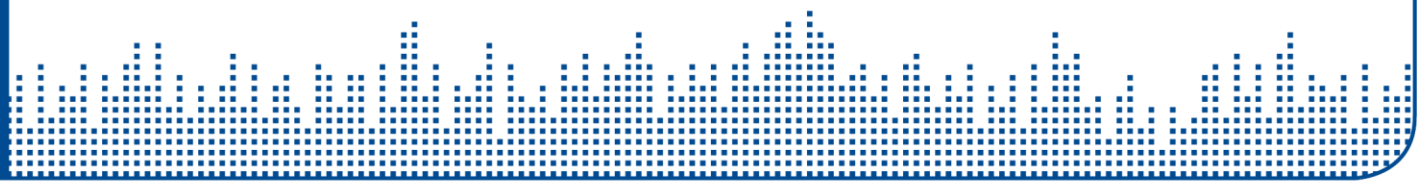
EXPANDED IF-MAP 2.0 ADDRESSES A BROADER SET OF APPLICATIONS

September 2010

Trusted Computing Group
3855 SW 153rd Drive, Beaverton, OR 97006
Tel (503) 619-0562 | Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org



Expanded IF-MAP 2.0 Addresses a Broader Set of Applications

From Network Security to Cloud Computing, Industrial Control Systems Security, Smart Grid, and beyond

In 2008, the Trusted Computing Group's Trusted Network Connect Working Group (TNC-WG) released its initial IF-MAP (Interface for Metadata Access Points) specification. This open standard extended the TNC architecture for network security to support standardized, dynamic data sharing through Simple Object Access Protocol (SOAP) exchanges among a wide variety of networking and security components.

The initial version of IF-MAP enabled integration of network security functions such as network access control (NAC), remote access, intrusion detection, endpoint profiling, behavior monitoring, data leak detection, etc. With several suppliers shipping IF-MAP support in their products, a number of end users have successfully piloted and/or deployed production systems based on IF-MAP 1.1.

But in the last two years, customers and suppliers have discovered new uses for IF-MAP. Because the protocol is highly extensible, they've been able to apply its publish and subscribe semantics to fields such as cloud computing, Industrial Control Systems and SCADA security, physical security, and more.

To enable and ease new applications of IF-MAP, TCG has now separated IF-MAP into a base protocol (IF-MAP 2.0) and a set of network security metadata (IF-MAP Metadata for Network Security 1.0). Now innovators can employ the base protocol without having to worry about the network security aspects. Because MAP servers are metadata-independent, they can be used for any application. Innovators only need to develop IF-MAP client code for their application. Several open source libraries can be used to ease this.

IF-MAP For Network Security

With IF-MAP's network security capabilities (described in the sidebar **The Power of IF-MAP**), customers are able to leverage and expand the capabilities of their existing network security products. For example, notifications from a security sensor can trigger an automated response to quarantine and remediate an infected machine. Products that support IF-MAP become smarter and stronger because they can leverage information obtained from other products that also support IF-MAP.

Products with IF-MAP support currently available from suppliers include the Great Bay Beacon endpoint profiler; Juniper Networks Unified Access Control (UAC) and SSL VPN appliances (SA); Infoblox DHCP Server and Orchestration Server; Insightix BSA Business Security Assurance suite; Lumeta IPsonar active network discovery solutions; Hirsch Electronics Velocity Physical Access Control System and Byres Security Tofino industrial security gateways.

The network security capabilities of IF-MAP have been considerably expanded with the new IF-MAP Metadata for Network Security specification. For example, new request-for-investigation metadata can trigger an in-depth investigation upon request. New enforcement-report metadata eases management by showing when automated enforcement action has been taken. Myriad improvements abound in the new specifications, which benefited from years of real-world deployment experience.

How does IF-MAP differ from previous techniques for integrating systems? IF-MAP allows the transition from an era of custom integration of application programming interfaces (APIs) and scripts that are costly, complex, brittle and require high maintenance to a unified communications and security environment where users can publish, subscribe and search the environment through the IF-MAP protocol. As shown in Figure 1, IF-MAP interconnects previously unconnected or certainly uncoordinated areas in infrastructure, management and applications areas and provides security and audit/compliance improvements. In addition, standards-based integration can reduce integration costs.

