Projeto de Formatura – 2023 – Press Release
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

---

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.

O objetivo do trabalho foi 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*. O diagrama da figura 1 representa a arquitura básica da prova de conceito utilizada para a simulação do uso de credenciais SVID no SPIFFE.

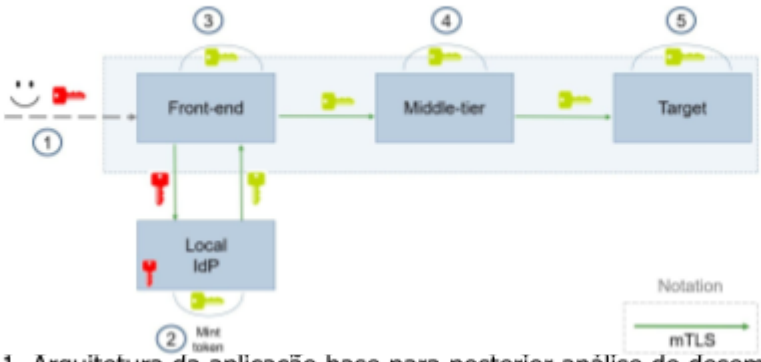

Figura 1. Arquitetura da aplicação base para posterior análise de desempenho dos SVIDs.

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.

Para a exposição dos resultados obtidos foi apresentada uma simulação da aplicação com acompanhamento dos *logs* de execução utilizado para o rastreamento do documento de identidade.

Integrante: Lucas R. Cupertino Cardoso
Professor(a) Orientador(a): Prof. Dr. Marcos Antônio Simplício Jr.