AUTENTICAÇÃO MULTI-FATOR PARA TELEMEDICINA USANDO DISPOSITIVOS MÓVEIS E SENHAS DESCARTÁVEIS

MULTI-FACTOR AUTHENTICATION FOR TELEMEDICINE USING MOBILE DEVICES AND ONE-TIME PASSWORDS

AUTENTICACIÓN MULTI-FACTOR PARA TELEMEDICINA UTILIZANDO DISPOSITIVOS MÓVILES Y CONTRASEÑAS DESECHABLES

Aldo von Wangenheim[1], Dayana P. B. Spagnuelo[2], Thaís B. Idalino[3], Jean E. Martina[3], Leonardo A. Ribeiro[4]

1 INCoD - Instituto Nacional de Ciência e Tecnologia para Convergência Digital, Universidade Federal de Santa Catarina
2 Interdisciplinary Centre for Security, Reliability and Trust, Campus Kirchberg, Université du Luxembourg
3 LabSEC – Laboratório de Segurança em Computação, Universidade Federal de Santa Catarina
4 Instituto de Informática, Universidade Federal de Goiás

Resumo. Sistemas de telemedicina necessitam de serviços de autenticação fortes para garantir o sigilo e a privacidade dos dados e, ao mesmo tempo flexíveis para atender as necessidade de profissionais e pacientes. O foco deste trabalho é a validação de um novo processo de autenticação. Propomos um serviço de autenticação voltado à telemedicina baseado em tecnologias de web services. Este serviço faz uso de métodos de autenticação escaláveis e baseados em duplo fator. Uma de suas principais características é a flexibilidade na configuração dinâmica dos mecanismos de autenticação. Neste trabalho apresentamos brevemente a engenharia de requisitos do sistema de segurança e alguns detalhes da sua implementação. Também apresentamos resultados de um primeiro estudo de validação com usuários.

Descritores: Segurança Computacional, Telemedicina

Abstract. *Telemedicine systems require authentication services that are strong enough to ensure confidentiality and privacy of data and, at the same time, flexible to meet the needs of professionals and patients. The focus of this paper is the validations of a new authentication process. We propose an authentication service for telemedicine based on web services. This service employs scalable authentication methods based upon a dual authentication factor. One of its main characteristics is flexibility in the dynamic configuration of the authentication mechanisms. In this paper we deal briefly with the requirements engineering of the security system and some details of its implementation. We also present the results of a first validation study with users.*

Keywords: *Computer Security, Telemedicine Descriptores: Seguridad Computacional, Telemedicina*

Introdução

Ambientes de telemedicina facilitam o acesso a serviços de saúde para pessoas que não poderiam tê-los da forma convencional. Seu crescimento expôs a fragilidade que estes ambientes possuem em

relação à segurança da informação que carregam. Uma das principais vulnerabilidades é o roubo de identidade, que pode se dar por adivinhação ou roubo das credenciais de um usuário em um sistema. Este tipo de ameaça aumenta se as informações contidas no sistema são frágeis e se o modelo de autenticação é fraco. Em sistemas de telemedicina, o roubo de identidade pode causar não somente o vazamento de informações privadas, mas diversas outras situações, como laudos adulterados. O uso de um modelo mais eficiente de autenticação, com métodos mais fortes, torna-se uma necessária alternativa para aumentar a segurança. Por outro lado, autenticações fortes estão vinculadas ao uso de dispositivos criptográficos específicos que exigem módulos de leitura para sua utilização. Isto gera *baixa interoperabilidade* que interfere diretamente na *mobilidade* e *usabilidade*. Dentro do ambiente de telemedicina um médico deve ser capaz de acessar o sistema à distância e de qualquer lugar e a qualquer tempo. Um impedimento pode significar risco à vida. A autenticação deve ser forte, mas não deve depender de dispositivos que prejudicam a mobilidade ou a usabilidade para funcionar.

