Multi-Factor Authentication in Telemedicine Systems

Dayana P. B. Spagnuelo, Jean E. Martina, Ricardo F. Custódio
Laboratório de Segurança em Computação
Departamento de Informática e de Estatística
Universidade Federal de Santa Catarina
Florianópolis, Brazil
{dayspagnuelo,everson,custodio}@inf.ufsc.br

Rafael Andrade
Instituto Nacional de Convergência Digital
Departamento de Informática e de Estatística
Universidade Federal de Santa Catarina
Florianópolis, Brazil
andrade@inf.ufsc.br

***Abstract*—Telemedicine systems require authentication services that are strong enough to ensure data confidentiality and privacy, and flexible to meet the needs of health professionals and patients. The focus of this work is the authentication process. We propose an authentication service for telemedicine technologies based on web services. This service makes use of scalable authentication methods based on two-factor authentication mechanisms. Its main characteristics are: flexibility of configuration for the authentication mechanisms, as well as the use of a robust system for recording events. In this paper we deal with the engineering requirements of the security system and the details of its implementation. We also discuss the efficacy and ease of use of different authentication methods.**

Keywords*-*Multi-factor Authentication; Telemedicine

I. INTRODUCTION

The increasing development in technology has enabled the use of electronic media for communication and the execution of services. In this context, information systems present viable solutions too many types of problems, including social ones. Similarly, telemedicine and e-health environments facilitate access to health services to people redas well as they simplify the use of technology by health care professionals [1].

However, this growth does not only bring benefits, it also exposes the fragility that many systems have in relation to information security. The authentication process, for example, can be responsible for many of the vulnerabilities and errors if it is not properly applied. Today, we still see a scenario where most systems use a login and password model-based authentication. This tends to be weak, given the current technological advances and capabilities of intruders. One of the main vulnerabilities of this model is identity theft, which may occur by the guessing or the stealing of a user's credentials. These types of attacks are fairly common since users are usually not aware of the existing threats.

The risk of such threats increases when the information in the system is private and the authentication model is weak. Given the sensitivity of the information in telemedicine systems, identity theft cannot only cause information leakages, but can also lead to serious or damaging circumstances that can harm the doctor/patient relationship. Thus, the use of a more efficient authentication with stronger methods becomes a way to increase the overall security. An important issue is that these methods must not make the access of health record and patient care more difficult.

Moreover, strong authentication methods are commonly related with the use of specific cryptographic devices [1][2][3][4][5]. Such devices are linked to specialized hardware to allow their use. These types of devices have low interoperability. In other words, they have a high impact on mobility and usability of a web system. Within the virtual environment of telemedicine there is still another problem: a doctor should be able to access medical systems from anywhere at any time because any impediment by the system can mean a life-threatening situation. Thus, the authentication model should be strong enough to guarantee security, but should not rely on devices that affect mobility and usability for the sake of efficiency.

This paper proposes a new authentication model that uses modular and flexible methods with a two-factor authentication as a secure web service. The proposal is based on the real needs of the Santa Catarina Integrated Telemedicine and Telehealth System (STT/SC, in Portuguese), a project of the Federal University of Santa Catarina (UFSC, in Portuguese) in partnership with the Santa Catarina State Health Office (SES/SC, in Portuguese). Within the proposal, the STT/SC integrates various methods of the two-factor authentication based on the possession of auxiliary devices, such as a cellphone, or physical presence in a particular geographical location by using land-line systems. An important feature in our proposed system is the flexibility of the authentication process by using a list of acceptable mechanisms.

The remainder of this paper is organized as follows: a brief discussion about the Integrated Telemedicine and Telehealth System is presented in Section II. Section III has an inventory of related work with an analysis of the adequacy of each work in regard to the subject. Sections IV and V describe the construction stages of the proposed model, from inception to completion. The implementation of the model is presented in Section VI. The authentication methods used in this work are presented in Section VII. Technical analysis of the authentication methods and the proposed model are presented in Section VIII. Finally, Section IX contains the conclusion and suggestions for future work.

II. Integrated Telemedicine and Telehealth System

The increase of information technology development in recent years has enhanced virtualization of various types of services. Among these types, the ones that deserve special attention are telematic environments. Telematic environments present viable solutions to many types of problems, including social ones like public health, citizenship, etc. [1]

As part of solutions to social problems The Catarinense Telemedicine Network (acronym for RCTM, in Portuguese) [6] is an example. Aiming to facilitate the access to tests of medium and high complexity in the country side, UFSC and SES/SC conceived the RCTM.

