Infoblox®

IF-MAP

Driving IT Agility through an Infrastructure Revolution

OVERVIEW

AT A GLANCE

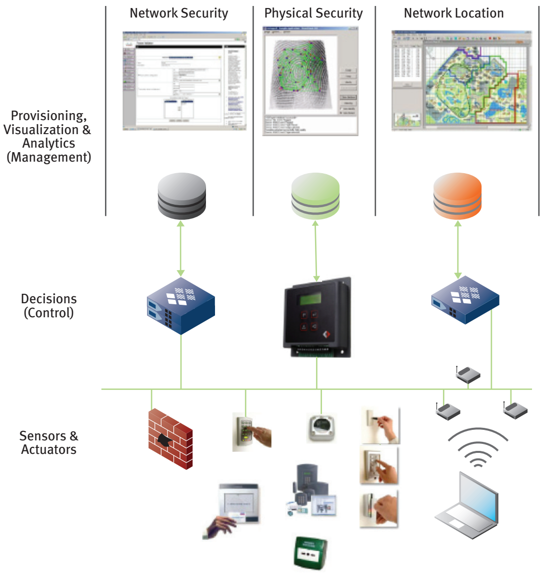
IF-MAP does for coordination & collaboration what IP has done for connectivity.

Effective use of information is essential if CIOs are to improve their organizations agility. The hospital administrator who knows patient status and location and can quickly locate equipment can dynamically reschedule services and reroute meals and medications to improve care, shorten stays and avoid errors and liability. The factory manager who can always locate critical parts and tools on the factory floor (or throughout the supply chain) can decrease cycle time, minimize inventory and eliminate lost hours and production delays.

Yet all too often, IT solutions fall short of their potential precisely because sharing essential information between business systems remains impossible or too complex and costly. Asset management systems can track people and devices, but rarely exchange that information with HR systems or enterprise applications. Network security systems don't share information with physical security systems. Manually stitching together these different applications is unfeasible as IT must incur high costs each time an application is changed, added or removed from the network. The time when corporate networks were fragmented by a jungle of networking protocols may be gone, but different applications and systems are as inaccessible to one another today as when they ran over SNA and IPX and AppleTalk.

The answer is a new technology standard called InterFace to Metadata Access Points—or "IF-MAP"—from the Trusted Computing Group (TCG) [http://www.trustedcomputinggroup.org]. IF-MAP standardizes the way devices and applications share information with one another. It does for coordination and collaboration what IP has done for connectivity. IF-MAP has been developed by senior engineers from a number of companies that are part of the TCG's Trusted Network Connect (TNC) subgroup, which includes HP, Juniper, McAfee, Microsoft, Symantec, and many other industry leaders.

A Network of Silos



Devices may share a common IP network, but still do not communicate with one another

The Third Generation of Network Computing

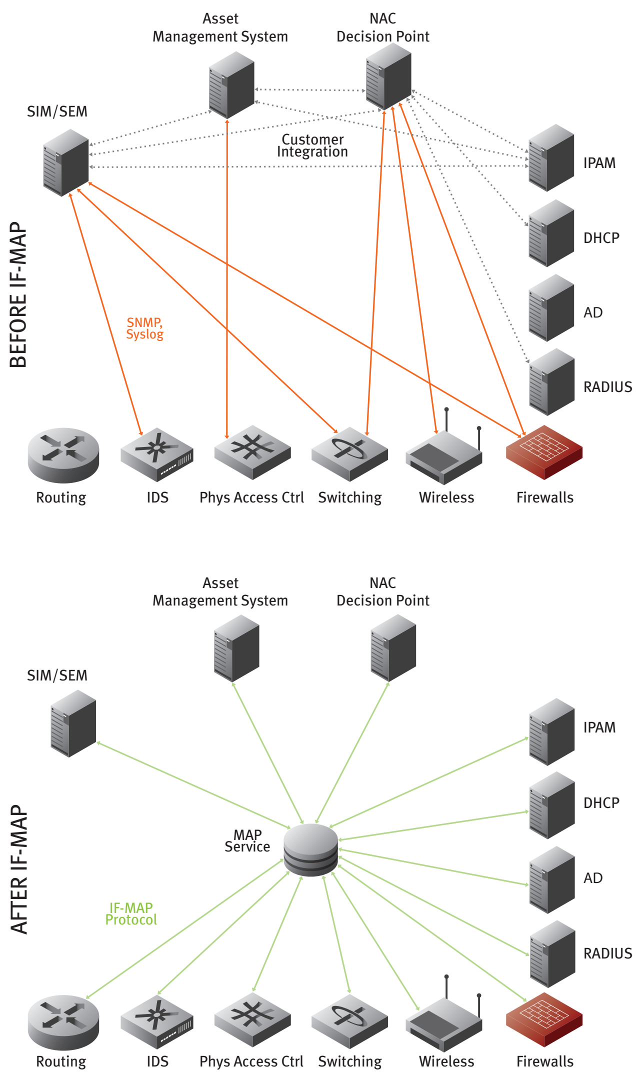
Today's IT networks are poised for the next generation in network computing. During the first generation, the IP stack won the protocol wars replacing SNA, AppleTalk, IPX and more as the standard for connecting all computers and computer-related peripherals and devices.

During the second generation of computing, IP emerged as the universal connection for anything—not just computers and computer peripherals. Our phones and cameras, sensors and actuators of all kinds—even parking meters—can share a common IP infrastructure, but continue to function independently of one another.

