



IF-MAP Metadata for ICS Security

Lisa Lorenzin

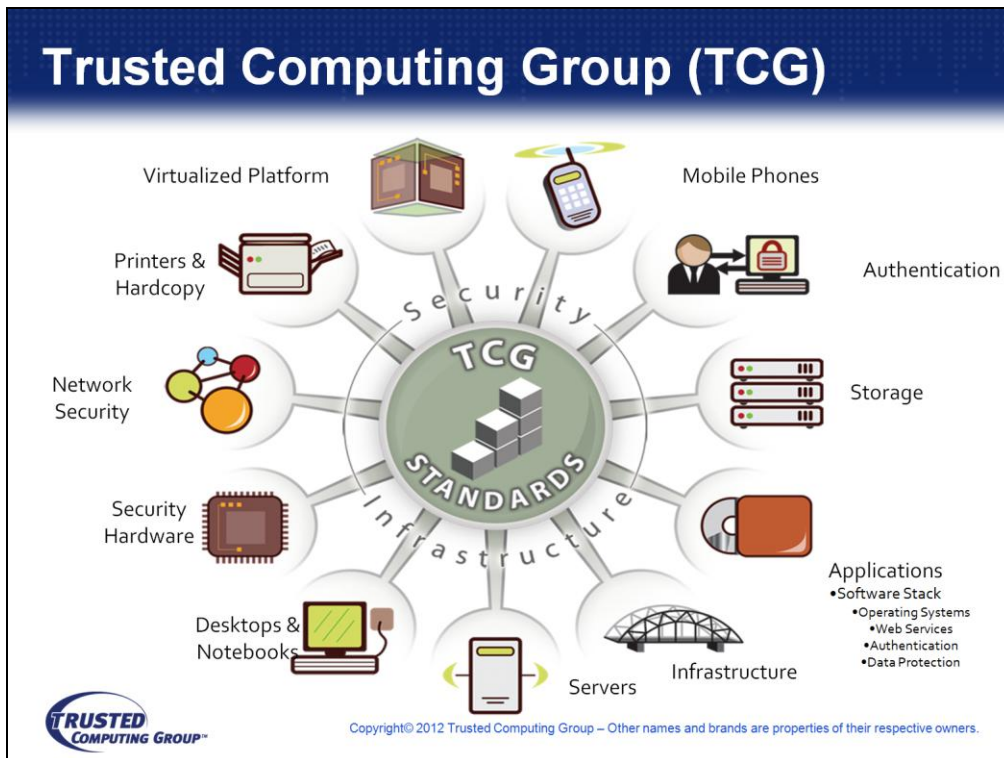
10/16/2012

Trusted Computing Group (TCG)

- Industry standards group
 - More than 100 member organizations
 - Includes large vendors, small vendors, customers, etc.
 - Includes product certification program for standards compliance
- Goal:
 - Help users protect their information (data, passwords, keys, etc.) from compromise due to external software attack and physical theft.
- Mission:
 - Develop, define, and promote open specifications for trusted computing and security
 - For hardware building blocks and software interfaces
 - For multiple platforms, peripherals and devices



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.



This slide shows the areas where TCG is developing standards. Each image corresponds to a TCG work group. In order to understand Trusted Network Connect, it's best to look at it in context with the other TCG standards.

We'll start with Security Hardware since that's where TCG started. TCG started by defining standards for a hardware security module called the Trusted Platform Module or TPM. The goal with TPM is to make ALL of the devices we use every day trustworthy. And the only solid basis for a trustworthy device is trustworthy hardware, the TPM. Without TPM, systems are always susceptible to viruses and worms and other nasty infections. TPM lets us stop those infections and keep our devices secure.

Most of the other TCG work groups are applications of the TPM. For example, the Desktops and Notebooks group defines standards for using the TPM to make desktop and notebook PCs more secure. The Server group works on making servers more secure with TPM. The Infrastructure group defines standards for managing and supporting TPMs. Applications looks at how software applications can use the TPM. Storage works on making storage devices more secure. Authentication defines ways for users to authenticate to their TPM to get access to their PCs (like biometrics and passwords). Mobile Phone defines standards for security on mobile phones. Virtualized environments must also be secured so we have a Work Group in that area. Printers and other imaging devices handle confidential data all the time so we must make sure they cannot be infected. And finally, Network Security. That's Trusted Network Connect or TNC, the subject of this talk.

Now before we go any farther, let me explain that TNC does not require a TPM to function. We recommend the use of a TPM for the strongest assurance levels but TNC does not require a TPM. TNC works with whatever you've got on your network and makes it all more secure.

Trusted Platform Module (TPM)

Security hardware on motherboard

- Open specifications from TCG
- Resists tampering & software attacks

Now included in almost all enterprise PCs

- Off by default; opt in

Features

- Secure key storage
- Cryptographic functions
- Integrity checking & remote attestation

Applications

- Strong user and machine authentication
- Secure storage
- Trusted / secure boot



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

Still, the TPM is really cool technology that we all have in our laptops so let's take a closer look at the Trusted Platform Module. What is a TPM, anyway? A TPM is a hardware security module included on the motherboard of most enterprise PCs today. Sometimes the TPM is a separate chip and sometimes it's built into an existing chip like an IO controller but it always complies with the TPM specifications defined by TCG so it always works the same way.

