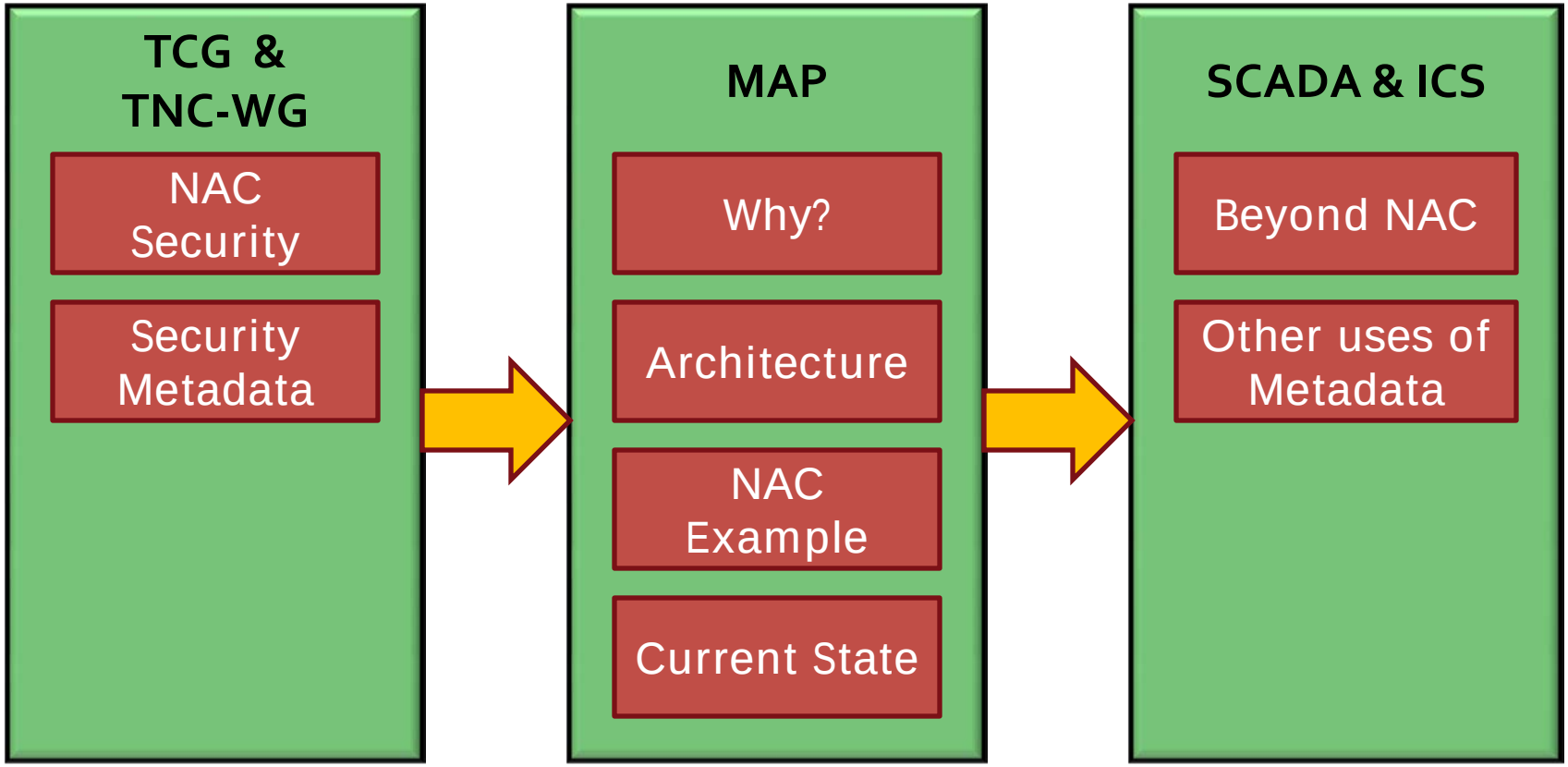
Metadata Access Point (IF- MAP)

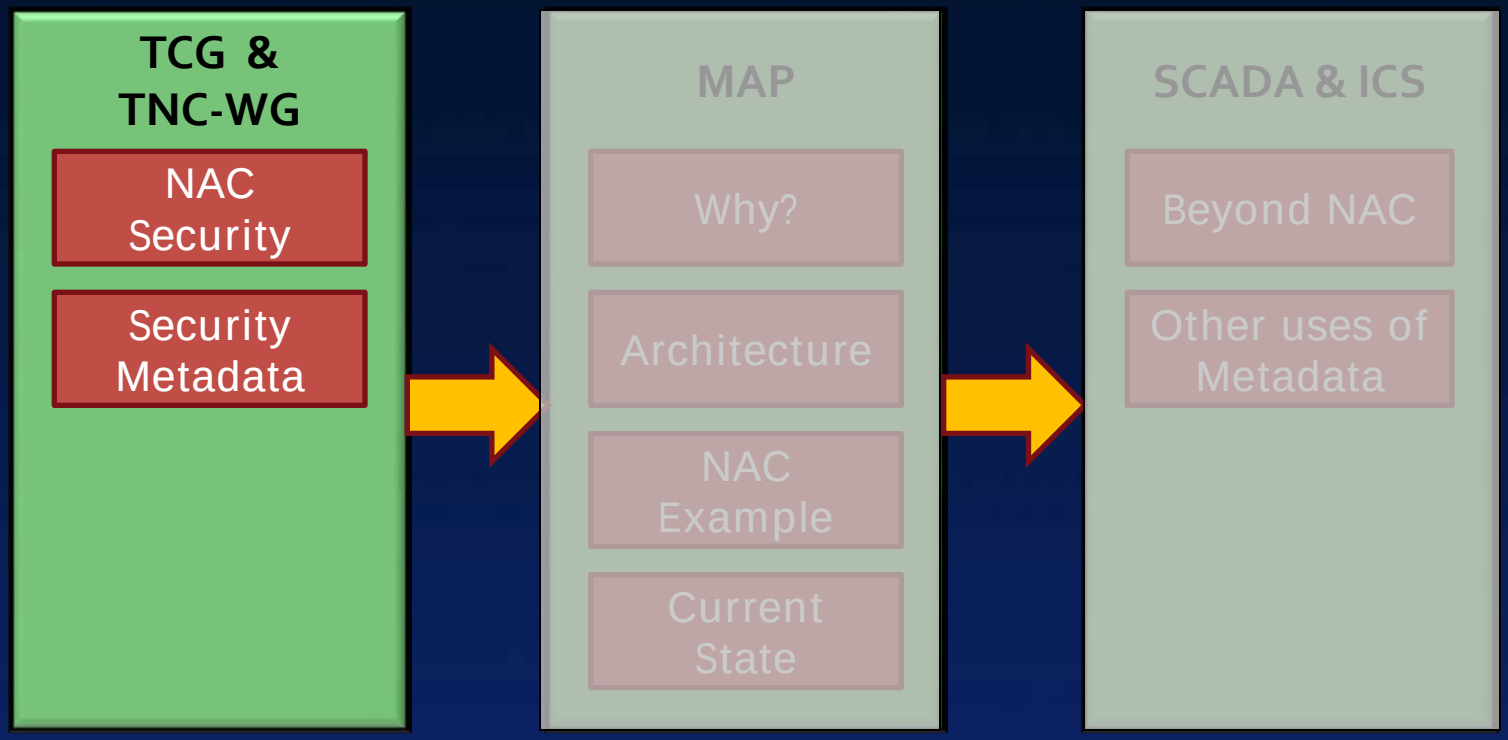
New Standards Protecting Old Technology

Eric Byres
Scott Howard
Oct 2010

Agenda



Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.



