Utilização da Visualização da Informação Aplicada à Segurança de Redes

Luiz Felipe de Camargo, José Remo Ferreira Brega Universidade Estadual Paulista "Júlio de Mesquita Filho" Bauru, Brasil camargo.luizfelipe@gmail.com; remo@fc.unesp.br Diego Roberto Colombo Dias Universidade Federal de São João del-Rei (UFSJ) São João del-Rei, Brasil diegocolombo.dias@gmail.com

Resumo—Considerando a necessidade de se monitorar as redes de computadores modernas e o ganho de qualidade ao se utilizar técnicas de visualização, objetiva-se desenvolver uma ferramenta de monitoramento com ênfase no uso de recursos visuais. Para tanto, procede-se inicialmente com uma revisão sistemática do assunto. Desta forma, em tempo são observados os resultados preliminares provenientes das etapas iniciais da revisão, o que permite concluir que a continuidade do projeto é interessante, de modo a se obter as contribuições propostas.

Área: Sistemas de Informação

I. INTRODUÇÃO

Cada vez mais as redes de computadores estão integradas a vida das pessoas, sendo necessário que elas permaneçam sempre em pleno funcionamento. Entretanto, o monitoramento efetivo para garantir o funcionamento de uma rede, através de registro de todos os incidentes ocorridos, gera uma quantidade enorme de dados, causando problemas para o gerente de redes ao analisar e obter novas informações a partir desta. A fim de solucionar este problema, pode-se fazer uso das técnicas de visualização da informação, utilizando a visão humana para auxiliar a interpretação dos dados.

O propósito geral do trabalho a ser realizado é aplicar as técnicas de visualização da informação de maneira a obter uma ferramenta para monitoramento de redes que ofereça uma visão integrada dos diversos aspectos que compõe a situação de uma rede. Espera-se que o presente trabalho sirva como base de consulta para futuros pesquisadores interessados na área de visualização da informação aplicada a segurança e monitoramento de redes e que seja desenvolvida uma ferramenta funcional conforme proposto.

Em 2014 Kotenko e Novikova [1] utilizaram técnicas de visualização para manipular dados de segurança de domínios de rede com operação crítica. Guimarães [2] realizou um trabalho buscando classificar diversos estudos que utilizaram técnicas visuais para gerenciamento de redes e serviços, obtendo 285 artigos publicados entre 1985 e 2013. Também em 2016, Papadopoulos [3] realizou um estudo detectando, através de uma abordagem visual, anomalias de roteamento no protocolo BGP.

VII Workshop do Programa de Pós-Graduação em Ciência da Computação: "Interação entre Academia e Empresa", Unesp, Rio Claro, 14 e 15 de setembro de 2017

A Seção 2 deste trabalho trata dos conceitos e técnicas utilizadas, seguida da Seção 3 que descreve a metodologia utilizada. Os resultados preliminares são apresentados na Seção 4. Por fim, tem-se as considerações finais.

II. CONCEITOS E TÉCNICAS

Segurança de informação é descrita como a proteção das informações de diversas ameaças que buscam colocar em risco a continuidade de um negócio. Através da segurança de informação se busca minimizar o risco decorrente destas ameaças, maximizando sempre o retorno sobre as oportunidades de negócio e investimentos [4]. A segurança está estruturada em três principais pilares: confidencialidade, integridade e disponibilidade. No entanto, podemos citar também outras propriedades: autenticidade, responsabilidade, não repúdio e confiabilidade. Os principais pilares são ilustrados na Figura 1.



Figura 1. Os pilares da segurança de informação.

Monitoramento, o resultado do ato de monitorar, é definido por Michaelis [5] em seu dicionário da língua portuguesa como acompanhar e observar o decurso de um processo, de uma operação ou de um aparelho.

Gerenciamento de redes, segundo Saydam [6], pode ser definido como o processo que envolve o desenvolvimento, a integração e a coordenação de todos os recursos de hardware, software e de elementos humanos para monitorar, testar, configurar, analisar, avaliar e controlar uma rede, seus elementos e recursos para prover em tempo real os requisitos necessários de desempenho operacional e de qualidade de serviço a um custo razoável.

A visualização da informação busca representar conjuntos de dados como imagens, auxiliando na compreensão e tornando a interpretação destes mais eficiente. O uso da

visualização é adequado quando há necessidade de aumentar as capacidades humanas em vez de substitui-las por métodos de tomada de decisão computacional. A criação de uma ferramenta de visualização deve ser realizada respondendo três perguntas: por que a tarefa está sendo executada, quais dados são exibidos nas visualizações, e como a linguagem de expressão é construída como opção de design [7]. O processo cíclico de questionamentos pode ser visto na Figura 2.



