Contribution ID: **80** Type: **Oral Presentation**

Lockers: An Innovative and Secure Solution for Managing Secrets in the EGI Cloud Infrastructure

Thursday, 28 March 2024 16:20 (20 minutes)

Secret management stands as an important security service within the EGI Cloud federation. This service encompasses the management of various types of secrets, including tokens and certificates, and their secure delivery to the target cloud environment. Historically, accessing secrets from virtual machines (VMs) has relied on OIDC access tokens, a method that harbors potential security vulnerabilities. In the event of VM compromise, these access tokens can be pilfered, enabling attackers to gain access to all user secrets.

The Locker mechanism introduces an innovative and robust approach to securely deliver secrets to VMs. Users can effortlessly create a locker, deposit their secrets within it, and then furnish the locker's token to their VMs. Key security attributes of the locker system include:

- Temporary and Autoclean: Lockers have a limited lifespan and quantity. Upon expiration, lockers are automatically purged, along with all the secrets contained within them.
- Isolation: Access to the secrets within a locker is exclusively through its associated token, which can solely be used for accessing the locker's secrets—nothing more. This isolation allows users to store tokens in Continuous Integration/Continuous Deployment (CI/CD) pipelines and similar tools, mitigating the risk of exposing personal secrets.
- Malfeasance Detection: The locker mechanism possesses the capability to detect if a token has been compromised and is being misused.

By adopting the locker approach, users can securely deliver secrets to VMs within the EGI Cloud federation, all while safeguarding their personal credentials from exposure. This innovative solution enhances the overall security posture of the cloud infrastructure, providing a robust foundation for secret management.

Primary author: TRAN, Viet (Institute of Informatics, Slovak Academy of Sciences)

Presenter: TRAN, Viet (Institute of Informatics, Slovak Academy of Sciences)

Session Classification: Network, Security, Infrastructure & Operations

Track Classification: Track 7: Network, Security, Infrastructure & Operations