Modelagem Conceitual para Proteção de Redes Segmentadas

Marcio Silva Cruz[1], Ferrucio de Franco Rosa[1,2]

[1] Universidade Campo Limpo Paulista (UNIFACCAMP)
Campo Limpo Paulista – SP – Brasil
[2] Centro de Tecnologia da Informação Renato Archer (CTI)
Campinas – SP – Brasil

cruzmarcios@hotmail.com, ferrucio.rosa@cti.gov.br

Abstract. *A research project is presented aiming at developing a conceptual model for protecting segmented networks. We aim to identify, formalize and relate important concepts, map vulnerabilities and attacks, in addition to describing risk protection or mitigation processes. Specifically, it addresses the development of a domain ontology aimed at identifying and modeling vulnerabilities and attacks on VLANs.*

Resumo. *Um projeto de pesquisa é apresentado com o objetivo de desenvolver uma modelagem conceitual visando a proteção de redes segmentadas. Busca-se identificar, formalizar e relacionar conceitos importantes, mapear vulnerabilidades e ataques, além de descrever processos de proteção ou mitigação de riscos. Especificamente, aborda-se o desenvolvimento de uma ontologia de domínio voltada a identificar e modelar as vulnerabilidades e ataques a VLANs.*

Palavras-chave – *Ameaça, Ataque, Ontologia, Rede, Segmentação, Segurança, Taxonomia, Vulnerabilidade, VLAN.*

1. Contexto e Revisão da Literatura

A modelagem conceitual de vulnerabilidades e ataques relacionados a VLANs (*Virtual local Area Network*) é crucial para propiciar a construção de métodos e técnicas sistemáticas de proteção de infraestruturas críticas. Ontologias podem contribuir neste contexto, pois são ferramentas de modelagem que possibilitam a formalização dos conceitos principais e de seus relacionamentos, além de possibilitar a criação de regras semânticas que podem ser usadas por sistemas inteligentes.

Uma revisão sistemática de literatura [Cruz et al. 2021] foi conduzida, onde foram analisados 18 artigos. Este mapeamento do estado da arte apontou métodos, modelos, ferramentas e domínios de aplicação que serviram de base para o desenvolvimento de uma ontologia de vulnerabilidades e ataques a redes VLAN.

Neste artigo, apresenta-se uma conceituação preliminar das classes principais na forma de uma taxonomia, a saber: VLAN, Ataque, Vulnerabilidade e Vetor de Ataque. O restante deste artigo está organizado da seguinte maneira: a Seção 2 descreve uma síntese do desenvolvimento do projeto; a Seção 3 apresenta uma visão geral da ontologia de domínio; e a Seção 4 aponta os objetivos a serem alcançados e considerações finais.

2. Síntese do Projeto de Pesquisa

No desenvolvimento do projeto, os objetivos e processos para uma modelagem conceitual visando a proteção das redes segmentadas são apresentados, identificando e modelando as vulnerabilidades inerentes a esta tecnologia e seus respectivos ataques. Para isso, um modelo conceitual é construído apoiado por uma ontologia de domínio.

Pretende-se: (i) Formalizar e relacionar conceitos importantes; (ii) Mapear vulnerabilidades e ataques a VLANs; (iii) Descrever processos de proteção ou mitigação de riscos; e (iv) Criar uma ontologia de domínio.

Os métodos técnico-científicos necessários à execução do projeto são oriundos da área de Ciência da Computação, especificamente, conhecimentos em segurança da informação, redes de computadores e modelagem conceitual, bem como, compreender os mecanismos e ferramentas voltados a construção de ontologia.

O projeto encontra-se na fase em que os conceitos estão sendo definidos e relacionados, e as instâncias sendo criadas. Na próxima seção, apresenta-se uma conceituação preliminar de classes importantes para entendimento do contexto da modelagem.