Neste trabalho apresentamos os primeiros resultados de validação de um novo modelo de autenticação modular e flexível, anteriormente proposto por nós, que se utiliza do **método de dois fatores de autenticação** e funciona como um *web service* seguro[1]. O serviço atua na camada de autenticação do sistema de telemedicina e integra vários métodos de autenticação de segundo fator baseados na posse de dispositivos como um telefone celular ou a presença em determinada localização geográfica pelo uso de sistemas de telefonia fixa. Uma importante característica é a flexibilidade do processo de autenticação através do uso de uma lista de mecanismos aceitáveis. O modelo foi projetado baseado nas reais necessidades do Sistema Integrado Catarinense de Telemedicina e Telessaúde (STT/SC)[2] [3]1. Ao longo deste trabalho percebeu-se que as necessidades de usuários desse tipo de sistema são distintas dos convencionais.

Procurou-se assim, uma solução de autenticação diferenciada baseada na posse de dispositivos comuns, como *smartphones*, telefones celulares ou ainda telefonia fixa.

Trabalhos Relacionados

As propostas envolvendo autenticação utilizando um segundo fator podem ser separadas em dois grupos: baseadas em certificados digitais e baseadas em biometria.

Em [4] é proposta uma arquitetura interoperável baseada em *web services* de autenticação e autorização que garantem a interoperabilidade entre diferentes sistemas e utiliza certificados digitais para garantir a identidade do usuário. Tanto [5] quanto [6] propõem um *framework* de autenticação baseado em *tokens* criptográficos. O foco do primeiro é o projeto de um *framework* capaz de autenticar fortemente um usuário de diferentes formas (através do uso de assinaturas, senhas ou biometria). O segundo postula uma Autoridade Certificadora de Identidades (ACI) que distribui e assina os certificados.

Com uma abordagem diferente [7] e [8] propõem *frameworks* de autenticação e autorização baseados em impressões digitais. O *framework* destina-se a reforçar o serviço de autorização do modelo de sistema de telemedicina de forma a garantir o acesso de seus usuários. [8] ainda emprega RFID que visa, além da autenticação, evitar que os dados saiam do hospital, não sendo possível autenticar-se fora dele.

Os primeiros trabalhos são baseados em certificados digitais, o que torna necessárias leitoras de *smart tokens*, que possuem baixa interoperabilidade entre sistemas operacionais, além de dificultar o uso de *tablets* ou celulares. Uma necessidade da telemedicina fica prejudicada: a *mobilidade*. Certificados digitais em *software*, por sua vez, necessitam ser instalados localmente no computador utilizado para assinar e não são opção para ambientes inseguros como *cybercafés* ou *LAN-houses*, ambientes cujo uso para laudos de urgência tem sido recorrente no STT/SC.

1 http://http//telemedicina.saude.sc.gov.br/

Os demais trabalhos utilizam-se de biometria como o segundo fator do processo de autenticação. A leitura de uma impressão digital é feita através de um hardware específico que possui os mesmos problemas das leitoras de *smart tokens.* Esta abordagem é ainda pior que o modelo baseado em certificados digitais: um usuário comum (paciente/médico) é forçado a utilizar um computador que satisfaça todos os requisitos operacionais de instalação da leitora e também está impedido de, em emergências, trabalhar em ambientes como *cybercafés* ou *LAN-houses.*

Com base nos pontos positivos dos trabalhos analisados e visando corrigir problemas apontados em cada um deles, foi realizado o levantamento dos requisitos da proposta de modelo de autenticação utilizando o STT/SC como caso de estudo. Este levantamento foi utilizado como base para o desenvolvimento da nossa proposta.

Requisitos

Focando exigências de uso diário em ambientes de telemedicina, foram identificados dois requisitos do serviço de autenticação que consideramos de maior importância:

a. **Mobilidade**: Um sistema de telemedicina não deve impedir o trabalho de um médico, pois isto pode significar risco à vida de pacientes. Um usuário deve ser capaz de acessar o sistema a partir de (a.1) *qualquer computador, tablet* ou telefone celular, desde que possua conexão à internet, em (a.2) *qualquer lugar. O serviço de autenticação não deve se interpor entre usuário e sistema. A utilização de métodos que necessitam de hardware específico como tokens, smart cards e biometria é inviável.*
b. **Dispositivo não-limitador**: Dispositivos utilizados como segundo fator nas autenticações não podem ser limitadores. *Tokens* e *smart cards* criptográficos são dispositivos que podem ser facilmente perdidos ou esquecidos, devendo ser substituídos por dispositivos de uso diário, como telefones celulares, garantindo a *flexibilidade do serviço. Um usuário não pode ser impedido de acessar o sistema mesmo quando não esteja de posse de algum dispositivo, devendo-se prever este tipo de situação e disponibilizar alternativas.*