The main purpose of the RCTM was to extend the the availability of medical equipment such as electrocardiograms, computer tomography and magnetic resonance to smaller cities. A pilot project was created in 2005, which began by connecting two cities in the interior of Santa Catarina with the state capital, Florianópolis [7].

The STT/SC is a virtual environment to support medicine, which aims to facilitate access to specific health services to people who could not have them in the conventional way. The main problems people face are physical disabilities, geographical distance, and financial difficulties. [8]. The STT/SC makes available over the web, images, signals and medical reports generated from accredited health institutions distributed throughout the state of Santa Catarina - Brazil. Currently, the system has an average of 50,000 examinations per month and has more than 2.5 million examinations and images stored since 2005.

While all this growth brought benefits, it also exposed weaknesses that the model has in relation to information security. The high sensitivity of the information may raise the risk of exposing them to attacks, damage, or compromise. Fraud and forgeries on medical diagnoses and altered entries are serious threats, as they can put people's lives in danger.

Identity theft is a common attack in this type of system. It is closely linked to the authentication process. For example, if the authentication process is weak and allow the use of short passwords, the chances of such an attack increases. Therefore, the adoption of a more efficient and stronger authentication system is a simple way to increase the overall security.

III. Related Work

Security in medical systems has gained the attention of governments, healthcare providers, research centers and, consequently, has been a recurring theme in the publications. Most proposals to the authentication process use a second factor of authentication and can be separated into two major groups: those based on digital certificates, and those based on biometrics.

Martínez et al. [1] propose an interoperable security design capable of providing secure authentication and authorization based on digital certificates. The proposal comes from a study of business models for applications of e-government and e-health, which often have the same needs when it comes to security. The model is based on authentication and authorization web services to ensure interoperability between different systems, and it uses digital certificates to ensure the user's identity.

With similar goals, Ahn and Shin [2] proposed a framework for authentication based on cryptographic tokens that aims to provide more security to protect the data of this type of system. The focus of this work is the design of a framework that is able to strongly authenticate a user in different ways (through the use of signatures, passwords or biometrics) and secure access to its data. In this model there is an effort to abstract the different technologies of smart tokens from the authentication layer, allowing the interoperability between several different services related to e-health systems.

Still following the same line, Al-Nayadi and Abawajy [3] propose the design and implementation of an architecture for authentication and authorization also based on digital certificates that aims to integrate different e-health systems maintained by various institutions in order to centralize patient's data. This model is based on the fact that each system has an Identity Certification Authority (ICA) that distributes and signs certificates of its users. Each ICA in the network trusts in the others and performs authentication to remote systems through verification of a certificate. The authorization is based on the attributes of each certificate.

With a different approach, Han et al. [4] proposes a framework for authentication and authorization based on fingerprints. The framework is intended to enhance the authorization of e-health services and to ensure access for their users. Authentication is based on fingerprints with a Personal Identification Number (PIN).

In a line similar of Han et al. [4], Garson and Adams [5] propose a system design for e-hospital security and privacy. Their work presented an authentication model based on fingerprint and RFID. In addition to user authentication, the proposal prevents data from leaving the hospital by blocking user authentication from outside the building. Not only concerned with the authentication process, the authors also present a new encryption method that seeks to prevent the system from theft, loss and copies of documents.

The papers presented above show a concern for interoperability between systems, and are mostly based on digital certificates. In such models is necessary to have smart card readers to perform basic operations. Such readers have low interoperability and make the use of the system in mobile devices more difficult. Therefore, the use of readers affects one of the main characteristics of a web system: mobility.

One alternative for solving the problem with the readers is to use the software certificate (also cited in the presented works) which allows the model to be interoperable and mobile, but also reduces the level of security that can be provided. Depending on the way which the certificates are stored, the required effort to attack the model is similar to attack a model that uses a simple password.

Other papers presented follow a line using biometrics as the second factor of authentication. The reading of a fingerprint is made by a specific hardware, which has the same problems of the smart card readers. Moreover, they often don't have compatibility with each other. In practice, this approach is even worse than the model based on digital certificates, since the user (patient/doctor) is forced to use a computer that meets all the installation requirements of the reader. Furthermore, this is a technique that has false positives and negatives rates higher than acceptable.