In the third generation of computing, we enable all connected systems to work together. Any system or application connected via the IP network will be able to easily share information with any other application or system—security and business policies permitting. A new array of intelligent, automated systems will be created, with consequences as profound as the adoption of IP for connectivity.

IF-MAP is a key enabler behind this third-generation of computing. The technology allows systems and applications to easily share data of all types, in real time. More specifically, IF-MAP defines a protocol and associated database used by applications and systems to publish information, subscribe to changes in information of interest, and search for relevant data. It's analogous to Facebook for network devices and systems, and can be used entirely within a company as well as between and among different organizations.

The IF-MAP Network Transformation



Why a New Protocol?

The challenge of collecting and disseminating data in real time among many applications and systems carries with it a unique set of requirements. Meeting this challenge requires the ability to accommodate diverse data types, data relationships and many, many devices and entities:

- **Unstructured Data** – There's no way to anticipate all of the different types of information that applications and systems may want to share on the network. There's network-related data, such as IP addresses and MAC addresses, and identity information, such as user names, roles and access rights. There's device information, such as the type of device, its manufacturer, and asset tag; physical data, such as location, temperature, and the state of the device (whether it's on or off, busy or free), etc. A data sharing system must be able to accommodate both pre-determined as well as user-defined data types without major effort.
- **Unstructured Relationships** – Just as it's impossible to anticipate all of the kinds of data that will be shared, it's equally difficult to anticipate the relationships between those elements. A user can be associated with many devices, and a device can be associated with many users. The same is true for related pieces of data. Attempting to capture all the potentially useful relationships using pre-defined, static structures quickly becomes restrictive and renders the system unable to adapt to real customer needs. Instead, an effective design must support emergent relationships where associations between users, devices and the related data are learned from the network itself.

- **Scalability** – With the rapid increase in the number of devices and systems that are on networks, a coordination system needs to scale to many millions of devices and data elements, and must be able to handle real-time transactions among many thousands of systems.

No prior technology meets these requirements. Relational databases and directories, such as LDAP, require pre-defined data types, data structures and hierarchies. They were not designed to support unstructured data and unknown relationships.

Infrastructure monitoring and management protocols, such as SNMP and Syslog, do not have an associated database technology, so while they're effective for exporting information about the status and activities of different devices and systems, there's nothing in the SNMP or syslog protocols that correlate information from multiple systems and support collaboration. Similar to working with proprietary APIs, integration via SNMP and syslog typically requires a significant integration effort and is more effective for monitoring and management applications than for real-time collaboration and coordination.

A New Approach

By contrast, IF-MAP is built around a new, more flexible, and scalable design that reduces the complexity and cost of system integration, enabling new worlds of collaborative systems and applications.

IF-MAP uses a publish/subscribe/search paradigm, as exemplified by Web applications and services. There is no pre-defined global structure for an IF-MAP database; rather, the global database structure (schema) emerges as each application and system publishes information to the IF-MAP service. Another key operation supported by IF-MAP is subscription. Systems compatible with IF-MAP can subscribe to changes in data of interest—such as a new device coming onto the network, or a user changing role, or an item moving from one location to another—and receive updates automatically.

These three operations—publish, search, and subscribe—are the simple yet powerful primitives for all IF-MAP transactions. This reflects what may be IF-MAP's greatest asset—its simplicity. Integrators working with IF-MAP have been able to deliver solutions using IF-MAP compatible systems in days rather than the weeks and months commonly required to integrate disparate systems.

Business and IT Impact

The Web Services model exemplified by SOA and related architectures has taken hold within IT organizations because it significantly reduces the time and cost required to develop, deploy and maintain applications. The resulting applications make organizations more efficient, more responsive and more compelling for their customers. The same is true for IF-MAP: A few of the initial use cases emerging from IF-MAP—barely the tip of the iceberg—include the following:

- **Application Security** – Some organizations have hundreds of applications that need to know if an employee or contractor's status has changed and they're no longer working for the company. Any delays in de-provisioning unauthorized users expose organizations to risk and liability. Having every application continuously poll the identity management system to look for changes is impractical. But by embedding an IF-MAP client stack in the HR system and in each application, a fairly simple task, applications can subscribe to changes in user status. They're notified immediately by the IF-MAP service if the identity management system publishes a change in a user's status from "employed" to "terminated".
- **Cyber/Physical Security Convergence** – All organizations struggle with preventing external hackers from hijacking their WiFi networks. With easy access to information from a building's physical access control system, a network security system can limit network access only to employees that are in the building or to registered building visitors.
- **Theft Prevention** – Hospitals and higher-education institutions grapple with stolen equipment all the time. With IF-MAP, a building security system can access information from facilities management and asset tracking systems, and sound an alarm or even lock the doors if expensive equipment starts moving to an exit.
- **Improved Customer Care** – Utilizing location information allows organizations to read-just their processes to provide better service and improve their bottom line. Hospitals can use IF-MAP to reduce the time needed to treat patients while improving customer care. By understanding a patient's location, an IF-MAP-enabled care management system could identify if a patient is out of their room and waiting for a test at lunch time. The system can locate alternate equipment, or deliver their lunch while they wait—and also provide the patient's temperature to the nursing station.