Section 1

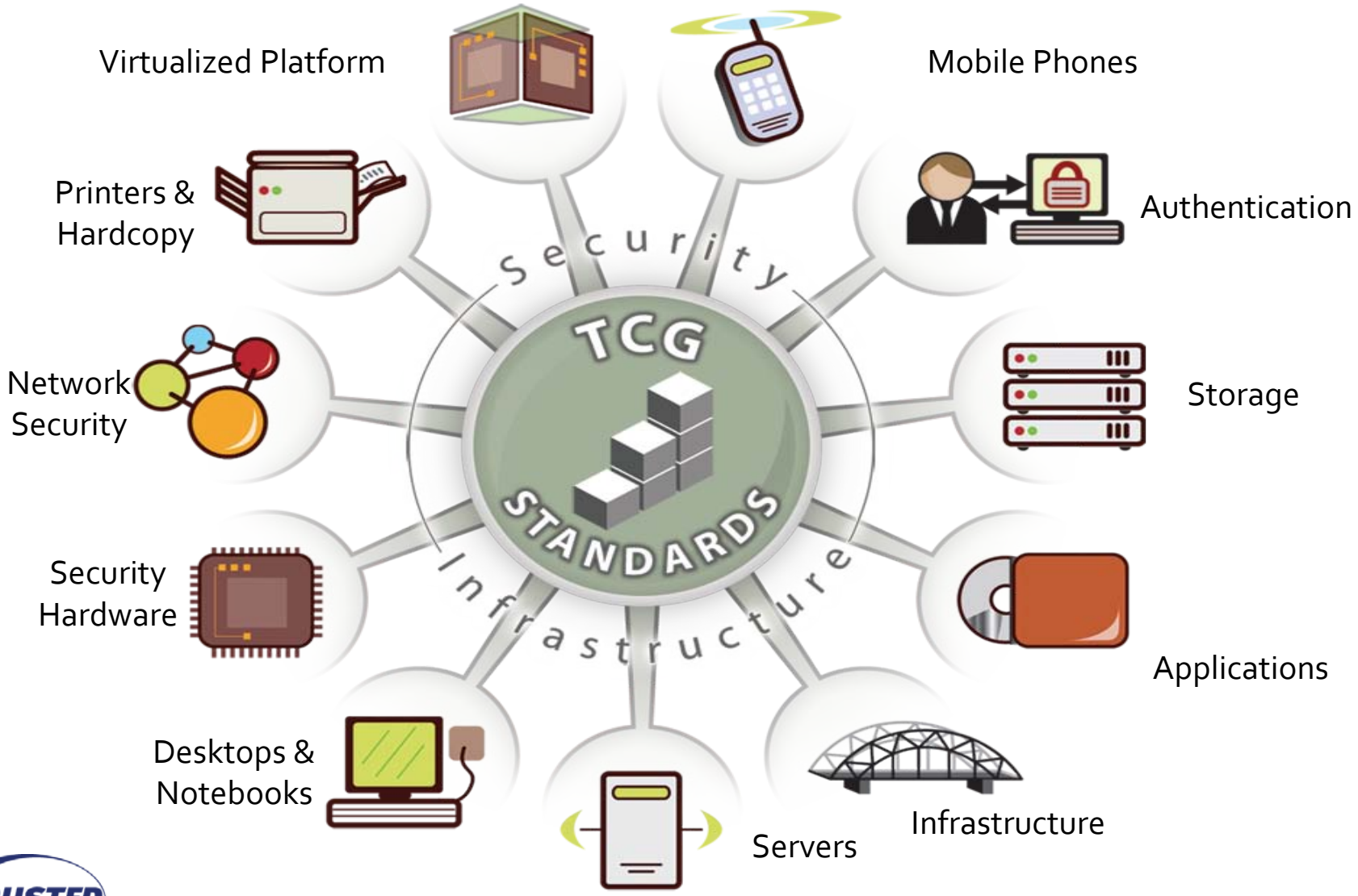
TCG and TNC Working Group

Trusted Computing Group

- 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© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

TCG Activities



Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Trusted Network Connect (TNC)

- Open Architecture for Network Access Control (NAC)
  - Completely vendor-neutral
  - Strong security through trusted computing
- Open Standards for NAC
  - Full set of specifications available to all
  - Products shipping for more than four years

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Why NAC Matters for ICS & SCADA

Controllers and Control Protocols have very weak authentication/authorization

- "If you can Ping it, you can own it"
- Need to be sure exactly what is on the control network
- Need to be sure they are behaving well (Infected with Stuxnet anyone?)
- How do we do that with existing technology?

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Example NAC Policy

To Access the Control Network…

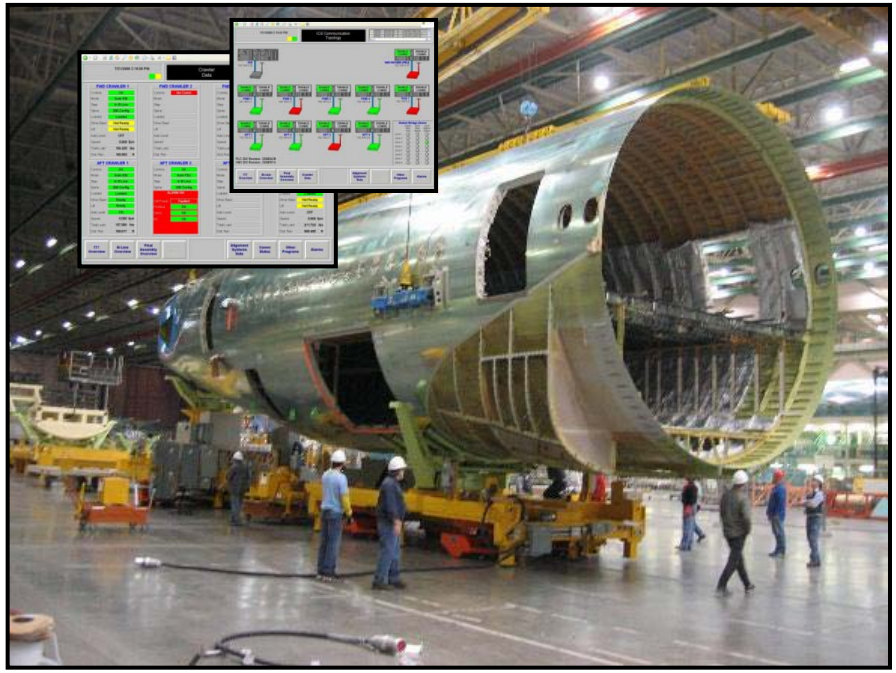
- User Must Be Authenticated and Authorized
  - With Identity Management System and AAA services
- Endpoint Must Be Healthy
  - Anti-Virus software running and properly configured
  - Recent scan shows no malware
  - Personal Firewall running and properly configured
  - Patches up-to-date
- Behavior Must Be Acceptable
  - No port scanning, sending illegal traffic, etc.

