University : T.C. İstanbul Kultur University
Institute : Institute of Graduate Studies
Department : Computer Engineering
Program : Computer Engineering
Supervisor : Assis. Prof. Dr. Öznur ŞENGEL
Degree Awarded and Date : Master's – June 2024

ABSTRACT

In the evolving landscape of software architecture, the microservice paradigm has emerged as a robust solution for creating scalable and maintainable systems. A critical challenge within this architecture is ensuring secure inter-service authentication and authorization, particularly in synchronous communication. This thesis delves into the intricacies of the JSON Web Token (JWT) mechanism, a prevalent method for securing these communications.

Extensive literature research was conducted to assess current approaches, highlighting both ineffective practices and innovative strategies. A predominant trend identified is the adoption of the SHA2-512 hashing algorithm for token signing. Despite its popularity, SHA2-512 has demonstrated vulnerabilities to length extension attacks, posing significant security risks.

To address these concerns, this research advocates for the implementation of the SHA3-512 hashing algorithm within the JWT mechanism. Even though SHA3 is not natively supported by JWT libraries within the Spring Boot framework which was used for the development of the application, another mechanism which allowed us to apply SHA3 in the token signing was adopted. SHA3-512 offers enhanced resilience against such attacks owing to its fundamentally different cryptographic structure. Through this approach, we aim to bolster the security framework of microservice architectures, mitigating risks and enhancing the protection of inter-service communications. The findings and proposals presented in this thesis provide a crucial step towards more secure microservice ecosystems.

Keywords: SHA2, SHA3, JWT, Microservice Architecture, synchronous communication, inter-service authentication and authorization

Üniversite : İstanbul Kültür University
Enstitü : Lisansüstü Eğitim Entitüsü
Anabilim Dalı : Bilgisayar Mühendisliği
Programı : Bilgisayar Mühendisliği
Tez Danışmanı : Dr. Öğr. Üyesi Öznur ŞENGEL
Tez Türü ve Tarihi : Yükseklisans – Haziran 2024

ÖZET

Yazılım mimarisinin gelişen dünyasında, mikro hizmet paradigması ölçeklenebilir ve sürdürülebilir sistemler oluşturmak için sağlam bir çözüm olarak ortaya çıkmıştır. Bu mimarideki önemli bir zorluk, özellikle senkron iletişimde, hizmetler arası kimlik doğrulama ve yetkilendirmeyi güvence altına almaktır. Bu tez, bu iletişimleri güvence altına almak için yaygın bir yöntem olan JSON Web Token (JWT) mekanizmasının ayrıntılarına iniyor.

Güncel yaklaşımları değerlendirmek adına kapsamlı bir literatür araştırması gerçekleştirildi ve etkisiz uygulamalar ile yenilikçi stratejiler vurgulandı. Belirlenen baskın bir eğilim, token imzalama için SHA2-512 karma algoritmasının benimsenmesi yönündedir. Popülerliğine rağmen, SHA2-512'nin uzunluk uzatma saldırılarına karşı savunmasız olduğu ve önemli güvenlik riskleri oluşturduğu gösterilmiştir.

Bu endişeleri gidermek için bu araştırma, JWT mekanizmasında SHA3-512 karma algoritmasının uygulanmasını savunmaktadır. SHA3, Spring Boot çatısı altındaki JWT kütüphaneleri tarafından doğal olarak desteklenmese de, uygulamanın geliştirilmesinde SHA3'ün token imzalamada uygulanmasına olanak tanıyan başka bir mekanizma benimsenmiştir. SHA3-512, kriptografik yapısı temel olarak farklı olduğu için bu tür saldırılara karşı daha güçlü bir direnç sunar. Bu yaklaşım sayesinde, mikro hizmet mimarilerinin güvenlik çerçevesini güçlendirerek riskleri azaltmayı ve hizmetler arası iletişimin korunmasını arttırmayı hedefliyoruz. Bu tezde sunulan

bulgular ve öneriler, daha güvenli mikro hizmet ekosistemlerine önemli bir adım olarak değerlendirilmektedir.

Anahtar Kelimeler: SHA2, SHA3, JWT, Microservice Mimarisi, senkron iletişim, servislerarası / hizmetlerarası doğrulama ve yetkilendirme