Our proposal is based on the strengths of the papers presented, and seeks to correct the problems identified and provides a better adaptation to the telemedicine systems. To achieve the goals of creating a new two-factor authentication process, we did an examination of requirements using the STT/SC as a case study. The process of construction of our proposal is presented in the following sections.

IV. Case study and requirements

To better understand the requirements of an authentication model looking at the medical context, we conducted a study about the use of this type of system using the STT/SC. Actual usage scenarios showed us that there are cases where users (usually medical specialists that provide reports) need to access the system from a computer outside the hospital, for example, when they are traveling. Thus, the first requirement is to maintain the mobility of the web system. The authentication service has to cope with that.

It is assumed that such a system should not block the work of a doctor, because this may put patients live at risk. Therefore, a user should be able to access the telemedicine system from any computer, tablet or mobile phone, since it has an Internet connection. Because of this requirement, the adoption of authentication methods that require cryptographic hardware, and that need specific readers, such as smart cards and biometrics, is unfeasible.

Moreover, it was noticed that there were cases where access to the system was urgent, and in these cases, the user should not have their access prevented. So in the same way that the device used to access the system cannot be limiting, the devices that are used as second factor of authentication should also not restrict access. And this is the second requirement of authentication model: flexibility.

Cryptographic tokens are very specific devices and can be easily lost or forgotten. Thus, we avoid the use of specific hardware and try to replace them with other devices of daily use, like cell phones, which normally are carried by users. Furthermore, the flexibility of the services requirements also requires a user to be able to access the system even when they are not in possession of any device required. The model should provide this kind of situation and offer alternatives.

V. Proposal

Besides the requirements presented in the previous section, we must also take into account requirements common to the authentication models. For that, we built the first prototype. This was a dedicated library responsible only for the authentication process and to make available a set of authentication methods, allowing the system to decide the way that these methods will be used. In order to allow STT/SC to decide witch method use to authenticate the users, the library had to be written in PHP [9], same programming language of STT/SC.

All authentication methods involved in this model are used as a second factor of authentication, i.e., in our proposal the user authenticates exactly the same way they do today and, in a second step, gives some information to prove that he has possession of certain unique device. The authentication methods used were selected in such a way that they would not change the characteristic of mobility of STT/SC. This was done using common devices, such as smartphones and landlines instead of specific cryptographic tokens. Furthermore, we do not use methods of authentication that depend on token readers, such as those based on smart cards and biometrics.

But even in this scenario, we cannot assume that all users of the system have the required device during authentication. To meet the requirement of flexibility, it was necessary to provide the possibility of changing the authentication method to an alternative (that depends on another type of device), which is also provided by the library. Therefore, the model preserves the characteristics of mobility and flexibility of the system, while it does not prevent access to its users as provided in the requirements.

The scenario presented above meets the requirements and fits well in cases where the user is not with his smartphone, or it is out of battery. However, it's not well suited to cases where the user makes constant access to the system but does not have such a device. This implies that one more process is needed to change the authentication method for each access attempt. To avoid frustrated users who might try to bypass the authentication process, a new model was proposed.

A new strategy was then conceived: each user has a list of authentication methods that are enabled. Thus, the user keeps disabled methods that uses devices which he does not have, and prevents cases as described previously. With the inclusion of user's data and the different combinations of authentication methods that the system may possess, this new model began to store a much larger amount of information. No longer behaving like a library, it became an authentication service. Now has its own context and independence from the system that uses it.

VI. Implementation

The proposed model was implemented as a secure authentication web service using the standard remote procedure call (RPC). In this implementation, we used the XML-RPC, which is a simple pattern of RPC that allows communication between systems of different architectures and languages. This is possible because the communication is done via HTTPS and the encoding of calls is done with XML, two standards quite solid and disseminated.

Since the goal of the service is only to authenticate users, we opted for a simpler protocol. Thus, we have avoided transforming the authentication (which only carries the credentials of a user) into a complex and long procedure.

The use of a mutually authenticated HTTPS was necessary to prevent the user's credentials transit in unprotected networks upon communication between the STT/SC and the web service.

The web service has an interface that centralizes all authentication methods available, called Authenticator. Each call to one of the methods of the Authenticator is actually the process of authenticating a user. The data of these users are maintained by the web service in a local database. Thus, it was necessary to introduce an administrative interface to the service for the maintenance of users. This interface is called ServiceManager and it takes care of all the maintenance of data related to users. These include the maintenance of lists of authentication methods enabled for each user and the system authentication policy.