TRUSTED COMPUTING GROUP™

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

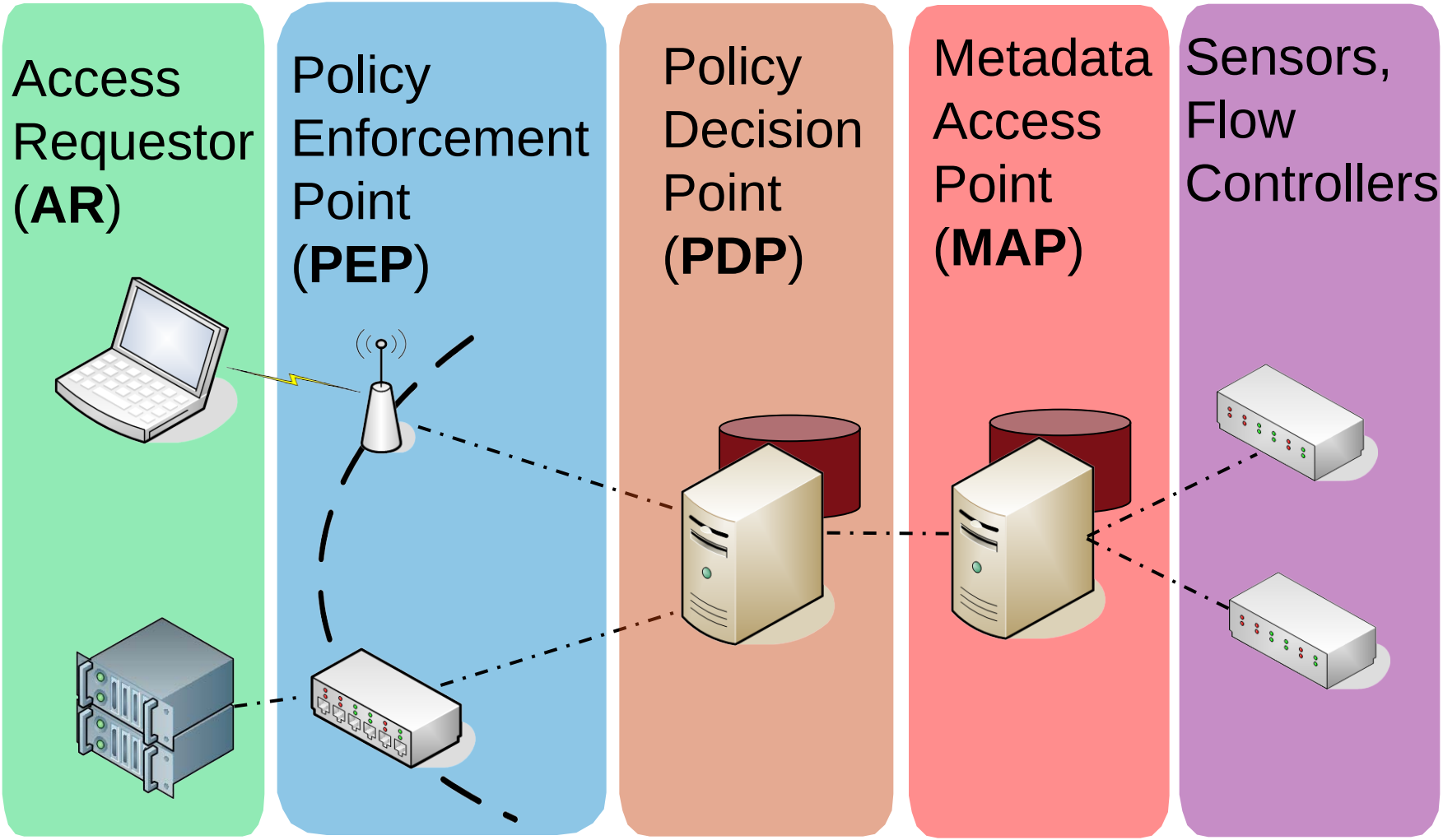
Real Life Example

- Crawlers are mobile manufacturing platforms full of PLCs and HMIs
- As they move they have different roles and access rights
- Relevant data includes:
  - Auth Tokens/Certs
  - Crawler position
  - Activities
  - Network conditions



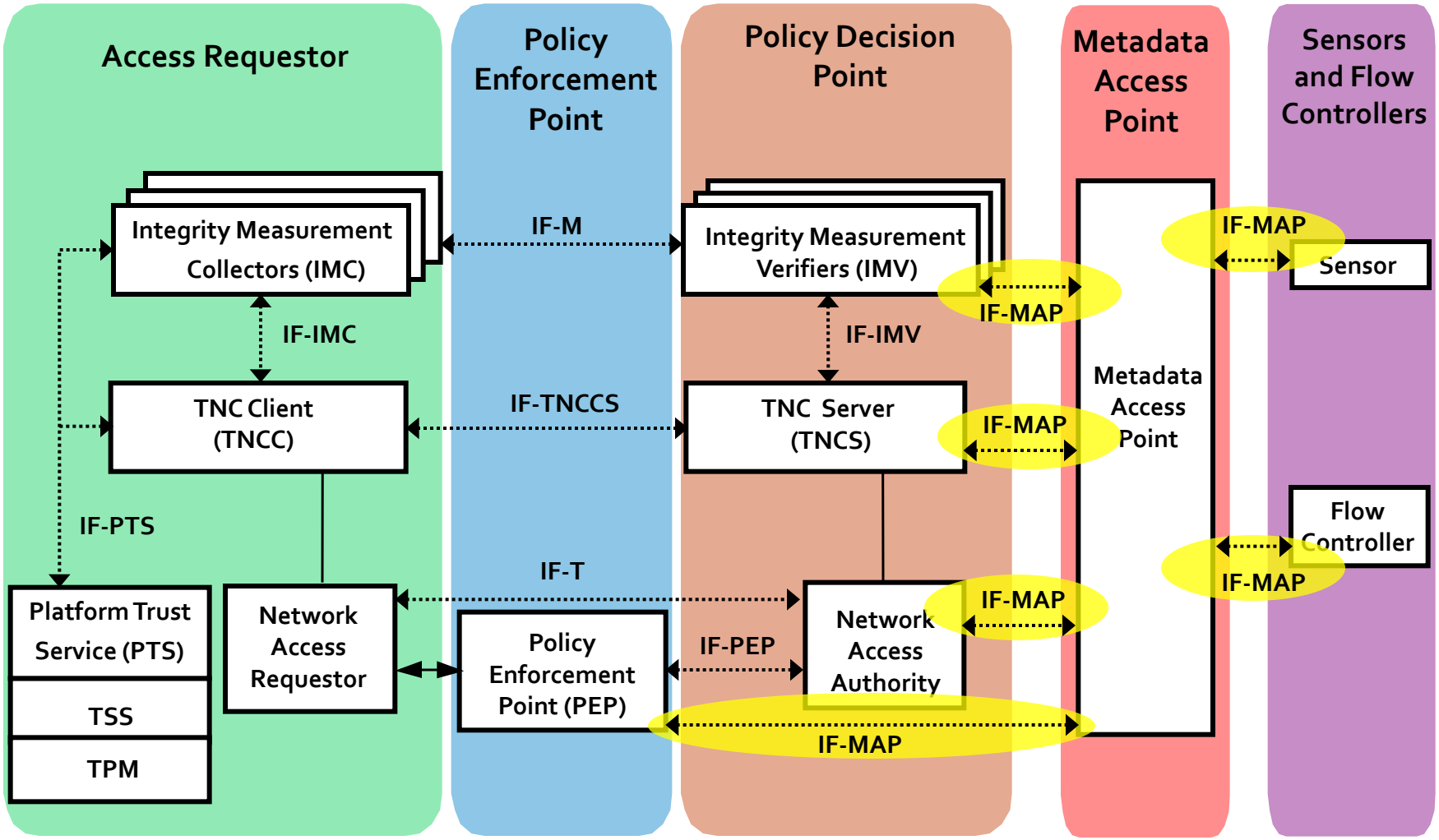
Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