Modelo de autenticação

Além dos requisitos apresentados acima, foram levados em consideração os requisitos comuns a modelos de autenticação, e partir destes desenvolveu-se uma biblioteca de autenticação dedicada, integrada a um *web service* seguindo os padrões já bastante sólidos do XML-RPC sobre HTTPS duplamente autenticado, garantindo a confidencialidade das mensagens e dados que trafegam. A biblioteca é responsável somente pela autenticação e disponibiliza um conjunto de métodos, deixando a cargo do *web service* sob o sistema de telemedicina a forma com que estes são utilizados.

Métodos de Autenticação

Os métodos utilizados neste trabalho são todos fatores de autenticação baseados em algo que o usuário *possui*. Em autenticações de múltiplos fatores cada fator deve ser de posse somente do usuário e um atacante deve ser incapaz de obtê-lo[9]. Os métodos escolhidos foram três: (i) *One-Time Password via Smartphone*, (ii) SMS e (iii) chamadas telefônicas para telefones autorizados do sistema de telemedicina.

One-Time Passwords (OTP)[10][11] são senhas descartáveis geradas a partir de uma semente previamente compartilhada. O processo de geração de OTPs deve possuir duas entidades[10]: uma *geradora* e um *servidor de verificação.* A geradora é um dispositivo de uso pessoal (smartphone) com um aplicativo especial.

SMS é um método de autenticação *out-of-band*. Autenticação *out-of-band* é definida como uma técnica de autenticação que permite que a identidade do usuário que originou a operação possa ser verificada por meio de um canal diferente do utilizado para iniciar a operação[12]. Envia-se uma senha alfanumérica aleatória via SMS (*Short Message Service*) para o celular do usuário que requisitou autenticação, que este utiliza como segundo fator da autenticação provando a posse da linha telefônica.

O *método de autenticação através de chamadas telefônicas* também é *out-of-band* e consiste em registrar o identificador de chamadas de uma ligação feita pelo usuário para telefones autorizados do sistema de telemedicina Estes são telefones VoIP que executam um *script* que obtém o identificador do remetente da chamada e, logo após, encerra a ligação, registrando, através do *web service* de autenticação, o identificador obtido. Quando o *web service* recebe um identificador ele identifica o usuário que possui o número cadastrado e registra o horário da chamada. Para se autenticar o usuário insere seu *login* e senha (primeiro fator) e informa que já fez a chamada, assim o serviço verifica se a informação é verdadeira. A figura 1 apresenta uma visão de alto nível do processo de autenticação e a figura 2 o fluxograma do processo.

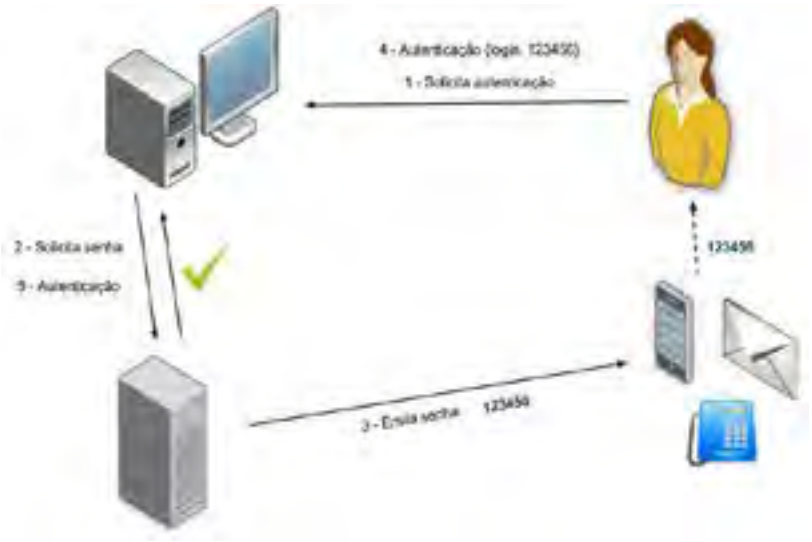

Figura 1: Visão de alto nível do processo de autenticação utilizando lista de mecanismos provendo duplo fator em testes no STT/SC.

