are also likely to use combinations like username: admin password: admin as recent discoveries around the Mirai botnet show [10]. One alternative is multi-factor authentication which combinates knowledge (username/password), ownership (smartphone) and/or individual biological properties (biometry). Access to a system is therefore granted if and only if the combination of all these challenges return successful. A downfall is that a stolen "root-secret" corrupts a whole system and therefore most problems of password-based authentication

are persistent and leading to a lower security level. Device and communication security in general is rather low in medical equipment. Drug infusion pumps can be remotely manipulated to change the dosage doled to patients and X-rays that can be accessed remotely by spying on a hospitals network [11]. Hospitals are often unaware that these devices bring high risks to their infrastructure. Security flaws are publicly disclosed, but it does not change risk assessement in hospital environments. A common security hole is the lack of authentication to such devices but also weak or no encryption [8]. Trust in networked SMDs is so low that former US vice president Dick Cheney had the wireless capability of his defibrillator disabled back in 2007 [7].

1.1 Authentication Systems

Todays authentication processes are more dynamic since the interaction of users and machines in the field of the Internet of Things. Especially the authentication towards SMDs has to be a variety of authentication methods, with different security levels depending on the user expierence, the security and response time while interacting with a SMD. The classic approaches like password-based authentication or smartcard-based authentication are not able to answer the new challenges developing from the human-machine interaction. On the one hand it is not possible to use password-based authentication for the authentication, for example against a drug infusion pump, due to the need of extra hardware like keyboards or pin-pads. Also the time consuming aspect of using passwords and the user-unfriendly process of managing passwords are not acceptable for small use cases. For high security use cases like the access to digital medical records a weak one-factor authentication is not applicable. On the other hand strong two-factor authentication methods like smartcard authentication are expensive due to the need of smartcards readers and smartcards or security tokens. The two examples, the authentication against a drug infusion pump and the access to digital medical records are showing two more demands emerging from the Internet of Things in the healthcare sector. Unlike authentication systems in the todays Internet, which are mainly working with a level of high or low security, authentication systems in the field of health care system should be able to adjust the security level based on the protection needs of the assets. This so called adaptive authentication is able to increase the usability where possible. Usability is a necessary feature in the whole field of authentication in IoT, due to the fact that the number of authentication processes will be a multiple of these a user has to perform nowadays. Furthermore the authentication systems have to conuence to an authentication eco-system that works with different technologies in different scenarios and use cases On the other hand strong two-factor authentication methods like smartcard authentication are expensive due to the need of smartcards readers and smartcards or security tokens. Furthermore the authentication systems have to confluence to an authentication ecosystem that works with different technologies in different scenarios and use cases [6]. Summarizing a modern authentication and access management system has to fulfill the following requirements [6]: It has to be *interoperable*, offer *adaptive* authentication

between security and usability, *reduce* complexity and cost efficiency and it must be *operational* in different scenarios and use cases

1.2 Communication Systems

An essential part that becomes even more relevant with further interconnectedness of medical staff and SMDs is efficient communication. In a system where billion things and humans are interconnected there is no need for redundant and slow communication. Current standardization processes like 5G want to enable tactile user experience through real time communication. To realize that one needs short reaction time and latency ($<$ 1ms) [1]. Especially in emergency situations it is a vital aspect to know every step of a life saving processes. Such processes are often definded in a theoretical form but not available in emergency situations. Therefore a lightweight process management tool would be the ideal way to solve this problem. Finally electronic communication is moving from asymmetrical towards symmetrical communication whereby the communicating peers can exchange their information in real-time and see the collaboration of the other peer which increases efficiency and promotes the exchange of information Taking into account the emerging interconnectedness of SMDs it is clearly distinguishable that current communication solutions are not capable of dealing with the increasing number of participants. Not a single platform provides support for communicating with devices or has an interface to connect with a SMD. Efficient, smart and secure chat-based communication is the key for the ongoing digitalization in different environments. These key-features are introduced by a novel platform called "Quvert" [2]. This approach will be expanded in this paper to support communication with SMDs in the Internet of things by combining Quvert with XignQR.

2 Used Technologies

Chapter 2 describes the technologies XignQR and Quvert that will be used to create the proposed architecture.

2.1 XignQR

XignQR [6] is an authentication and signature system that fits into a modern authentication eco system. The concept behind XignQR addresses all the requirements mentioned in chapter 1.1. Therefor the XignQR-System comprises of four actors, shown in figure 1:

1. Authentication Manager The authentication manager is the identity provider and broker. It is the main part in the authentication process between an user and a service provider/relying party (3.). It mediates the authentication result from the user authentication to the service provider. It also enforces the security and trust level of the used digital identity requested by a service

Fig. 1. Interaction of the four Actors

provider on server-side. At the beginning of an authentication process the security policy of a service provider and the users self-defined security policy is compared. The policy information are combined and enforced. User behavior is collected and used for risk-based authentication. From the users view the authentication manager helps to prevent the loss of privacy. The authentication manager proxies the PKI and is responsible for the provisioning of the PKI functionality. The PKI, digital certificates and cryptographic protocols are playing a key role in reference of interoperability, adaptive authentication and multi-functional deployment in a variety of use cases. For easy integration multiple ID-Protocols like SAML or OpenIDConnect are supported to enable federation between different identity and service providers to build an authentication eco system. To ensure integrity, authenticity and privacy the whole communication is signed with the users and components elliptic curve private keys and symmetrically encrypted with derived session keys.

