Schreier G, Hayn D, Hörbst A, Ammenwerth E, editors. Proceedings of the eHealth2012. 2012 Mai 10-11; Vienna, Austria. OCG; 2012.

A PRIVACY PRESERVING HOME MONITORING SYSTEM

Fillafer M[1], Slamanig D[1], Stingl C[1], Zaminer C[1]

Abstract

In this paper we present a security concept to establish a privacy-preserving home monitoring system. Our key requirement is that the system is hosted by an arbitrary service or cloud provider but the provider has no possibility to access patient's data in a meaningful way. This means that the provider is solely responsible for the availability and performance of the system and the patient can store sensitive data without any fear of misuse. Furthermore this also implies that data stolen by hackers cannot be linked to patients and patients interacting with the system are fully unobservable. We describe an implementation of this system based on so called anonymity techniques that can be applied to any information system containing person-related sensitive data.

Keywords* – *Home monitoring, privacy preserving security system, anonymity techniques

1. Motivation

Pervasive healthcare, the application of pervasive computing technologies for healthcare, health, and wellness management, which is about making healthcare available everywhere, anytime and to anyone is getting increasingly popular. Advances in wireless technologies such as intelligent mobile devices and sensors enable a wide range of applications such as mobile telemedicine, patient monitoring, location-based medical services, emergency response and management, pervasive access to medical data, personalized monitoring and lifestyle incentive management [12]. Thus, required medical information can be made available at any place any time using sophisticated devices and widely deployed wireless networks. For instance, the Continua Health Alliance, a consortium of more than 230 companies, is working towards the interoperability of wired and wireless telehealth devices like vital parameter sensors and services in the fields of chronic disease management, independent aging as well as health and physical fitness. In pervasive healthcare applications, such as home monitoring, the persistence layer (backend) functionality to store and access the data is usually provided by a third party, e.g., some (cloud) service provider. By virtue of their sensitive character, health related data of users need to be protected against unauthorized access and manipulation. However, even if the providers are accountable organizations, i.e., comply fully with applicable laws and regulations governing the collection and use of data, this does not mean that they are not susceptible to incidents. Those can be unplanned data disclosures, malicious break-ins, and sometimes also insider attacks resulting in unauthorized access to potentially sensitive and valuable information. Indeed, the very centralization of information makes providers high value targets for attacks. The best way to counter such threats is to take as a basis for an adversary a malicious insider, i.e., a person employed with the provider administering the system and thus having full access to the infrastructure. Obviously, if even an insider is not able to gather

[1] Carinthia University of Applied Sciences, Department of Medical Engineering, Klagenfurt

enough privacy sensitive information, then an external adversary who breaks into the system won't be able too. Hence, the sine qua non when designing such systems should be the reduction of trust assumptions in the provider and to base privacy on adequate technical protection. The latter issue is reasonable since an actual study shows that more than 50% of all attacks against information systems are conducted by insiders [5].

2. Contribution

In this paper we present a concept and an implementation of a privacy preserving home monitoring system. In this scenario we assume that an individual is a registered user of an information system and regularly sends vital parameters measured by biomedical sensors to this system. The stored vital parameters are monitored by authorized medical staff to support decisions. A key issue within our system – and telemonitoring systems in general - is that the vital parameters, e.g. the ECG of a person, do not contain any person-related information. This means, having access to these raw data does not disclose the related individual. We present the design and implementation of a system that breaks the link between these raw data and person-related information, i.e. pseudonymizes these information, and allows individuals to store and access their data without revealing their identity to the system. Thus, users are fully unobservable, whereas it is guaranteed that only authorized individuals work within the system (see *Figure 1*).