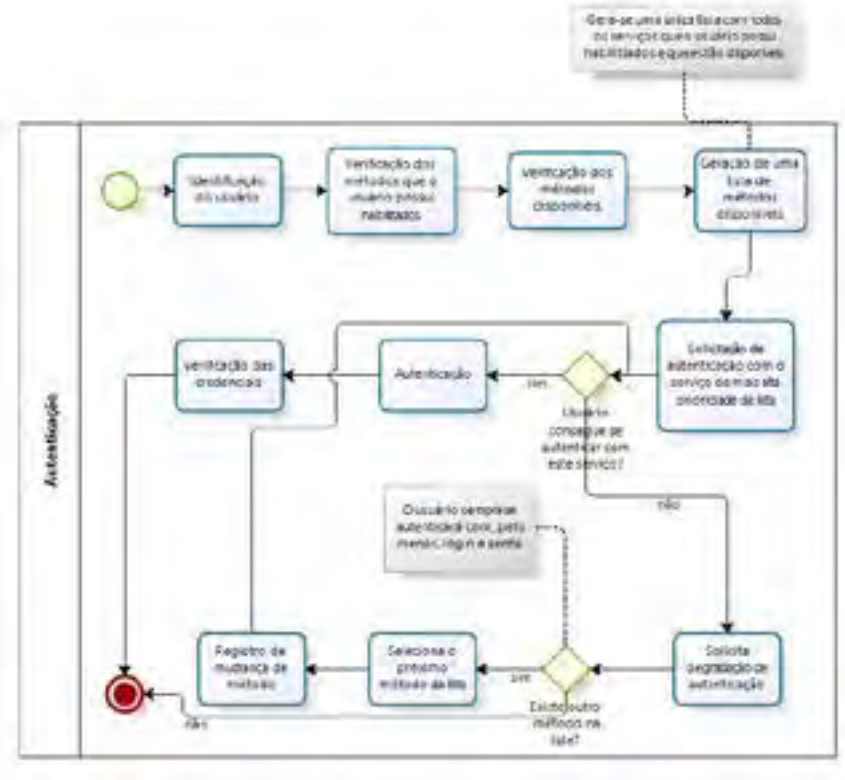

Figura 2: Fluxograma do processo de autenticação utilizando lista de mecanismos provendo duplo fator em testes no STT/SC.

Justificativas

Todos os métodos de autenticação envolvidos neste modelo são utilizados como o segundo fator da autenticação presentemente em uso: o usuário autentica-se exatamente da mesma forma que faz hoje e, numa segunda etapa utiliza um método adicional de confirmação de identidade, onde cada usuário possui uma lista de métodos de autenticação habilitados. Os métodos de autenticação utilizados foram selecionados de forma a não atrapalhar a característica de mobilidade da telemedicina em Santa Catarina, utilizando dispositivos comuns como smartphones e telefones fixos ao invés de tokens criptográficos. Não são utilizados métodos de autenticação dependentes de hardware de leitura como smart cards e biometria de forma geral.

Canais alternativos de autenticação possibilitam que, mesmo num cenário onde a forma de autenticação definida como a mais prioritária seja realizada através da utilização de um *smartphone*, não se pode assumir que todos os usuários de um sistema possuem tal *smartphone* a sua disposição quando da autenticação. Desta forma, a biblioteca prevê a alteração do método de autenticação para um menos prioritário (que normalmente depende de outro tipo de dispositivo). Assim, o modelo preserva a característica de mobilidade e de flexibilidade do sistema, não impedindo o acesso dos seus usuários, conforme prescrito no segundo requisito.

Resultados

Análise dos Métodos de Autenticação

No modelo de OTP utilizamos *smartphones* como geradores de senhas. Por serem dispositivos de uso pessoal, usuários estão habituados com suas formas de interação. Por conta disto este modelo

não causa grande impacto sobre a usabilidade de sistemas de telemedicina dado que não exige que um usuário interaja com dispositivos criptográficos desconhecidos, que por vezes possuem um uso não muito intuitivo.