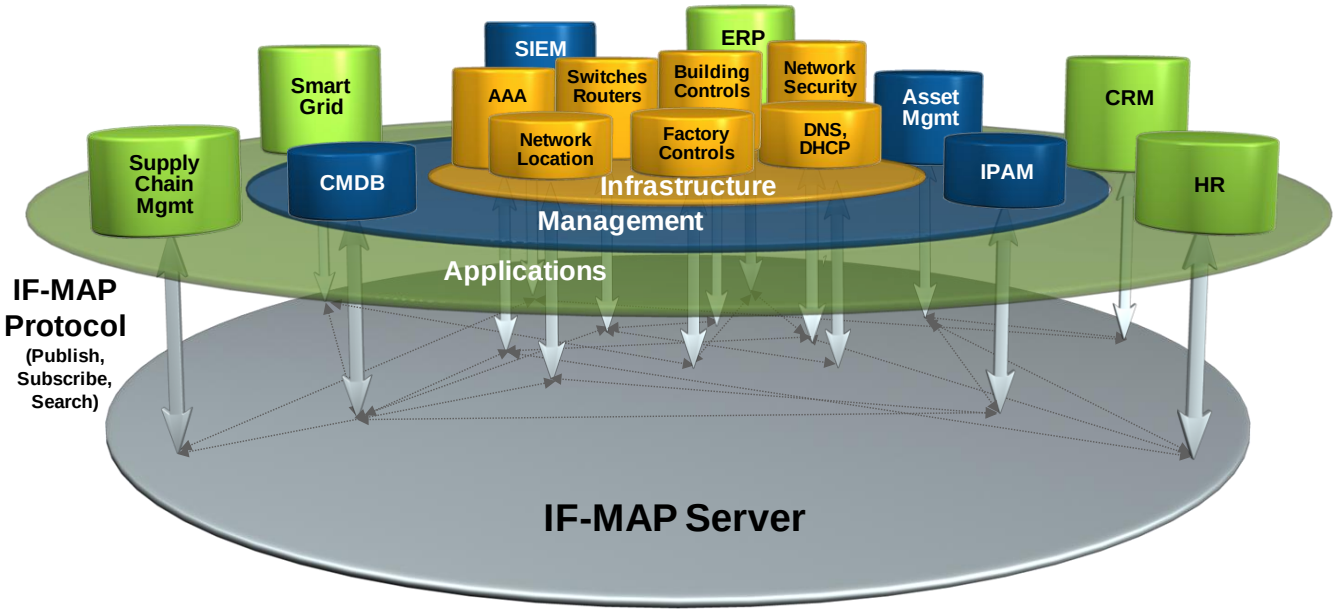


Figure 1. With IF-MAP, the automatic aggregation, correlation and distribution of data to and from different systems occurs in real time. Source: Infoblox

Anticipating New Applications

With today's rapidly increasing technology capability, products and systems are increasingly more integrated and more virtual with frequent changes occurring on a regular basis. As a result, a database is needed to identify what's happening, when, where and with whom. Rapid, automated responses can then occur in a highly efficient manner. IF-MAP was developed to provide the enabling protocol for this rapid-response database. Now that IF-MAP 2.0 has separated the base protocol, potential applications are boundless, including:

- Unified communications
- Integration of physical security with information security
- Industrial control systems security
- Cloud computing

A brief description and use case example for each puts the exciting possibilities for these applications into perspective.

Unified Communications

Unified communications is all about consolidating work phones, mobile phones, and computers with all their associated email, voicemail and instant messages - all the different communication activities that are not connected together now - into one cohesive system. There can be a central communication device such as an iPhone, iPad, laptop or whatever the user chooses. There can also be a unified communication service like Google Voice where all messages go into one place for access from multiple devices. All these communications devices and services come together over a TCP/IP network. With unified communications technology in place, many interesting changes can take place. For example, a user can have email read over

the phone, or have voicemail transcribed, or have instant messaging on the same device used for phone calls. Unified communications allows many interesting feature possibilities.

In this unified communications world, many security issues arise. For example, the user will want to ensure that his unified communications inbox is not being hacked. A corporation will want visibility regarding what is going on across all of their unified communications modes and systems. This includes providing security and real-time visibility across all client devices: desktop PC, laptop, iPhone or whatever. IF-MAP 2.0 with its publish, subscribe and search operations as well as its database capabilities enables this visibility and increased security.

