TNC MAP Content Authorization 1.0 FAQs

FAQs for TNC MAP Content Authorization, Version 1.0, Revision 35

FREQUENTLY ASKED QUESTIONS

Q: What is IF-MAP?

A: IF-MAP, the interface for a Metadata Access Point, is a standard client/server protocol for accessing a Metadata Access Point (MAP). The MAP server has a database for storing information about network security events and objects (users, devices, etc.); it acts as a central clearinghouse for information that infrastructure devices can act on. The IF-MAP protocol defines a powerful publish/subscribe/search mechanism and an extensible set of identifiers and data types. MAP clients can publish metadata and/or consume metadata published by other clients.

The original IF-MAP specification was published in 2008 and most recently updated in May of 2012. It extends the TNC architecture to support standardized, dynamic data interchange among a wide variety of networking and security components, enabling customers to implement multi-vendor systems that provide coordinated defense-in-depth and enable security automation.

Q: What is MAP Content Authorization?

A: This specification defines an authorization model that restricts the operations each MAP Client can perform on MAP content— the metadata in a MAP server.

Q: Why was this standard created?

A: The content in a MAP server has high value and needs to be protected from inappropriate access. A defense-in-depth strategy must recognize that even infrastructure elements controlled by an IT department will sometimes be compromised. Also, there is great interest in placing IF-MAP clients on devices belonging to end users, which may be at even higher risk of compromise.

Unauthorized access to the content of a MAP server could enable a malicious IF-MAP client to gather information about its environment, at a minimum. By changing the content of a MAP server, the malicious IF-MAP client could grant improper access or enable other forms of attack. An authorization system is needed to mitigate these risks.

Q: What are the benefits of standardizing MAP Content Authorization?

A standard authorization model is advantageous to both implementers and end users. For example, a vendor developing an administrative client for authorization purposes may be reluctant to have their implementation depend on one MAP server's authorization system. And an end user deploying an IF-MAP enabled infrastructure which relies on authorization should not be locked into one MAP server. A standard authorization model makes authorization policy portable across multi-vendor environments and enables comprehensive access control.

A standard model also allows data and recommended policy elements to be designed together, ensuring that access to the data can be appropriately controlled.

Q: Wasn't an existing authorization model suitable?
A: The MAP Content Authorization specification leverages the existing OASIS eXtensible Access Control Markup Language (XACML). XACML was chosen for its flexibility, extensibility, and fine-grained access control. The MAP Content Authorization specification illustrates and makes use of an XACML profile, explaining how XACML is employed when MAP clients seek access to the content of a MAP.

MAP servers implementing the MAP Content Authorization specification will utilize an XACML profile and consult an XACML PDP (either internal or external) to enable application of access control to IF-MAP clients seeking to read and access MAP content.

Q: Who has the most to gain from MAP Content Authorization?
A: Enterprises and organizations implementing intelligent network security frameworks will gain confidence in the security of the framework itself. And environments requiring multiple security enclaves, such as industrial control systems infrastructures or multi-tenant service providers, can ensure that IF-MAP Clients' access is restricted to MAP content appropriate for their enclave.