OTPs são comuns e bem aceitos em ambientes bancários por se tratarem de ambientes com operações de alto risco. Similarmente a ambientes bancários, operações em sistemas de telemedicina também podem ser consideradas de alto risco, uma vez que um ataque pode significar risco à vida. Não existem, no entanto, referências na literatura do uso desta estratégia de segurança na área da Telemedicina. Geradores de senhas são seguros pela natureza sensível ao tempo ou sincronizada da autenticação, onde aleatoriedade, imprevisibilidade e singularidade dos OTPs aumentam substancialmente a dificuldade de um atacante obter uma senha[12]. O processo de geração de um OTP é offline e ataques virtuais só podem ser realizados quando a senha for utilizada. Considerando que após sua utilização os OTPs são invalidados, as chances de sucesso de um ataque deste tipo são bastante baixas. O ataque por adivinhação também possui uma chance de sucesso bastante pequena[13]. Pelo fato de smartphones serem de natureza pessoal, ataques físicos como roubo serão facilmente percebidos. Ao contrário de ataques virtuais, estes normalmente não são discretos e o usuário, sabendo do ataque, pode tomar as devidas providências para amenizá-lo, tais como cancelamento ou bloqueio temporário de sua conta.

O modelo de SMS de autenticação é uma alternativa de abrangência muito maior que o primeiro. A quantidade de contas móveis em maio de 2012 no Brasil era de mais de 254 milhões[14]. Grande parte dos usuários já possui celular e já estão habituados com o sistema de SMS. O modelo de SMS porém possui um custo para o sistema de telemedicina, cada autenticação requer o envio de uma mensagem e, conforme a quantidade de acessos aumenta, o custo de manter o modelo aumenta também. Como uma alternativa a este custo elevado foi apresentado o terceiro modelo, baseado em identificador de chamadas, que possui as mesmas características do modelo SMS, utiliza-se de dispositivos que os usuários já possuem e já conhecem, utiliza uma rede independente da internet e o nível de segurança também é similar. A primeira vantagem deste modelo em relação ao de SMS é que é gratuito para o sistema de telemedicina e também pode ser um método gratuito para os usuários.

O modelo de autenticação baseado em chamadas telefônicas é a grande contribuição deste modelo. Mesmo sendo contraintuitivo, agrega muito mais segurança ao sistema. O uso de simples chamadas telefônicas a partir de telefones fixos permite a criação de um novo fator de autenticação que difere dos tradicionais “o que você sabe”, “o que você possui” e “quem você é”. Passamos a ter o “onde você está” atrelado a localização física do terminal telefônico. Dessa forma podemos exigir que determinadas autenticações ocorram em lugares específicos dentro de um hospital por exemplo.

Figura 3: Validação de usabilidade estratificada do modelo e aplicativos OTP Android e iOS

utilizados.

Validação do Modelo

Quando usuários encontram tarefas de segurança frustrantes, estes tendem a contorná-las ou ignorá-las[15]. Desta forma, a avaliação da usabilidade e flexibilidade do modelo foi identificada como um fator chave e escolhida como o foco de um primeiro estudo de validação. Com auxílio da SES/SC, amostras de usuários de diversos municípios foram submetidos a um teste de usabilidade. Objetivamos obter indicadores para 3 quesitos: *facilidade de uso, segurança,* e *complexidade do processo.* Facilidade e complexidade foram escolhidos objetivando identificar se o processo está muito longo e burocrático. Um processo longo pode desmotivar usuários a utilizar o modelo. O quesito de segurança foi escolhido para identificar se os usuários entendem o porque das modificações no processo e se se sentem mais seguros com o novo modelo.