Not only does IF-MAP hold the key for revolutionizing the way businesses address strategic problems, the architecture will also change the way IT operates. Initially, IF-MAP was designed to support network access control (NAC) and to those ends it has extensive security features built in. But the applications of the IF-MAP architecture go far beyond network security:

- **Data Center Optimization** – Within the data center, IF-MAP allows organizations to integrate information from physical servers, power systems and data center air conditioning systems with virtual server management systems. This makes it possible to cut power costs by automatically finding available server capacity and moving work-loads to shut down unnecessary servers.

- **Automated Network Provisioning** – IF-MAP will allow IT to automate the process of virtual machine provisioning and deployment. Instead of the network services team having to coordinate with the server team to deploy or move a virtual machine (VM), all of the necessary policy and state information can be published in IF-MAP database. Automated provisioning of networks is not only more effective than today's manual processes, it is also a requirement to support dynamic environments such as private and public clouds.

IF-MAP Status

The initial version of the IF-MAP specification was released in May, 2008, and an update was released in May, 2009. Since then a number of companies, including vendors of network equipment, network security systems, wireless location systems, physical security systems and others have demonstrated and released IF-MAP compatible products. For such a young standard, the adoption rate has been impressive. Importantly, a number of large enterprises are deploying IF-MAP and are using it to improve existing processes and support new initiatives. And the standard continues to evolve as more use cases are added.

What Next?

In principle, IF-MAP doesn't make possible anything that can't be done already today with existing protocols and custom programming, just as network connectivity was possible before IP became the universal data communications protocol. By standardizing and simplifying information sharing, IF-MAP has the potential to transform not just IT, but also whole organizations and industries. This will not occur overnight, but early support from vendors and end users suggests that IF-MAP can deliver immediate benefits today and is a powerful architecture for the future.

For more information visit *www.infoblox.com/solutions/overview-if-map.cfm* http://www.isa.org/InTechTemplate.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=85723

April 2011

Web Exclusive

Control network secure connectivity simplified

Solving the security issues involved with connecting control networks to corporate networks simplified with standards-based interfaces

Fast Forward

- Industrial control systems require security to avoid compromises from attacks that occur with disturbing frequency as well as unintentional incidents.
- Control system secure connectivity can leverage advances in network security coordination.
- The Trusted Computing Group's Trusted Network Connect standards, including the IF-MAP interface, provide compatible and simplified interfacing of network access control between control networks and IT networks.

By Scott Howard and Lisa Lorenzin

The susceptibility of control systems to security issues continues to confront organizations. While it may be rare to penetrate a control system directly from the Internet, corporate connections, remote support links, USB keys, and laptops create pathways for the typical worm or advanced hacker. Once inside, attacking an industrial control system is not difficult—in some cases, even the most basic scanning by a hacker or worm can wreak havoc.

Since no company wants the adverse attention that an industrial network attack causes, many attacks are undocumented. However, it is not difficult to find evidence of their frequent occurrence; the Repository for Industrial Security Incidents has many examples of such incidents. The 2009 white paper "Hacking the Industrial Network" identifies 30 documented attacks, along with their major implications, that have occurred since 1997. The incidents range from the dumping of millions of gallons of sewage to the remote destruction of a generator to the emergency shutdown of a nuclear facility. The nuclear plant shutdown is of great importance, as it was caused by connectivity between business and control system networks. A description of the incident is presented in *Protecting Industrial Control*

Systems from Electronic Threats, by Joseph Weiss (www.isa.org/link/Protecting_bk). The impacts of lost production and remuneration are obvious and can easily cost millions of dollars; even worse are the potentially life-threatening consequences of these disruptions. In spite of this, organizations spend less than a fraction of 1% of the Information Technology (IT) budget to protect their industrial control networks, according to the white paper's author.

Recent standards such as the ISA99 series allow the secure interfacing of hardware and users to networks, which can greatly reduce the effort and cost of protecting previously isolated control networks. Learning from the misfortunes of others should motivate those who are not currently concerned.

Most IT organizations understand technologies like anti-virus systems, firewalls, and virtual private networks (VPNs). However, not all operational organizations understand these tools can be used for protecting the plant floor. Unfortunately, coordinating these technologies can be a major engineering management challenge. For example, if a VPN concentrator has a list of people allowed to remotely access the control system, and Human Resources dismisses one of those people, how is that information conveyed to the VPN concentrator in a timely manner? Or similarly, if an engineer has just used his badge to sign into the control room, how can the VPN concentrator be informed so it does not allow the same account to be used from somewhere else at the same time?

Certainly, there are many communication protocols that can allow different systems to exchange information—OPC, FTP, telnet, SNMP, syslog, RADIUS, HTTP, and SQL are just a small sample of the alphabet soup of options. The trouble is each vendor has its preferred solution, which often needs extensive configuration, and most typical solutions are point to point. Thus, a complex and hard-to-maintain spider web of security device to security device interconnects is often required. The previous VPN example may require SNMP to connect to the network hardware maintenance system, syslog to report events to the security center, Active Directory to interface to the Windows account management system, telnet for configuration, SQL to interface with the HR database, and a custom serial link to the badge code reader. This is expensive to deploy and unsupportable over the long term.