The policy is a form of combining the authentication methods and its level of priority. In other words, a user will authenticate with the method that the system considers the most priority. The list of enabled authentication methods defines which methods the user can use, i.e., if a user does not have a smartphone, then all authentication methods that rely on such a device are disabled.

With this approach it was possible to automate the change of the authentication method. The web service uses the policy and the list of enabled methods of the user, and with this information it mounts a third list with the intersection of both, ordered in the same way that the policy. It is still possible to analyze if the methods that depend on the internet are online, avoiding attempts that would result in failure.

The Figure 1 describes an authentication process in the telemedicine system integrated with the authentication service. In the first step, the user gives his credentials to the system. In the second step, the system pass the credentials to the authentication service, so that can verify it (step 3). If the verification succeeds the authentication service combines the list of enabled methods of the user and the policy to make a third list with the intersection of both (step 4). In other words, the third list contains the methods that the user is able to use (the user has the required device) and the system supports, sorted by the priority of the policy. In the step 5, the authentication service requires to the telemedicine system to use the priority method, in this case Phone call. In the step 6, the system requires to the user to use the Phone call method. In the step 7, the user makes the call, concluding the authentication process. In this case the system avoided two methods that user cannot use to authenticate himself because he does not have the required devices.

In this approach, the change of the authentication method is a sporadic process, where the user says he is not in possession of any of the requested devices and bypasses the second check. Such cases are provisioned in the service, since flexibility is a requirement, but are recorded in a database of logs and accounted for by user. These data are available to the system, so it can use the records in the way it wants, the system can allow a specific number of bypasses, or even block access to a user if it detects a possible attack.

In this new model, the only actor existent is the telemedicine system. This emphasizes the separation between the layers of authentication and authorization. The service does not worry about which user is performing the operation, since it has been authorized by the STT/SC. Each of the three specific requirements has been addressed in this model. Mobility and flexibility are characteristics inherited from the first model and the impact on usability is reduced by automating the change of authentication methods.

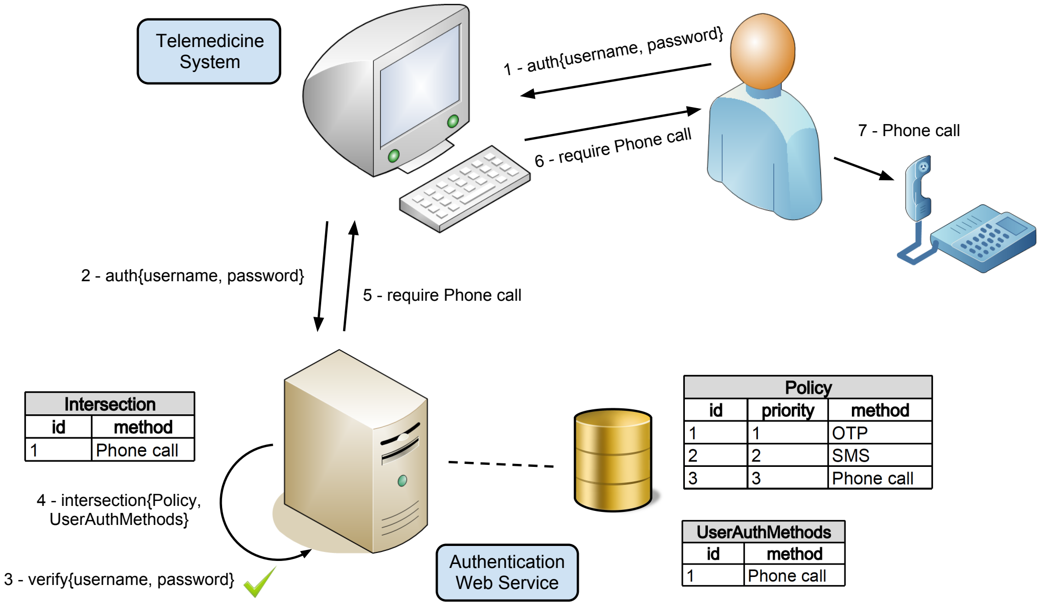
VII. Authentication Methods

The methods used in this work are all authentication factors based on something the user possesses. According to Cheng [10] in multi-factor authentication system, each factor must be in possession only of the user and an attacker should not be able to access it easily.