Because the TPM is hardware, it provides a strong basis for building a trustworthy endpoint. It can't be infected or compromised through software. The features of the TPM include secure key storage, cryptographic functions like signing and encryption, and integrity checking capabilities. What can you use it for? You can start with strong user and machine authentication. Essentially, the TPM can function as a smart card built into the PC, a form of strong authentication. But that's not all. Because the TPM is built into the PC and always present, it's a great place to store keys for securing storage. Microsoft Windows Vista includes a feature called BitLocker that provides full disk encryption to protect your data in case your laptop is stolen. BitLocker supports TPM for key storage but it can also be used without TPM. Without a TPM, BitLocker stores the encryption key on the hard disk. Does anybody see a problem with that? Yes, that's right. Anyone who steals your laptop can just read the encryption key off your hard disk, use a dictionary attack to get your passphrase, and decrypt your data. If the key is stored on the TPM, it's much harder to get the key. You have to break the TPM. I'm not saying that's impossible but it will require tunneling electron microscopy or other hard attacks. And the last application of the TPM is for trusted boot, which works nicely with TNC. I'll talk more about that later. Let me just emphasize, though, that TPM is not required for TNC. It's an optional way to increase the security of TNC. But you can always do TNC without TPM or vice versa.

Trusted Network Connect (TNC)

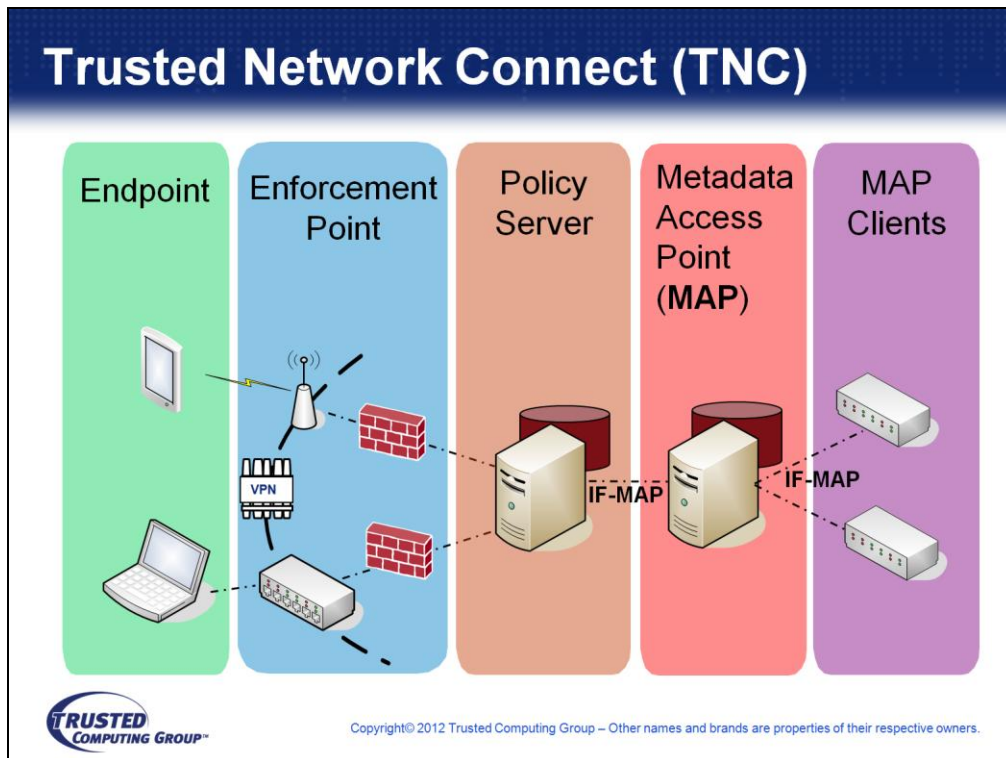
- Open Architecture for Network Security
 - Completely vendor-neutral
 - Strong security through trusted computing

- Open Standards
 - Full set of specifications available to all
 - Products shipping for more than four years



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

TNC is an open architecture for network access control. If you're not sure what NAC is, we'll cover that in a second. For now, the main point here is that TNC defines an open standard for NAC so that customers can take products from several different vendors and put them together into a NAC solution. TNC is a well established and widely used. There's a full set of TNC standards available to all on the TCG web site, there are dozens of products that implement those standards, and hundreds of happy customers are using those products. Where does all this goodness come from? Well, the TNC standards were developed by the Trusted Computing Group or TCG, an industry standards group focussed on secure computing (or "trusted computing", as we prefer to call it). The TCG has more than a hundred members, including all the large vendors in high tech and lots of the small vendors as well as a few forward-thinking customers like Boeing and the NSA.



So how does TNC work? It's really quite simple. This is the TNC architecture but every NAC architecture is basically the same. On the left, you see the Access Requestor. That's a device that's trying to access a protected network or resource. The Policy Enforcement Point is a guard that grants or denies access based on instructions from the Policy Decision Point or PDP. The PDP is really the brains of the operation. It looks at the policy that you have configured and decides what level of access should be granted. Then it tells the Policy Enforcement Point, which executes those instructions.

There are many options for enforcement – common choices are a wireless access point and a switch, but many people use a firewall or a VPN gateway. Each of these has its own pros and cons. For example, a wireless access point with 802.1X can totally block unauthorized users. But it probably won't have fine-grained access controls. That's why a lot of NAC systems support a combination of different Policy Enforcement Points.

