Autenticação Semântica Gráfica

Graphical Semantic Authentication

Leonardo dos Santos Dourado e Edison Ishikawa
Programa de Pós-Graduação em Computação Aplicada, Departamento de Ciências da Computação
Universidade de Brasília
Campus Universitário Darcy Ribeiro, Brasília - DF, Brasil
{eng.leonardo.dourado, edison.ishikawa}@gmail.com

Resumo — **Atualmente a autenticação somente com usuário e senha não garante um nível de segurança aceitável. Para reforçar a segurança no processo de autenticação estão sendo utilizados múltiplos fatores de autenticação, porém o fator do tipo o que você tem gera inconveniente para o usuário, pois o mesmo sempre que for autenticar deverá fazer o uso de algum dispositivo complementar durante o processo de autenticação. Por outro lado, os fatores biométricos podem mudar com o passar do tempo, necessitam de dispositivos auxiliares que aumentam o custo e também podem depender de aspectos ambientais para funcionar corretamente. Visando eliminar alguns inconvenientes da autenticação por múltiplos fatores, este trabalho propõe a autenticação por meio de representações semânticas em triplas OWL (Web Ontology Language) de conceitos identificáveis em imagens como forma de aumentar a segurança no processo de autenticação. Para isto, uma prova de conceito foi modelada e implementada, demonstrando que a robustez deste sistema de autenticação depende da complexidade das relações existentes na base semântica (ontologia) e na simplicidade das relações identificadas nas imagens.**

Palavras Chave – Autenticação semântica gráfica; Autenticação semântica humana; Autenticação gráfica.

Abstract — **Authenticate on the system using only the authentication method based on username and password is not enough to ensure an acceptable level of information security for a critical system. It has been used in a multi factor authentication to increase the information security during the authentication process. However factors like what you have cause an inconvenience to the users, because the users during the authentication process always will need to have a device in their possession that complements the authentication process. By the other side of the biometric factor might change during the time, it needs an auxiliary device that will increase the costs and it also might be dependent from environmental conditions to work appropriately. To avoid some problems that exist in multi factor authentication, this work purposes authentication through semantic representation in OWL (web Ontology Language) tuples of recognized concepts in images as a form to increase the security in the authentication process. A proof of the concept was modeled and implemented, it has a demonstration that the robustness of this authentication system depends on the complexity of relationship in the semantic base (ontology) and in the simplicity of the relationship identified in the images.**

Keywords – Graphical semantic authentication; Human Semantic Authentication; Graphical Authentication.

I. INTRODUÇÃO

A autenticação utilizando usuário e senha é a forma mais comum de autenticação [1], no entanto a autenticação em sistemas críticos utilizando apenas usuário e senha não é aconselhada, e é insuficiente para garantir um nível de segurança aceitável. A senha pode ser comprometida por meio do compartilhamento com outros usuários, por meio de ataque de dicionário [2], rainbow table [2], engenharia social [3], keyloggers [1] e shoulder surfing [1]. A complexidade da senha é uma necessidade a ser considerada quando é utilizado esse tipo de autenticação [3].

Segundo Almulhem [4], impor uma política de senhas fortes pode levar o usuário a escrever a sua senha em algum lugar e expor a senha diretamente. Senhas muito grandes e complexas dificilmente serão memorizadas pelos usuários.

De acordo com Ometov [3] et al., usuário e senha não são adequados para prover um nível de segurança adequado em face da quantidade de ameaças que esse método de autenticação está suscetível. A autenticação de dois fatores foi proposta para resolver o problema da fragilidade do método de autenticação usuário e senha, e para agregar à autenticação tradicional um fator que o usuário possui ou um que usuário é, visando aumentar a robustez no processo de autenticação.