Our proposal tries to use personal devices, which are usually carried all the time by users, thus making any attempted attack easily noticeable. We avoid the use of specific cryptographic tokens because they are not common objects for users of medical systems, and they usually have low interoperability, besides that, they are very expensive. There are three methods chosen to be developed in this research: One-Time Password, SMS and phone calls.

As it's name suggests One-Time Passwords [11] are passwords that are used only once, generated from a previously shared seed. According to Haller et al. [11], the process of generating OTPs should have two entities: a generator and a validation server. The generator is usually a device of personal use, in this work we use a smartphone with an application developed based on Google Authenticator to generate passwords [12].

The SMS (Short Message Service) based method is an Out of band authentication method. According to FFIEC [13] an Out of band, authentication can be defined as an


Telemedicine System
1 - auth{username, password}
6 - require Phone call
7 - Phone call
2 - auth{username, password}
5 - require Phone call
4 - intersection{Policy, UserAuthMethods}
3 - verify{username, password}
Authentication Web Service

Intersection	
id	method
1	Phone call

Policy		
id	priority	method
1	1	OTP
2	2	SMS
3	3	Phone call

UserAuthMethods	
id	method
1	Phone call

Figure 1: Authentication Service

authentication technique that allows the identity of the user who originated the transaction to be verified through another channel from the one used to start the operation. This method consists in sending a random alphanumeric password via SMS to the user's cellphone. When the user receives the password it is used as a second factor of authentication to prove the possession of the phone line (cellphone).

The phone calls based authentication method is also Out of band and consists of recording the caller ID of a call made by the user to one of the allowed phones in the telemedicine system. The allowed phones are VoIP phones that run a script that gets the caller ID when a call is received and ends it. The script also records via the web service authentication the obtained caller ID. When the web service receives an ID it identifies the user who owns that number and records the time of the call. To authenticate, the user enters his username and password (first factor) and in a second stage informs that already made the call. The service verifies that the information is true and checks whether the operation has not expired. The expiration time of a call and the allowed class of the phone (fixed or mobile) is defined by the telemedicine system. The fact that the user has executed a call to one of authorized numbers is a proof of possession of the second factor, in this case access to a cellphone or landline.

VIII. Analysis

This session presents an analysis on security and usability of each authentication method. The analysis is based on their characteristics, as well as other general analysis of the proposed model.

The technical analysis of the authentication methods is based on the Eletronic Authentication Guideline [14] of NIST - USA (National Institute of Standards and Technology). The guideline contains recomendation for remote authentication over open networks, like internet. The technical guidance supplements OMB guidance, that defines four levels of assurance (Level 1 to 4) in terms of the consequences of the authentication errors and misuse of credentials. The NIST guidance specific technical requirements for each of the four levels of assurance in five areas. In this analysis we consider only the area of tokens.

A. Analysis of authentication methods

In our proposal, One-Time Passwords uses smartphones as passwords generators. Because they are personal devices, users already are familiar with their interfaces and their forms of interaction. Because of that, this model does not cause a great impact on the usability of STT/SC. It does not require a user to interact with unknown cryptographic devices, which are difficult to use sometimes.

One-Time Passwords are quite common and well accepted in banking environments. Similarly to these environments, operations in medical systems can also be considered of high risk. Thus, the use of OTP in a system like that is justified.

According to FFIEC [13] passwords generators are secure for the time-sensitive nature or synchronized authentication. Also according to FFIEC [13], randomness, unpredictability, and uniqueness of the OTPs substantially increase the difficulty of an attacker to obtain a password. Moreover, the process of generating an OTP is offline and cyber attacks could only be realized when the password is already used. Whereas after its use, OTPs are invalidated, the chances of success of such an attack are quite low.

The attack by guessing also has a very small chance of success too. According to M'Raihi et al. 2005 [15] the probability of success of a guessing is:

$$Sec = \frac{s.v}{10^{Digit}}$$

The probability is a function of size s of the window provided by resynchronization method, the quantity v of attempts that an attacker can do before being blocked and the amount of digits that the OTP has.

Because smartphones are of a very personal nature, physical attacks like theft would be easily perceived. Unlike cyber attacks, robberies and thieves of physical devices are not usually discrete and the user knowing the attack and its consequences, may take appropriate action to mitigate it, such as cancellation or temporary blocking his account.