TNC Architecture

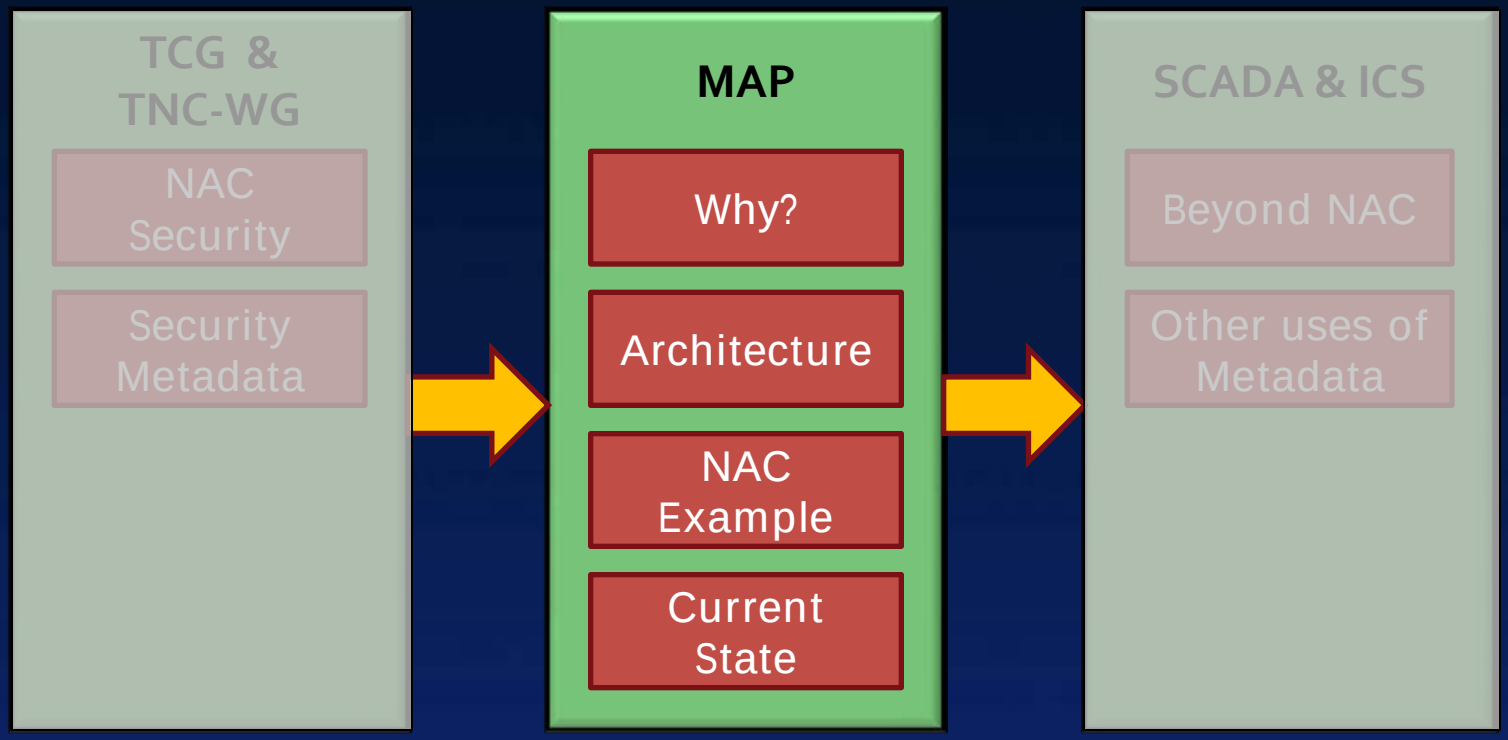


Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

TNC Architecture



Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.



Section 2

Metadata Access Points (MAP)

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 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© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Coordination Challenge

- Security infrastructure is complex, heterogenous, and usually distributed
- 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© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

MAP: Metadata Access Point

- Why create a new protocol instead of using existing capabilities?
  - E.g., relational databases or directories?

- The answer lies in the 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© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

MAP: Metadata Access Point

- MAP is specifically designed to fit the security coordination use case
  - Optimized for loosely structured metadata
  - Publish/Subscribe capability for asynchronous searches
  - Highly scalable architecture
- Based on the assumption that **you will never find <u>the</u> data relation schema to satisfy all needs**
  - Need to move forward in spite of a lack of full relation specifications

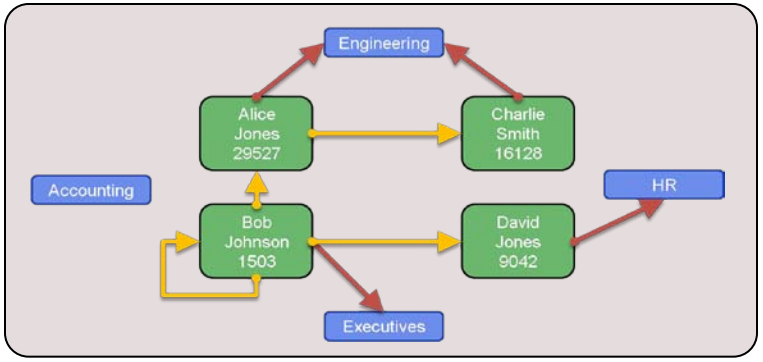
Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

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© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

More Wrong Ways

- SNMP
- Syslog
- LDAP
- Telnet
- SSH

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

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
- Metadata in particular is designed to be extensible

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

The 3 IF- MAP Access Operations

Publish:

Tell others that…<metadata…>

- Clients store metadata into MAP for others to see
  - Example: Authentication server publishes when a user logs in (or out)

Search:

Tell me now if…*match*(metadata pattern)

- Clients re rticular identifier and linked identifiers
  - Example: An application can request the current physical location of the user or device

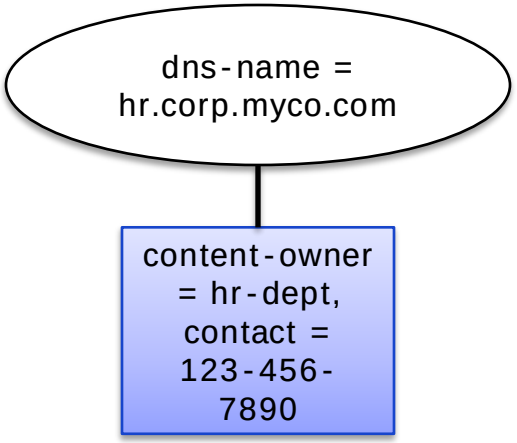
Subscribe:

Tell me when…*match*(metadata pattern)

- Clients request asynchronous results for searches that match when others publish new metadata
  - Example: Tell me when any user's status goes from "employee" to "terminated"

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Remote Access Use Scenario



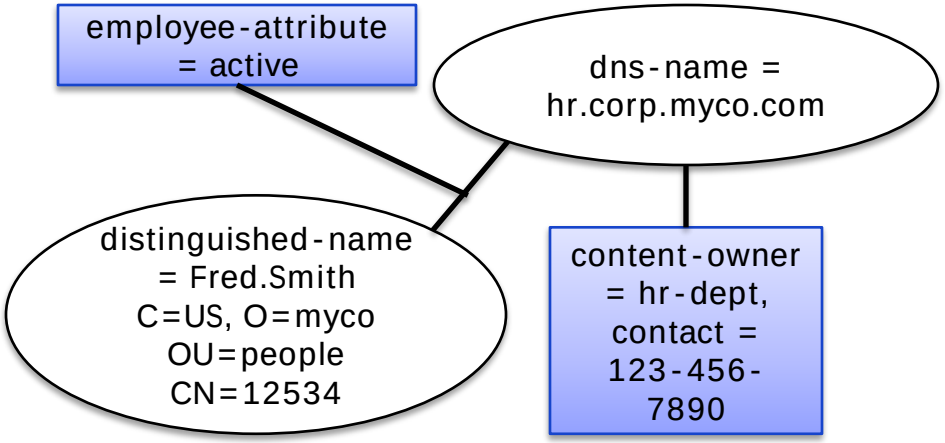
1. Initial setup:
   a) HR publishes its metadata to MAP. This will the one side of the links it will later create for each employee.
   b) Servers each subscribe to a pattern that will match newly added employees

VPN Server

identifier = “dns-name[name=hr.corp.myco.com]”
match-links = “employee-attribute[name=“active]
max-depth = “1” result-filter = “distinguished-name”