As autenticações de dois fatores e de múltiplos fatores aumentaram a segurança no processo de autenticação significativamente, mas a autenticação de mais de um fator possui alguns problemas conhecidos, como os seguintes que foram citados por Ometov [3] et al.:

- nem todo usuário pode utilizar autenticação biométrica, alguns tipos de autenticação precisam de sensores como: leitor de smartcard, leitor de impressão digital, microfone para o reconhecimento de voz, câmera para o reconhecimento facial, etc, e isso gera custo adicional;
- outros tipos de autenticação exigem a disponibilização de dispositivos para os usuários como: smartcards, tokens, telefones celulares, etc;

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3

- tecnologia como a de reconhecimento facial pode não funcionar em ambientes com a iluminação ruim ou com câmeras de baixa qualidade e a tecnologia de reconhecimento de voz pode não funcionar em ambientes com muito barulho [3]; e
- o uso de autenticação que dependa de celular pode não funcionar, caso o celular não esteja conectado à internet (dependendo do tipo de autenticação) ou com a falta de carga na bateria do celular [5].

Diante dos possíveis problemas expostos e relacionados à utilização de autenticação utilizando apenas usuário e senha ou da autenticação múltipla, outros tipos de autenticação pouco comum podem ser utilizadas como alternativa para mitigar os problemas relatados, como as autenticações gráficas ou/e semânticas.

Almulhem [4] afirma que senhas gráficas proveem uma alternativa promissora às senhas tradicionais alfanuméricas, são atrativas porque as pessoas geralmente lembram com mais facilidade de imagens do que de palavras. A senha gráfica consiste em utilizar fotos como senha ou padrões que são definidos pelo usuário.

Em seu trabalho Bouder et al. [1] afirmam que a senha conceitual (semântica) é menos suscetível ao ataque de Shoulder Surfing, porque um conceito é mais difícil de identificar do que uma senha normal. Além disso, guardar signifcados é como elaborar formas mnemônicas de memorização, o que facilita lembrar a senha.

Este trabalho tem como objetivo propor um mecanismo de autenticação semântica gráfica utilizando imagens para complementar o processo de autenticação comum, sem a dependência de dispositivos auxiliares e aumentando a robustez da autenticação.

O restante do artigo está estruturado da seguinte forma: na próxima seção o referencial teórico necessário à compreensão do trabalho é apresentado, na seção III é feita uma revisão bibliográfica, a seção IV descreve a metodologia de pesquisa Design Science Research adotada neste trabalho, a seção V mostra o estudo de caso da modelagem semântica da presente proposta e, por fim, a seção VI apresenta algumas considerações finais e trabalhos futuros.

II. Referencial Teórico

A. Segurança da Informação

O NIST (National Institute of Standards and Technology) [6] [7] define segurança da informação como proteger a informação e sistemas da informação de: acesso, utilização, divulgação, interrupção, modificação e destruição não autorizada. Segurança da informação significa proteger ativos de atacantes, desastres naturais, condições ambientais adversas, falhas de energia, roubo, vandalismo e qualquer outra ameaça indesejável [8].

Segundo Andress [8], quanto mais aumenta o nível de segurança, geralmente menor será o nível de produtividade, então se o nível de segurança for muito alto, o nível de produtividade tende a zero. Equilibrar os requisitos mínimos de segurança com a usabilidade e produtividade é um desafio.

B. Autenticação

A autenticação de um usuário é o ato de confirmação de que a pessoa que interage com o serviço é quem diz ser [9]. O processo de autenticação é geralmente o primeiro controle de aceso lógico que o usuário precisa superar para que tenha acesso ao sistema almejado. Atualmente existem três fatores que podem ser utilizados no processo de autenticação e esses fatores são: o que você sabe, o que você é e o que você tem.

Para acessar qualquer serviço ou recurso na infraestrutura de tecnologia da informação, o usuário deveria estar autenticado [10]. Os usuários deveriam utilizar credenciais de acesso e o sistema deveria comparar essas credenciais com um banco de dados para identificar o usuário [10]. Geralmente neste processo de autenticação o usuário digita o usuário e a senha, e o sistema valida a credencial inserida pelo usuário no sistema.

C. Autenticação com usuário e senha

Na época dos primeiros computadores de grande porte (Mainframes) problemas de segurança da informação envolvendo autenticação e autorização já existiam. Segundo Bonneau, Herley, Orschot e Stajano [11], a senha (Password) foi originalmente implantada na década de 60 no acesso aos computadores de grande porte (Mainframes) de tempo compartilhado (Time Sharing). A senha era utilizada como forma de proteger o computador de grande porte contra o acesso não autorizado e limitar o acesso aos recursos do sistema.

