Benchmark study for multiple security documents enhancing SPIFFE/SPIRE environment

Henrique Zanela Cochak[1], **Charles Christian Miers**[1]

[1]Graduate Program in Applied Computing - Santa Catarina State University (UDESC)

henrique.zc@edu.udesc.br,

charles.miers@udesc.br

Abstract. *After specifying and creating new security tokens and cryptographic algorithms under the 'Secure Federated Identity Management: Enhancing and Extending the SPIFFE Architecture" project, a performance assessment is required to measure and compare the computational efficiency, execution speed, and resource consumption of each security token and algorithm. This paper proposes the analysis employing Docker and Kubernetes environments as initial study cases.*

1. Introduction

One of the biggest open-source Identity and Access Management (IAM) solution related to workloads authentication is the Secure Production Identity Framework for Everyone (SPIFFE) framework, focusing on generating identities for workloads [SPIFFE 2024] and plays a pivotal role in enabling organizations to manage workload identities, ensuring verifiable mTLS connections between services [Feldman et al. 2020]. Its main specifications cover service identification through SPIFFE IDs, a string that uniquely and specifically identifies a workload as Uniform Resource Identifiers (URIs) format, encoding it a cryptographically-verifiable document defined as SPIFFE Verifiable Identity Document (SVID), and the APIs for SVID issuance and retrieval.

The current scope of SPIFFE centers around workload identity and authentication in distributed systems, but the authentication context is currently limited to the identity of the workload directly sending or receiving a message, and currently does not possess support for end-user delegation unlike protocols such as OAuth 2.0, SAML, or OpenID Connect. To enhance the SPIFFE capabilities without going beyond its scope, the project "Secure Federated Identity Management: Enhancing and Extending the SPIFFE Architecture" first created a new security document to address the issue of delegated identity assertions in a systematic manner, binding a user's identity token to the workload authorized to make requests on that user's behalf whereas a very similar concept is used by Microsoft with its "on-behalf-of flow" [Microsoft 2024]. A second improvement includes a new token model called "nested token", originally based on Biscuits security model [Biscuits 2024], implementing a decentralized mechanism allowing local token creation or extension with authenticated statements, expanding new novel validation mechanisms and digital signature formats, with innovative schemes for token issuance and extension, while adding the possibility of traceability of a token flow across multiple services. Lastly incorporate a new security token directly into the SPIFFE framework, allowing new types of document with multiple/concatenate signatures, reduced token validation cost and size, depending on the pre-selected scheme.

2. Proposal

Analyzing the project as a whole, this paper proposes a benchmark study of the computational consumption of each new token, which may encompass different cryptography algorithms with its own life cycle, and inspect specific goals such as token size and growth whenever the nested model is utilized considering the main use cases considered inside the project. The performance assessment will first be held with the Docker platform, as it provides a controlled, reproducible setting for benchmarking and easy portability, thus providing the initial step for comparison. The next step involves the container orchestration Kubernetes. This strategic shift is motivated by Kubernetes' strengths in orchestrating containers, enabling scalable, flexible, and efficient management of diverse workloads and this transition aligns with the project's goal of accommodating increased complexity and dynamic resource requirements while maintaining a focus on ease of use and scalability, eventually to study the behavior of such security tokens and algorithms under this concept. This choice is important due to an understanding of the behavior of algorithms close to commercial microservices environments within possible federated architectures is relevant for the addition of such algorithms within the SPIFFE/SPIRE framework.

All resource capture will be performed by the Prometheus monitoring system tool [Prometheus 2024], which provides a high-granularity capture routine, reaching values as small as milliseconds. This tool collects and stores your metrics as time series data, meaning metric information is stored with the timestamp it was recorded, along with optional key-value pairs called labels. This tool was chosen for two reasons: the ability to monitor and capture time series in microservices environments, and because there is the possibility of its complete operation in a Golang package, allowing its addition in a simpler way in the proof of concept of the project. Another tool to help achieve the goal is the Apache JMeter, a tool to test and simulate web requests between endpoints.

Acknowledgements: This work was supported by Hewlett Packard Enterprise (HPE), and in part by CNPq (grant PQ 304643/2020-3), FAPESP (grant 2020/09850-0), and CAPES (Finance Code 001). This work was funding by FAPESC, UDESC, USP and developed at LabP2D/LARC.

References

Biscuits (2024). Biscuits cryptography reference. https://doc.biscuitsec.org/reference/getting-started/introduction. Accessed in: 01 Feb. 2024.

Feldman, D., Fox, E., Gilman, E., Haken, I., Kautz, F., Khan, U., Lambrecht, M., Lum, B., Fayó, A. M., Nesterov, E., Vega, A., and Wardrop, M. (2020). Solving the bottom turtle — a SPIFFE way to establish trust in your infrastructure via universal identity.

Microsoft (2024). Microsoft identity platform and OAuth 2.0 On-Behalf-Of flow. https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-on-behalf-of-flow.

Prometheus (2024). Introduction. https://prometheus.io/docs/introduction/overview/. Accessed in: 01 Feb. 2024.

SPIFFE (2024). Spiffe concepts. https://spiffe.io/docs/latest/spiffe-about/spiffe-concepts/.