Visualização da Informações Aplicada à Segurança de Redes de Computadores

Um Estudo de Caso da Rede sem Fio da Unesp

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*—Com a necessidade de monitorar as redes de computadores, objetivou-se realizar um estudo para compreender a construção de uma ferramenta de monitoramento utilizando Visualização da Informação. Para tanto, procedeu-se com uma revisão sistemática sobre o assunto e um levantamento de requisitos junto aos gestores de rede da Unesp. Com a análise dos dados provenientes foi desenvolvida uma proposta de ferramenta e um protótipo. Desta forma, são observados os resultados que permitem concluir as tendências para criação da ferramenta e aplicabilidade dos conceitos validados com o protótipo.**

Área: Sistemas de Informação

I. Introdução

De modo a garantir o funcionamento de suas redes, o administrador de redes de computadores deve utilizar softwares para realizar o monitoramento delas. Entretanto, o monitoramento efetivo através do registro de todos os incidentes acabam por gerar uma quantidade considerável de dados. De modo a solucionar este problema, pode-se fazer uso das técnicas de Visualização da Informação, utilizando a visão humana para auxiliar a interpretação dos dados [1]. Quanto ao projeto apresentado neste trabalho, seu objetivo principal consiste em elaborar a arquitetura e implementar uma aplicação baseada em web para visualização das informações relacionadas a rede sem fio de uma universidade através de *dashboards*.

Guimaraes et al. realizou uma revisão sobre gerenciamento de redes, classificando 285 artigos publicados entre 1985 e 2013 [2]. Dasgupta et al. buscou compreender o fator humano na análise de fluxos de dados [3]. Bem semelhante ao presente trabalho pode-se citar o trabalho realizado por McKenna et al. utilizando também *dashboards* [4].

Na Seção II serão expostos conceitos para fundamentar o restante do trabalho. Na Seção III será descrito o cenário onde o trabalho se encontra inserido, será detalhado o problema tratado e será apresentada a proposta de solução e o protótipo criado, a seguir serão analisados e discutidos os resultados na Seção IV. Por fim, a Seção V contém a conclusão.

VIII Workshop do Programa de Pós-Graduação em Ciência da Computação: "A Visibilidade do Programa de Pós-graduação", Unesp, Presidente Prudente, 12 e 13 de novembro de 2018.

II. Conceitos e Técnicas

Segurança da Informação é descrita como a proteção das informações de diversas ameaças que buscam colocar em risco a continuidade de um negócio. A Segurança da Informação, de maneira simplificada, tem como preocupação o acesso das informações transmitidas pela rede por pessoas não autorizadas, para leitura ou mesmo modificação [5].

A Visualização da Informação busca representar conjuntos de dados como imagens, auxiliando na compreensão e tornando a interpretação destes mais eficiente. A criação de uma ferramenta de visualização deve ser realizada respondendo três perguntas: por que a tarefa está sendo executada, quais dados são exibidos, e como a linguagem de expressão é construída como opção de design [6]. O autor Colin Ware justifica o uso da visualização da seguinte maneira: "Por que deveríamos nos interessar em visualização? Porque o sistema visual humano é um buscador de padrões de enorme poder e sutileza. O olho e o córtex visual do cérebro formam um processador massivamente paralelo que fornece o canal com maior banda nos centros cognitivos humanos"[7].

Um *dashboard* é uma exibição visual das informações necessárias para alcançar um ou mais objetivos que se ajustam inteiramente a uma única tela de computador, de modo que possa ser monitorado rapidamente [8].

III. Metodologia de Desenvolvimento

A. Revisão Sistemática de Literatura

Foi realizada uma revisão sistemática de literatura sobre Visualização da Informação aplicada à Segurança de Redes de Computadores, realizada em diversas bases de dados e que depois das devidas fases de seleção resultou na inclusão de 60 estudos primários. Esta revisão mostrou tendências que contribuem no processo de construção, como o uso de linguagens compatíveis com o desenvolvimento Web e bibliotecas e *frameworks* visuais, tendências que contribuem com a definição do objetivo da ferramenta, como o foco no estado geral e detecção de anomalias gerais em redes TCP/IP e a tendência em se desenvolver uma técnica visual própria.

B. Cenário e análise de requisitos

O monitoramento da rede sem fio da Unesp é realizado através da ferramenta Zabbix, entretanto, algumas limitações são encontradas, principalmente no que se diz respeito ao acesso às informações dentro da interface. Devido à complexidade da rede sem fio da universidade, optou-se pelo desenvolvimento inicial de uma ferramenta utilizando o contexto de somente uma unidade universitária e posterior expansão para as demais. De modo a se obter uma ferramenta de monitoramento baseada em *dashboards* completa, buscou-se identificar, dentro da estrutura da universidade, os níveis organizacionais e mapear os dados presentes em seus respectivos *dashboards*.

C. Prototipação

Foi desenvolvido um protótipo utilizando as linguagens PHP e Javascript, com apoio da biblioteca de visualização D3.js, escrita em Javascript. Na Figura 1 pode-se ver os módulos que compõe o protótipo. Durante o processo de construção do protótipo, certas decisões foram tomadas acerca do design da aplicação, buscando agregar funcionalidades e melhorar a experiência do usuário. Na Figura 2 pode-se visualizar algumas das decisões de design citadas.