Na década de 60 ocorreram incidentes de segurança da informação relacionados as senhas de usuários de computadores de grande porte (Mainframes) que foram quebradas por serem fracas ou por terem sidos descobertar e até mesmo senhas armazenadas sem estarem criptografadas [11]. Esses tipos de problemas relatados envolvendo senha há quase 60 anos atrás ocorrem até os dias atuais.

D. Autenticação Biométrica

A autenticação biométrica é um sistema de controle de acesso que autentica indivíduos baseando-se em seus traços biométricos. Diferentemente da senha ou de qualquer sistema de autenticação convencional, traços biométricos como impressões digitais, iris, voz, face e características comportamentais ligadas a um indivíduo são de difícil manipulação, como as caracterísitcas dos passos ao andar [12].

A autenticação biométrica está dividida em dois grupos principais: fisiológico e comportamental. A impressão digital, características do rosto, DNA, formato do corpo e iris são características fisiológicas. O padrão de digitação, voz, letra, maneira de andar são características comportamentais [13].

Para utilizar autenticação biométrica é importante ter um ambiente operacional robusto [3]. Um exemplo de falta de robustez no ambiente é no caso do reconhecimento de voz que foi testado em um ambiente silencioso e foi implantado em um ambiente barulhento, podendo impossibilitar a utilização desse tipo de biometria [3]. O funcionamento de algumas soluções de autenticação biométrica dependem de condições ambientais ideais para o seu funcionamento.

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3

E. Autenticação com múltiplo fator

De acordo com Colnago et al. [5], uma forma de reduzir os riscos relacionados a insegurança das senhas é utilizar a senha em conjunto com um outro fator de autenticação. Os fatores de autenticação são identificados em três categorias: alguma coisa que você sabe, alguma coisa que você tem e alguma coisa que você é.

O fator do tipo alguma coisa que você sabe é o conhecimento que o usuário tem e que será utilizado no sistema de autenticação, por exemplo: senha ou respostas para questões de segurança [5].

O fator do tipo alguma coisa que você tem são dispositivos como: token, celular, smartcard ou objetos como um papel com códigos de acesso [5] que são utilizados no sistema de autenticação.

O fator do tipo alguma coisa que você é é a biometria que será utilizada no sistema de autenticação como: impressão digital, retina, iris, reconhecimento de voz, reconhecimento facial [5].

A autenticação de dois fatores é definida como a utilização de duas categorias de métodos de autenticação diferentes em conjunto [5]. A autenticação com múltiplos fatores é definida como a utilização de duas ou mais categorias de métodos de autenticação diferente em conjunto.

Os problemas identificados durante a implantação de solução de 2FA na Universidade Carnegie Mellon foram os seguintes [5]:

- o usuário esqueceu o telefone e não consegue autenticar;
- acabou a bateria do celular do usuário e não consegue autenticar;
- não tem conexão de dados no celular e não consegue autenticar;
- o aplicativo do celular não está sincronizando com a conta no servidor.

F. Web Semântica

Web Semântica é um termo que define a informação em sua forma mais granular e a faz inteligível para um programa de computador [14]. A Web Semântica vai além do processamento de dados, ela permite que programas consigam extrair informações suficientes para que o programa de forma independente gere informação e construa relacionamentos [14].

A Web Semântica idealizada por Berners-Lee provê vários padrões de linguagens de representação, ferramentas de desenvolvimento e métodos para permitir que as máquinas possam interpretar os dados baseando-se em seu conteúdo semântico [15]. Por meio dos relacionamentos é possível que uma máquina faça inferências utilizando os dados [15].

A Web Semântica provê padrões, linguagens de representação, ferramentas compatíveis e métodos de desenvolvimento que podem ser utilizados para construir relacionamento entre dados em formatos e origens heterogêneas para que o computador possa interpretar o seu significado e executar tarefas complexas [15].

G. Ontologias

O termo ontologia tem origem na Filosofia e significa na Filosofia o estudo da existência [16]. A ontologia cria conhecimento comum e uma linguagem semântica não ambígua para representar o conhecimento [17]. A definição de ontologia de Wu, Zhang e Cao [17] foi aplicada no contexto da computação, mais precisamente na área de segurança da informação. A ontologia descreve conceitos e relationamentos de alguns fenômenos do mundo [18].