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Remote Access Use Scenario



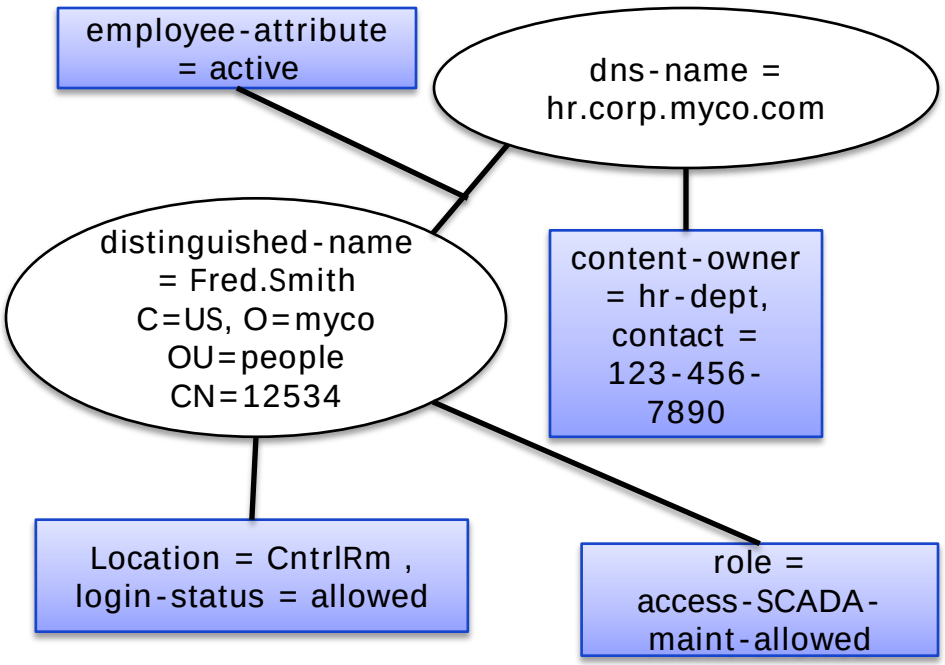
2. New Employee:
   a) HR publishes an *"employee-attribute=active"* metadata link between itself and new employee's identifier
   b) VPN Server gets notification of new employee due to its subscription
   c) VPN Server creates a new user account

VPNServer

identifier = "dns-name[name=hr.corp.myco.com]"
match-links = "employee-attribute[name="active]
max-depth = "1" result-filter = "distinguished-name"

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Remote Access Use Scenario



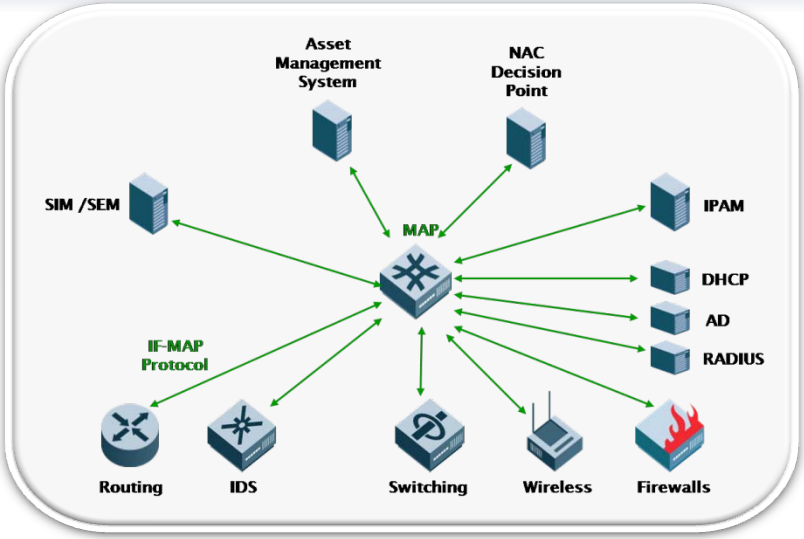
3. Other Data:
   a) Related identifier and link metadata published by others.
   b) VPN Server gets role of employee from ICS system published metadata
   c) VPN Server gets location of employee from GPS sensor published metadata

ServerVPN

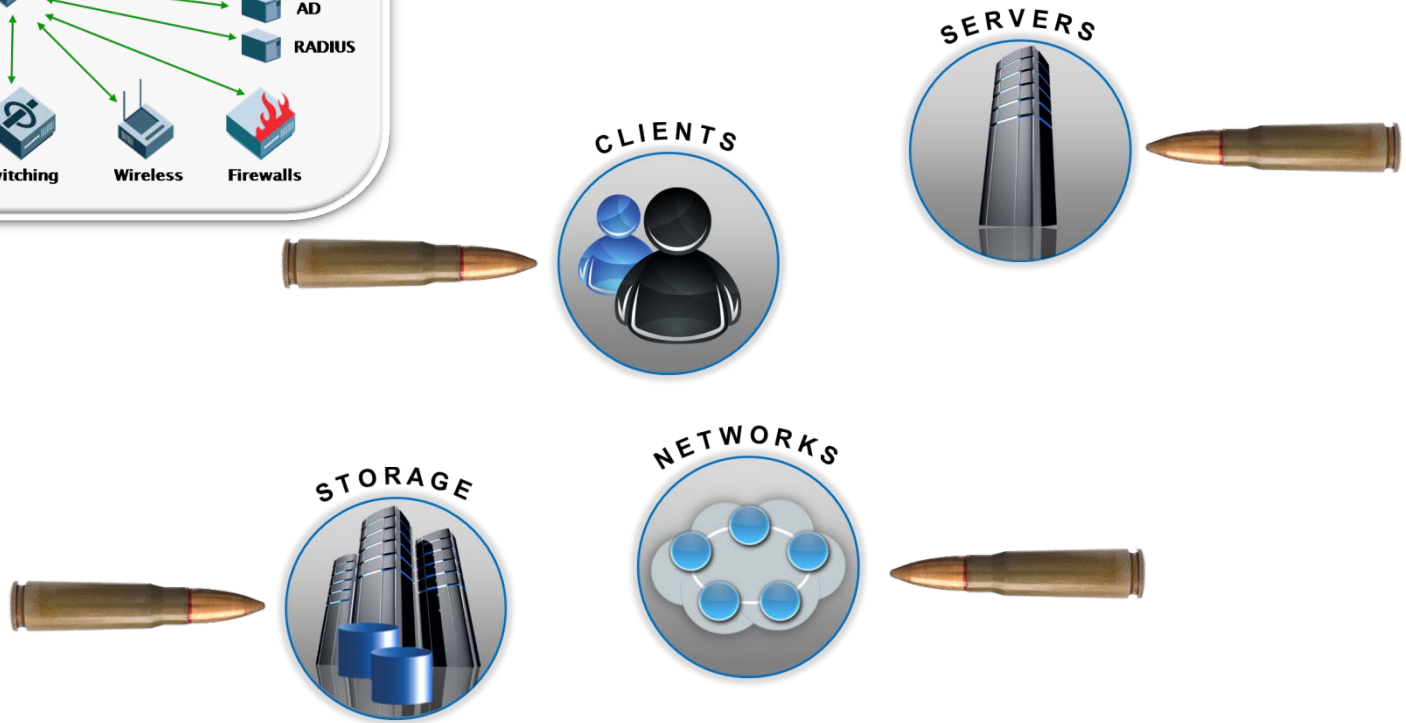
identifier = “dns-name[name=hr.corp.myco.com]”
match-links = “employee-attribute[name=“active”]
match-links = “employee-location[name=”CntrlRm”]

