TIER API Security Task Force Charter

Problem Statement

API security needs to be made an integral part of the API design process. Yet too often API designers' approach to security (including authentication, authorization, delegation and access control) has been ad hoc and perfunctory. There is as yet no comprehensive set of best practices nor has a comprehensive set of relevant standards been finalized.

Stakeholders, Influencers and Influences

The primary intended audience for these guidelines is the internal TIER initiative developer community. Second, but probably second only in terms of timeline, is the audience of integrators who will be using TIER-developed APIs in the course of their work. APIs and API clients have to have a shared model and toolset for API security to make progress in this area.

Still different audiences will need to be invited to engage on different aspects of this work. It will be important for team members to bring the perspective and represent the interests of at least the following stakeholder groups:

1. The TIER Security and Audit Working Group
2. API designers and developers
3. Campus API and security service providers
4. Campus integration teams
5. Application developers

Charter

The TIER API Security Task Force must develop recommendations that provide guidance to API developers on ways to adequately address security issues. The Task Force must keep in mind that TIER design and development teams are the first and most important audience for WG deliverables. Those teams will be the ones implementing concrete APIs, using them to integrate component services with each other and with other systems at the adopting campuses. To that end, the WG must establish and maintain effective two-way communication with the design and development teams.

The Task Force must address at least the following areas:

- Coordination with the TIER Security and Audit Working Group
- Recommendations found in the OWASP REST Security Cheat Sheet
- Authentication of the API client and/or the user on whose behalf the call is being made
- Application of appropriate access control over API access at the level of specific API methods
- When used to retrieve a resource representation, the API must filter the returned information so that data access policies are enforced
- Equivalent levels of security must be defined for any proposed event-driven message-based integration strategy

The Task Force must sequence its work in a way that provides early guidance to the developers of APIs with the most serious security issues.

Membership

Membership in the Task Force is open to all interested parties. Keith Hazelton will serve as the chair of the Task Force. Other API WG members who have already expressed an interest in serving on the Task Force include José Cedeño, Gabor Eszes, Warren Curry, Ethan Disabb, Jim Fox, Chris Hyzer, Chris Hubing and Brian Savage.

Deliverables Timeline

By April 2017: Complete a first draft of a TIER API Security Guidelines document and invite community review

- Work with API developers to build and test a guideline-conformant security solution for a specific API

Request for Internet2 Assistance: N/A

See Also

TIER Data Structures and APIs Working Group Home

TIER Entity Registry Working Group

TIER Working Groups Home

InCommon Working Groups