What about monitoring behavior? Well, there are a huge number of devices already deployed in our networks to monitor behavior: intrusion detection systems, leakage detection systems, endpoint profiling systems, and so on. The TNC architecture lets you integrate all those existing systems and many more with each other and with your NAC system.

This integration uses a Metadata Access Point, which is basically a database that stores information about who's on your network, what device they're using, what their behavior is, and all sorts of other information. Your existing security systems use this Metadata Access Point or MAP to integrate with each other and with your NAC system.

Problems Solved by TNC

Network and Endpoint Visibility

- Who and what's on my network?
- Are devices on my network secure? Is user/device behavior appropriate?

Network Enforcement

- Block unauthorized users, devices, or behavior
- Grant appropriate levels of access to authorized users/devices

Network Access Control (NAC)

Device Remediation

- Quarantine and repair unhealthy or vulnerable devices

Security System Integration

- Share real-time information about users, devices, threats, etc.

Security Automation



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

Let's talk about what TNC does for you.

First, TNC gives you the ability to see who's on your network, what devices are in use, are those devices secure, and is the behavior appropriate. Great visibility!

Second, TNC lets you establish a policy for your network and block unauthorized users, devices, or behavior. You can even give different levels of access to different users and devices, based on the job they have to do.

Third, you can establish automated remediation to fix unhealthy devices before they get infected or infect someone else.

Those three things together are called Network Access Control or NAC. So TNC provides open standards for NAC.

But TNC goes beyond that. It includes an optional component called a MAP which is a database that links together all your security systems so they can share information about what they're seeing on your network: active users and devices, incoming attacks, and so on. This enables security automation, which is very powerful!

TNC Advantages

Open standards

- Non-proprietary – Supports multi-vendor compatibility
- Interoperability
- Enables customer choice
- Allows thorough and open technical review

Leverages existing network infrastructure

- Excellent Return-on-Investment (ROI)

Roadmap for the future

- Full suite of standards
- Supports Trusted Platform Module (TPM)

Products supporting TNC standards shipping today



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

TNC offers some very important benefits. Because TNC is all about open standards, you won't get tied into one vendor. You can choose any vendor you want and it will all work together. It's all designed and tested to do that. That provides a real financial benefit. You can reuse your existing network and security gear so your costs will be much lower than a proprietary approach. And that means higher ROI. TNC also has a great roadmap for the future. Whatever you want to do in network security, you can do it with TNC. And products that implement the TNC standards have been shipping for many years now.

WHAT IS IF-MAP?



Coordination Challenge

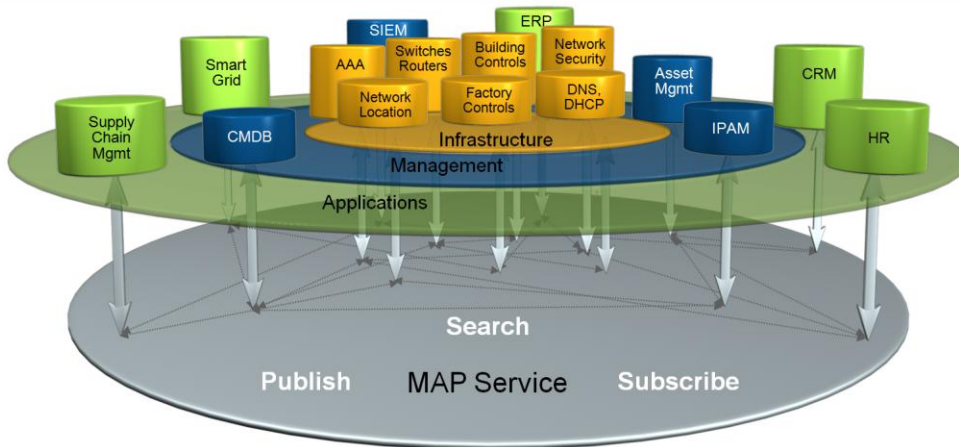
- Security infrastructure is complex, heterogenous, and usually distributed
 - And it is only getting more so
- Large, real-time data flows between infrastructure components
 - Needed for coordination between Sensors, Flow Controllers, PDP's, etc.
 - Components often interested in different patterns & events
- Timely routing and reliability of delivery of this data is critical for coordination