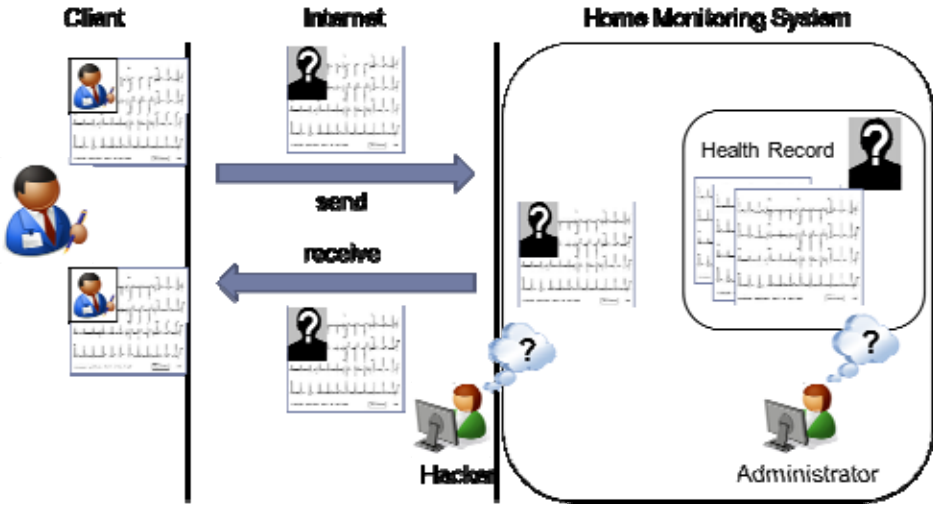

Figure 1: Anonymous access to a home monitoring system.

We suppose that the entire system is hosted by an arbitrary service or cloud provider. In our approach, the provider is solely responsible for the availability and performance of the system. The main issue of the approach is that user's privacy is completely separated from these aforementioned tasks. This means that even an administrator of the provider is not able to misuse data within the system although the administrator has full access to all components of the system. As a consequence, the same arguments hold for any external adversary who can in general gain at most the privileges of an administrator. Commonly the protection against malicious insiders is purely organizational, i.e., non-disclosure agreements. Clearly, such measures cannot prevent misuses but can at least discourage it. The prevention of data misuse by administrator seems to be impossible, when considering the privileges of administrators. But we will show that a combination of so called anonymity techniques can be used to achieve the goal "prevention of misuse". Within the project "Privacy Enhanced Cloud Based Health Tracking" which was funded by the Carinthia University of Applied Sciences we have implemented a privacy preserving home monitoring system which achieves the goal. The components of the security concept are designed in a way that they can be applied to any information system containing person-related sensitive data and hosted by a service

or cloud provider. But before we are going into detail we will discuss security related issues which are necessary to understand our paradigm.

3. Security Issues

It must be emphasized that security aims may be implemented by means of administrative, physical and/or technical safeguards. For instance, the non-disclosure of health data regarding employees can be achieved among others by non-disclosure agreements and content encryption respectively. In the former case it is obviously necessary to trust employees that they will behave according to the non-disclosure agreement. Clearly, a violation might lead to the disclosure of all health data that can be accessed by these employees. Hence, the trustworthiness of employees is absolutely necessary. On the other hand, proper data encryption mechanisms guarantee that solely authorized parties are able to access health data. Since employees of a provider are clearly not involved in a treatment process, they will not be given access to health data and are therefore not authorized. Consequently, employees are not able to misuse these data at all. This example shows that in general technical measures are more adequate than administrative or physical measures, since they reduce the necessary trust to the provider and their employees.

When designing a security concept for a system one has to specify which attacks the system is able to withstand and consequently which adversaries need to be taken into consideration. Usually, systems are focusing on adversaries that are not part of the system and want to attack a system from the outside (external adversaries). Below we define the types of adversaries that are important for our considerations.

- Internal adversaries: These adversaries, such as employees of the provider hosting the information system, conduct attacks mainly against the information system. Although these attacks frequently occur (see [5]) they are often not considered as potential attacks when designing security measures of systems. In general one tries to prevent insider attacks by means of organizational measures such as security policies and/or non-disclosure agreements. The aforementioned measures are necessary but not sufficient, since they can only discourage misuse but not prevent it at all.
- External adversaries: These adversaries are usually considered and can either behave active, i.e. hackers, or passive, i.e. eavesdroppers. In contrast to passive adversaries who are only eavesdropping, active adversaries also manipulate transferred and/or stored data. Insiders can always obtain unauthorized access to health data more easily than external adversaries. Therefore, a reliable security concept needs to address insider attacks at least as carefully as external attacks.

While both of these two types of adversaries can conduct attacks discussed below, insiders can usually mount attacks on a system much easier than external adversaries.

- Attacks on the client component: The main focus of these attacks is to steal user's authentication credentials (e.g., username/password) or medical data accessed by a user via the user's client. Methods to launch these attacks can, for instance, be phishing, pharming and using several types of malware, e.g., Trojan horses, key loggers, etc., running on the user's client, i.e. the user's smartphone.
- Attacks on the transmission channel: The goals of attacks on the transmission channel are the same as above, but the risk is potentially higher since data of many different users may be stolen. The methods of these attacks are, however, different and may include, for instance, sniffing and person-in-the-middle attacks.
- Attacks on the information system: The main focus of these attacks is to reduce the availability of the system, and to manipulate or steal data. The first type of attack can be

accomplished, for instance, by flooding attacks to achieve denial of service (DoS). The latter attacks typically use exploits for components of the information system, or are launched by insiders who abuse their privileges by, for example, copying files from the storage or stealing a copy of a database.