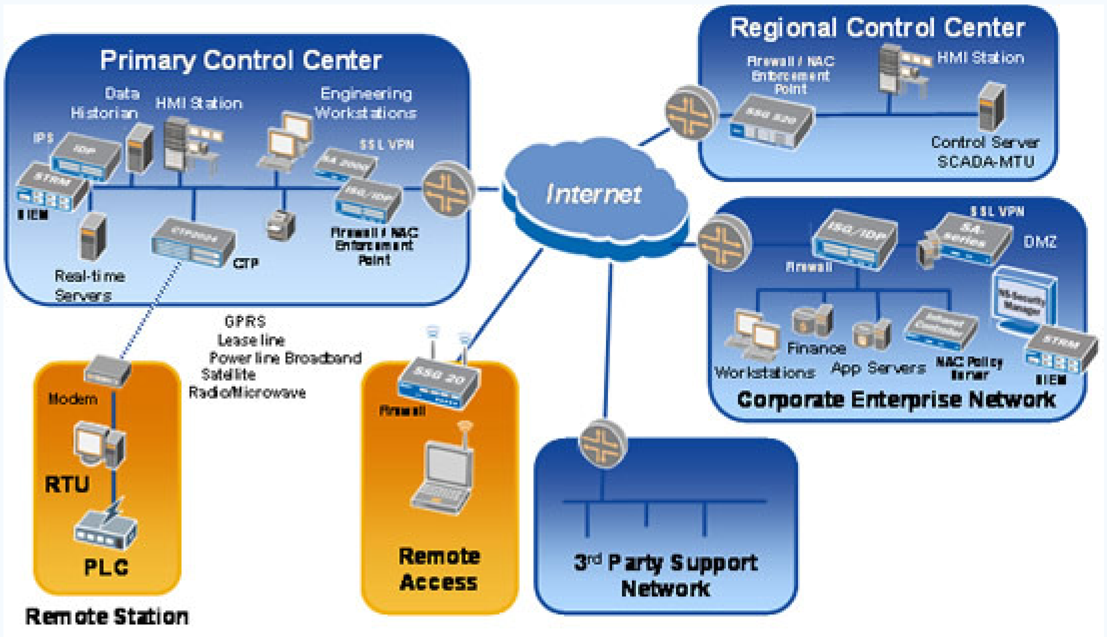
In the IT world, the term network access control (NAC) describes a key approach for managing network security. NAC uses endpoint health checking and user identification to thwart malicious attacks and deny access to unauthorized users while allowing access to properly credentialed individuals. NAC solutions have been developed by several companies, initially using proprietary technology, for over a decade. The most effective solutions available today use open, standards-based security developed by the Trusted Computing Group (TCG) (see sidebar) to communicate and achieve interoperability between the disparate security technologies/products used to protect control system networks.

TCG's Trusted Network Connect (TNC) establishes a standards-based approach for NAC (see sidebar). TNC's open architecture and standards provide a toolkit that allows control network designers to build much more complex, yet flexible, security systems than by committing to a proprietary single source or by struggling with multiple protocols and potential incompatibility between products from different vendors. The TNC Interface to Metadata Access Points (IF-MAP) standard (see sidebar) enables a multi-vendor, interoperable approach to protecting control system networks by providing unified security information. Security technology can leverage IF-MAP to ensure any person or device on the network meets a large number of criteria, such as possession of valid certificates or passwords, being in the correct location, and meeting current patch or AV levels, before the device can communicate on the network. Two use case examples show how solutions based on IF-MAP can solve the common and emerging security problems in control systems.

Use case 1: Electric utilities

IF-MAP enables federation of user and session information between a remote access user and internal access controls. This enables transparent but protected access to the control system network for systems engineers connecting via a remote access solution. Electric utilities provide an excellent example of the need for improved security.

Originally, control systems were operated as isolated, self-contained end-to-end networks; however, for a variety of reasons, more and more control system networks are being interconnected with corporate enterprise networks and greater overall IT connectivity. An electric Independent System Operator (ISO) managing geographically dispersed systems might look for reduced cost via consolidation, common network infrastructure, and remote debugging and maintenance. Real-time production information available across an interconnected network enables an ISO to manage shortages and sell excess, as well as comply with compliance requirements.



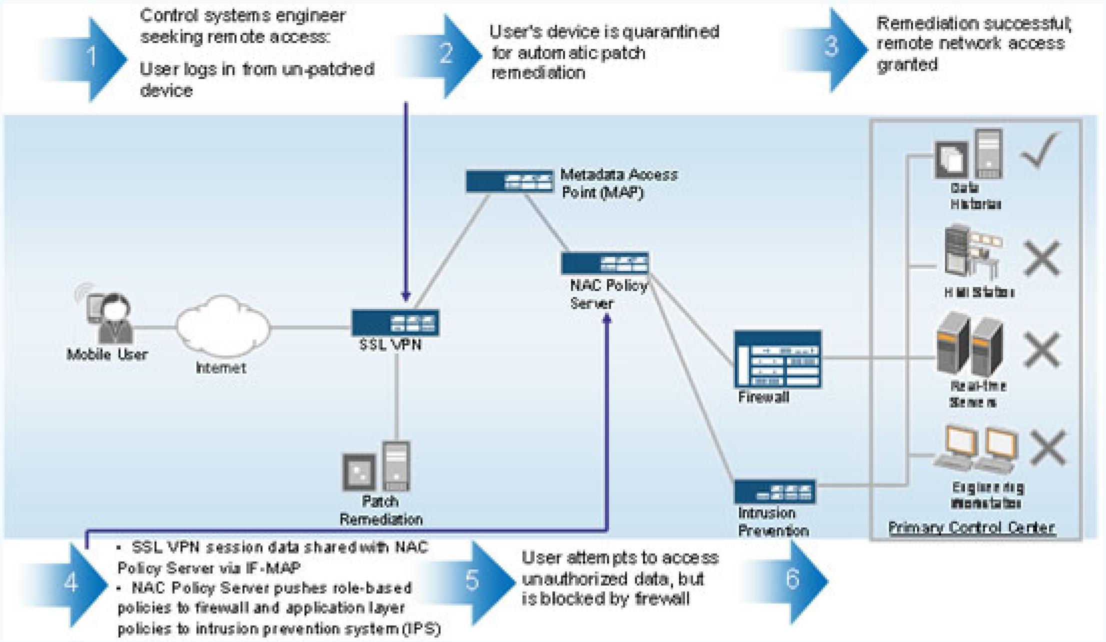
In a SCADA system, a primary control center may be interconnected with a variety of remote locations as well as the corporate IT network.