Simple connectivity is insufficient for good coordination



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

Interface to a Metadata Access Point



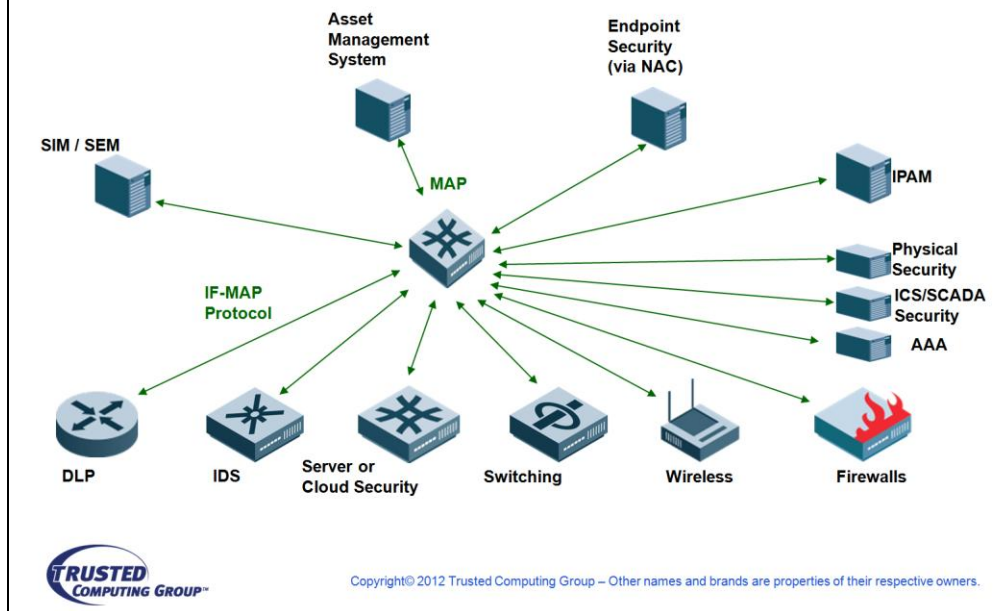
IF-MAP: XML > SOAP > HTTPS



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

The IF-MAP open standard makes it possible for any authorized device or system to publish information to a MAP server, to search that server for relevant information, and to subscribe to any updates to that information. Just as IP revolutionized communications, IF-MAP will revolutionize the way systems share data.

Security Automation



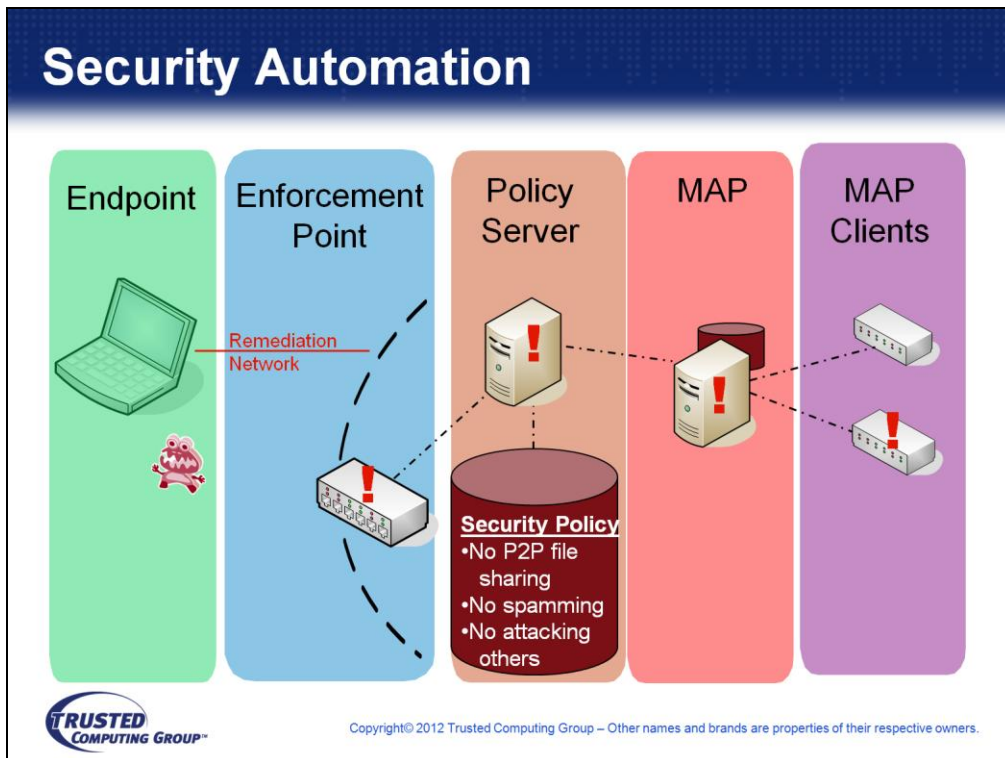
The MAP is really a central database for sharing information between different security systems.

Today, we have many forms of security, but they are rarely integrated together. Yes, it's possible to integrate security systems but it requires lots of custom integration work by the vendor or the customer. Custom integration is very expensive and it only works for a particular combination of vendor products. There are a few standards such as SNMP and syslog but they are very primitive, just grabbing problem alerts.

With the MAP, we use a single standard protocol called IF-MAP so all these systems can share information with each other using standard commands and data formats. Why is that so valuable? Well, your NAC system knows who's on the network, what their role is in the organization, what device they're using, what the IP address of that device is, and so on. If you share that information out to other security systems, they can do their jobs better.

For example, today your Network Intrusion Detection System just watches traffic on the network and looks for suspicious behavior. If it sees someone port scanning, it raises an alert. But what if your IDS knew which users go with which IP addresses? Then it would know that port scanning is normal for a security administrator but not normal for a guy in the shipping department. The IDS can become identity-aware and it can do a much better job with fewer false positives and fewer false negatives. Not only that, if the IDS does see some really nasty behavior, it can send an event to the MAP and store that in the record of the device that caused the problem. The MAP will immediately notify anyone who subscribed to changes in that record, such as the NAC system that let that device on the network. And then the NAC system can take action to block that device off the network.

So the MAP helps all of our security systems become more intelligent by giving them the information that they need to get their job done better. And it shares that information in real time, using a standard protocol and extensible data formats.