O teste foi realizado da seguinte forma: um agente da Secretaria de Saúde do Estado visitava uma instituição (normalmente hospital) parceira do STT/SC, e apresentava o novo modelo para alguns usuários. Em um primeiro momento os usuários realizavam a autenticação com um usuário de teste já cadastrado. Logo em seguida cada um deles era instruído a realizar o cadastro de um novo usuário e a utilizar o sistema. Cada usuário respondeu um questionário baseado na Escala de Usabilidade de Sistema (SUS) [16] . Este questionário consiste afirmações em uma escala Likert, que o usuário deve indicar o grau de concordância. Em nosso questionário, foram adicionadas 7 afirmações mais específicas sobre a segurança do processo e sobre a utilização do software no celular às 10 questões do SUS. Cada uma das classificações pode ser vista na figura 3. A avaliação foi realizada com o apoio de 23 usuários escolhidos pela SES/SC, utilizando apenas o método de autenticação baseado em OTP. Estes usuários foram classificados por perfil da profissão, em três classes: laudadores (39% - médicos e dentistas); operadores (26% - técnicos administrativos, jornalistas e técnicos de informática); e técnicos (35% - enfermeiros, técnicos de enfermagem e técnicos que operam aparelhos de exame). Para cada um dos testes foi utilizado um dos protótipos mostrados na figura 3, dependendo do modelo de smartphone que o usuário possuía.

Discussão e Trabalhos Futuros

Neste trabalho apresentou-se um novo modelo de autenticação baseado em *web service* seguro. Este novo modelo é voltado às necessidades de segurança de sistemas de telemedicina. Para que se cumpra com os principais requisitos que este tipo de sistema exige, o modelo se utiliza de autenticação de múltiplos fatores, disponibilizando para tal, um conjunto de métodos de autenticação que podem ser combinados de forma a prover mais confiabilidade ao processo. O modelo difere do que é praticado em Informática em Saúde na atualidade através de da integração de duas características principais:

a. **Segurança**: o emprego de um nível de segurança maior do que o praticado em Saúde na atualidade através do uso de autenticação de múltiplos fatores, sendo novidade na área da Telemedicina, e
b. **Disponibilidade**: a capacidade de prover resiliência a falhas no fator secundário de autenticação através do emprego intregrado de múltiplos canais alternativos de autenticação (smartphone, SMS, telefone fixo), dando maiores garantias de disponibilidade do serviço em situações de emergência e urgência.

Possui ainda a vantagem de operar como um *web service* e, portanto, não impor aos sistemas limitações tecnológicas, como linguagem de implementação, além de não requerer o uso de *tokens* criptográficos específicos, podendo ser facilmente integrado a diversos sistemas. Sua característica de alta interoperabilidade e sua eficácia puderam ser demonstradas através de uma versão operável do serviço; a proposta encontra-se completamente implementada e integrada a um sistema de telemedicina

em operação. Nossa análise demonstrou que o modelo proposto se adequa bem aos sistemas de telemedicina uma vez que provê flexibilidade e evita a interposição do sistema entre a

relação médico-paciente. O modelo de autenticação atualmente preconizado no Brasil pelo Conselho Federal de Medicina pressupõe o uso de um e-CPF ou e-CRM, que é representado por um smartcard e exige o uso hardware específico na forma de leitoras, impossibilitando a sua aplicabilidade a muitas situações de urgência, comuns em Telemedicina, onde o médico laudador estará fora de seu local de trabalho e longe de um computador fixo com leitor de cartão ou capaz de permitir inserção segura de um token criptográfico. O modelo aqui proposto não possui estas restrições.

O modelo cobre os principais ataques envolvendo o processo de autenticação. Utilizando diferentes métodos de autenticação de segundo fator provemos ainda um sistema escalável e flexibilizamos a autenticação. Podemos ainda prover propriedades de autenticação não existentes na maioria dos outros sistemas, como a autenticação geográfica, baseada no uso do identificador de chamadas de telefonia fixa.

As respostas estratificadas permitem observar que Laudadores e Operadores possuem comportamentos bastante similares, concordando quanto à facilidade de uso e a segurança do modelo, e discordando sobre a complexidade, ficando estes resultados próximos dos resultados esperados. Os usuários com perfil de Técnico obtiveram uma avaliação pior, observando-se neutralismo nos quesitos de facilidade de uso e complexidade (valores próximos a 3). Acredita-se que esta classe de profissionais necessite de mais atenção no treinamento de utilização do novo modelo.

Estamos trabalhando na adição de novos métodos de autenticação. Nossos próximos passos na melhora dos mecanismos de autenticação são a inclusão de um sistema criptográfico baseado em identidades (*identity based* encryption) para permitir a autenticação de usuários não cadastrados no sistema e a implementação de um sistema de autenticação através de QR Codes via web usando o método Tiqr [17].