Unfortunately, with increased connectivity comes increased exposure to risk. External attackers gain visibility into, and potential access to, once-isolated systems now indirectly exposed to the Internet via the corporate network. Free web-based search engines, such as Shodan, enable finding exposed SCADA systems for the Internet-based attacker. And even without a malicious agent launching a directed attack, collateral damage such as network congestion and platform infection from common viruses and worms can take on new significance when control system processes are affected.

The North American Electric Reliability Corporation (NERC) developed Critical Infrastructure Protection (CIP) standards to ensure reliability of the North American electric system by providing a cybersecurity framework for identifying and protecting critical network-accessible assets. The NERC CIPs requires electric utilities to implement perimeter security and only allow authorized users access to critical resources through those perimeters. However, utilities want to provide systems engineers and administrators remote access to the control system network. This allows them to implement changes in an emergency situation, or even during normal operations, and avoid commuting to a particular location.

To implement secure remote administrative access to control system networks, the utilities must ensure compliance with the NERC CIP requirements for perimeter authorization. For secure access, data must be transmitted back and forth across the perimeter between the control systems network and the corporate IT network, but users must be authorized to access that data, and endpoints accessing that data should be inspected and verified through a health check to ensure they do not introduce potentially malicious traffic. This approach appears to be consistent with the guidelines on control and business network connectivity being prepared by the NERC Control System Cyber Security Working Group.

The figure below shows the unification of remote and local access control, transparently to the accessing user. A firewall enforcement point separates the control system network from the corporate IT network, which contains an SSL VPN (Secure Sockets Layer Virtual Private Network) and NAC Policy Server. In these environments, network administrators often have already implemented some sort of network segmentation internally. Users have to authenticate to a policy server to get through that firewall. In this example, the control systems engineer is permitted to access historical data but denied access to unauthorized resources. Identity-based access control enables termination of his remote access session, in addition to his internal network access, when unauthorized traffic is detected from his endpoint.



1 Control systems engineer seeking remote access:

User logs in from un-patched device

2 User's device is quarantined for automatic patch remediation

3 Remediation successful; remote network access granted

4
- SSL VPN session data shared with NAC Policy Server via IF-MAP
- NAC Policy Server pushes role-based policies to firewall and application layer policies to intrusion prevention system (IPS)

5 User attempts to access unauthorized data, but is blocked by firewall

6

Transparent remote/local access control for a network allows access for authorized users to policy-determined locations.

Extending access to remote users through an SSL VPN highlights the need for coordination between security components. The SSL VPN provides access to the corporate IT network, and a NAC Policy Server provisions access control policies to the firewall protecting the control systems network. The goal is to allow an authorized user, who has already been authenticated and health-checked by the SSL VPN, access through the firewall into the control system network without forcing a secondary authentication. Since a network security element (the SSL VPN) has already authenticated the user and validated the health of their endpoint, this eliminates the need for an additional authentication process to access the internal NAC-protected resources.

This is where IF-MAP comes in. As shown above, with IF-MAP implemented in the appropriate components, the SSL VPN device can federate its user session information by publishing it to a metadata access point (MAP). When the user's access attempt reaches the firewall enforcement point, the firewall queries the policy server to find out whether to allow that traffic or not. The policy server can search the MAP and, because it finds the user's established session as published by the SSL VPN, it can dynamically provision access instead of requiring the user to perform a second authentication and health check. Using the same IF-MAP mechanisms, if the intrusion prevention system detects malicious activity originated from that user, it can publish information about the policy violation. The SSL VPN and NAC Policy Server can consume that information and take appropriate action, terminating the user's remote access session as well as removing the access policies provisioned to the firewall.

One of the highly visible growth areas in electric utilities that will require improved security is smart grid. With smart grid, real-time information produced by control systems is increasingly used by business decision-makers. This creates an even greater need for secure, yet flexible, enforcement of the perimeter between the corporate IT network and the control system network. Smart grid is only one aspect of the broader need for security in the electric utility industry, just as the electric utility industry is one of many industries that can benefit from standards-based control system cybersecurity.