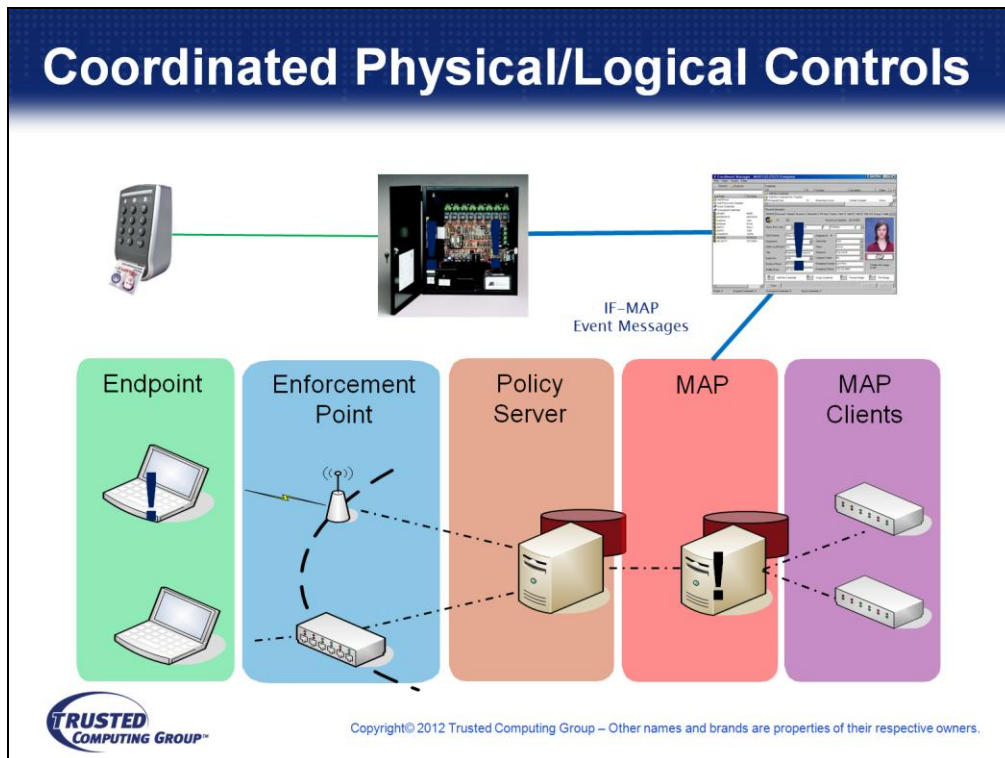


Here's an example of using IF-MAP to integrate endpoint behavior into an access control decision. So we've got some sensors in the network to monitor behavior. And we've got a security policy that specifies what behavior is acceptable.

Now, when a device connects to the network, there could be an authentication and compliance check - but this policy doesn't have one so the device is placed on the production network. If the device starts violating the NAC policy by trying to spread a worm, that will be detected and stopped by one of the sensors.

But, even more important, that sensor will publish information about the attack it stopped to the Metadata Access Point (MAP). A notification will be sent to the Policy Server, which will decide that's not acceptable and tell the Enforcement Point to move the user to a remediation network.

So you see that the whole network security system is working together here. Each part is doing its own thing and they're all integrating in a compatible way, using the open TNC standards.



Another example of the evolution of security automation is the integration of physical and logical access control.

Consider a typical badge access system. Readers capture and pass credential info; a control panel authenticates identity and enforces policy; and an access control server provisions policy. In this case, the access server also publishes location metadata via IF-MAP to a Metadata Access Point.




A user arrives at the front door and badges in. The badge reader passes his information on to the panel, which approves his entry into the building. The panel logs that information and also sends that message on to the access server, which captures the events and uses the IF-MAP protocol to publish location metadata to the MAP with the user's location.

That metadata can be accessed on a subscription basis by other authorized devices; in this case a policy server subscribes to the MAP such that it can check for the physical entry events and location data.

When the user gets to his desk, he is granted access to the network and its resources. Physical presence has become a policy requirement for network access; this makes the network more secure, and it helps physical security understand who is inside a building or in a particular part of a building.

IF-MAP Element Model

Model Components:

	Identifiers	All objects are represented by unique identifiers
	Links	Connote relations between pairs of objects
	Metadata	Attribute containers attached to Identifiers or Links

Important Properties:

- All identifiers and links exist implicitly, but have no meaning until metadata is attached to them
- Identifier and Metadata types are defined in XML schemas
 - Common elements standardized; designed to be extensible



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

What Is Security Metadata?

- Metadata = Data about other data
 - A file's name and size are metadata about the file's data (the content)
 - "A picture of a car" is descriptive metadata about a file containing an image of a car
- Network security metadata describes attributes of network data flows and associated principals
 - Who is associated with what data flows?
 - What credentials were used?
 - What policy decisions have been made?
 - Recent unusual behaviors?



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

Why IF-MAP?

- Why create a new protocol instead of using existing capabilities?
 - E.g., relational databases or directories?
- Nature of the coordination problem, and strengths and weaknesses of each possible approach
 - Coordination data is loosely structured and changes frequently
 - Infrastructure elements interested in different attributes and patterns



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

Properties of Security Coordination

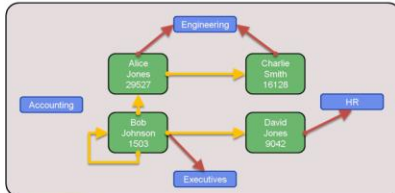
Relational Database



LDAP Directory



MAP Database



1. Lots of real-time data writes
2. Unstructured relationships
3. Diverse interest in changes to the current state as they occur
4. Distributed data producers & consumers