Smartphones are sophisticated and expensive equipment. Thus, the SMS authentication is an alternative that is more far-reaching, in regards to smartphones. According to ANATEL (Brazilian Agency of Telecommunications) [16] the amount of mobile accounts in May 2012 in Brazil is more than 254 million, a sum greater than the population which according to the population census of 2010 [17] is about 190 million. And one of the advantages of this model is the fact that most users already have cellphone and already are familiar with the SMS system too.

According to Alzomai et al. [18] the main advantage of using an SMS-based model is that the messages are sent through the mobile phone network, which is separate and independent from the internet. According to Jøsang et al. 2007 [19] security schemes like this are based on the assumption that it is difficult for an attacker to steal a user's cellphone or to attack the mobile network. The chances of success of an attack by guessing are similar to those in previous model since the characteristic of randomness is also present in this model.

However, the SMS model has a high cost for the STT/SC. Each authentication requires sending a message and, the cost of maintaining the model increases with the number of accesses. As an alternative to this high cost was presented the third model, based on caller ID.

The model based on caller ID has the same features of the SMS model: it uses devices that users already have and know; it uses an independent network and the security level is also similar. The advantage of this model over SMS is that it's free for the STT/SC and can also be a free method for users, depending on the contract plan with the carrier.

B. Analysis of the Model

The security level of the model is very tied to the level of security provided by each of the methods that the STT/SC uses. According to the technical guidance of NIST, basic OTP generators can be considered a Single-factor OTP device. These types of device can reach 2 in the level of assurance. Because our application uses a password to block access to the OTP generator, it can be considered a Multi-factor OTP device – since the password is something that the user knows, and the OTP proves that the user has the generator device – reaching 3 in the level of assurance.

The SMS-based method can be considered an Out of band token, it means that is uniquely addressable and supports communication over a channel that is separate from the primary channel for authentication. According to the technical guidance of NIST, these types of tokens can reach 2 in the level of assurance. Likely the OTP device, this token can reach the level 3, but only in cases where the user becomes aware of the existents threats and configures his cellphone to use some kind of password to block it.

The caller ID based method does not fit the tokens classification of NIST because it does not use any password in the process. Despite that, it can be also considered an Out of band token because of its similarity with the SMS-based method, and reach a level of security close to the provided by the level of assurance 2.

However, the methods presented are only one of the factors used in the authentication process. According to Di Pietro et al. [20], an attacker who successfully break some of the methods presented, still would not have access to the STT/SC without knowing the user's login credentials. Furthermore, our proposal gives the system the freedom to define how to use the methods, so that it can use more than one at a time, increasing the difficulty of an attack.

The authentication process is completely separated from the business rules of STT/SC. This means that the web service can be used in security critical areas of the system, not just the login. By increasing the number of factors used in an authentication or the amount of sessions that require authentication, it increases the level of security. Of course, overuse may lose usability. According to Alzomai et al. [18], when users encounter frustrating security tasks, they tend to avoid them or ignore them. Thus the flexibility of the model is shown as an important feature because it allows the system to define where and how it wants to use the web service.

IX. Conclusion and Future Work

This paper presented a new authentication model based on secure web service. This model is geared to the security needs of STT/SC, which contains high sensitive information. In order to fit the main requirements of this type of system, the model uses multi-factor authentication. It also provides a set of authentication methods that can be combined to provide greater flexibility and reliability to the process.

Our model operates as a web service and therefore does not imposes some technological limitations, such as the implementation language. It also does not require the use of specific cryptographic tokens. For that it can be easily

ISBN: 978-1-61208-252-3

integrated into various systems. Its high interoperability and its efficiency could be demonstrated by a prototype of the service. The proposal is fully implemented and integrated into a telemedicine system in operation in all the cities of the state of Santa Catarina and used by more than 6,000 users (doctors, nurses and technicians).

Our analysis shows that, the proposed model fits well to telemedicine systems. It provides flexibility and can be molded in order to meet the needs of such systems. In this analysis, we included the main features of STT/SC, which are flexible enough to avoid interposition between the system and the doctor-patient relationship. Its high interoperability and system event log robustness is also demonstrated.

Besisdes that, our analysis also demonstrates a increase in the security of the authentication process of the STT/SC. That can be demonstrated by the levels of assurance, which reaches 1 when the system uses only the simple password based method, and reaches up to 3 with our proposal.

The analysis also demonstrated that the model covers the major attacks involving the authentication process. In our model we can provide authentication properties not present in most other models, such as guaranteeing geographical authentication, based on the use of landline system.