Ontologias são muito utilizadas para diversas finalidades e em diferentes áreas de estudo [18]. Ontologias são utilizadas para o processamento de linguagem natural, gerenciamento do conhecimento, comércio eletrônico, integração inteligente de informações e Web Semântica em áreas como engenharia do conhecimento, banco de dados, engenharia de software [18].

III. Trabalhos Relacionados

A. Autenticação Gráfica

Almulhem [4] em seu trabalho propôs um sistema de autenticação entitulado sistema de autenticação de senha gráfica. O sistema de Almulhem [4] é um sistema de autenticação gráfica simples que combina senhas gráficas com senhas textuais.

No processo de autenticação utilizando o sistema proposto por Almulhem [4], o usuário primeiro digita seu usuário e então o sistema exibe a imagem associada ao seu usuário. O usuário deve selecionar corretamente os pontos de interesse (POI) e digitar as palavras corretas relacionadas a cada POI.

A fraqueza deste sistema é que a imagem é sempre a mesma e, por meio do ShoulderSurfing é possível observar onde o usuário clicou (POI) e o que ele digitou em cada POI.

Diferente do sistema proposto por Almulhem [4], este trabalho propõe um sistema onde o usuário não terá sua senha conceitual associada a uma imagem específica ou terá que clicar em pontos específicos predefinidos na imagem que foram selecionados anteriormente, pois utilizará uma senha semântica que estará presente em imagens diferentes e quanto maior for a quantidade de imagens na base de dados, menor será a probabilidade de repetição das imagens para o usuário durante o processo de autenticação.

B. Autenticação Semântica Humana

Em seu trabalho Lorant, Wary, Salembier, Moustafa e Mathias [19] introduziram um sistema de autenticação gráfica entitulado (HSA - Human Semantic Authentication). Durante o processo de autenticação no sistema de Lorant, Wary, Salembier, Moustafa e Mathias [19] o usuário deve identificar quatro conceitos que constituem sua senha conceitual clicando nas áreas da imagem onde os conceitos estão presentes.

O HSA tem como objetivo aumentar a resistência do sistema de autenticação contra ataques humanos e automatizados [19]. São definidas zonas nas imagens e os conceitos são codificados nestas zonas [19].

No HSA [20] o usuário memoriza as quatro senhas conceituais que poderiam ser: amarelo, ferramenta, animal e

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3

comida, e deve selecionar durante o processo de autenticação áreas nas imagens que possuam esse conceito para ser autenticado.

O sistema proposto neste trabalho não utiliza a codificação em áreas nas imagens e nem apresenta apenas uma imagem para o usuário por vez, conforme no sistema de autenticação semântica humana de Salembier et al. [20] e Lorant, Wary, Salembier, Moustafa e Mathias [19]. Além disso, as relações da senha semântica do presente trabalho são relações descritas por triplas OWL (sujeito, predicado, objeto) existentes nas imagens, e não apenas palavras que descrevem algo que pode existir na imagem.

C. Genoma Visual

Em seu trabalho Krishna [21] et al. apresentaram a coleção de dados entitulada Genoma Visual (Visual Genome dataset) com objetivo de possibilitar que os objetos e seus relacionamentos nas imagens possam ser descritos de forma a gerar conhecimento de máquina. O conjunto de dados do Genoma Visual é utilizado no reconhecimento de objetos em imagens, seus possíveis relacionamentos com outros objetos na imagem e na reposta de perguntas relacionadas aos objetos, e seus relacionamentos. Esta coleção de dados de imagens não foi projetatada para servir como base para um sistema de autenticação.

O sistema proposto utiliza web semântica e ontologias para realizar a descrição das imagens, gerando conhecimento de máquina e criando capacidade de inferência computacional para autenticação, diferente da descrição realizada nas imagens do banco de dados do Genoma Visual [21], onde foi utilizada a linguagem natural para descrever as imagens.

Imagens existentes na base de dados do Genoma Visual [21] foram utilizados neste trabalho.

IV. METODOLOGIA

A metodologia de pesquisa adotada neste trabalho foi o Design Science Research adaptado de Dresch, Aline, Lacerda e Antunes [22].

A imagem Fig. 1 mostra as fases do Design Science Research.

