Enhancing Software Supply Chain Security: Workshop and Call for Position Papers on Standards and Guidelines

Speaker Contact Information
Name: Andrew Whelchel, CISSP-ISSEP, ISSAP, CAP, CCSP
Position Statement Area: 3 (E.O. Section 4(I))
Title: Senior Solution Engineer
Contact: m. 615.554.8724
e. andrew.whelchel@saviynt.com

The Opportunity for IT Modernization and the Cyber Challenge to APIs

The days of perimeters and networking gear alone to stop malicious attackers are gone. One primary reason is that if malicious attackers can succeed in an attack on identity, firewalls and access lists become permeable to the digital attack. Today, attackers are finding further opportunities to accelerate these attacks through privilege escalation from initial identity attacks to software supply chain access with APIs as the communications medium.

Whether it is a powerful new mission system or a retrofit of an existing system, APIs (Application Programming Interfaces) provide the decoupling of data and applications to allow the rapid and parallel advancements in the modernization of mission systems today.

Enabling this decoupling, APIs allow the rapid advancement in a broad range of critical capabilities, including:

- Cyber multi-domain operations
- Rapid mission system updates
- Advanced hardware/software interfaces
- Joint agency mission systems interoperability

Though APIs are crucial to the ongoing rapid modernization already in flight, they also represent a newer, deeper, and broader potential risk. Purpose-built to provide broad access to enterprise data (vs. traditional applications), APIs expose more comprehensive data sets, function processing, and signal feedback. So naturally, this broad and deep risk exposure level presents risks that must be addressed to successfully secure critical software in federal mission systems.

The risks and potential threats from these risks of unsecured APIs include multiple types, including:

- Operational data leakage
- Intercepted API call exposure and or substitutions
- API principal access compliance/invalidation
- Unauthorized access to API function and data stream

The risk from these threats is a particularly significant concern in IoT/OT and multi-domain operations where there is potential that cyber actors damage kinetic and physical assets in addition to digital ones. Furthermore, operations to secure these APIs from threats are complicated by perimeter boundaries that dissolve in modern applications and peer cyber threats presenting themselves from outside and inside the traditional network construct.

Guidelines from Presidents Executive Order on Improving Cybersecurity (14028)
The President's Executive Order on Improving the Cybersecurity of the Federal Government (14028), issued on May 12, 2021, particularly in section Section 4(I), provides a call to action for the use of the principle of least privilege for a reduction in risk in federal use of critical software. A key concern of least privilege is addressing and enforcing whether a principal or service has access to an API (and for how long). A further need to address is the challenge of how to monitor least privilege and automatically mitigate access to APIs to maintain low surface area risk for critical federal software.

The position recommended for guidance consideration is to enforce least privilege for access to an API via identity context such that critical software can:

- Establish (and log) identity context for each API usage with a no standing access approach
- Enable identity context as a single control plane across multiple clouds or hybrid environments for rapid privilege de-escalation
- Allow machine to machine secrets rotation tied to Zero Trust policy for risk minimization
- Enable feedback of zero trust context signals into API access for a defensive cyber operation to de-escalate the privilege upon identifying insider and other malicious threats

In addressing this, the optimal approach combines attribute-based authorization (and de-authorization when risk-appropriate) to services and cloud-based privileged access for real-time access when needed. This approach allows risk-based access to APIs for services to scope access to least required privilege and simultaneously allows immediate ability to disengage all service level access when risk signals and enables policy needed to drive this due to unacceptable risk.

In taking the least privilege approach for API access, federal agencies also benefit from fulfilling other Executive Orders and NIST publications on ICAM and Zero Trust. Taking this least privilege first approach for APIs also better supports multi-cloud access for acceleration and faster (and easier) compliance reporting for APIs authorizations and access requests.