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

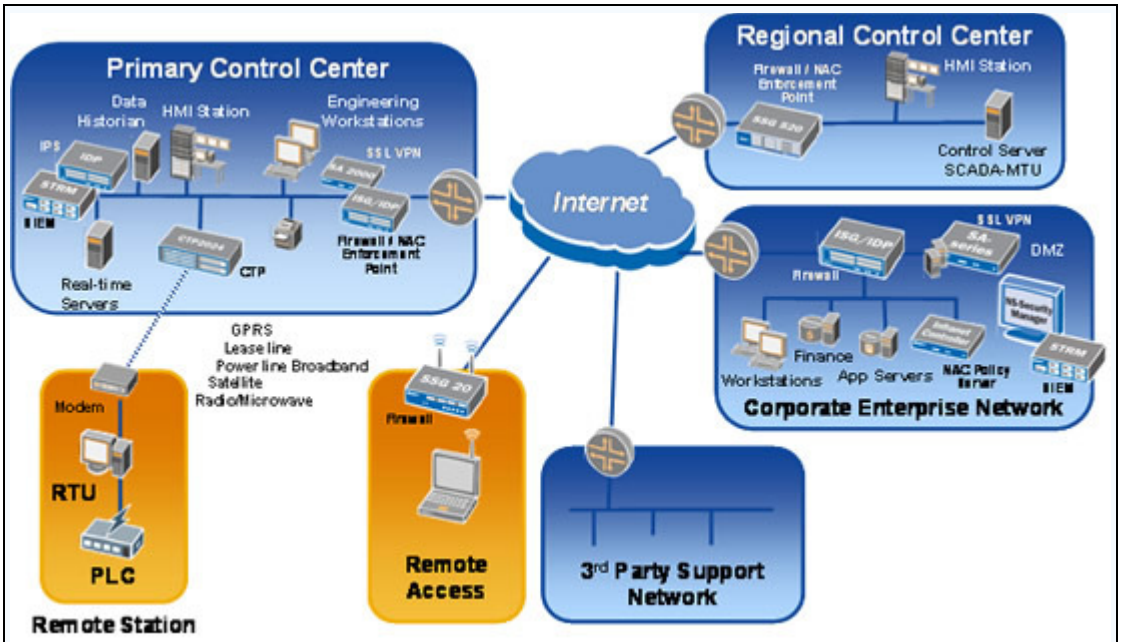
attacks and deny access to unauthorized users while allowing access to properly credentialed individuals. NAC solutions have been developed by several companies, initially using proprietary technology, for over a decade. The most effective solutions available today use open, standards-based security 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.

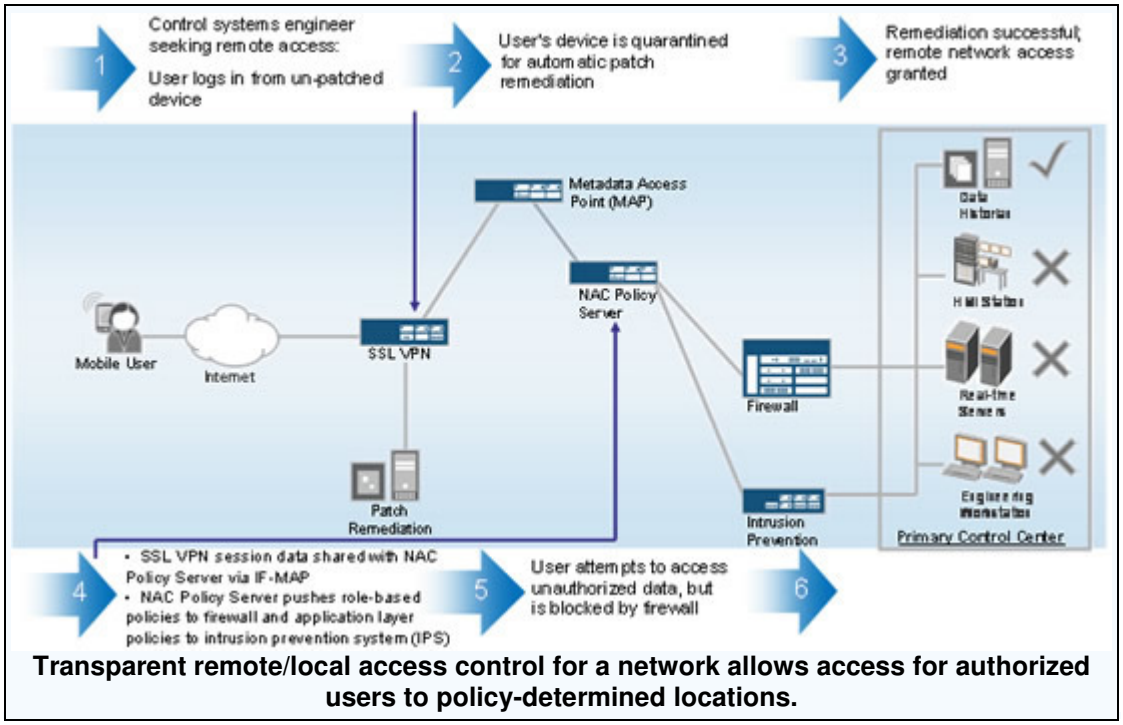
Unfortunately, with increased connectivity comes increased exposure to risk. External attackers gain visibility into, and potential access to, once-isolated systems now indirectly exposed to the Internet via the corporate network. Free web-based search engines, such as Shodan, enable finding exposed 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.