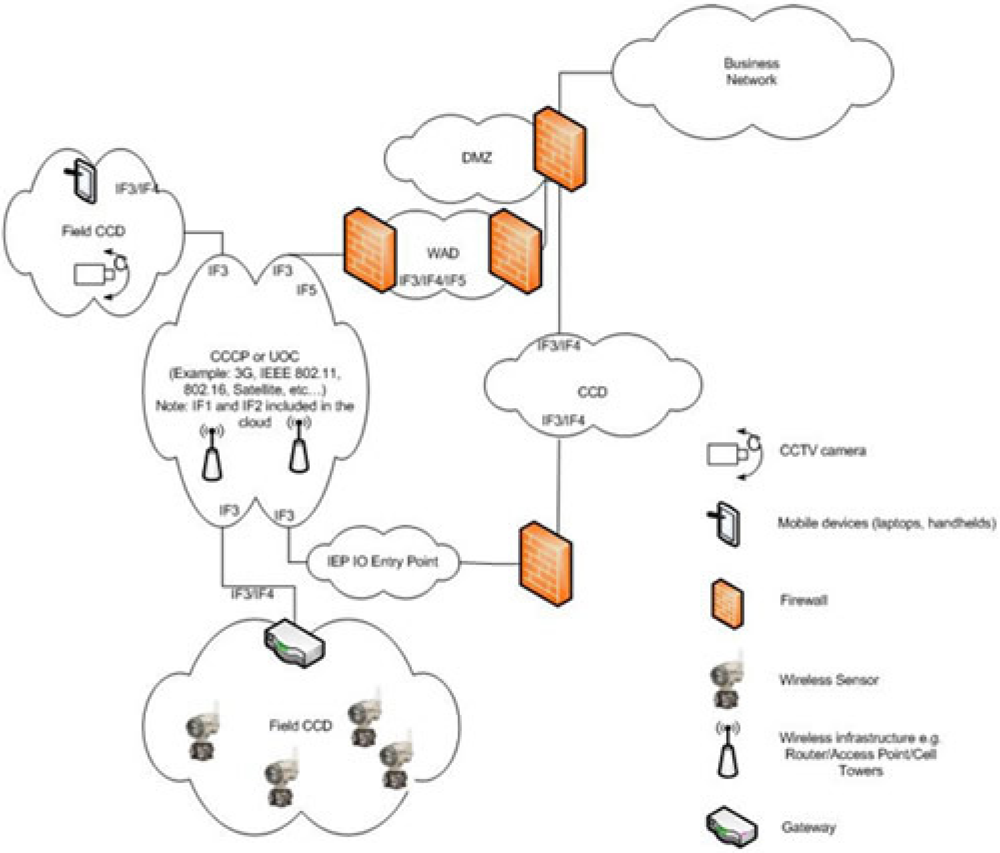
Use case 2: Network access for remote users

The second use case involves wireless control systems, an increasingly important means of communication in many industrial environments because of the reduced cost from avoiding the installation and maintenance of hard-wired networks. For example, in the aerospace industry, because of the size of the airframe, mobile tools travel around the airframe instead of the product traveling down an assembly line. The crawler robots, or simply crawlers, use wireless technology to connect to the network and communicate with each other and to fixed systems, such as inventory control. To avoid problems, a security appliance that incorporates TCG’s IF-MAP provides firewall services to isolate the programmable logic controllers on the crawlers from potential intruders. The appliance only allows access to the specific network connections required for correct plant operation.

The security process starts with an IF-MAP capable security enforcement point—in this case, Byres Security’s Tofino Security Appliance—collecting corporate security certificates through the MAP. Next, the MAP provides the company’s security policy, including firewall rules and VPN security associations. If an unauthorized user or system attempts to gain access to network services, access is denied, and the appliance reports this information to the MAP in real time. Depending on the other security hardware and software involved, the appropriate response can include alerting the network security team, logging the incident in a database, or changing the security policy.

A tool for wireless security

In addition, ISA is considering the inclusion of IF-MAP as one of the potential solutions for backhaul security in the ISA100 standard. The breadth of ISA100 across all industries and manufacturing environments, as well as the concern for interfacing wireless technology to control and business local-area networks, is similar to those areas covered by TCG’s TNC. The ISA100.15 Backhaul/Backbone Networks RFI example topology for process automation users is shown below. Comparing this to the figures above shows the similarities in key perimeter elements between the two architectures.


Business Network
DMZ
Field CCD
IF3/IF4
WAD
IF3/IF4/IF5
IF3
IF3
IF5
CCCP or UOC (Example: 3G, IEEE 802.11, 802.16, Satellite, etc…) Note: IF1 and IF2 included in the cloud
IF3/IF4
CCD
IF3/IF4
IF3
IF3
IEP IO Entry Point
IF3/IF4
Field CCD
CCTV camera
Mobile devices (laptops, handhelds)
Firewall
Wireless Sensor
Wireless infrastructure e.g. Router/Access Point/Cell Towers
Gateway

The ISA100.15 topology of Backhaul/Backbone Network transition from the control system to the business environment has several interface (IF) points and firewalls to protect the control network.

Conclusion

To avoid this situation, newer standards-based technologies for IT networks may be applied to the management of security for control system networks. With IF-MAP, the vital information needed to securely connect control systems to the enterprise network and minimize the risk from unauthorized access can be coordinated from a variety of sources. The end results are control systems that are easier to manage and more secure.

ABOUT THE AUTHORS

Scott Howard is a participant, Trusted Network Connect Work (TNC) Group, Trusted Computing Group (TCG). **Lisa Lorenzin** is a contributing member, TNC Work Group, TCG (http://www.trustedcomputinggroup.org/).