2. Personal authentication device (PAD) The PAD is represented in form of a smartphone and the personalized XignAPP. It acts as user interface, as QR-Code scanner and as token reader for the optional Security Token. During the personalization process the app is equipped with user specific cryptographic material that is used for the challenge response authentication protocol. Since there are no passwords or shared secrets transmitted, all the mentioned attacks in 1 will not succeed. These information are analyzed by the authentication manager (1.) to enforce the policies and initiate multiple authentication factors on-demand. The use of the smartphone as PAD enables the use of many different authentication factors, from classical PIN

entries over biometrie and security tokens to new mechanism like photo-authentication or video-chat based authentication.
3. Service Provider/Relying Party The service provider is the component the user want to get access to. For example a website or a production machine. The integration is done by one of the many supported ID-protocols. As an entry point for the authentication a QR Code is used. The QR Code contains an ID, static or session-based, representing the service provider, an URL to the authentication manager and a digital signature. The authentication process starts with the scan of the QR Code with personalized XignAPP.
4. Security Token (optional) A security token can optionally be added to the PAD to increase the security level while increasing the usability through enabling new kinds of multi-factor authentication without interaction.

2.2 Quvert

Quvert enables fast, reliable, usable and secure business communication based on a chat-system. It introduces mechanisms to conduct legally watertight agreements. It enables a visualizable and configurable knowledge management and other features to develop an internal knowledge big data: Quvert.Knowledge. The foundation of Quvert is a secure, distributed and reliable server which is currently based on Matrix an open protocol for real time communication. This is especially important in terms of service availability because it enables to send data via multiple service providers, like the SMTP protocol does in emails. It is based on RESTful HTTP APIs to create an open interface. Messages are cryptographically signed and persisted. Quvert also enables end to end encryption between devices by using a double ratchet protocol. Therefore Matrix offers a lot of secure interoperability between different services through TLS. Third party identities can easily be tied to matrix ids so one can use already existing accounts to use matrix. The mobile and desktop applications have a composed user interface and are easily usable by technological unaffine users. The encryption scheme is the OLM protocol which is derived from Signal, which has already proven that it is capable of securing connections efficiently [5]. The platform is designed in a modular way so every client can specify their needs and Quvert can adapt to it. Another advantage is the fact that IoT devices no matter from which vendor they are is not stored in silos anymore but devices can publish events in certain rooms and users in the room that have been authenticated can get those events. This can be used to easily transmit data from machines or sensors to humans that are working with this data.

3 Proposed Architecture

To be able to communicate with a SMD one needs to authenticate against it. This authentication can be done with a smartphone that scans a QR-code attached to a smart object. After the initial scanning an authentification process is triggered [4]. The QR code can be replaced by any other entry point for

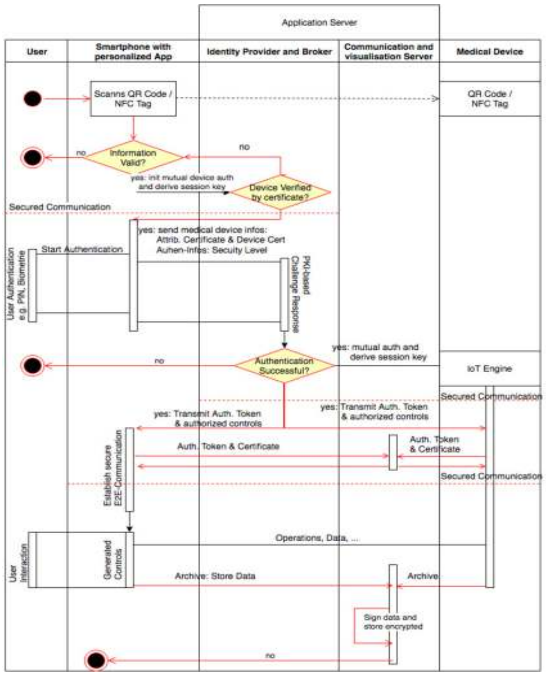

Fig. 2. Schematic view of an authentication

example a NFC or geotag. After the succesful validation of the QR Code or Tag the authentication process is iniated depicted in Fig. 2. At this point the smartphone app uses the information of the QR Code to initiate the mutual device authentication between smartphone and the identitiy part of the application server. Within the mutual authentication a session key is derived. After that, the whole communication between app und server is encrypted and digitaly signed. The app receives the attribute and device certificate of the SMD and is now able to verify the SMD, e. g. by capabilities or location information. The request contains also the security level of the user authentication that is needed to gain access to the device or data. Part of the user authentication, for example by fingerprint, is the PKI-based challenge response authentication between the identity provider and the users smartphone app. If the use has been successfully authenticated, the identity provider starts the mutual authentication process towards the SMD, for a secure channel. Now the authentication results and the authorized device control elements are pushed as Auth.-Token to both parties, the smartphone app and the SMD. Both devices iniate a connection of the secure channel to the communication and control bus. Over the secure channel a key exchange protocol is conducted, for example OLM, to establish a secure channel between the smartphone and SMD over the application server. At this point only both devices are able to read and manipulate data. The bus system only notices communication and logs these messages. An attacker has to successfully

