Trusted Network Connect
IF-MAP 2.1 FAQ

May 2012

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. It extended 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.

On May 7, 2012, Trusted Computing Group published updates to several IF-MAP specifications: IF-MAP 2.1, IF-MAP Metadata for Network Security 1.1, and TNC Architecture 1.5.

Q. What benefits does IF-MAP offer to users of security products?

A. Users of IF-MAP enabled products can implement more effective, integrated security systems, gaining the following benefits:

- Coordinated security response across multiple products from multiple vendors, ranging from endpoint security to AAA, NAC, IDS/IPS, Data Loss Prevention, firewalls, etc. to infrastructure such as SIEM, CMDB, physical access control systems.
- Stronger security with lower operating costs since sensors (e.g. IDS) can be tied automatically into flow controllers (e.g. firewalls), reducing the need for human intervention and accelerating security responses.
- Customer choice and flexibility, leading to lower initial costs. No need to buy all security products from one vendor to get coordinated, integrated security.
- Easier integration of data from multiple vendors and devices into security event management (SEM) and other logging and reporting systems.

IF-MAP enabled products facilitate security automation, which has many benefits. These benefits include:

- Fewer false alarms (and therefore lower operating costs) since sensors can tune their detection algorithms based on user and machine identity and role.
- Simpler, more intuitive policies based on user identity and role instead of IP address.
- More comprehensible incident reports from sensors since they can include user identity.

Q. What benefits does it offer to vendors of security products?

A. Using open standards to integrate security products provides many benefits over a single-vendor approach or custom integrations:

- Easily integrate products from multiple vendors, or multiple products from one vendor, to meet customer needs and build solutions

- Quickly respond to emerging threats by integrating new information, such as security intelligence, into products as needed
- Extensible schema allows for easy support for vendor-specific data. Vendors can design metadata to meet the needs of their individual products and solution.

Q. Who has incorporated IF-MAP capabilities into commercial products?

A. Many vendors, including the following, offer commercial products with IF-MAP support:

- Byres Security (http://www.tofinosecurity.com)
- Enterasys Networks (http://www.enterasys.com)
- Great Bay Software (http://www.greatbaysoftware.com)
- Hirsch Identive (http://www.hirsch-identive.com)
- Infoblox (http://www.infoblox.com)
- Insightix (http://insightix.com)
- Juniper Networks (http://www.juniper.net)
- LogiSense (http://www.logisense.com)
- mikado soft GmbH (http://www.mikadosoft.de)
- Lumeta Corporation (http://www.lumeta.com)
- NCP Engineering (http://www.ncp-e.com)
- Q1 Labs (http://q1labs.com)

Q. Is there open source support for IF-MAP?

A. There are several open source projects that use IF-MAP, including:

- ESUKOM (http://www.esukom.de)
- TRUST@FHH (http://trust.inform.fh-hannover.de)
- omapd (http://code.google.com/p/omapd/)
- OpenHIP (http://www.openhip.org)
- strongSwan (http://www.strongswan.org)
- Various IF-MAP client projects (http://ifmapdev.com/client-projects)

Q. How does IF-MAP work with other TNC architecture specifications?

A. IF-MAP is a complementary specification that extends the capability of the TNC architecture. The original TNC standards (such as IF-IMC/IMV, IF-PEP, and IF-TNCCS) enable compliance checking for protected endpoints based on interrogation of the endpoint. The addition of observational information, such as behavior and location information, via IF-MAP enables coordination between security and networking components that aren't involved in the original endpoint communication.

Q. What is the status of IF-MAP?

IF-MAP specifications define a mature framework of operations and standard metadata which is continually being enhanced by the Trusted Computing Group. Products using IF-MAP have been shipping since 2008, contributing to an established IF-MAP ecosystem; new features have been added to the standard in IF-MAP 2.0 and now in IF-MAP 2.1 to make it more flexible and broadly applicable to expanding use cases. IF-MAP 2.1 is an incremental evolution of the IF-MAP spec, building upon experience gained from two years of deployment and production use of IF-MAP 2.0 enabled technologies.