Ameaças à Validade

Duas ameaças relacionadas ao viés de seleção foram identificadas: (a) foram convidados a responder o questionário apenas médicos, pesquisadores, gestores e técnicos indicados de forma arbitrária pela SES/SC; (b) a maioria dos entrevistados teve seu primeiro contato com OTPs em *smartphones* durante o processo de avaliação. Isto pode ter influenciado as respostas para alguns itens. Entendemos, no entanto, que para uma primeira validação do protótipo do sistema, este risco é aceitável.

Reconhecimentos

Este trabalho teve o apoio da Secretaria de Estado da Saúde de Santa

Catarina - SES/SC, da Financiadora de Estudos e Projetos - FINEP (Projeto CIMSaúde), do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq e da Fundação de Amparo à Pesquisa de Santa Catarina – FAPESC

REFERÊNCIAS

[1] Spagnuelo, D. P. B., Martina, J. E., Andrade, R., and Custodio, R. F. (2013). Multifactor authentication in telemedicine systems. In eTELEMED 2013, *The Fifth International Conference on eHealth, Telemedicine, and Social Medicine*, 2013

[2] Maia, R. S., von Wangenheim, A., and Nobre, L. F. (2006). A statewide telemedicine network for public health in brazil. *In IEEE 19th International Symposium on Computer-Based Medical Systems (CBMS 2006)*, pages 495–500.

[3] Wallauer, J., Macedo, D., Andrade, R., and von Wangenheim, A. (2008). Building a national telemedicine network. *IT Professional*, 10:12–17.

[4] Martínez, J.-F., Hernández, V., Valero, M.-A., Gómez, A., Pérez,E., Pau, I., Álvarez, H., and Vadillo, L. (2007). 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*, EATIS '07, pages 41:1–41:7, New York, NY, USA. ACM.

[5] Ahn, G.-J. and Shin, D. (2002). Towards scalable authentication in health services. *In Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshopson, pages 83 – 88.*

[6] Al-Nayadi, F. and Abawajy, J. (2007). An authentication framework for e-health systems. *In Signal Processing and Information Technology, 2007 IEEE International Symposium on, pages 616 –620.*

[7] Han, S., Skinner, G., Potdar, V., and Chang, E. (2006). A framework of authentication and authorization for e-health services. *In Proceedings of the 3rd ACM workshop on Secure web services*, SWS '06, pages 105–106, New York, NY,USA. ACM.

[8] Garson, K. and Adams, C. (2008). Security and privacy system architecture for an e-hospital environment. *In Proceedings of the 7th symposium on Identity and trust on the Internet*, IDtrust '08, pages 122–130, New York, NY, USA. ACM.

[9] Cheng, F. (2011). Security attack safe mobile and cloud-based one-time password tokens using rubbing encryption algorithm. *Mob. Netw.* Appl. , 16(3):304–336.

[10] Haller, N., Metz, C., Nesser, P., and Straw, M. (1998). A One-Time Password System. RFC 2289 (Standard).

[11] Lamport, L. (1981). Password authentication with insecure communication. *Commun. ACM*, 24(11):770–772.

[12] FFIEC (2005). Authentication in an Internet banking environment. http://www.ffiec.gov/press/pr101205.htm. Acesso em 01/05/2016.

[13] M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., and Ranen, O. (2005). HOTP: An HMAC-Based One-Time Password Algorithm. RFC 4226.

[14] Agência Nacional de Telecomincações (2012). *Quantidade de acessos/plano de serviço/unidade da federação.* http://sistemas.anatel.gov.br/SMP/Administracao/ Consulta/AcessosPrePosUF/tela.asp. Acesso em 01/03/2012.

[15] Alzomai, M., Josang, A., McCullagh, A., and Foo, E. (2008). Strengthening sms-based authentication through usability. *In Parallel and Distributed Processing with Applications, 2008. ISPA '08. International Symposium on, pages 683 –688.*

[16] Brooke, J. (1996). SUS: A quick and dirty usability scale. In Jordan, P. W., Weerdmeester, B., Thomas, A., and Mclelland, I. L., editors, *Usability evaluation in industry.* Taylor and Francis, London.

[17] SURFnet (2013). tiqr. https://tiqr.org/. Acesso em 01/05/2016.

Contato

Aldo von Wangenheim
aldo.vw@ufsc.br