attack both encrypted sessions, to gain access to the data or device. Since the communication is fully secured the control elements for the user are generated as follows: The user gets to interact with the SMD and can only interface every control that he is authorized to control. To derive which controls the user is able to access the following scheme as depicted in Fig. 3 is used. The SMD offers the attributes of the devices and the user offers the attributes of the User Authorization Token (UAT) which could be derived from the rule he is assigned to by an identity provider. From the intersecting set of available attributes the user interface will be generated and therefore user errors are avoided by design to obviate incorrect operations. If there is no intersecting set the application will throw an error because he is authenticated but not authorized to use the device.

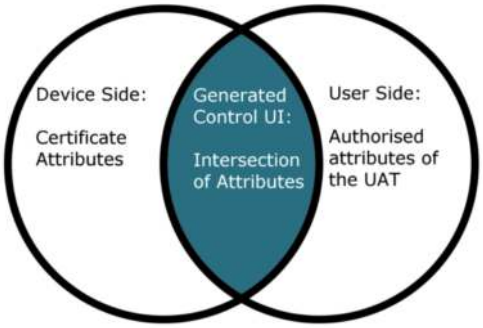

Fig. 3. View of userinteraction with a smart object

4 Discussion, Outlook and Conclusion

By using this architecture it is possible to authenticate a user with his smartphone against different SMO by scanning a QR-code attached to it. The platforms that are used for this architecture preconceive data security and privacy so that the possibility of manipulation is still possible but it is very hard to break or fraud the application and its backend. Especially if control authentication is granted a holistic contemplation must be done. Every transmission and every endpoint becomes a critical point where security and integrity has to be assured. All of this has to be done in a secure manner without losing the usability of the system. This will soon be a challenging task for the involved researchers. XignQR is capable of authenticating a machine against another machine and Quvert could operate as a bus system where machines can communicate and push or pull data to specific rooms while an administrator has the ability to overview all the machine communication for maintenance or analysis purposes

in a tidy and clean interface. XignQR is an authentication and a signature system that is also offers the ability to be used in process management. Future work will focus on implementation of the proposed framework as well as simulation and testing. Thus the proposed application can be evaluated and further drafted. Another current goal of this project is to identify and describe other use cases because the platform can be expanded to all kinds of scenarios. All in all the described application could serve as a visionary tool for communicating with smart objects in an efficient and secured way but there is still a lot of research and work to do.

References

1. Andrews, JG, Buzzi, S, Choi, W, Hanly, SV, Lozano, A, Soong, ACK, Zhang, JC (2014): What will 5G be? Selected Areas in Communications, IEEE Journal on, 32(6):10651082.
2. Barchnicki, S (2016): Eine Antwort auf die Frage nach effizienter Kommunikation von Morgen, IT-Sicherheit.
3. Beutelspacher, A (2005): Kryptologie. Eine Einfhrung in die Wissenschaft vom Verschlsseln, Verbergen und Verheimlichen ; ohne alle Geheimniskrmerei, aber nicht ohne hinterlistigen Schalk, dargestellt zum Nutzen und Ergtzen des allgemeinen Publikums. 7. Auflage. Vieweg, Wiesbaden.
4. Cagnazzo, Matteo and Hertlein, Markus, Pohlmann, Norbert(2016), An Usable Application for Authentication, Communication and Access Management in the Internet of Things, Information and Software Technologies: 22nd International Conference, ICIST 2016, Druskininkai, Lithuania, Proceedings, Springer International Publishing, p. 722-731
5. Frosch, T., Mainka, C., Bader, C., Bergsma, F., Holz, T. (2014). How Secure is TextSecure?.
6. Hertlein, M., Manaras, P., Pohlmann, N.(2015): Bring Your Own Device For Authentication (BYOD4A) The XignSystem. In Proceedings of the ISSE 2015 Securing Electronic Business Processes Highlights of the Information Security Solutions Europe 2015 Conference, Eds.: N. Pohlmann, H. Reimer, W. Schneider; Springer Vieweg Verlag.
7. Kolata,G. (2013): `http://www.nytimes.com/2013/10/29/science/of-fact-fiction-and-defibrillators.html?_r=0` [access 2016-12-09]
8. National Center of Biotechnology USA, 2015, Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem, `https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/` [access 2016-12-09]
9. Symantec Corporation (2014): Internet Security Threat Report 2014 :: Volume 19, `https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf` [accessed 2016-12-14]
10. Symantec Corporation (2016): `https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks` [access 2016-12-09]
11. Zetter, K.(2014), Hospital equipment vulnerable, `https://www.wired.com/2014/04/hospital-equipment-vulnerable/` [access 2016-12-09]