BrEduDevice: Um Mecanismo Eficaz para a Gestão de Identidades em Sistemas de Detecção de Intrusão Federados

Helio N. C. Neto, Diogo M. F. Mattos, Natalia C. Fernandes

[1]MídiaCom - PPGEET/TET/UFF
Universidade Federal Fluminense - UFF

Resumo. *Sistemas de detecção de intrusão (Intrusion Detection System — IDS) baseados em aprendizado federado treinam um modelo de aprendizado de máquina global baseado na agregação de modelos locais dos IDS participantes, sem o compartilhamento de dados privados sobre cada rede local ou que transitam nessas redes. Contudo, a criação desse tipo de serviço depende da formação de uma federação confiável, com a devida gestão dos participantes e de suas contribuições no ambiente de aprendizado colaborativo. Este trabalho projeta um mecanismo de gestão de identidade federado para a criação de um serviço colaborativo de IDS entre as instituições de ensino usuárias da Comunidade Acadêmica Federada (CAFe). Para que dispositivos autentiquem na CAFe, é proposto um novo esquema chamado BrEduDevice para armazenar atributos referente a um dispositivo. A proposta de autenticação de dispositivos via Shibboleth estende o fluxo de autenticação para utilizar certificados digitais.*

1. Introdução

Soluções de análise de tráfego de rede baseadas em modelos de aprendizado de máquina centralizados são propostas promissoras, pois produzem alta acurácia na identificação de ameaças quando treinadas com uma ampla base de dados rotulados [Andreoni Lopez et al., 2019, Viegas et al., 2019]. Contudo, apesar da qualidade do aprendizado de máquina centralizado, seu perímetro de atuação é reduzido, visto que o modelo só aprende com base em dados provenientes de sua rede local. Com o advento do aprendizado federado [Brendan McMahan et al., 2017], surge a possibilidade de treinamento colaborativo, no qual os participantes treinam colaborativamente um modelo de aprendizado de máquina global, de forma distribuída e sem compartilhamento de dados. O objetivo do aprendizado federado é efetuar o treinamento do modelo global, processando os dados localmente nos dispositivos, gerando modelos locais e agregando no modelo global. Durante o processo de treinamento, os participantes treinam um modelo local compartilhado colaborativamente, mantendo os dados no dispositivo do participante. Assim, os dispositivos dos participantes enviam atualizações intermediárias a um servidor central durante cada iteração de agregação. O servidor agrega os modelos intermediários e distribui o novo modelo agregado aos participantes.

O IDS baseado em aprendizado federado funciona em um ambiente colaborativo e, então, é necessário que todos os participantes tenham comprometimento e responsabilidade nas suas colaborações para o modelo global. Há, portanto, a necessidade de se construir uma federação em que exista confiança entre os participantes. Tal confiança pode ser obtida por uma gestão de identidades eficiente, que garanta a autenticação, a

Este trabalho foi realizado com recursos da CNPq, CAPES, FAPERJ e RNP.

rastreabilidade e o não-repúdio, de forma em que participantes não colaborativos ou que prejudiquem o ambiente colaborativo possam ser excluídos da federação do serviço de IDS.

Este trabalho tem como principal objetivo o projeto de um mecanismo de gestão de identidade para um sistema de detecção de intrusão federado [Cunha Neto et al., 2021]. Esse sistema de detecção funciona como uma organização virtual, na qual membros de cada instituição da federação poderão colaborar com modelos locais de detecção de intrusão ou apenas receber o modelo global, caso possam se beneficiar dele mas não sejam autorizados para contribuir. A federação proposta usa a Comunidade Acadêmica Federada (CAFe) como base, pois é uma federação de identidade amplamente adotada por instituições de ensino e pesquisa brasileira. Uma das contribuições deste trabalho é a proposta de um novo esquema LDAP, chamado `BrEduDevice`, para armazenar atributos referentes a um dispositivo, permitindo, assim, identificar e autenticar dispositivos. Para autenticar os dispositivos, propõe-se a extensão do fluxo de autenticação Shibboleth para dispositivos utilizando certificado digital. A proposta considera que o provedor de serviço (*Service Provider* — SP) possui o certificado de todos os provedores de identidade (Identity Provider — IdP) da federação e, assim, autentica apenas dispositivos que se autenticam com certificados assinados por essas autoridades de certificação (*Certification Authority* — CA). O fluxo de autenticação utiliza o perfil *Enhanced Client or Proxy* (ECP) para autenticar os dispositivos, pois o perfil permite autenticação sem a utilização do navegador.