Q. What's new in IF-MAP 2.1?

The primary new feature of IF-MAP 2.1 is the introduction of extended identifiers, which add extensibility to the IF-MAP identifier space to correspond to existing extensibility of the IF-MAP metadata space. TCG and vendors are now able to define new types of identifiers to enable new use cases. For instance, a new network identifier can be specified. IF-MAP enabled DHCP servers, and other sensors, may link IP address identifiers to such a network identifier, so that the topology of the physical network is reflected in the MAP. Policy decision points, flow controllers, and other MAP clients may search for newly discovered IP addresses by starting at a well-known network identifier.

Another new feature of IF-MAP 2.1 is operational metadata supporting detection of clock skew between a MAP client and server. Time synchronization is important for several aspects of IF-MAP, from SSL negotiation to event consumption and response to troubleshooting. If a disparity is detected between the time on the MAP client and the MAP server, the MAP client can adjust its local clock or compensate for the difference so that timestamps in metadata are accurate relative to MAP server local time.

Other enhancements in IF-MAP 2.1 include new normative requirements and clarification of technical aspects of the specification, improving testability and increasing ease of interoperability for implementers.

Q. Are products based on the new IF-MAP compatible with the products using the prior version?

A. Yes. IF-MAP 2.1 was designed to be backwards compatible with IF-MAP 2.0, so currently implemented products will work seamlessly with products implementing the new version.

Q. How is IF-MAP being used in the enterprise today?

A. Common uses of IF-MAP in the enterprise today include:

- Seamless remote and local access control, providing single sign-on for either initial access to a network, or remote access to a network, coordinated with access control enforcement deeper in the network
- Integration of physical and logical access control, so user location obtained from a badge access system can be used as input into a network access policy decision
- Usage of IF-MAP as a point of coordination for industrial control system security, for policy enforcement and certificate lifecycle management
- Leveraging IP address mappings to MAC addresses from DHCP servers to enable network-based enforcement for MAC authenticated devices
- Integration of detailed behavioral information from threat sensors such as IPS, endpoint profiling / behavior monitoring, and network leak detection systems into network access control policy decisions

Q. What are some other potential use cases for IF-MAP?

A. IF-MAP enables coordinated policy dissemination; security automation; integration with new types of sensors and security devices; and other forms of coordination between disparate networking and security components. Many possible scenarios can be envisioned based on these functions; examples include:

- A content management database (CMDB) receives notification of a new device on the network – perhaps via notification that a DHCP server has assigned an IP address to a new MAC address – and scans the new endpoint, then updates its data store

- A security administrator modifies an existing security policy, or adds a new policy, and various policy servers / sensors are notified, triggering a re-evaluation of the network's endpoints
- An application server publishes a request for bandwidth for a particular user based on the service the user is accessing; network infrastructure components change QoS settings for those traffic flows based on that request
- An analysis system determines that there's an attack underway; in addition to triggering a response, it notifies security administrators of the attack taking place, populating a dashboard with information to create a "heat map" of the attack

Q. How can my organization participate in the development of the IF-MAP specification?

A. Any interested party can provide input on the IF-MAP standard by sending comments and questions to admin@trustedcomputinggroup.org .

Contributing members of the Trusted Computing Group can participate in ongoing development of the IF-MAP interface and related metadata schemas; TCG members are encouraged to engage the Trusted Network Connect Work Group. For information about joining TCG, contact admin@trustedcomputinggroup.org .

Q. Where can I go for more information?

- TCG - Network Security Solution
  - http://www.trustedcomputinggroup.org/solutions/network_security
- TCG - Trusted Network Connect
  - http://www.trustedcomputinggroup.org/developers/trusted_network_connect
- IF-MAP Community
  - http://if-map.org