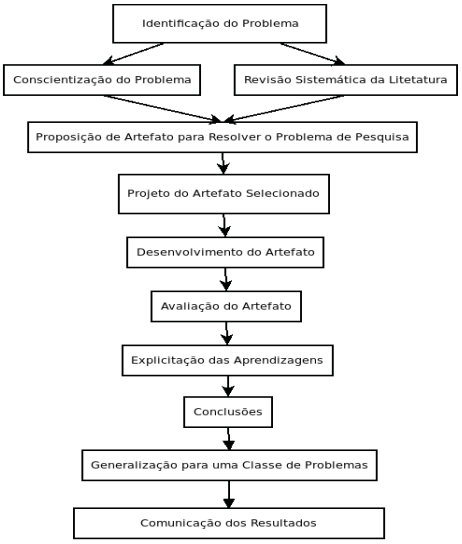

Figure 1. Etapas do design science research adaptado de Dresch, Aline, Lacerda e Antunes [22].

A Fig. 1 mostra as etapas deste trabalho que inclui a identificação do problema, revisão da literatura com artigos no estado da arte, proposição do mecanismo de autenticação e as demais etapas conforme na figura supracitada.

V. AUTENTICAÇÃO SEMÂNTICA GRÁFICA

A solução proposta tem como objetivo simplificar a utilização de uma segunda autenticação em conjunto com a autenticação por meio de usuário e senha, eliminando a necessidade de implementação de dispositivos auxiliares de autenticação ou a exigência de que o usuário tenha algum dispositivo em sua posse para utilizar de forma complementar no processo de autenticação.

Este trabalho tem como proposta a criação de um sistema de autenticação complementar que utiliza relações que podem ser identificadas facilmente pelo usuário por meio da inferência durante o processo de autenticação. A validação é realizada comparando as relações existentes na imagem com as relações da senha semântica definidas e armazenadas em banco de dados para o referido usuário.

Nesta solução existe a necessidade de descrição das imagens utilizando web semântica e a ontologia adotada para a descrição das imagens no sistema.

A Fig. 2 mostra o mapa conceitual da ontologia utilizada para realizar a descrição das imagens no sistema.

ISBN: 978-989-54659-0-3

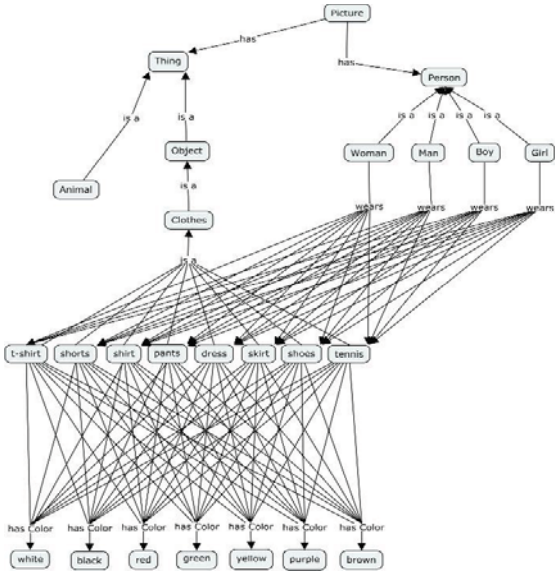

Figure 2. Mapa conceitual da ontologia utilizada no sistema.

É possível observar na Fig. 2 que utilizando esta ontologia é possível utilizar mais de 200 relações distintas na descrição de elementos nas imagens, mostrando a robustez do sistema.

O conhecimento é descrito de forma similar a da sintaxe do RDF (Resource Description Framework), mas de forma que o dado possa ser armazenado em banco de dados, possa ser vinculado as imagens que serão armazenadas no sistema de arquivos e possa ser pesquisado neste banco imagens que possui as relações das senhas semânticas dos usuários que serão exibidas durante o processo de autenticação.

A Fig. 3 mostra tela de descrição das imagens no sistema.

Figure 3. Tela de descrição de imagem.

A Fig. 3 mostra o processo de descrição semântica de uma de muitas relações possíveis em uma imagem no sistema de Autenticação Semântica Gráfica utilizando a ontologia definida na Fig. 2. As relações descritas nas imagens estarão disponíveis para os usuários durante o processo de definição das relaçoes da senha semântica. Conforme demonstrado na Fig. 3, as relações existentes entre os diversos elementos das imagens são descritos utilizando o formato sujeito, predicado e objeto.