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

Real-time Security Coordination

- IF-MAP is specifically designed to fit the security coordination use case
 - Optimized for loosely structured metadata
 - Publish/Subscribe capability for asynchronous searches
 - Highly scalable, extensible architecture
- Design is based on the assumption that you will never find the data relation schema to satisfy all needs
 - So you can move forward in spite of a lack of full relation specifications

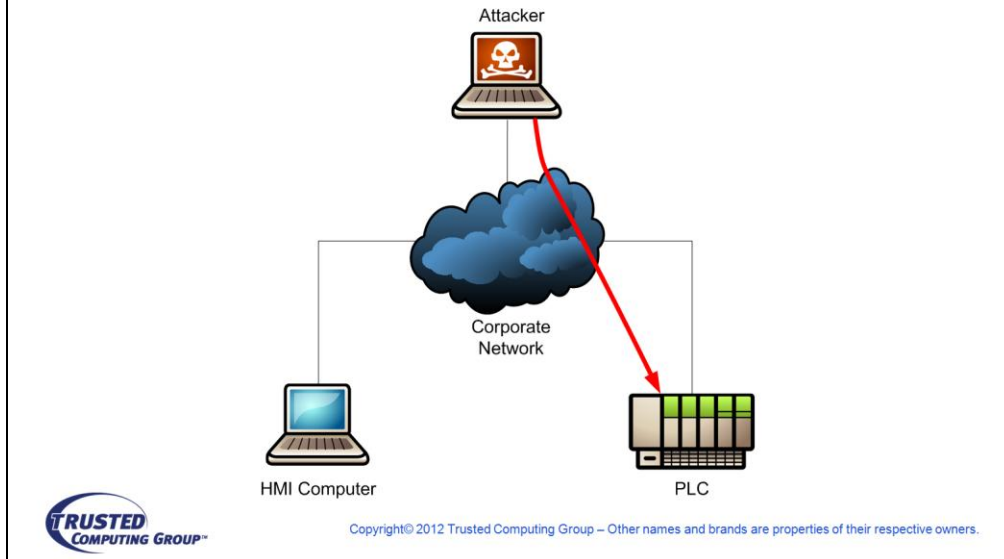


Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

IF-MAP METADATA FOR ICS SECURITY



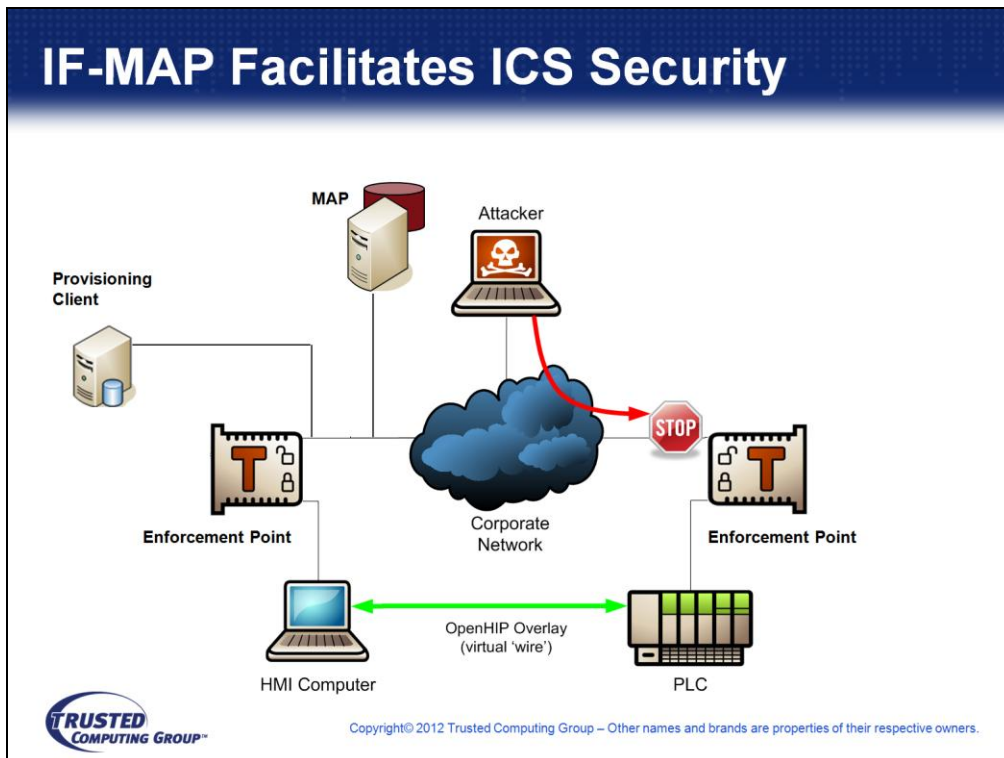
ICS Security Challenge



Imagine a manufacturing line, where a physical process is controlled by a digital component called a Programmable Logic Controller (PLC). The other piece of that system is an operator display panel, the Human Machine Interface (HMI), which is typically physically remote from the actual process that needs monitoring. As we see changes in the process, we should be able to see the operator display update in real-time.

The HMI uses a legacy protocol called Modbus to poll the controller and retrieve these process variables and display them. Used to be run over a serial connection, but it's been ported to TCP now. One of the problems with the Modbus protocol and many others in this space is that there's zero security features in the protocol. The key issue is: no authentication. So we have no way of knowing whether requestor is authorized to gain access to that, or even who is sending data to it. If you can ping that controller, you can issue commands to it.