2. Fluxo de Autenticação Baseado em Certificado

A CAFe permite uma autenticação federada de pessoas pertencentes a diferentes instituições, podendo ser utilizada na implementação de diversos serviços. Dentro desse contexto, surge a necessidade de autenticar dispositivos associados a essas instituições. Para tanto, há que se garantir um modelo que associe dispositivos a usuários autorizados, de tal forma que o dispositivo possa se autenticar de forma segura, sem o uso da credencial do usuário responsável pelo dispositivo. No caso do cenário de IDS federado, o dispositivo é o IDS participante. Nesse sentido, a credencial do dispositivo consiste de um certificado que é assinado pelo IdP. No mecanismo proposto, todo IdP é uma autoridade certificadora que é responsável por assinar os certificados dos participantes. O SP possui uma lista com o certificado de todos os IdPs que fazem parte da federação. Assim, quando um usuário solicita um recurso ao SP utilizando seu certificado assinado pelo IdP, o SP consegue redirecionar a autenticação ao IdP responsável por este usuário.

A autenticação dos dispositivos é feita através de um fluxo de autenticação Shibboleth modificado. Para isso, o modelo utiliza um fluxo de autenticação multi-fator. Esse fluxo de autenticação verifica se a autenticação é oriunda de um navegador ou utiliza o perfil ECP. No caso da autenticação oriunda de um navegador, significa que um usuário está tentando se autenticar. Logo, a autenticação deve ser feita através de usuário e senha. Entretanto, se a autenticação é feita através do perfil ECP, significa que um dispositivo esta tentando se autenticar. No fluxo de autenticação de dispositivos proposto, o IDS participante envia uma solicitação de autenticação utilizando o seu certificado. O SP verifica se quem assinou o certificado do dispositivo foi um IdP cadastrado. Em caso positivo, o SP encaminha o dispositivo ao IdP para autenticação. O dispositivo envia uma solicitação de autenticação ao IdP utilizando seu certificado. O IdP verifica se o certificado do dis-

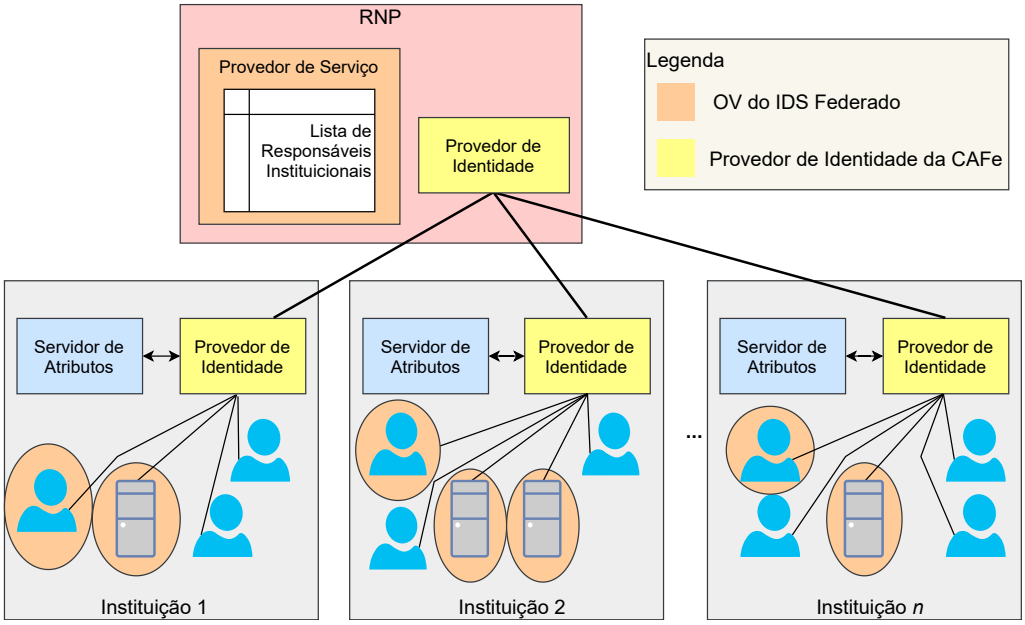

Figura 1. Arquitetura do mecanismo de gestão de identidade para autenticação de dispositivos. No mecanismo proposto, os dispositivos e seu responsável institucional farão parte da OV.

positivo está válido e não foi revogado pelo usuário que cadastrou o dispositivo na CAFe. Caso o certificado pertença a um dispositivo da infraestrutura do IdP, então, o IdP cria uma asserção *Security Assertion Markup Language* (SAML) para liberação do acesso ao dispositivo. Então, o dispositivo pode receber o modelo global que é basicamente o modelo de aprendizado de máquina treinado colaborativamente para detectar intrusões.