A Fig. 4 mostra tela do sistema onde o usuário define ou altera sua senha semântica.

Figure 4. Tela de definição da senha conceitual no sistema.

No Sistema de Autenticação Semântica Gráfica, o usuário deve criar sua senha semântica selecionando relações já descritas de imagens. A senha semântica do usuário é definida no formato Sujeito, Predicado e Objeto conforme exibido na Fig. 4 e pode possuir várias relações. Quanto mais relações existirem na senha semântica, mais forte ela será.

Figure 5. Tela com exemplo de senha conceitual.

A Fig. 5 mostra um exemplo senha semântica e como ela pode ser definida.

Durante o processo de autenticação, o usuário deve autenticar utilizando usuário e senha normalmente, após a validação destas credenciais, o usuário deve realizar a autenticação complementar no sistema de autenticação semântica gráfica.

O processo de autenticação no sistema de autenticação semântica gráfica é realizado da seguinte forma:

- o sistema seleciona imagens que possuem a 1º relação da senha semântica do usuário;
- o sistema escolhe de forma aleatória uma imagem entre as imagens que foram selecionadas no passo anterior que possuem a 1º relação;
- o sistema seleciona três imagens de forma aleatória que não possuem a 1º relação da senha semântica do usuário;
- o sistema seleciona de forma aleatória as posições em que serão exibidas para o usuário a imagem que possui a relação que faz parte da senha semântica do usuário e as três que não possuem;
- o usuário clica na imagem escolhida e os passos anteriores serão realizados novamente para a 2º relação da senha semântica e assim sucessivamente até a última relação.

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3

A Fig. 6 mostra tela de autenticação do sistema de Autenticação Semântica Gráfica.

Figure 6. Tela de autenticação do Sistema.

Conforme exibido na Fig. 6, o usuário deve selecionar a imagem que possui a 1º relação da sua senha semântica clicando na imagem e outras imagens serão exibidas para o usuário onde uma possui a sua próxima relação. Esse processo será repetido até que a quantidade de relações definidas na senha semântica sejam validadas. O usuário deve selecionar as relações de sua senha semântica na ordem que foram definidas para que consiga autenticar com sucesso no sistema.

VI. Conclusões e Trabalhos Futuros

Durante as pesquisas dos trabalhos no estado da arte na área de sistema de autenticação, foi identificada uma lacuna em relação a usabilidade das soluções atuais, por este motivo propusemos o sistema de Autenticação Semântica Gráfica, de forma a resolver o problema identificado e com abordagem diferente das já existentes. Este sistema permite a combinação de várias relações permitindo a geração de senhas semânticas robustas com poucas relações, ou seja, fáceis de memorizar e difíceis de quebrar.

Com os resultados obtidos neste trabalho é possível afirmar que o sistema de autenticação semântica gráfica aumenta a segurança do método de autenticação usuário e senha, e permite supor algumas vantagens em relação a usabilidade quando comparado com os sistemas de autenticação de dois ou mais fatores.

No próximo trabalho o sistema de autenticação semântica gráfica será avaliado por meio de testes com vários grupos de usuários.

Um trabalho futuro poderia avaliar a utilização de *machine learning* para realizar a descrição semântica das imagens.

Referências Bibliográfica

[1] H. L. Bouder, G. Thomas, E. Bourget, M. Graa, N. Cuppens, e J. Lanet, "Theoretical Security Evaluation of the Human Semantic Authentication Protocol", Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, vol. 2, pp. 332-339, Julho 2018.

[2] W. Luo, Y. Hu, H. Jiang, e J. Wang, "Authentication by encrypted negative password", IEEE Transactions on Information Forensics and Security, vol. 14, pp. 114–128, Janeiro 2019.

[3] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, e Y. Koucheryavy, "Multi-Factor Authentication: A Survey", Cryptography vol. 2, pp. 1-31, Janeiro 2018.

[4] A. Almulhem, "A graphical password authentication system", World Congress on Internet Security (WorldCIS-2011), pp. 223-225, Janeiro 2011.