Resources

ISA99, Industrial Automation and Control Systems Security

http://www.isa99.org

ISA100, Wireless Systems for Automation

http://www.isa100.org

Trusted Network Connect and IF-MAP

http://www.trustedcomputinggroup.org/solutions/network_security

http://www.trustedcomputinggroup.org/developers/trusted_network_connec

"Hacking the Industrial Network"

http://www.innominate.com/content/view/169/1/lang,en/

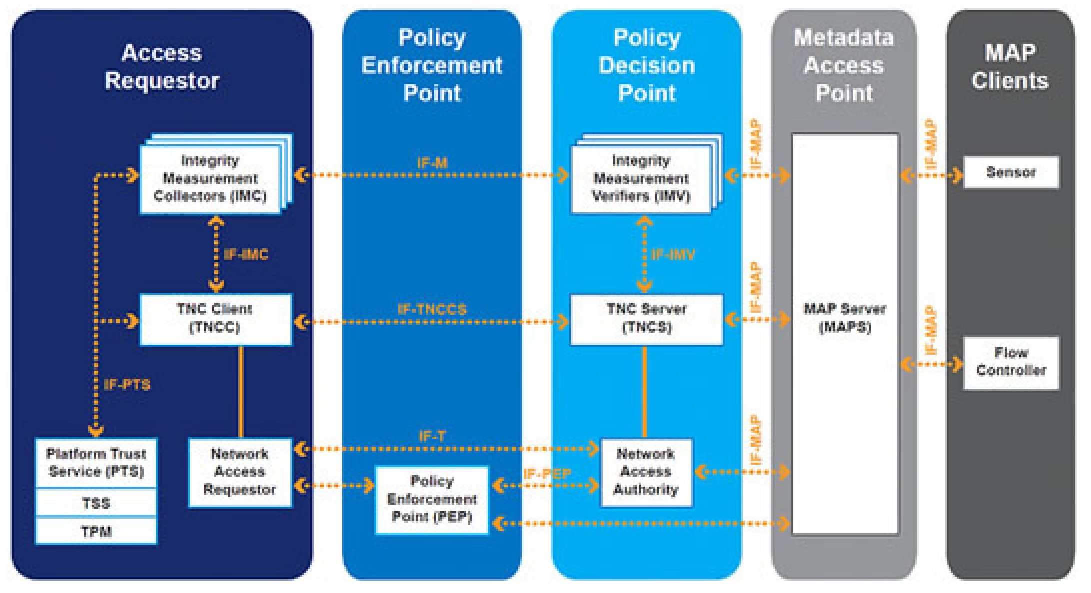
The Trusted Computing Group

The Trusted Computing Group (TCG) consists of members from more than 100 leading electronic system products, components, software and service companies, as well as end users with security concerns such as Boeing, General Dynamics and Lockheed Martin. TCG has been developing open standards for enterprise security for many years. With trust as an integral part of its name, the organization tackled trust and security issues in computing products starting at the most fundamental level and has extended its efforts to all aspects of the enterprise including clients, servers, networking and security components, and endpoints such as PCS, printers, and other devices that connect to the network.

TCG standards encompass multiple areas of technology. At the heart of TCG efforts is a standards-based hardware element called the Trusted Platform Module (TPM), an integrated circuit providing hardware-based authentication, encryption, and attestation capabilities. On the storage front, encryption standards from TCG enable self-encrypting drives that offer advanced access authentication and hardware-based encryption. Access control and coordination specifications from the Trusted Network Connect (TNC) workgroup provide a standards-based framework for Network Access Control (NAC) that bases network access decisions on security state information. Other workgroups within TCG focus on applying TCG concepts to clients and servers, mobile devices, multi-tenant environments such as cloud computing, and more.

Trusted Network Connect (TNC) & IF-MAP

To address the security issues inherent in allowing a wide variety of endpoints to access a protected network, the Trusted Computing Group developed the Trusted Network Connect (TNC) architecture and standards. The TNC architecture is shown below; dotted lines indicate the standards enabling interoperable communication between components.



TCG's Trusted Network Connect architecture has several standard interfaces including the interface to Metadata Access Points (IF-MAP).

TNC provides a standards-based approach to network access control (NAC). Starting with the three basic NAC elements of an Access Requestor (endpoint), Policy Enforcement Point (such as a switch or firewall), and Policy Decision Point (NAC policy server), TNC provides the crucial benefit of open standards to enable multi-vendor interoperability.

In addition to the three-element NAC model, the TNC architecture includes networking and security elements that report information about the network, called *sensors*. (These sensors are quite different from those used in control systems—they include any network device that can provide useful information about the network itself, as well as the users and devices on it. For example, an intrusion detection system might be a sensor; so might a badge card reader, as it could provide information about the location of a person signing into the network.) Another TNC element is a flow controller, a security device such as a firewall that makes and enforces access control decisions.

Communication between these components and the rest of the TNC architecture occurs through a central clearinghouse, the Metadata Access Point (MAP), via TNC's Interface to Metadata Access Points (IF-MAP). IF-MAP adds an integrated, real-time view of security that enables products to work together in a coordinated manner to grant access as appropriate.

IF-MAP is a critical missing link between systems that would normally not communicate with each other. It offers networking and security components the ability to publish, subscribe to updates on, and search for information. This functionality provides real-time updates on what the connected systems are seeing in the network—essentially social networking for machines. With this capability, the IF-MAP protocol enables machine-to-machine coordination of highly automated and globally scalable industrial processes and IT. For security systems that are already network connected, IF-MAP support can usually be obtained through a software upgrade, offering stronger security at low incremental cost.

Securing Critical Industrial Processes in Real Time

Application Note #120
AN-120
Version 1.0

The Need for Security in Real Time

The susceptibility of critical SCADA systems to security issues confronts many organizations. While it may be rare to penetrate a control system directly from the Internet, corporate intranet connections, remote support links, USB keys, and laptops create pathways for the typical worm or hacker. Once inside, impacting an industrial control system is not difficult — in some cases, even the most basic scanning by a hacker or worm can wreak havoc.