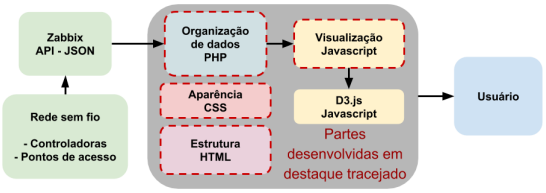

Figura 1. Diagrama mostrando os módulos que formam a aplicação, em destaque os que foram desenvolvidos.

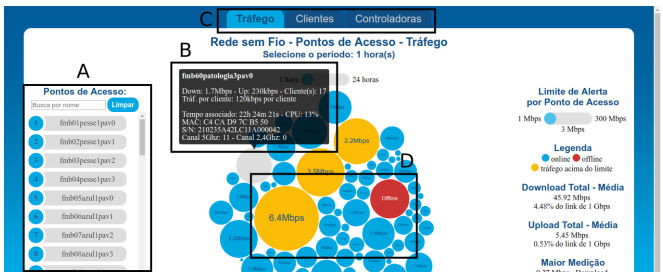

Figura 2. Decisões de design — Detalhe A mostra a lista lateral e o campo de busca, B mostra o detalhamento dos dados do ponto de acesso, C mostra as abas superiores e D mostra os elementos com as cores alteradas.

IV. Resultados Preliminares

Como resultado principal se tem a proposta desenvolvida com seu protótipo, ambos estão de acordo com o direcionamento obtido através da revisão sistemática de conteúdo e do levantamento de requisitos realizados.

A. Relevância e limitações

O presente projeto se mostra relevante principalmente por se tratar de uma aplicação concreta de diversas tecnologias e áreas da Computação, a construção do protótipo e o tratamento dos dados provenientes do Zabbix foram planejados de modo que a expansão para outras unidades fosse facilitada. Outro ponto relevante é a facilidade de uso em comparação com o Zabbix e sua interface.

Como limitação pode-se citar o problema de desempenho da aplicação, isso se deve a necessidade de consultar grandes quantidades de informações históricas sobre os equipamentos em um servidor fisicamente distante. No estado atual do protótipo não foi possível realizar testes com dados de outras unidades além da unidade universitária escolhida, por conta das permissões fornecidas para utilização do Zabbix centralizado.

B. Trabalhos futuros e continuidade

Para continuidade do projeto, a aplicação será reprojetada para atender aos perfis de uso identificados no levantamento de requisitos. A questão do desempenho será reestudada. Serão estudadas soluções para obtenção dos dados que foram previstos e que ainda não estão disponíveis. Está em desenvolvimento um módulo para definição e configuração dos parâmetros de conexão do Zabbix com a ferramenta de visualização. Será estudado um método de organização dos dados para filtragem dos pontos de acesso por prédios e departamentos.

V. Considerações Finais

O presente estudo buscou investigar a área de pesquisa da Visualização da Informação aplicada à Segurança de Redes de Computadores através da execução de uma revisão sistemática de literatura. A partir da realização desta revisão se desenvolveu uma proposta com apoio do Grupo de Redes de Computadores da Unesp para aplicação da Visualização da Informação à rede sem fio da universidade. Foi desenvolvido um protótipo para suprir a demanda, considerando no desenvolvimento as melhores práticas de design e aspectos de Segurança de Informação e Visualização da Informação.

Referências

[1] K. Jacobs, *Data-Driven Security: Analysis, Visualization and Dashboards*, 1st ed. Wiley Publishing, 2014.

[2] V. T. Guimaraes, 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 and Tutorials*, vol. 18, no. 1, pp. 285–323, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7166305/

[3] A. Dasgupta, D. L. Arendt, L. R. Franklin, P. C. Wong, and K. A. Cook, "Human Factors in Streaming Data Analysis: Challenges and Opportunities for Information Visualization," *Computer Graphics Forum*, sep 2017. [Online]. Available: http://doi.wiley.com/10.1111/cgf.13264

[4] S. McKenna, D. Staheli, C. Fulcher, and M. Meyer, "BubbleNet: A Cyber Security Dashboard for Visualizing Patterns," in *Proceedings of the Eurographics / IEEE VGTC Conference on Visualization*, ser. EuroVis '16. Goslar Germany, Germany: Eurographics Association, 2016, pp. 281–290. [Online]. Available: https://doi.org/10.1111/cgf.12904

[5] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*. Pearson Prentice Hall, 2011, vol. 52, no. 169. [Online]. Available: https://books.google.com.br/books?id=2xWHAQAACAAJ&hl=pt-PT&source=gbs_book_other_versions

[6] T. Munzner and E. Maguire, *Visualization analysis & design*, 2015.

[7] C. Ware, *Information Visualization: Perception for Design (Interactive Technologies)*. Morgan Kaufmann, 2004.

[8] S. Few, *Information dashboard design*. O'Reilly Sebastopol, CA, 2006.