[5] J. Colnago, S. Devlin, M. Oates, C. Swoopes, L. Bauer, L. Cranor, e N. Christin, "It's not actually that horrible: Exploring Adoption of Two-Factor Authentication at a University. Proc. of CHI", CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, pp. 1-11, Abril 2018.

[6] W. Barker, "Guideline for identifying an information system as a national security system", National Institute of Standards and Technology (NIST), SP 800-59, Agosto 2003.

[7] M. Nieles, K. Dempsey, e V. Pillitteri, "An Introduction to Information Security", National Institute of Standards and Technology (NIST), SP 800-12, Junho 2017.

[8] J. Andress, "The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice", 1st ed., Syngress Publishing, 2011.

[9] M. Belk, C. Fidas, P. Germanakos, e G. Samaras, "The interplay between humans, technology and user authentication: A cognitive processing perspective", Computers in Human Behavior, vol. 76, pp. 184-200, Novembro 2017.

[10] L. Mercl, V. Sobeslav, P. Mikulecky, M. Macinka, I. Awan, M. Younas , P. Ünal e M. Aleksy, "Infrastructure authentication, authorization and accounting solutions for an openstack platform", Mobile Web and Intelligent Information Systems, pp. 123-135, Julho 2019.

[11] J. Bonneau, C. Herley, P. C. van Orschot, e F. Stajano, "Passwords and the evolution of imperfect authentication", Communications of the ACM, vol. 58, pp. 78-87, Julho 2017.

[12] Zhou, K. e J. Ren, "Passbio: Privacy-preserving user-centric biometric authentication", IEEE Transactions on Information Forensics and Security, vol. 13, pp. 3050–3063, Dezembro 2018.

[13] A. Wójtowicz e K. Joachimiak, "Model for adaptable context-based biometric authentication for mobile devices", Personal Ubiquitous Computing, vol. 20, pp. 195-207, Abril 2016.

[14] J. M. Perrin, "A Practical Perspective on Preparation for the Semantic Web", The Journal of Academic Librarianship, pp. 364-366, Junho 2017.

[15] D. J. Kim, J. Hebeler, V. Yoon, e F. Davis, "Exploring Determinants of Semantic Web Technology Adoption from IT Professionals' Perspective: Industry Competition, Organization Innovativeness, and Data Management Capacity", Computers in Human Behavior, vol. 86, pp. 18-33, Setembro 2018.

[16] S. S. Alqahtani, E. E. Eghan, e J. Rilling, "Tracing known security vulnerabilities in software repositories – A Semantic Web enabled modeling approach", vol.121, pp. 153-175, Junho 2016.

[17] S. Wu, Y. Zhang, e W. Cao, "Network security assessment using a semantic reasoning and graph based approach", Computer & Electrical Engineering, vol. 64, pp. 96-109, Novembro 2017.

[18] E. Kurilovas, e A. Juskeviciene, "Creation of Web 2.0 tools ontology to improve learning", Computers in Human Behavior, vol. 51, pp. 1380-1386, Outubro 2015.

[19] G. Lorant, J. P. Wary, P. Salembier, Z. Moustafa, e C. Mathias, "Evaluation ergonomique d'un système d'authentification graphique", Actes de la conférence EPIQUE 2015, pp. 8-10, Julho 2015.

[20] P. Salembier, Z. Moustafa, R. Héron, C. Mathias, G. Lorant, e J. P. Wary, "Experimental studies of a graphical authentication system based on semantic categorisation", Em Actes De La 28IèMe Conference Francophone Sur L'Interaction Homme-Machine, IHM '16, pp. 134-143, Outubro 2016.

[21] R. Krishna, Y. Zhu, O. Groth, J. Johnson, K. Hata, J. Kravitz, S. Chen, Y. Kalantidis, L. Li, D. A. Shamma, M. S. Bernstein, e L. Fei-Fei, "Visual Genome: Connection Language and Vision Using Crowdsourced Dense Image Annotations", International Journal of Computer Vision, vol. 123, pp. 32-73, Maio 2017.

[22] Dresch, Aline, D. P. Lacerda, e A. V. Antunes, "Design Science Research: A Method for Science and Technology Advancement", 1 st ed., Springer International Publishing, 2014.

ISBN: 978-989-54659-0-3