3. Ontologia de Domínio: conceituação preliminar em forma de taxonomia

O projeto de uma ontologia é um processo iterativo para determinar o escopo e definir os conceitos (classes), propriedades, relações, axiomas, restrições e instâncias. Este projeto de pesquisa está sendo desenvolvido observando essas características e a implementação será feita em *Web Ontology Language* (OWL) [W3C OWL Working Group 2012]. Ontologias baseadas em OWL possuem recursos ricos para definir inequivocamente relações e hierarquias complexas e verificar suas consistências por meio de inferência, além de representar informações que não são apenas legíveis por humanos, mas também compreensíveis por máquina [Syed et al. 2016].

Nesta seção, apresenta-se, em forma de taxonomia, uma visão geral da ontologia que está sendo construída, contendo as principais classes (Figura 1). *VLAN* é uma tecnologia capaz de separar redes em domínios específicos. *ATAQUES* às VLANs podem afetar os ambientes computacionais, causando interrupções nos serviços e outros problemas de segurança. Estes ataques exploram *VULNERABILIDADES* e características de operação das VLANs para obter acesso a informações críticas.

Uma conceituação preliminar das classes *VETOR DE ATAQUE* e *IMPACTO DO ATAQUE* é apresentada. A Classe *VETOR DE ATAQUE* descreve como os ataques atingem seus ativos e a Classe *IMPACTO DO ATAQUE* descreve que tipo de *PROPRIEDADE DE SEGURANÇA* [Rosa et al. 2018] um ataque influenciará. Exemplos do uso da Classe *PROPRIEDADE DE SEGURANÇA* é apresentado na Subseção 3.2.

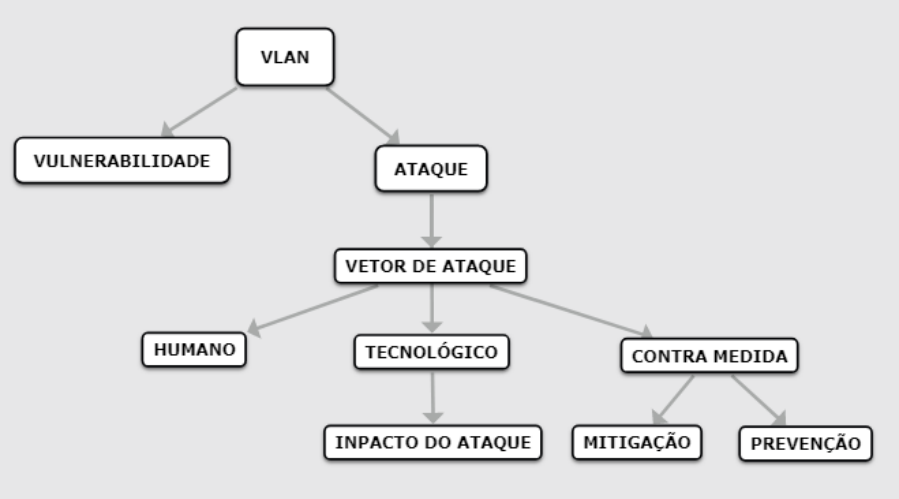

Figura 1. Taxonomia de Vulnerabilidades e Ataques a VLANs

3.1 Vetor de Ataque

Um vetor de ataque é definido como um caminho pelo qual um invasor pode obter acesso a um dispositivo computacional, sendo a característica mais importante do ataque. Essa definição também inclui vulnerabilidades, pois podem ser exigidas várias vulnerabilidades para se iniciar um ataque bem-sucedido. Pode ser difícil classificar um ataque em um dos vetores de ataque, pois quando há ataques combinados (e.g., Ataque ARP ou Salto de VLAN [Convery 2004] poderão ser usados vários meios para atingir o alvo. No entanto, vetores de ataque podem ser mapeados e expressos em uma ontologia. Nos próximos parágrafos são exemplificadas algumas instâncias da Classe *VETOR DE ATAQUE*.