Physical Security Meets Information Security

Physical security and IT security have historically been separate - even to the extent of having a different reporting structure in the organization. Today, physical security is technology intense. It uses computers, handheld devices and, in fact, most physical security systems are now being connected with networks. Connected devices include badge readers that are used not only for building access but also for computer access and restricted room access. Video and other forms of electronic surveillance, such as anti-shrinkage or anti-shoplifting that use radio frequency identification (RFID) capabilities are a highly automated part of physical security. Even the security cameras that previously connected to closed-circuit TV video monitoring stations are often now connected over TCP/IP.

Sharing the same protocols and sometimes even the same network that information technology uses presents a challenge and an opportunity. To address both, the physical security organization needs to get more savvy about the IT aspect and vice versa. Physical security systems must be protected by existing network security tools since these systems are now subject to not only physical attacks but also IT attacks by hackers.

When physical security and IT security systems are connected together and share information in a useful manner, IT security can actually benefit from information received from physical security. For example, if an employee who is not in the building (as detected by physical security) logs into her desktop (as detected by IT security), something is probably wrong and an appropriate response should be generated. By sharing information, physical security systems can be used to respond to problems detected by IT security and vice versa. IF-MAP is the key to sharing information between these security systems.

Industrial Control Systems Security

Industrial control systems such as SCADA (Supervisory Control and Data Acquisition) systems that manage processes and DCS (Distributed Control Systems) that control processes have evolved as isolated systems with numerous protocols. These protocols include Ethernet, CAN (controller area network), BACnet, Modbus, Fieldbus, ARCNET, LonWorks, HART (Highway Addressable Remote Transducer), Profibus, SERCOS and more. In addition, wireless protocols also are being implemented in the factory environment. These local area networks (LANs) are increasingly being connected to internal enterprise business networks and to the internet as well.

The Smart Grid is an excellent example of industrial systems connecting using Internet protocols. In this case, power plants and the electrical distribution grid are connected to the internet. Residential and business power consumers are the other part of the Smart Grid control network. The object is to monitor household energy usage through the use of smart meters and networks so that high energy loads such as dishwashers, clothes washer and driers are used at night during the off-peak hours. Even the ac system can be turned down when energy usage is too high.

Unfortunately, an unprotected system on a network is vulnerable to attack by hackers. Even industrial systems that are connected internally but not connected to the Internet still use Internet protocols or others that are even more vulnerable. This makes it relatively easy for someone to hack those systems.

As a result, industrial controls systems and the Smart Grid environment can benefit from IF-MAP. IF-MAP can ensure that the only device on the network that can control a particular critical load such as a chemical pump is the device that is supposed to control that pump. Today, that type of security is rather primitive. In fact, compared to desktop security, it is surprising how easy an industrial system can be hacked. Examples are easily found of hackers releasing millions of gallons of sewage and even attacking the power grid. A list of over 30 attacks is summarized in Hacking the Industrial Network where the author notes that "the expense of protection is a fraction of 1% of the IT budget."

While it may not be possible to prevent all attacks, the best available information security technology should be implemented in those embedded computing applications to prevent as many attacks as possible. For those industrial companies using IT, the best available IT security should be used to protect the network. As the industrial control systems security people like to point out, in their line of work, "without adequate protection, if something gets hacked, it leaves a big hole in the ground." In some cases, this just involves getting the monitoring equipment off line for a brief period of time. Because IF-MAP provides rapid information sharing and notification of problems, it is an ideal match for industrial control systems where time is of the essence.

Cloud Computing

The game changing capabilities of cloud computing are constantly being touted. However, there are two key aspects about cloud that make it different from traditional data center networking and computing environments. One is its shared aspects. The cloud is owned by someone else - not by the user whose data and applications are running in the cloud. And it is shared among multiple customers. As a result, the multiple tenants (customers) whose data are all running at one time in the cloud need a trusted, multi-tenant infrastructure.