In order to improve the authentication service offered it is suggested to add new authentication methods. Our next steps in improvement of authentication mechanisms are the inclusion of an identity based encryption to allow authentication of users not registered in the system. We also plan the implementation of a system for sending one-time password (OTP) via dial tones, which makes the OTP method even more affordable.

X. Acknowledgement

The authors would like to thank Coordenação de Aperfeiçoamento de Pessoal de Nível Superior for supporting this work and Laboratório de Segurança em Computação for assisting this work and helping to improve it from the very beginning.

References

[1] J.-F. Martínez, V. Hernández, M.-A. Valero, A. Gómez, E. Pérez, I. Pau, H. Álvarez, and L. Vadillo, "Security services provision for telematic services at the knowledge and information society," in *Proceedings of the 2007 Euro American conference on Telematics and information systems*. New York, NY, USA: ACM, 2007, pp. 41:1–41:7.

[2] G.-J. Ahn and D. Shin, "Towards scalable authentication in health services," in *WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on*, 2002, pp. 83 – 88.

[3] F. Al-Nayadi and J. Abawajy, "An authentication framework for e-health systems," in *Signal Processing and Information Technology, 2007 IEEE International Symposium on*, Dec. 2007, pp. 616 –620.

[4] S. Han, G. Skinner, V. Potdar, and E. Chang, "A framework of authentication and authorization for e-health services," ser. SWS '06. New York, NY, USA: ACM, 2006, pp. 105–106.

[5] K. Garson and C. Adams, "Security and privacy system architecture for an e-hospital environment," ser. IDtrust '08. New York, NY, USA: ACM, 2008, pp. 122–130.

[6] Cyclops, "Sistema catarinense de telemedicina e telessaúde," https://www.telemedicina.ufsc.br/rctm, 2010.

[7] J. Wallauer, D. Macedo, R. Andrade, and A. von Wangenheim, "Building a national telemedicine network," *IT Professional*, vol. 10, pp. 12–17, 2008.

[8] A. von Wangenheim, L. F. de Souza Nobre, H. Tognoli, S. M. Nassar, and K. Ho, "User satisfaction with asynchronous telemedicine: A study of users of santa catarina system of telemedicine and telehealth." *Telemed J E Health*, vol. 18, no. 5, pp. 339–46, 2012.

[9] The PHP Group, "Php documentation," http://php.net/, 2013.

[10] F. Cheng, "Security attack safe mobile and cloud-based one-time password tokens using rubbing encryption algorithm," *Mob. Netw. Appl.*, vol. 16, no. 3, pp. 304–336, Jun. 2011.

[11] N. Haller, C. Metz, P. Nesser, and M. Straw, "A One-Time Password System," RFC 2289 (Standard), Internet Engineering Task Force, Feb. 1998.

[12] T. B. Idalino and D. Spagnuelo, "Senhas descartáveis em dispositivos móveis para ambientes de telemedicina," in *SBSeg 2012 WTICG*, http://sbseg2012.ppgia.pucpr.br/, Nov 2012.

[13] FFIEC, "Authentication in an internet banking environment," Outubro 2005, http://www.ffiec.gov/press/pr101205.htm.

[14] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, and E. A. Nabbus, "Sp 800-63-1. electronic authentication guideline," Gaithersburg, MD, United States, Tech. Rep., 2011.

[15] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm," RFC 4226 (Informational), Internet Engineering Task Force, Dec. 2005.

[16] Agência Nacional de Telecomincações, "Quantidade de acessos/plano de serviço/unidade da federação," http://sistemas.anatel.gov.br/SMP/Administracao/Consulta /AcessosPrePosUF/tela.asp, 2012.

[17] IBGE, "Sinopse do censo demográfico 2010," http://www.censo2010.ibge.gov.br/sinopse/, 2010.

[18] M. Alzomai, A. Josang, A. McCullagh, and E. Foo, "Strengthening sms-based authentication through usability," in *ISPA '08. International Symposium on*, Dec. 2008, pp. 683 –688.

[19] A. Jøsang, M. A. Zomai, and S. Suriadi, "Usability and privacy in identity management architectures," ser. ACSW '07. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2007, pp. 143–152.

[20] R. Di Pietro, G. Me, and M. Strangio, "A two-factor mobile authentication scheme for secure financial transactions," in *ICMB 2005*, July 2005, pp. 28 – 34.