With respect to data theft, it is usually much easier to attack a client and to steal the data available to the client than attacking the information system, although attacking the information system may enable access to the data of the entire system.

4. Methods

In this section we firstly define three requirements that are necessary when considering internal and external adversaries and their impact on the protection of the patient's privacy. Secondly we briefly present technical methods which are used in the implementation of our project to realize the requirements.

4. 1. Requirements

- Unlinkability of patients and their medical data: Any person who even has access to the entire system but is not explicitly granted access rights, cannot link medical data to the patient. This means that a single user is explicitly granted for one action if the user is the initiator of the action or if the user obtains a token from a granted user to perform the action. The unlinkability guarantees that it is not possible to determine the links between patients and their medical data. Hence, even if data are stolen or data leakage as a failure of the provider occurs, medical data cannot be linked uniquely to patients, and consequently patient's privacy cannot be compromised. We note that this requirement is not trivial since information systems in general use databases to manage data and thus contain explicit links between patients and their data. Hence a database administrator has full access to all data stored in the system. Even if unlinkability is realized within the system a standard authentication would counteracted the requirement. This is due to the fact that all actions performed could be linked to the authenticated user. Consequently, an insider could easily figure out the relation between administrative and medical data. Thus, we need the two subsequent requirements.
- Non-identification of users: A user, e.g., a patient, browsing his/her health data, can never be identified by any observer of the system (insiders or external parties). This includes the authentication and every subsequent action within the system.
- Unlinkability of actions within the system: Unlinkability means that it is infeasible to link different actions of a user within the system. This aspect in combination with the aforementioned requirement prevents profiling of users. Let us assume that we have linkability of actions within the system but the corresponding patient cannot be identified. By observing the system, it is possible to gradually figure out parts of patient's health data. The more complete the set of data obtained, the higher the probability of identifying the patient. Note that if only a subset of the health data is known to correspond to a specific patient, this is also true for the entire data. However, by satisfying unlinkability of actions, this information leakage no longer exists.

4. 2. Realization of the Requirements

As a consequence of the last section we conclude that data within the system must not to be linked to patients and that authenticating users must not be identified. This can be covered by applying the

following three techniques: data anonymity, anonymous authentication and communication anonymity.

- Data Anonymity: This concept enables people to store and access data in a structured way using the infrastructure of a (potentially untrusted) provider, so that solely qualified persons (the "owners" of data and people who were explicitly granted access rights) are able to determine which subset of data belong to them and are able to access them. A system based on this concept guarantees provable security based on standard cryptographic assumptions. One main issue for the design of the concept was a minimal impact on the efficiency of the system. In particular, using hierarchical data models this implies a constant number of additional cryptographic operations for each relationship between two object types. For a detailed description of this concept and the mechanism for sharing medical data we refer the reader to [11].

Implementation aspects: In order to hide the complexity of the implementation from application developers we have implemented a so called Pseudonymity-API (see Figure 2) that consists of a client and a server component. The client component realizes all cryptographic operations that are necessary to access user's data and data that was granted to the user (shared with this user). The server component, which is represented by a set of SOAP-web services, is solely responsible for checking whether the operation is authorized and for the execution of the desired action. The concept for authorization will be described the following subsections.