Ataque ARP. O Protocolo de Resolução de Endereço (*Adress Resolution Protocol* – ARP) é responsável por mapear endereços de Controle de Acesso ao Meio (*Media Access Control* – MAC) em uma rede local. Quando um endereço de MAC não é conhecido, um pacote ARP-REQUEST é enviado usando uma solicitação de difusão de rede na forma da pergunta "Qual é o endereço MAC de um dispositivo configurado com o endereço IP incluso?". Por outro lado, é possível que um dispositivo envie seu MAC a todos, sem que uma solicitação seja feita. Nesse caso o pacote enviado é um G ARP (*Gratuitous* ARP). O intruso se aproveita dessas possibilidades e identifica o MAC do dispositivo-alvo, o qual deseja se passar por ele, e envia um G ARP (endereço MAC do dispositivo-alvo). O *switch*, ao recebe-lo, atualizará sua tabela MAC com o novo IP correspondente ao endereço MAC recebido, e adicionará a informação ao *cache* da tabela ARP. Assim, todo tráfego que for destinado ao endereço MAC do dispositivo-alvo, será encaminhado ao dispositivo do intruso. Através deste ataque, é possível causar Negação de Serviço (*Denial of Service* – DoS), ou ser usado como vetor de um ataque MITM (M*an In The Middle*).

Ataque Salto de VLAN. VLAN *Hopping* é um ataque à rede segregada em que o intruso envia pacotes destinados a um dispositivo em uma VLAN diferente, normalmente não alcançada por ele. Este tráfego é marcado com um ID de VLAN diferente a que o intruso pertence e, comportando-se como um *switch*, pode negociar entroncamento possibilitando enviar e receber tráfego entre outras VLANs. Como o

invasor pode acessar outras VLANs, isso é denominado ataque de salto de VLAN. Na configuração de um sistema para se passar por um *switch* (*Switch-Spoofing*), exige-se que o intruso tente se conectar usando os protocolos de marcação e entroncamento apropriados, por exemplo, emular o protocolo IEEE 802.1Q, protocolo de entroncamento de VLAN e o Protocolo de Tronco Dinâmico (DTP). Assim, o intruso é capaz de simular uma porta *trunking* e negociar através do DTP com outro *switch*; caso obtenha sucesso, o intruso será membro de todas as outras VLANs. Consequentemente, será possível causar DoS, ou MITM.

Ataque Estouro da Tabela CAM. Este ataque se concentra na tabela da Memória Endereçável de Conteúdo (CAM), que armazena informações como endereços de MAC em uma porta física, juntamente com os parâmetros de VLAN associados. Tabelas CAM têm tamanho fixo, o que as torna um alvo de ataque. Tal qual um ataque de estouro de *buffer*, o objetivo é preencher a Tabela CAM. O invasor fica em uma porta física e gera um grande número de entradas MAC. Quando a tabela CAM atinge seu limite, o tráfego sem uma entrada CAM é enviado em todas as portas da VLAN em questão. O tráfego com uma entrada CAM não é afetado, mas os *switches* adjacentes podem ser [Watkins e Wallce 2008].

3.2 Propriedades de Segurança Afetadas pelos Ataques

Propriedades de Segurança são atributos ou características da segurança da informação. Embora se tenha utilizado na conceituação 6 propriedades de segurança (*Disponibilidade, Integridade, Confidencialidade, Autenticidade, Privacidade e Resiliência*), outras propriedades podem ser incorporadas, dependendo da abordagem a ser considerada. A seguir as propriedades utilizadas são definidas sinteticamente e os principais ataques, no contexto de VLAN, que afetam as propriedades são apresentados.

Disponibilidade – Esta propriedade visa garantir que os usuários tenham acesso a informações e recursos. O principal ataque contra a disponibilidade é a Negação de Serviço Distribuída (DDoS), onde os recursos de computação e comunicação de um sistema podem ser esgotados rapidamente, impactando a disponibilidade do sistema.