O cadastro de um IDS participante é feito por um usuário previamente autorizado no IdP, chamado de responsável institucional. Para cadastrar um IDS participante, deve-se preencher os atributos definidos no esquema `BrEduDevice`. Cada dispositivo é associado a um responsável dentro da instituição, responsável pela gerência e operação da máquina. Após o preenchimento, o IdP entrega como saída o ID de usuário do IDS e seu certificado assinado. Ao acessar pela primeira vez o serviço, entradas adicionais relativos ao novo IDS são inseridas no provedor de atributos no provedor de serviço do IDS federado.

O mecanismo de gestão de identidade para o sistema de IDS federado é uma Organização Virtual (OV) formada pelos responsáveis institucionais e IDSs participantes, como pode ser visto na Figura 1. O cadastro, exclusão e atualização fazem parte das atribuições dos responsáveis institucionais.

3. O Esquema BrEduDevice

O esquema `BrEduDevice` é responsável por armazenar atributos de um dispositivo genérico. Esse esquema será utilizado como base para autenticar os IDS participantes da federação. O Esquema `BrEduDevice` é concebido para fornecer atributos básicos de dispositivos no meio acadêmico. Alguns atributos específicos para o IDS federado devem ser armazenados em um provedor de atributos dinâmicos, tal como o COmanage[1]. A Tabela 1 apresenta os atributos do esquema `BrEduDevice` proposto.

[1]https://incommon.org/software/comanage/. Acessado em 09/09/2021

Atributo	Descrição	Mandatório
ID	Identificador único do dispositivo	Sim
Nome	Nome ou apelido do dispositivo	Sim
Responsável	DN do responsável pelo dispositivo	Sim
Certificado	Certificado assinado pelo IdP	Sim
Departamento	Departamento alocado ao dispositivo	Sim
Organização	Organização responsável pelo dispositivo	Sim
Número de Patrimônio	Número de patrimônio associado	Sim
Data de Aquisição	Data em que o dispositivo foi comprado	Sim
Data de Desativação	Data da desativação do dispositivo	Não
Número de Série	Número de série do dispositivo, se houver.	Não
Endereço MAC	Endereço MAC da placa de rede	Não
Endereço IP	Endereço IP atribuído ao dispositivo	Não
Endereço Inst.	Endereço em que o dispositivo se encontra	Não
Dispositivo Móvel	Campo marcado quando o dispositivo é móvel	Não

Tabela 1. Tabela contendo os atributos do esquema `BrEduDevice`. O DN será uid='id_dispositivo', ou=devices, dc='instituição', dc=br. O objectclass é brEduDevice.

4. Conclusão

Em um ambiente de detecção de intrusão baseado em aprendizado federado há a necessidade da criação de uma federação na qual exista confiança entre os participantes. Essa federação deve prover autenticação dos dispositivos participantes e armazenar atributos que promovam a identificação de participantes que possuem dados que melhor contribuem com o treinamento. Este trabalho propôs um mecanismo para a gestão de identidade para um serviço de IDS Federado. Essa federação visa garantir que apenas IDS autorizado participem do treinamento, além de armazenar atributos importantes para o treinamento.

Referências

Andreoni Lopez, M., Mattos, D. M., Duarte, O. C. M. e Pujolle, G. (2019). Toward a monitoring and threat detection system based on stream processing as a virtual network function for big data. *Concurrency and Computation: Practice and Experience*, 31(20):e5344.

Brendan McMahan, H., Moore, E., Ramage, D., Hampson, S. e Agüera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. Em *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, AISTATS 2017*, volume 54.

Cunha Neto, H. N., Mattos, D. M. F. e Fernandes, N. C. (2021). Fedsa: Arrefecimento simulado federado para a aceleração da detecção de intrusão em ambientes colaborativos. Em *Anais do XXXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, p. 280–293, Porto Alegre, RS, Brasil. SBC.

Viegas, E., Santin, A., Bessani, A. e Neves, N. (2019). Bigflow: Real-time and reliable anomaly-based intrusion detection for high-speed networks. *Future Generation Computer Systems*, 93:473 – 485.