That's the state of the art in control systems. Until now, they've been small islands of automation, very little interconnection with other systems. Running over serial, had to have a physical serial connection to it - typically you had to be physically in front of the machine to mess with it, physical security was fine. Another thing about this environment is that these systems, once they're in place, are designed to stay in production for decades. Now these systems are getting more and more interconnected with the enterprise network and outside as well, and we're running into the same types of security issues that we've been working on in enterprise systems.



A single manufacturing line could have hundreds, or even thousands, of these PLCs. Replacing them is out of the question, as is retro-fitting them to add on security. But what if we had the ability to insert a transparent security overlay to protect these legacy components?

Deployment and lifecycle management for such a network would be a huge challenge – unless you had a mechanism for provisioning certificates, communication details, and access control policies to the overlay components. And that’s exactly what one company, Boeing, has done with IF-MAP by using vendor-specific metadata for provisioning of certificate information and access control policy.

The first step is to add the overlay protection. In this case, the enforcement points are customized component designed for SCADA networks that can create a “virtual wire” – protected communication, transparent to the end devices – using OpenHIP. A MAP and a provisioning client enable centralized deployment, provisioning, and lifecycle management for the myriad enforcement points.

In this case, the provisioning client publishes metadata to the MAP to define the HMI and PLC and specify security policies that allow them to talk to each other, but do not allow external access to them. For example, when the HMI comes into the network and queries for a PLC, the first thing the HMI does is an ARP lookup. The enforcement point receives that traffic, searches the MAP server, and finds access control policy that this particular HMI can talk to that particular PLC.



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

This isn't just a neat thought experiment – it's actually in production deployment on the Boeing manufacturing lines for the 777 and 747 aircraft. The airplane you took to this conference might have been assembled by components in a control network protected by IF-MAP enabled technology!

ICS Metadata Specification

- **Purpose:**
 - Facilitate the necessary coordination for deployment, operational management, and security of large-scale industrial control systems
 - Builds upon the ISA100.15 architectural model, use cases, and functional requirements
- **Approach:**
 - Defines a set of metadata types and coordination behaviors for a various MAP client functional roles
 - Supports many BHIs and multiple overlay networks
 - BHI connectivity policies and overlay ICS device connectivity policies
 - Delegated management functions – different roles can manage different overlays



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

Relation to other TNC/TGG specifications

- Leverages IF-MAP specification
 - Includes a new metadata schema and new extended identifier definitions
- Does not require implementation of TNC NAC nor the associated requirements of the Metadata for Network Security specification
 - BHI implementers may choose to implement TNC client functionality
- Cryptographic identities and remote attestation
 - BHI implementers may choose to use TPM HSM and remote attestation functionality



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

ICS Specification: Operational Roles

- **BackHaul Interface (BHI) Role**
 - Communicates with other BHIs to establish overlay networks; notifies on security events/state changes
- **Overlay Manager Role**
 - Provides overlay network membership assignments and connectivity policies for consumption by BHIs
- **Administrator Role**
 - Manages creation, deletion, and management of overlay networks



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

ICS Specification: Operational Roles

- **BHI Role:**

- Publishes information about its configuration and state to facilitate operational monitoring and communications rendezvous with other BHIs.
- Searches and Subscribes to connectivity policy information published by overlay administrator applications
- Subscribes to changes in state to other BHIs in its overlay network(s)
- Notifies for security events, interface changes (mobility events, redundant link failover)



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

ICS Specification: Operational Roles

- **Overlay Manager Role:**
 - Publishes
 - BHI overlay membership information
 - BHI-to-BHI connectivity policies for consumption by BHI PEP function
 - ICS-to-ICS device communications connectivity policies for consumption by BHIs PEP function
 - Subscribes to metadata changes and notifications associated with BHI events
 - Provides a user interface or linkage functionality to a separate user interface for managing administrators managing overlay networks



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

ICS Specification: Operational Roles

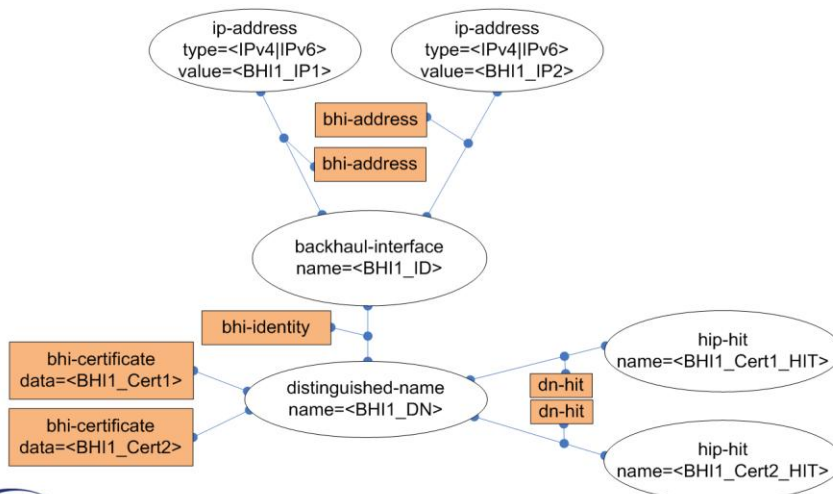
- **Administrator Role:**
 - Publishes metadata into the MAP graph to manage the creation and deletion of overlay networks
 - Publishes metadata into the MAP graph to delegate management of individual overlay networks to principals and/or LDAP groups
 - Provides MAP graph monitoring and repair functionality to detect and correct unusual conditions (e.g., orphaned overlay networks)