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Benefits

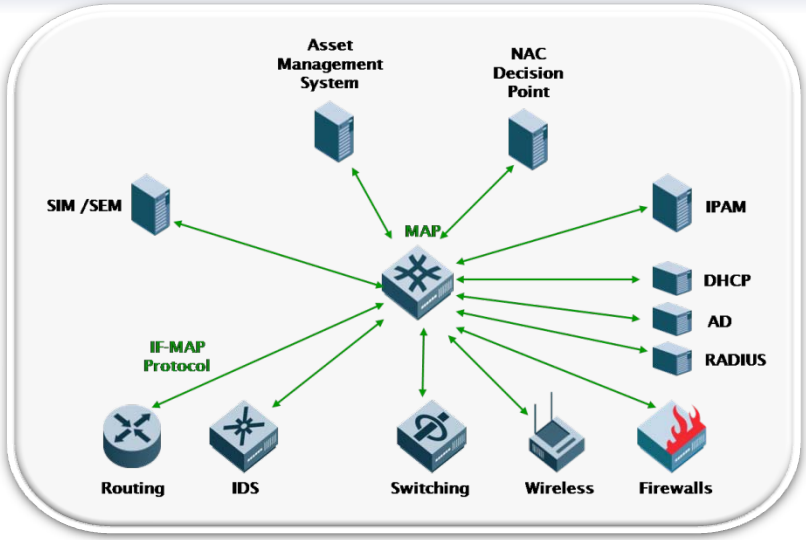


Stronger security



Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

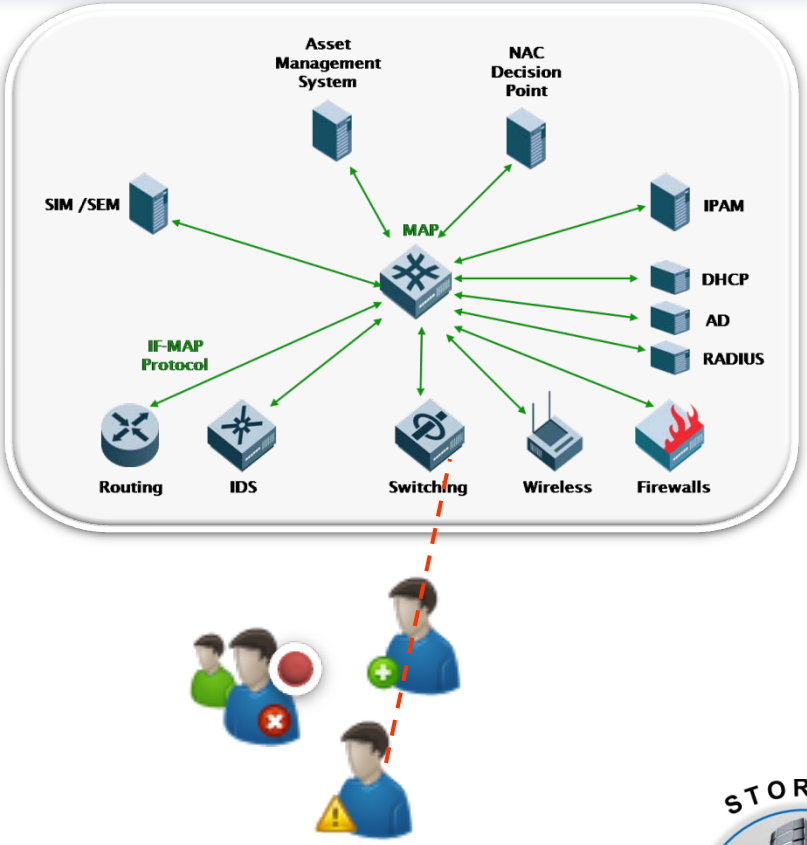
Benefits



Faster Response

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

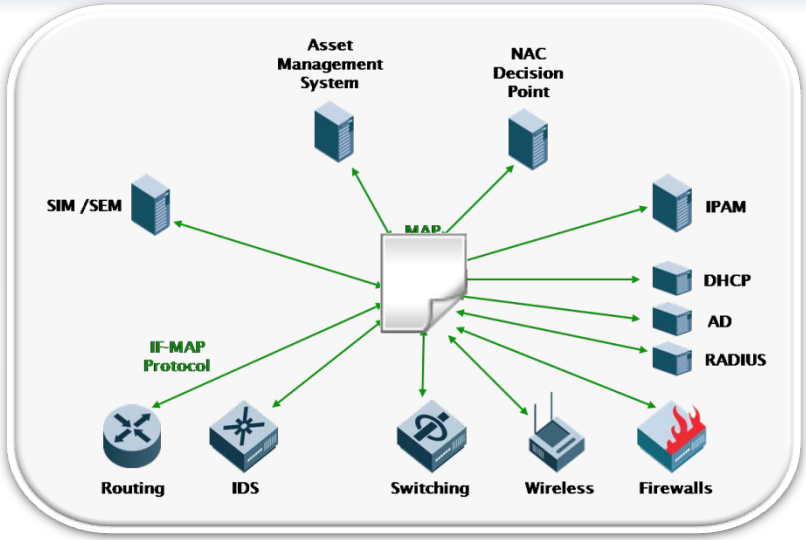
Benefits



More flexibility

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

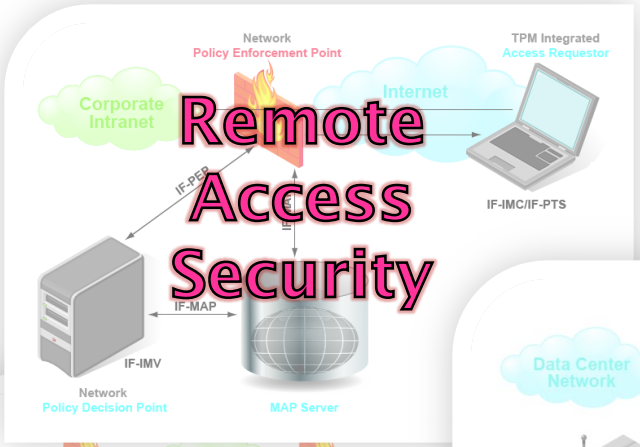
Benefits

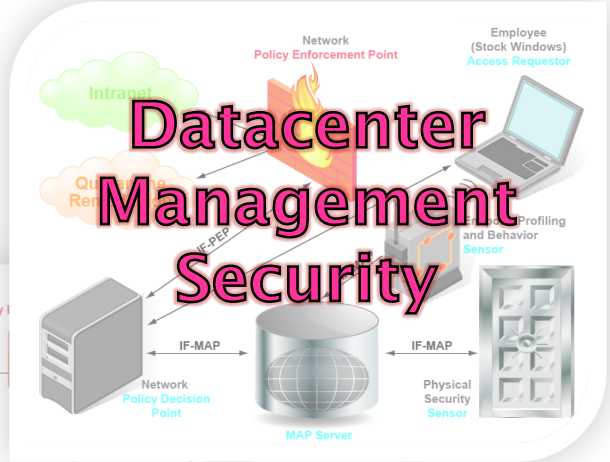


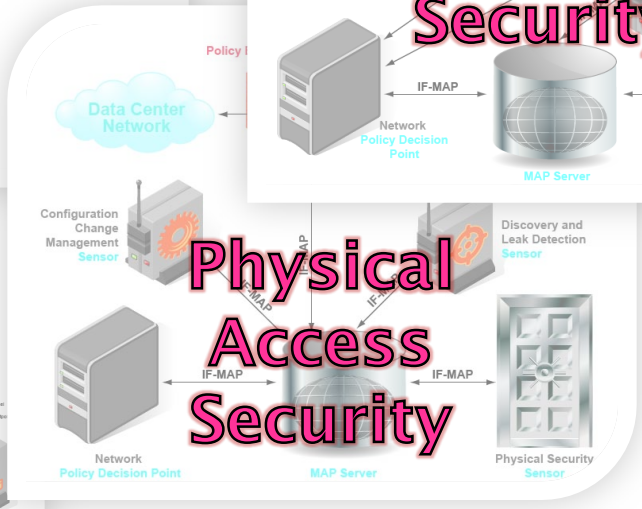
Single security policy

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Current Participants







enterasys Secure Networks

Juniper Networks

Infoblox

LUMETA

Microsoft

nSolutions Effortless Infrastructure

BOEING

TOFINO

Great Bay Software Inc.