The other unusual thing about the cloud that is becoming more common is virtualization. There is extensive use of virtualization in the cloud. There are virtual machines (virtual computers), virtual servers, virtual storage and virtual networks. Enterprises use virtualization in their own corporate data centers, enabling rapid changes. The pace of change is even greater in the cloud. Users go to the cloud because they want the ability to quickly get 100 virtual machines up and running and then shut them down. They want to be able to scale them up and scale them down as their needs change without having to actually purchase all that equipment themselves.

A multi-tenant infrastructure with extensive virtualization makes providing detailed, real-time information difficult – without IF-MAP. However, IF-MAP can keep track of where things are and what's being done, providing notifications when things change or just a database that can be queried as needed. This can include information about which software is running in which virtual environment and which physical server or virtual machine that software is running on.

Using IF-MAP, virtual machines and virtual networks in cloud can be identified and assigned to appropriate resource requests. As shown in Figure 2, an "inter-cloud registry" helps cloud providers and users to match workload needs with cloud assets. The development of an inter-cloud registry service based on IF-MAP is an ongoing project at the Open Cloud Consortium (OCC).

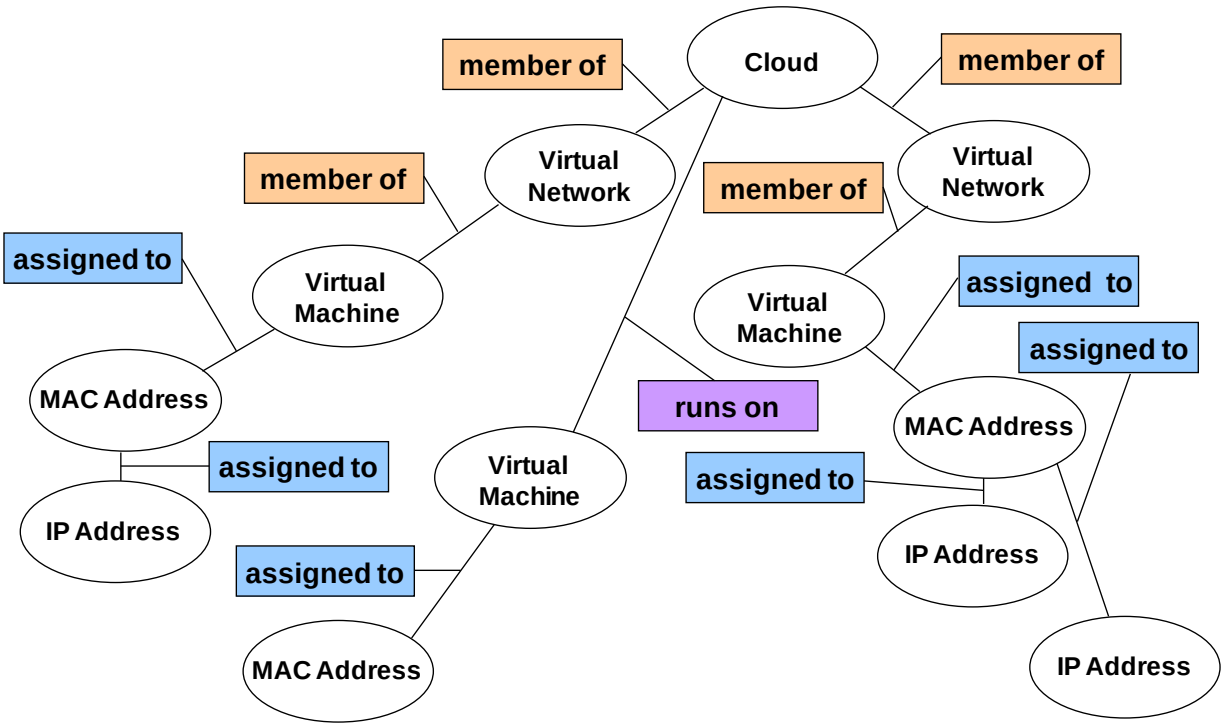


Figure 2. Dealing with the impact of virtualization and cloud computing on the network requires capabilities enabled by IF-MAP 2.0.