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

ICS Metadata Examples

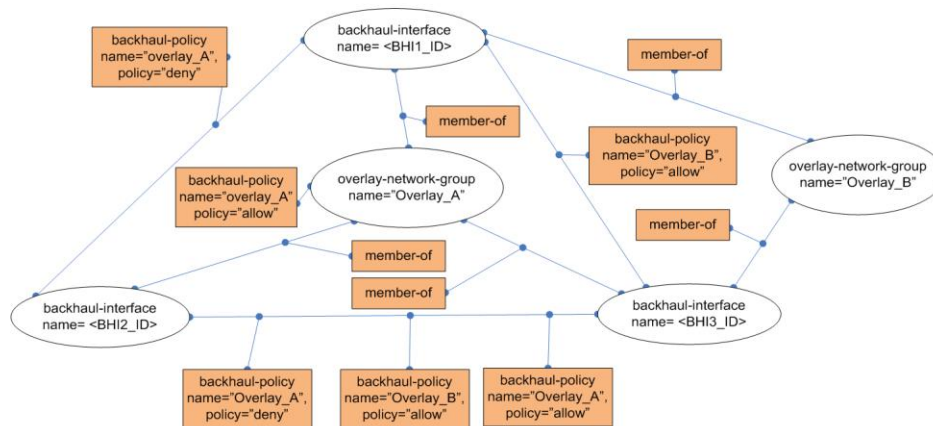
BHI Publishes to MAP:



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

ICS Metadata Examples

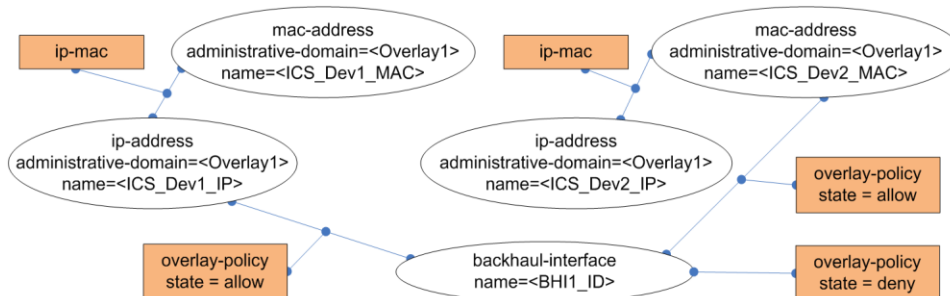
Example of an overlay network in MAP graph:



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

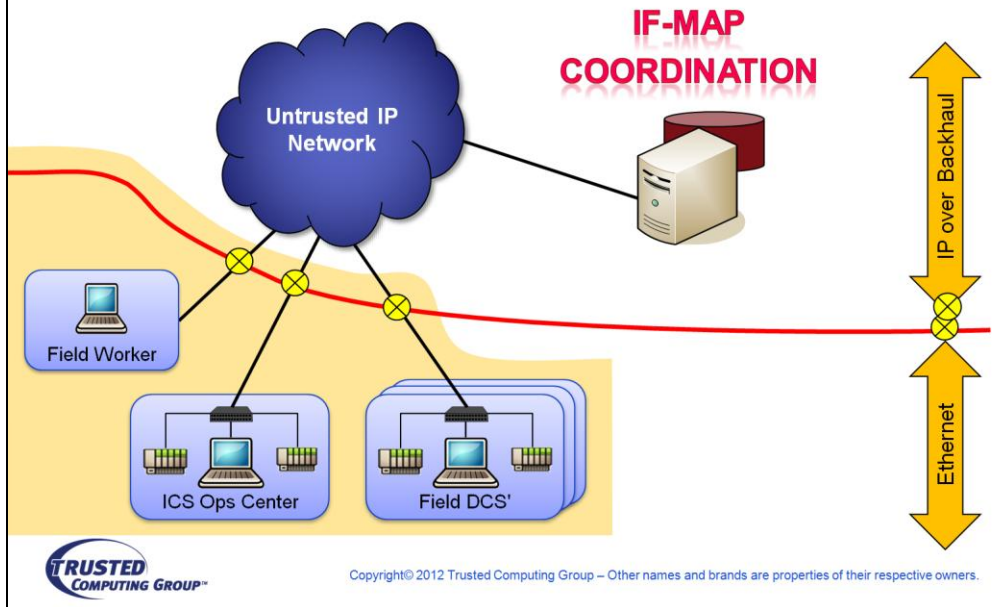
ICS Metadata Examples

Example of an overlay policy in MAP graph:



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.

Dynamic Overlay Management



Resources

- Trusted Computing Group:
 - <http://www.trustedcomputinggroup.org>
- Trusted Network Connect Working Group:
 - http://www.trustedcomputinggroup.org/developers/trusted_network_connect/
- IF-MAP Metadata for ICS Security:
 - <http://bit.ly/R7OYUj> (spec) | <http://bit.ly/Tr5OvU> (FAQ)
http://www.trustedcomputinggroup.org/resources/tnc_ifmap_metadata_for_ics_security
http://www.trustedcomputinggroup.org/resources/tnc_ifmap_metadata_for_ics_security_10_faqs

- Spec Editors:

Steven C. Venema

Steven.C.Venema@Boeing.com

Lisa Lorenzin

llorenzin@juniper.net



Copyright© 2012 Trusted Computing Group – Other names and brands are properties of their respective owners.