Projeto de Formatura – 2023

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia de Computação

Tema: **Proposta de melhoria da expressividade de credenciais SPIFFE para gerenciamento de identidades em ambientes federados**

Introdução

Dezenas de milhares de ataques cibernéticos ocorrem anualmente segundo técnicas de *phishing* ou roubo de credenciais de funcionários. Com o advento de aplicações em nuvem e a disseminação da força de trabalho móvel o acesso a recursos é feito a partir de diferentes redes. Esses fatores contribuem para um aumento da suscetibilidade a eventuais ataques.

Nesse contexto, o gerenciamento seguro de identidades - *Identity Management* - refere-se ao conjunto de métodos e práticas usados durante o manuseio de identidades digitais de participantes de um sistema, sejam eles indivíduos, *softwares* ou *hardwares*. Uma solução de IdM federado capaz de permitir a identificação segura de sistemas de *software* em ambientes dinâmicos e heterogêneos é o *Secure Identity Framework for Everyone* - SPIFFE. Os documentos de identidade verificáveis representando a identidade de um componente de *software* é um SVID - *SPIFFE Verifiable Identity Document*. São documentos que existem na modalidade de dois certificados comumente utilizados: X.509 e JWT.

Objetivo: avaliar o desempenho do SPIFFE valendo-se de um novo formato de credencial visando melhorar a *performance* do *framework*. O nome dessa melhoria é *Lightweight SVID*.

Figura 1. Logotipo do *framework open-source* do SPIFFE para gerenciamento de identidades.

Metodologia

O diagrama da figura 2 representa a arquitura básica da prova de conceito utilizada para a simulação do uso de credenciais SVID no SPIFFE.

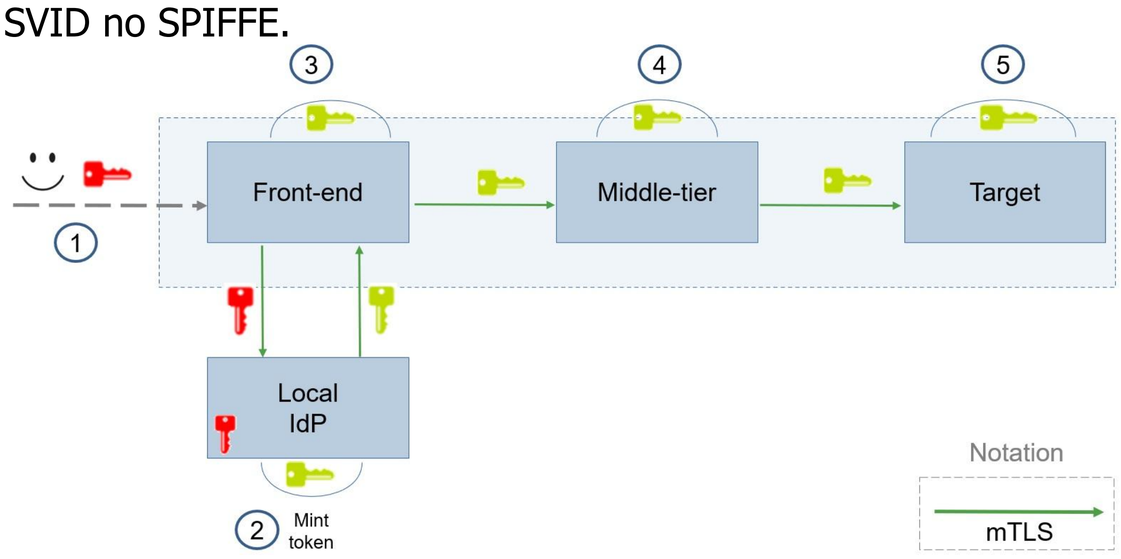

Figura 2. Arquietura da aplicação base para posterior análise de desempenho de SVIDs.

O modo de funcionamento em questão será o *modo ID*. Nele, de maneira análoga a uma *Public Key Infrastructure* - PKI - o *SPIRE server* age como uma autoridade certificadora raiz no sentido de ser um fornecedor de identidade (*Identity Provider*) seguro pelo qual as *workloads* conseguem obter um SVID.

Nesse cenário, o documento de identidade proposto como melhoria em substituição aos SVIDs nativos do SPIFFE pode funcionar segundo duas maneiras: (1) envio do LSVID como parte da requisição; e (2) LSVID como parte do campo *issuer* no *payload* antes de assinar e enviar à *workload* seguinte. No segundo caso, seria possível verificar todas as *workloads* anteriores ao (*n+1)-ésimo workload* segundo os seguintes passos:

$$\text{true} \xleftarrow{?} \text{Verify}\,(\mathcal{L}_n,\ \mathcal{L}_n.pk_n) \Rightarrow \text{true} \leftarrow \text{Validate}\,(pk_{n+1}, \mathcal{L}_n)$$

As experiências consistiram na simulação do *modo ID* com SVIDs nativos e LSVIDs (modificação proposta) para comparação entre o formato baseado em certificados X.509 e aquele que pretende-se apresentar como alternativa mais leve.

A captação de requisições, bem como toda a automatização da repetição do processo a fim de obter um número considerável de dados a serem analisados (e em intervalo coerente com uma aplicação executando em cenário real) foram feitas com as tecnologias *Prometheus* e *Apache Jmeter*.

Figura 3. Ferramentas para obtenção e análise de dados na prova de conceito da credencial LSVID.

Os resultados obtidos demonstraram a viabilidade do LSVID em comparação ao SVID de modo a se obter *tokens* menores e mais leves e garantir a expressividade das identidades emitidas ao longo de todo o caminho da aplicação.

Conclusão

A utilização de credenciais mais leves e capazes de manter a expressividade demonstraram uma melhora de desempenho na aplicação hipotética usada como prova de conceito da proposta de melhoria.

Agradecimentos

Integrantes: Lucas R. Cupertino Cardoso

Professor(a) Orientador(a): Prof. Dr. Marcos Antônio Simplicio Jr.