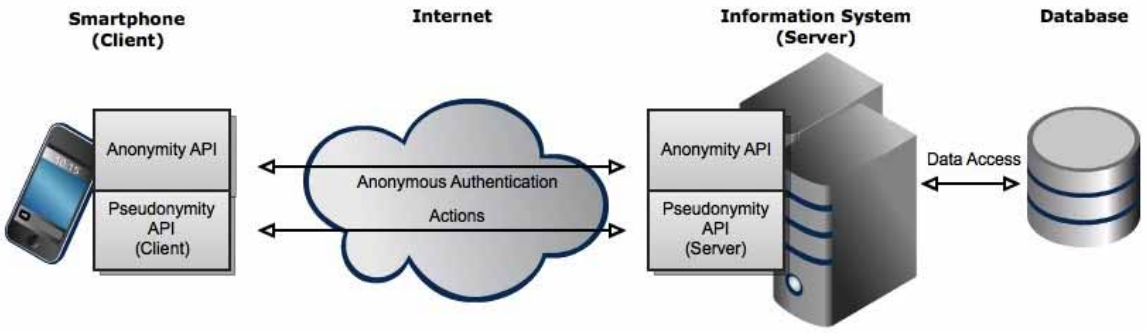

Figure 2: Schematic overview of the system architecture

- Anonymous Authentication: In contrast to conventional authentication methods, which establish a unique identification of the authenticating user, anonymous authentication enables users to authenticate without disclosing their own identity to the verifying party. There are many different techniques for anonymous authentication in the literature [1, 2, 8, 12]. In general, a user in an anonymous authentication protocol is able to prove membership in a group of authorized users to a verifier (the information system), whereas the verifier does not obtain any information on the actual identity of the authenticating user. For instance, anonymous authentication from public-key encryption as proposed in [8, 10] can be employed efficiently with moderate implementation effort. Loosely spoken, this can be realized by means of parallelization of a standard challenge-response protocol based on public-key encryption. This means that the system encrypts a randomly chosen string using the public keys of a set of users (the anonymity set) and sends this sequence of ciphertexts to the anonymous user. If the anonymous user is able to decrypt one of these ciphertexts and provides the same strings as the one sent by the system, the system is guaranteed that the user knows one of the private keys corresponding to the users in the anonymity set. However, the system cannot determine the identity of the user and the user is anonymous within the anonymity set.

Implementation aspects: Within the project we have implemented three methods for anonymous authentication. In particular, we have implemented anonymous authentication from (probabilistic) public key encryption [8,9] the ring identification scheme of [7]. In order to enable comfortable integration in future projects, all authentication methods are accessible via a unified application programming interface (API) which hides the complex implementation details from the application developers.

Nevertheless they have the opportunity to control the level of anonymity provided by the protocols by means of XML-based configuration files, e.g. the size of the anonymity set. This component realizing the aforementioned functionality is denoted by Anonymity-API (see Figure 1) within the project.

- Anonymous Communication: Mechanisms that provide anonymity and unlinkability of messages sent over a communication channel are denoted as anonymous communication techniques and have been studied intensively in recent years [6]. There are several implementations available which are realized as overlay networks and can be used for Internet communication without any implementation effort. These anonymous communication channels provide anonymity of users against eavesdroppers and curious communication partners who are no longer able to identify users by their messages. Anonymity, especially against curious communication partners, can be preserved if electronic interaction does not rely on additional identifying information at higher network layers, i.e., the application layer. For example, a user who queries a public web page using an anonymous communication channel may remove all identifying information from higher network layers, and thus will stay anonymous. The efficiency of this method depends highly on the degree of anonymity, e.g., the number of mix nodes, but it implies latencies in the communication.
- Anonymous yet Authorized Transactions: When single actions within the information system need to be unlinkable, a naive but very inefficient approach would be to perform independent anonymous authentications for every single action. A far more efficient way to achieve unlinkability is to combine anonymous authentication with unlinkable transactions as proposed in [9]. After an initial anonymous authentication, the user receives a ticket which can be linked to neither the authentication nor the user, but can be used to authorize a single action in the system. Every showing of a ticket prompts issuing a new ticket, whereas this ticket can be shown in a way that it is unlinkable to either the user or its issuing. Combination of anonymous communication, anonymous authentication and anonymous yet authorized transactions allows users to work anonymously but with authorization and unlinkability in the system.

Implementation aspects: During the anonymous authentication, the client creates a so called blinded ticket. A ticket is realized as a XML-structure that among others contains a unique random number to prevent double spending of tickets in the system. This means that is guaranteed that every ticket can only be used once. In case of a successful authentication, the server signs the ticket and returns it to the client. A signed ticket authorizes the client to conduct an action with the system. But when the server is provided the same ticket during issuing and showing, then the server is able to link them by means of their serial number. This would of course destroy the desired unlinkability. A very efficient way to overcome this problem is to use a blind signature scheme [3,4]. This means that the client randomizes the ticket before sending it to the server. Hence it is guaranteed that the server does not obtain any information about the ticket and as a consequence of the random number. The key aspect of this approach is that the server signs the randomized ticket and the client is able to remove the randomization from the signed ticket. As a consequence, the client holds a valid signature for the original ticket. Hence, the server has produced a valid ticket which the server has never seen during issuing and thus unlinkability is realized. In order to further illustrate the interplay of the aforementioned methods we present a typical workflow from the client's

perspective. In this scenario we assume that an individual periodically uses medical sensors to acquire vital parameters that are sent to a central information system via a mobile device.