TRAPEZE NETWORKS

HIRSCH ELECTRONICS

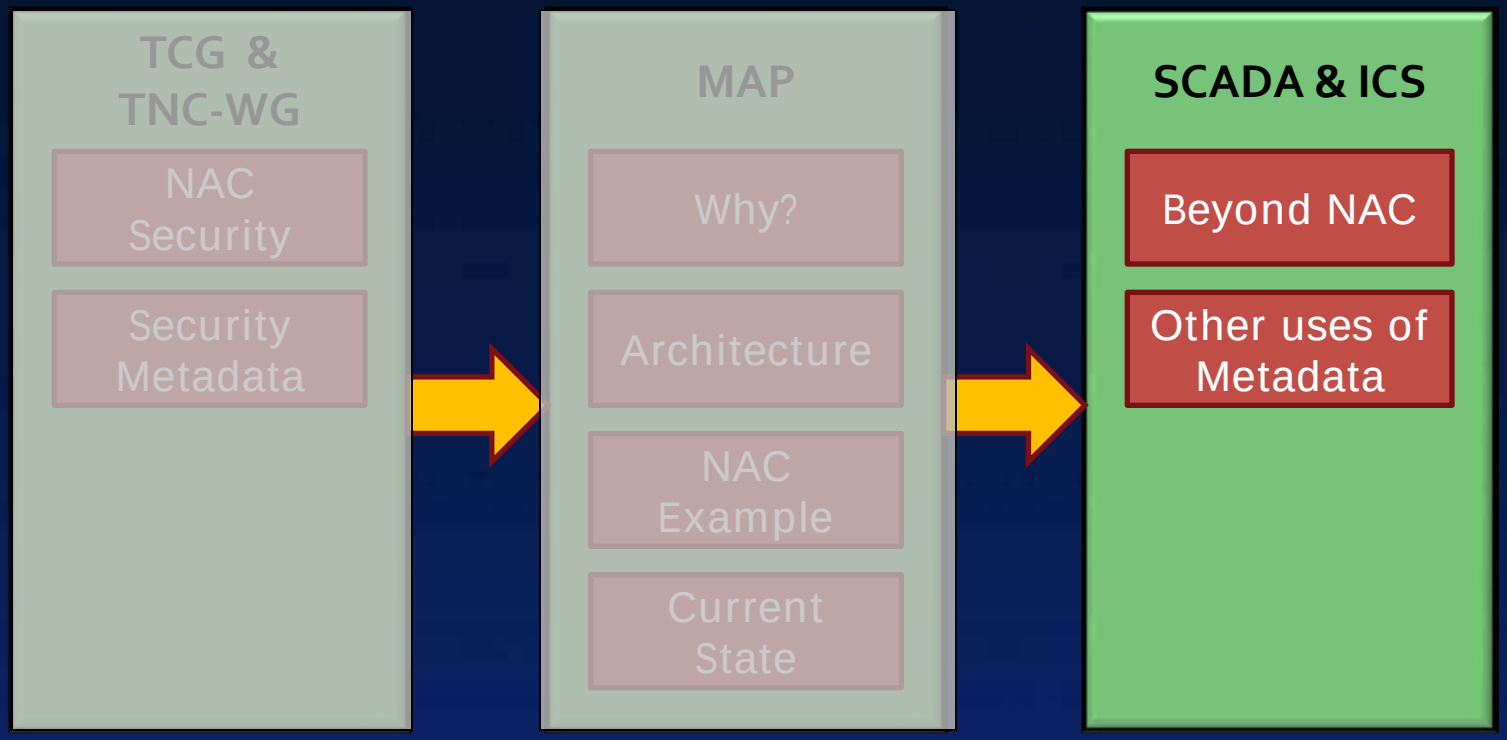
ProCurve Networking by HP

McAfee

wave

TRUSTED COMPUTING GROUP

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

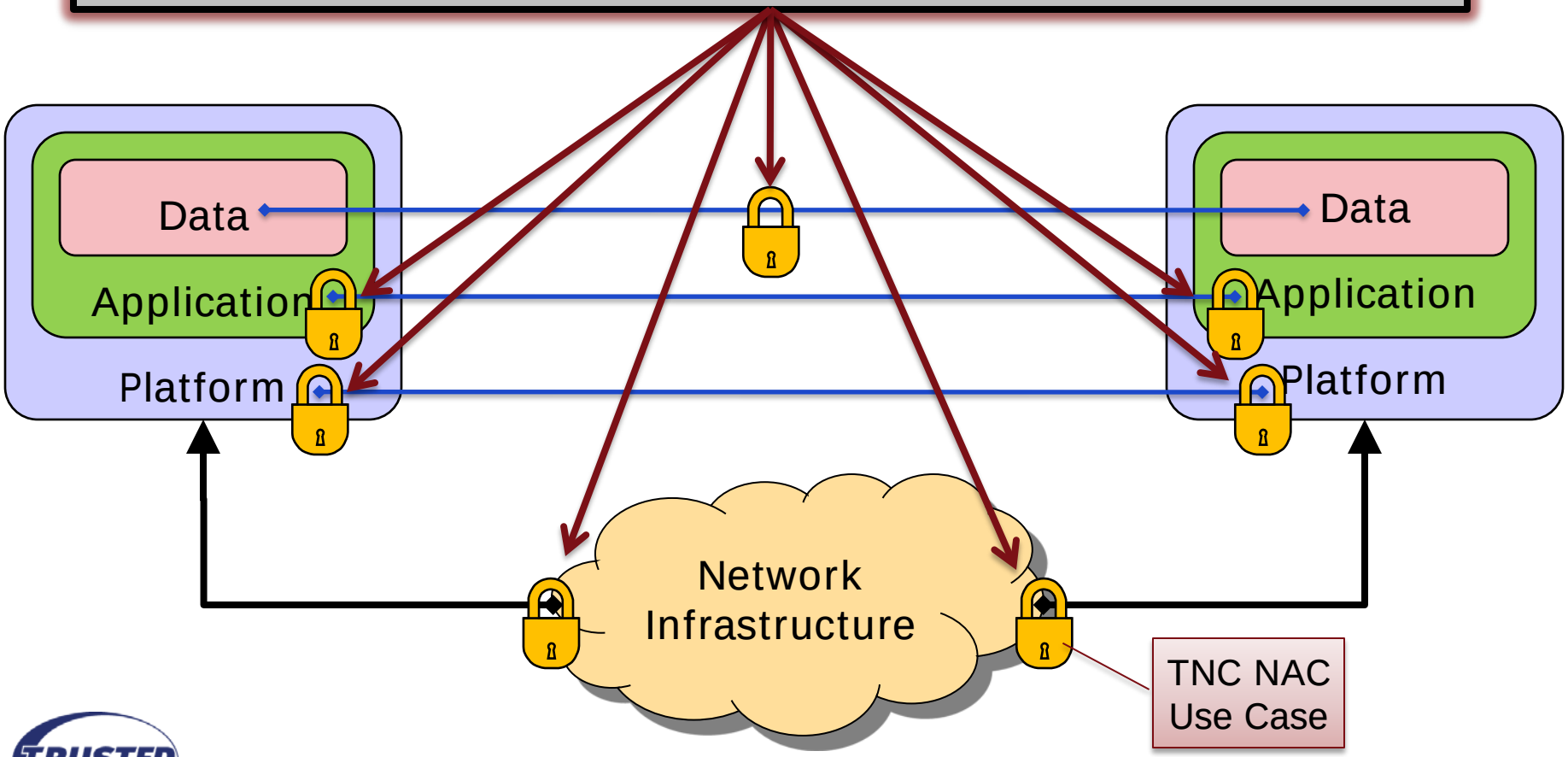


Section 3

SCADA & ICS Uses

Beyond NAC: The Larger Security Picture

MAP was designed for the TNC NAC use case…
but other use cases have much of the same coordination needs.



Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Other Uses of Metadata & MAP

Extensions of the Security Use case:

- Combined physical security and SCADA cyber security
- Convergence of IT networks/security and industrial controls security

Location Services:

- Coordination of supply chains and process flow across one or more Enterprises

Process/Event coordination:

- Too many business process today are coordinated synchronously or (worse yet) open loop
- The asynchronous Pub/Sub notification capability built into the MAP database can give us a new coordination pattern for many business processes

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Event Coordination Example

- Scenario:
  - Employee leaves company, recorded as change in status in HR database from *active* to *inactive*
- Question:
  - How are perimeter security services notified?
  - How are all the various SCADA/ICS applications and servers notified?
  - How are suppliers and partners notified?
- Big coordination problem…

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Event Coordination Example

- The “old” way:
  - All need-to-know servers and applications poll the HR database periodically (daily?) and carefully look for changes
    - Raises issues related to access control, PII, timeliness, and performance
    - Requires careful engineering of all interconnected systems. Changes in HR system ripple out to all others!
    - What does this imply for future reliability and scalability? What about acquisition and divestitures?

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Event Coordination Example

- The “new” way:
  - HR publishes employee identifiers and status metadata to MAP
  - All “interested” applications subscribe to metadata updates that result in “status” changing to “in

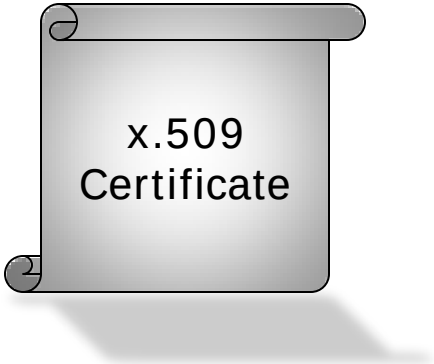
    Many systems can coordinate through MAP with no knowledge of each other’s API’s

    rs
    - HR need not publish other, more sensitive information (PII, etc.)
    - Scales well in the face of many applications

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Public Key Infrastructure for SCADA

- Full lifecycle management for cryptographic identities must be
  - Secure
  - Scalable
  - Robust



- Embedded systems are particularly sensitive to this issue (E.g., certificate expiry or revocation)
- Working on automating much of the identity lifecycle management using coordination through IF-MAP

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Example #2: ISA100.15 Back Haul

Goal: Secure ICS comms over untrusted links

- Specifically includes multiple wireless technologies
- WG Title: “Wireless Backhaul”

Use cases drawn from users in Oil/Gas, Energy, and Manufacturing

- Satisfy both distributed SCADA and SCADA over in-plant network services

Participants:

- ExxonMobile, Shell, GE, Boeing, etc.
- Honeywell, Siemens, Yokogawa, Cisco, etc.
- Cooperation activity with Fieldbus Foundation
- Collaboration with Security & Embedded Systems Forums at The Open Group

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

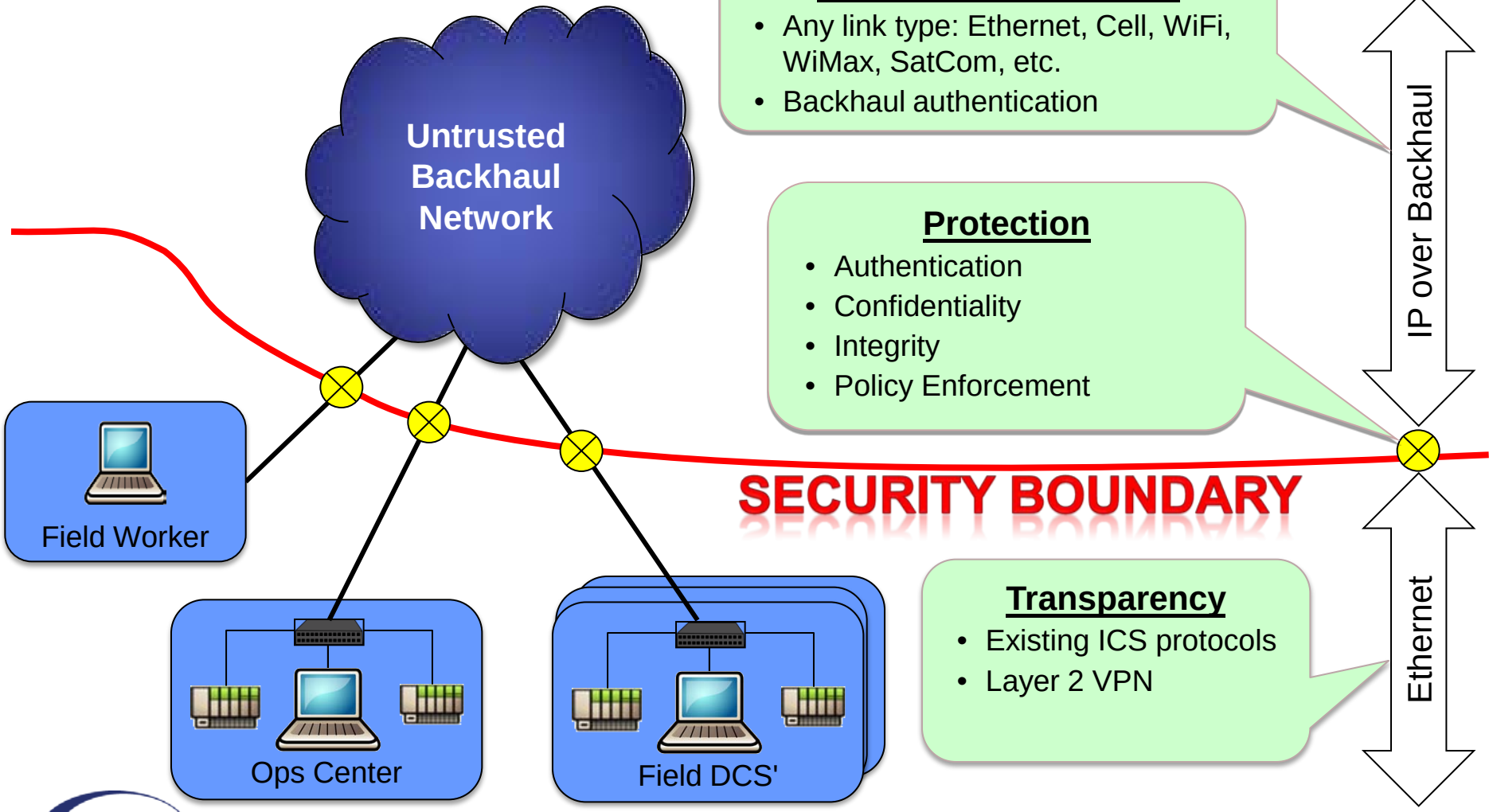
ISA100.15 Requirements

Documented Requirements include:

- A/I/C assurance
- Certificate-based authentication
- Dynamic policy tied to certificate identities
- Scalable, Manageable, Interoperable
- Compatible with standard link technologies
  - WiFi, WiMAX, Cellular, SatComm, microwave, etc.

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

ISA100.15 Functional Goals



Backhaul Connectivity

- Any link type: Ethernet, Cell, WiFi, WiMax, SatCom, etc.
- Backhaul authentication

Protection

- Authentication
- Confidentiality
- Integrity
- Policy Enforcement

Transparency

- Existing ICS protocols
- Layer 2 VPN

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Summary

- TCG & TNC-WG

Simple connectivity is insufficient for good coordination

- MAP

A published standard for data and event coordination with many users and interoperable products

- SCADA & ICS

MAP can help in many SCADA/ICS use cases where coordination is a key requirement

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.

Contact Information

- Trusted Computing Group:
  - http://www.trustedcomputinggroup.org
- Trusted Network Connect Working Group:
  - http://www.trustedcomputinggroup.org/developers/trusted_network_connect/

Eric Byres
eric@tofinosecurity.com

Copyright© 2009 Trusted Computing Group – Other names and brands are properties of their respective owners.