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

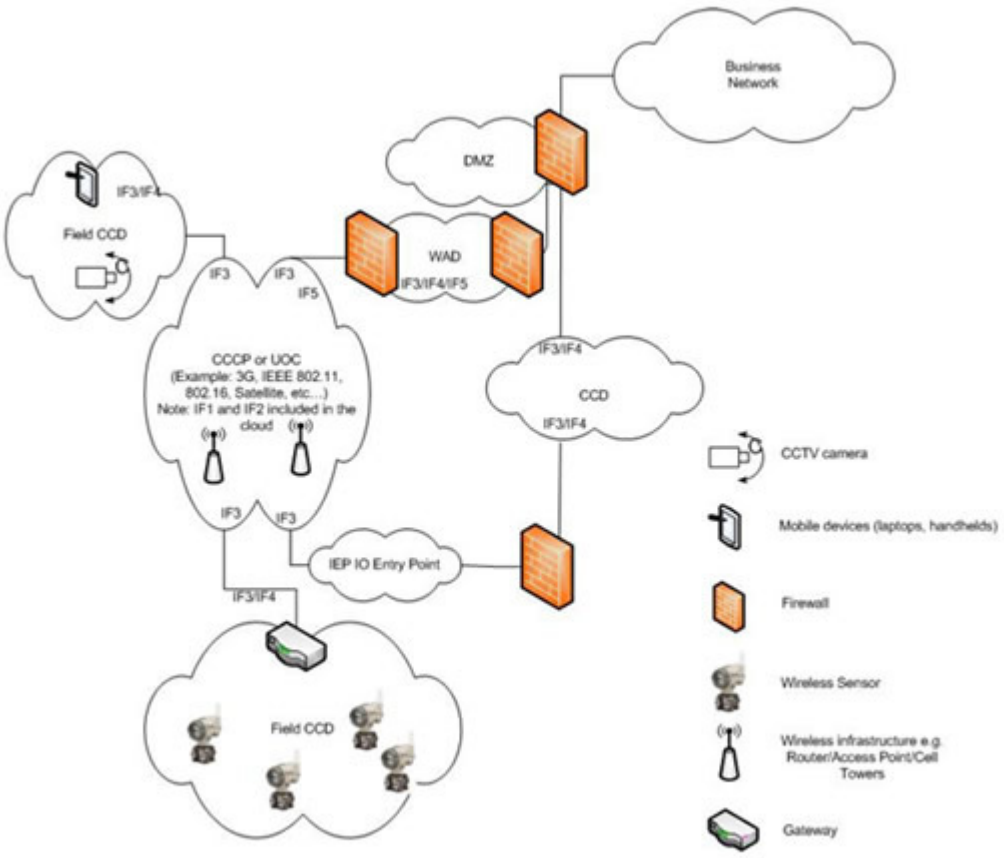
The second use case involves wireless control systems, an increasingly important means of communication in many industrial environments because of the reduced cost from avoiding the installation and maintenance of hard-wired networks. For example, in the aerospace industry,

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.



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/

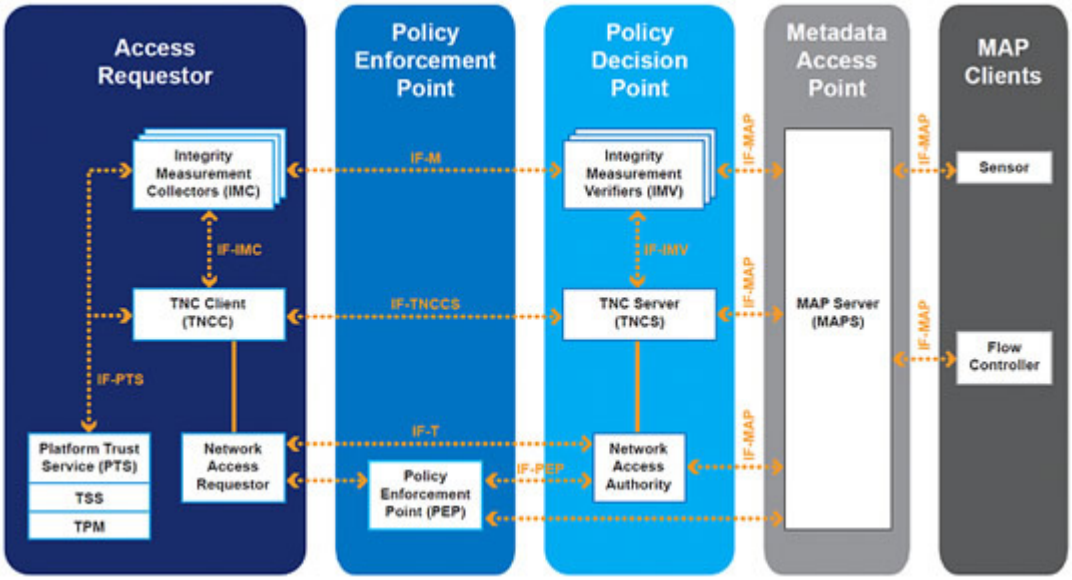
The Trusted Computing Group

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.