1. The individual attaches the sensor to the body and starts the client application.
2. The client application starts the anonymous authentication (AA) with the server. Then the client sends a blinded ticket and receives a blindly signed ticket.
3. The client unblinds the blindly signed ticket and holds a valid ticket.
4. This ticket is used to create a new pseudonymized measurement ($Action_1$ = Insert measurement) for the authorized individual within the system and a new ticket is issued by the server.
5. Sensor data collected ($Action_2$ = Insert data) by the client application are sent to the server in combination with a valid ticket.
6. At the end of the measurement the client need not to close the session since the client does not share any state with the server, i.e. the connection is stateless.
7. The ticket received at the end of the last action is discarded.

Table 1. Schematic workflow.

Step	Client	Server
2	AA, Blind($Ticket_1$) →	Successful Authentication?
		← Sig(Blind($Ticket_1$))
3	Sig($Ticket_1$) = Unblind(Sig(Blind($Ticket_1$)))	
4	$Action_1$, Sig($Ticket_1$), Blind($Ticket_2$) →	$Ticket_1$ valid? Perform $Action_1$
		← Sig(Blind($Ticket_2$))
3	Sig($Ticket_2$) = Unblind(Sig(Blind($Ticket_2$)))	
4	$Action_2$, Sig($Ticket_2$), Blind($Ticket_3$) →	$Ticket_2$ valid? Perform $Action_2$
		← Sig(Blind($Ticket_3$))
	Etc.	

5. Conclusion

In this paper we have presented a novel system to store person-related sensitive data without fear of misuse anymore even though the system is hosted by a provider that is potentially not fully trustworthy. This assumption is realistic since more than 50% of all attacks against information systems are conducted by insiders. Hence we have focused on administrators, since they can be considered as the most powerful adversaries. Our paradigm is that if it is possible to prevent misuse by administrators, then misuse of other internal or external adversaries can also be prevented. The security concept was realized by combining anonymity techniques that hide all links between users and their data. Furthermore, we could show that the impact of the techniques on the performance of the system is minimal. As a consequence we conclude that the security concept can be applied to all systems that store person-related information to protect patient's privacy without any negative impact on the entire system.

6. References

[1] Ateniese G, Camenisch J, Joye M, Tsudik G. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In Proc. of CRYPTO 2000. LNCS, vol. 1880, pp. 255-270. Springer- Verlag, 2000.

[2] Boneh D, Boyen X, Shacham H. Short Group Signatures. In Proc. of CRYPTO 2004. LNCS, vol. 3152, pp. 41-55. Springer-Verlag, 2004.

[3] Boldyreva A. Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme. In PKC 2003, vol- ume 2567 of LNCS, pp. 31–46. Springer.

[4] Chaum D. Blind Signatures for Untraceable Payments. In CRYPTO'82, pp. 199–203. Plemum Press.

[5] Computer Security Institute (CSI). Computer Crime and Security Survey 2007.
http://www.gocsi.com/forms/csi survey.jhtml

[6] Danezis G, Diaz C. A Survey of Anonymous Communication Channels. Technical Report MSRTR-2008-35, Microsoft Research, 2008.

[7] Persiano, P., Visconti, I. A secure and private system for subscription-based remote services. ACM Trans. Inf. Syst. Secur. 6(4): pages 472-500, 2003.

[8] Slamanig D. Anonymous Authentication From Public-Key Encryption Revisited (Extended Abstract). In Proc. of CMS 2011, pp. 247-249, LNCS vol. 7025, Springer-Verlag, 2011.

[9] Slamanig D, Rass S. Anonymous But Authorized Transactions Supporting Selective Traceability. In Proc. of SECRYPT 2010, IEEE Communications Society, 2010.

[10] Slamanig D, Schartner P, Stingl C. Practical Traceable Anonymous Identification. In Proc. of SECRYPT 2009, pp 225-232. INSTICC Press, 2009.

[11] Stingl C, Slamanig D. Health Records and the Cloud Computing Paradigm from a Privacy Perspective. Journal of Healthcare Engineering, 2(4):487-508, 2011.

[12] Teranishi I, Sako K. k-Times Anonymous Authentication with a Constant Proving Cost. In Proc. of Public-Key Cryptography 2006. LNCS, vol. 3958, pp 525-542. Springer-Verlag, 2006.

[13] Varshney, U. (2003) Pervasive Healthcare. IEEE Computer, 36, 138–140.

Corresponding Author:

Christian Stingl
FH Kärnten
Villacherstraße 1
9800 Spittal/Drau, Austria