Figura 2. Questionamentos para geração de uma visualização.

Revisão sistemática é uma técnica que busca executar revisões abrangentes da literatura acerca de um tema, avaliando os resultados de forma não tendenciosa, explicitando sempre seus critérios de seleção, de modo que o pesquisador que for utilizar a revisão possa avaliar a qualidade da mesma e executá-la novamente. Esta técnica foi desenvolvida inicialmente para utilização na área de medicina, porém, vem cada vez mais sendo utilizada em outras áreas do conhecimento [8].

III. METODOLOGIA DE DESENVOLVIMENTO

Inicialmente, para realização deste trabalho, está em execução uma revisão sistemática utilizando os termos: information visualization, information security, network security, network availability, network security, visualization, security visualization, security data visualization e visual analytics.

As buscas iniciais foram realizadas utilizando strings de busca nas bases de dados ACM Digital Library, IEEE Xplore Digital Library, Scopus e Engineering Village, a seleção destas foi realizada considerando a relevância, afinidade com as áreas de estudo e quantidade de resultados obtidos nos testes preliminares. Para apoio a realização da revisão utiliza-se a ferramenta StArt, desenvolvida pelo LaPES da UFSCar. Como critérios de seleção dos artigos foram definidos como critérios de inclusão a afinidade com o tema, a relevância do trabalho e a presença de uma aplicação prática, já como critérios de exclusão foram considerados a falta de afinidade com o tema e os assuntos envolvidos, redes e visualização, extensão do trabalho (resultado extremamente curtos, com uma ou duas páginas foram desconsiderados) e se é um trabalho em si (anais de eventos retornados foram desconsiderados).

IV. RESULTADOS PRELIMINARES

Após a realização da identificação dos estudos relacionados foram obtidos 212 resultados, que passaram pelo processo de seleção, sendo selecionados para a continuidade do estudo 64 trabalhos, conforme pode ser observado na Figura 3.

Aplicando a técnica de wordcloud nos resumos dos estudos selecionados, podemos verificar os termos mais presentes, entre eles: rede, dados, segurança, análise, visual e etc., como é possível visualizar na Figura 4.

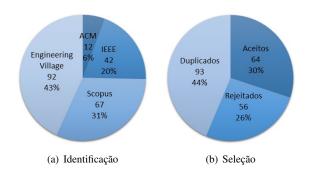


Figura 3. Resultados obtidos até o momento.



Figura 4. Wordcloud dos termos presentes nos resumos dos trabalhos aceitos na etapa de seleção.

V. Considerações Finais

O trabalho encontra-se ainda em estado inicial, podendo sofrer alterações significativas até sua finalização. Será dada continuidade a revisão sistemática, passando para a fase de extração. Finalizada a revisão a mesma será apresentada dentro da disciplina de Estudos Especiais e servirá como base para o desenvolvimento da dissertação.

REFERÊNCIAS

- I. Kotenko and E. Novikova, "Visualization of security metrics for cyber situation awareness," in 2014 Ninth International Conference on Availability, Reliability and Security, Sept 2014, pp. 506–513. [Online]. Available: http://ieeexplore.ieee.org/document/6980325/
- [2] V. T. Guimarães, C. M. D. S. Freitas, R. Sadre, L. M. R. Tarouco, and L. Z. Granville, "A survey on information visualization for network and service management," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 285–323, Firstquarter 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7166305/
- [3] S. Papadopoulos, K. Moustakas, A. Drosou, and D. Tzovaras, "Border gateway protocol graph: detecting and visualising internet routing anomalies," *IET Information Security*, vol. 10, no. 3, pp. 125–133, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7448516/
- [4] ABNT, NBR ISO/IEC 27002:2005 Tecnologia da informação Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.
- [5] Michaelis, "Dicionário eletrônico michaelis," 2017. [Online]. Available: http://www.michaelis.uol.com.br/moderno/portugues
- [6] T. Saydam and T. Magedanz, "From Networks and Network Management into Service and Service Management," *Journal of Networks and System Management*, vol. 4, no. 4, pp. 345–348, 1996.
- [7] T. Munzner, "Chapter 01. What?s Vis, and Why Do It?" in Visualization Analysis and Design, ser. AK Peters Visualization Series. A K Peters/CRC Press, oct 2014, pp. 1–19. [Online]. Available: http://dx.doi.org/10.1201/b17511-2
- [8] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of Systems and Software*, vol. 80, no. 4, pp. 571–583, apr 2007. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S016412120600197X