IF-MAP provides users with visibility into what is occurring in the virtual environment of cloud computing as things change. Because it is an open standard, IF-MAP allows users to have that visibility even if they are running different vendor software than their cloud provider. As long as each entity supports this open standard, customers can have instantaneous visibility into what is occurring in the cloud. They not only know what problems are arising, they can potentially even request certain services of the cloud in real time in response to a problem as it occurs. For example, if an employee is violating company policies in the cloud, they can deny him/her access. If machines are under attack, the customer may be able to instantly add denial of service protection for applications even though it was not previously ordered.

Conclusions

IF-MAP 2.0 enables smarter, more effective security in an increasingly network-connected world. Not only have the network security capabilities of IF-MAP 1.1 been extended to offer more features, the base protocol has been split off to enable new applications to be easily developed, going far beyond network security. This paper has described four of these new applications: unified communications, integration of physical security with information security, industrial control systems security, and cloud computing.

In addition to providing a very timely response to the demands of these new applications, the TNC Working Group has demonstrated the flexibility of the IF-MAP specification and its ability to quickly respond to new input. When the specification was originally designed, separation was provided between the base capabilities and the metadata itself, which is at a higher level. This foresight has allows the IF-MAP specification to be easily extended to address new situations and yet remain backward compatible.

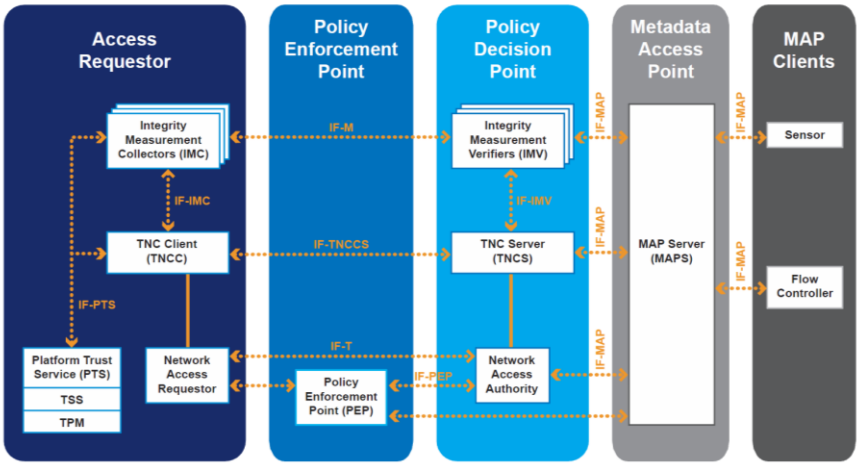


Figure 3. Basic TNC architecture is defined in the first three boxes on the left. The extended TNC architecture includes the last two on the right and requires IF-MAP, a powerful new approach to IT orchestration.

The Power of IF-MAP

The Trusted Network Connect (TNC) architecture is shown in Figure 3. This architecture starts with the three basic NAC elements on the left, but adds in the crucial element of open standards to enable multi-vendor interoperability. Each of these standards is indicated by a dotted line with the name of the standard on it (e.g. IF-M).

Then the TNC architecture extends beyond the three-element NAC model to include other security monitoring devices ("sensors") as well as entities that make and enforce decisions ("flow controllers"). These components communicate with each other and with the rest of the system through a Metadata Access Point (MAP), a central database. The interface (IF) that enables this connectivity is called IF-MAP. Analogous to the internet's Domain Name System (**DNS**), but with even more capability, IF-MAP is a shared, real-time network information service. It automatically aggregates and associates real-time information from many different sources while supporting both pre-defined data types and vendor-specific extensions (both called "metadata").

IF-MAP is a critical missing link between otherwise disparate systems that cannot interoperate. It is the core of a new approach to security and IT orchestration driven by the power of extensible metadata and standardization.

The three main features of IF-MAP are publish, subscribe and search. Somewhat like Twitter or LinkedIn for internet protocol (IP) devices and systems, this functionality is essentially social networking for machines. It provides real-time updates on what the connected systems are seeing. Designed for machine-to-machine coordination of highly automated and globally scalable industrial processes and IT, the IF-MAP protocol is not intended to replace existing standards for business services or banking transactions. Since many security systems today are already network connected, IF-MAP support can usually be obtained through a software upgrade, offering stronger security at low incremental cost. The TNC architecture with IF-MAP provides an enterprise with the tools to address many security, connectivity and orchestration issues associated with the increasingly complex network.