Integridade – Esta propriedade é definida como a capacidade de se proteger contra a modificação indevida das informações, i.e., garantir que as informações dos sistemas não foram interceptadas e modificadas indevidamente. O principal ataque contra a integridade é o Ataque ARP.

Confidencialidade – Esta propriedade é referente à garantia de que as informações dos sistemas não serão divulgadas ou reveladas a entidades não autorizadas. O principal ataque contra a confidencialidade é o Ataque ARP.

Autenticidade – Esta propriedade confirma a veracidade de uma informação, documento ou ato de uma entidade (informação autêntica). Os principais ataques são Phishing e MITM.

Privacidade – Esta propriedade é referente a garantia de que o sistema não divulgará informações pessoais (intimidade pessoal) sem autorização. O principal ataque contra a privacidade é o Ataque ARP.

Resiliência – Esta propriedade é a garantia de que o sistema seja capaz de operar sob condições extremas, como ataques cibernéticos. Os principais ataques são Dos e DDos

3.3 Impacto do Ataque

O impacto do ataque é a violação dos atributos ou propriedades de segurança que consequentemente influenciará o nível de impacto. O *Impacto do Ataque* possui níveis de impacto, de forma qualitativa, como segue:

Crítico – quando um intruso possui controle total sobre o alvo, até o ponto em que as operações não poderão ocorrer, ou possui acesso a informações críticas.

Alto – quando um intruso possui controle significativo sobre o alvo ou possui acesso a informações críticas.

Médio – quando um intruso possui controle moderado sobre o alvo ou acesso às informações moderadamente importantes.

Baixo – quando um intruso possui controle mínimo sobre o alvo ou somente acesso a informações relativamente sem importância.

Por exemplo, como o Ataque ARP pode afetar tanto a *Integridade quanto a Confidencialidade e Privacidade*, ao se analisar o impacto desse tipo de ataque, o nível é considerado crítico.

4. Considerações Finais

Neste artigo, apresentou-se o projeto de pesquisa em andamento, que aborda o desenvolvimento de uma ontologia de domínio destinada a identificar e modelar vulnerabilidades e ataques a redes VLAN. Pretende-se, ao final do projeto, formalizar e relacionar os conceitos, mapear vulnerabilidades e ataques a redes VLAN, apresentar um conjunto core de processos de proteção ou mitigação de riscos e criar uma ontologia de domínio em OWL usando a ferramenta *Protégé*.

Por meio de técnicas de modelagem conceitual, este trabalho destina-se a ser útil para pesquisadores que buscam desenvolver métodos e processos sistemáticos baseados em ontologia voltados à proteção de ataques a redes segmentadas.

5. Referências

Convery, S. Network Security Architectures **-** Expert guidance on designing secure. 1ª ed. Indianapolis – USA.: Cisco Press, 2004.

Cruz, M. S.; De Franco Rosa, F.; Jino, M. A Study on Ontologies of Vulnerabilities and Attacks on VLAN. In: LATIFI, S. (Ed.). Advances in Intelligent Systems and Computing. 1ª ed. Cham - Switzerland: Springer, Cham, 2021. p. 115–119.

De Franco Rosa, F.; Jino, M.; Bonacin, R. Towards an Ontology of Security Assessment: A Core Model Proposal. Advances in Intelligent Systems and Computing, v. 738, n. April, p. 75–80, 2018.

Syed, Z. et al. UCO: A Unified Cybersecurity Ontology. AAAI Workshop - Technical Report, v. WS-16-01, p. 195–202, 2016.

W3C OWL Working Group. W3C OWL Web Ontology Language. Disponível em: <https://www.w3.org/TR/owl2-overview/>. Acesso em: 19 ago. 2022.

Watkins, M.; Wallace, K. CCNA Security **-** Official Exam Certification Guide. 1ª ed. Indianapolis – USA.: Cisco Press, 2008.