Unfortunately, 99% of all SCADA and process control devices do not support even basic authentication and authorization functions. Thus these devices cannot take advantage of any of the security infrastructures offered by many corporate IT departments. Complicating the matter even more, many SCADA end users have found the common VPN solutions to be either unbelievably complex to manage in real time or ill-suited for handling the protocols that are found in automation networks.

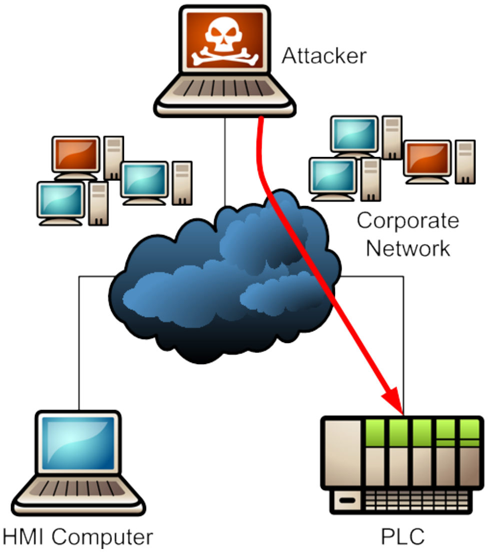


Figure 1: Insecure SCADA communications over the corporate network make cyber attacks trivial

Figure 2: Mobile “crawlers” contain the PLC’s that manage the safe and reliable assembly of aircraft

Securing Aerospace Manufacturing

A major aerospace manufacturer faced exactly this issue when securing the systems used in the production of their long-range passenger aircraft. Large, highly mobile crawlers with extensive Programmable Logic Controllers (PLC) and Human-Machine Interface (HMI) components are vital for the assembly of new aircraft. In order to coordinate that assembly, these PLCs require secure access to each other and to the corporate network in real time.

Since the PLCs are installed on mobile platforms, they require wireless access to communicate. However, the models of PLCs currently on the market cannot participate in the corporate PKI system, which is a requirement for secure wireless communications. Furthermore, the plant security solution system must dynamically modify security policy (and allow PLC to PLC connections) based on information from a large variety of sources that change rapidly. For example, the position of a crawler or the card scan of an operator will determine which PLCs can interconnect.

SCADAnet Endboxes Secure PLCs

The solution is an architecture called SCADAnet. SCADAnet provides a simple and secure encryption system between control devices. Each crawler is protected by a SCADAnet Endbox. These Endboxes then securely interconnect with other Endboxes over a variety of secure or insecure networks, including the corporate Intranet, various cellular services or even the Internet. The Endboxes interact with the corporate IT security services, including the corporate Public Key Infrastructure, to provide an encrypted Overlay Network between the PLCs assigned to them by the crawler operators.

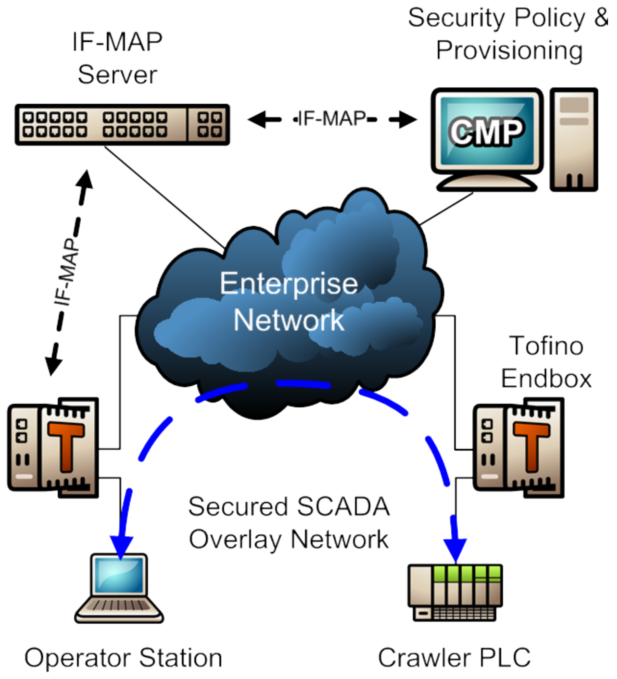


Figure 3: SCADA communications over the corporate network are secured using Endboxes that obtain real time policy information from the IF-MAP server

Figure 4: An Industrially hardened Tofino Endbox

IF-MAP Ties It All Together

Tying all the Endboxes together in a scalable manner is a central publish/subscribe repository of network information based on the Interface-Metadata Access Protocol (IF-MAP) technology. This Trusted Computing Group standard allows systems from different vendors to publish information that the Endboxes can use to determine security policy in real time. For example, if the IP address of an Endbox changes because a crawler has moved into the range of a new wireless access point, then this information can be propagated to other Endboxes so that critical communications are not disputed. Or if an operator that is not approved for a given crawler swipes into the badge reader, the crawler can be immediately disconnected from the critical control network.

Summary

The SCADAnet architecture, IF-MAP and Tofino Endboxes provide a framework that allows the IT department to manage access to its services and yet let the SCADA engineers maintain full control over their network systems and devices.

BYRES SECURITY INC.

TELEPHONE:	1 250 390 1333
TOLL FREE:	1 877 297 3799 (N. America)
EMAIL:	sales@tofinosecurity.com