Security Orchestration with IF-MAP

Gary Holland, Lumeta/IMRI

2 November 2011

Agenda

- Threat Landscape and Federal Networks
- Trusted Network Connect
- Explanation of IF-MAP
  - What is IF-MAP?
  - What problems does IF-MAP address?
  - How does IF-MAP solve those problems?
  - SCAP & TNC/IF-MAP
  - Use cases
- IF-MAP Adoption
- Summary

Cyber Threat Sources & Trends

- National Governments
- Terrorists
- Industrial Spies
- Organized Crime Groups
- Hacktivists
- Hackers
- Malware
- Botnets
- Cyber warfare
- Threats to VoIP and mobile devices
- The evolving cyber crime economy

Sources: US-CERT http://www.us-cert.gov/control_systems/csthreats.html; GTISC Emerging Cyber Threats Report for 2012 http://www.gtisc.gatech.edu/doc/emerging_cyber_threats_report2012.pdf

Trusted Network Connect & IF-MAP

Open Architecture for Network Security

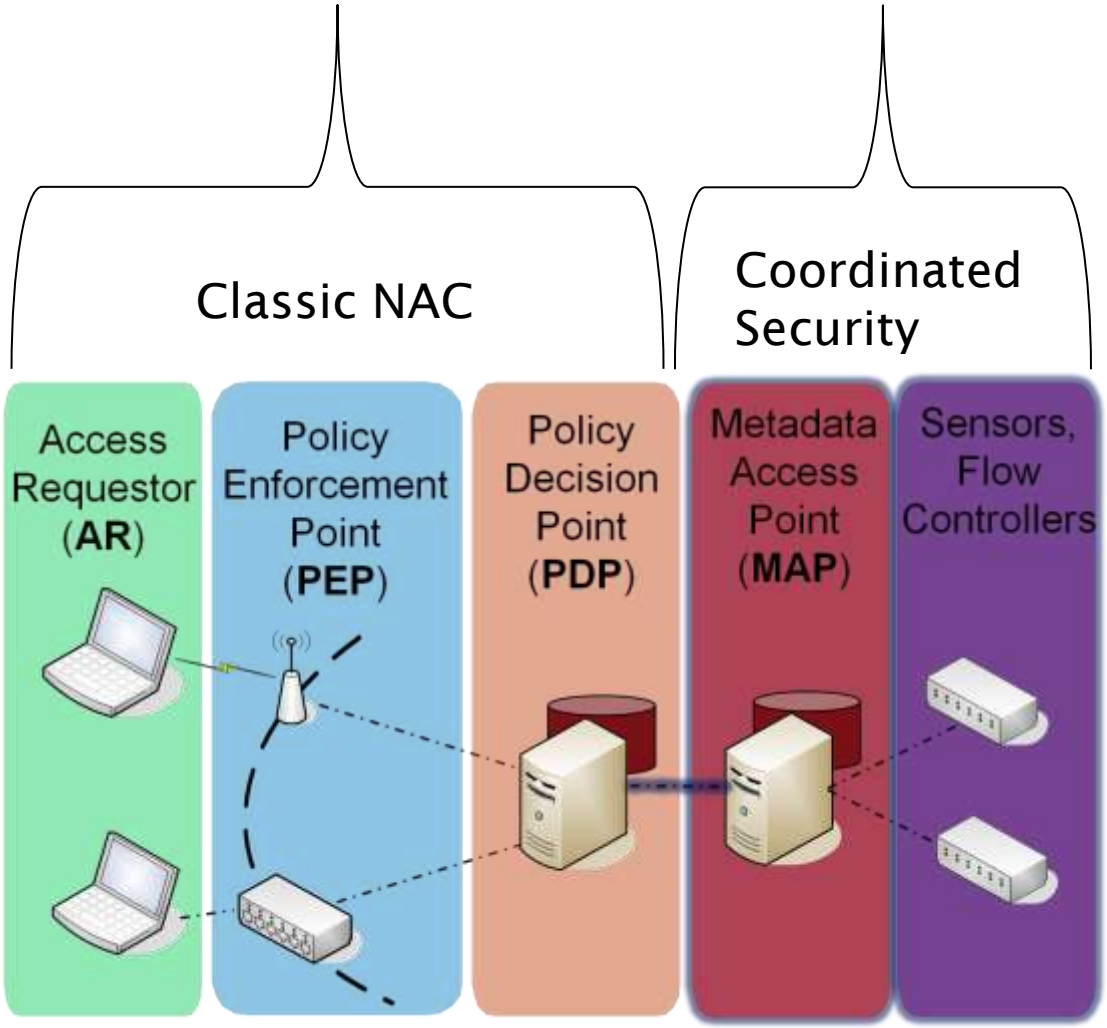
- Completely vendor-neutral
- Strong security through trusted computing

Open Standards for Network Security

- Full set of specifications available to all
- Products shipping for more than five years

Developed by Trusted Computing Group (TCG)

- Industry standards group
- More than 100 member organizations
- Includes large vendors, small vendors, customers, etc.



What is IF-MAP?

Open Standard for Security and Network Orchestration

- First published in May 2008 by the Trusted Computing Group
  - Industry consortium including most large IT vendors
- Freely available for anyone to implement
- Growing base of vendor and product support

Shared database for information on network devices, their state, and their activities

- A clearing house for information on IP devices and systems

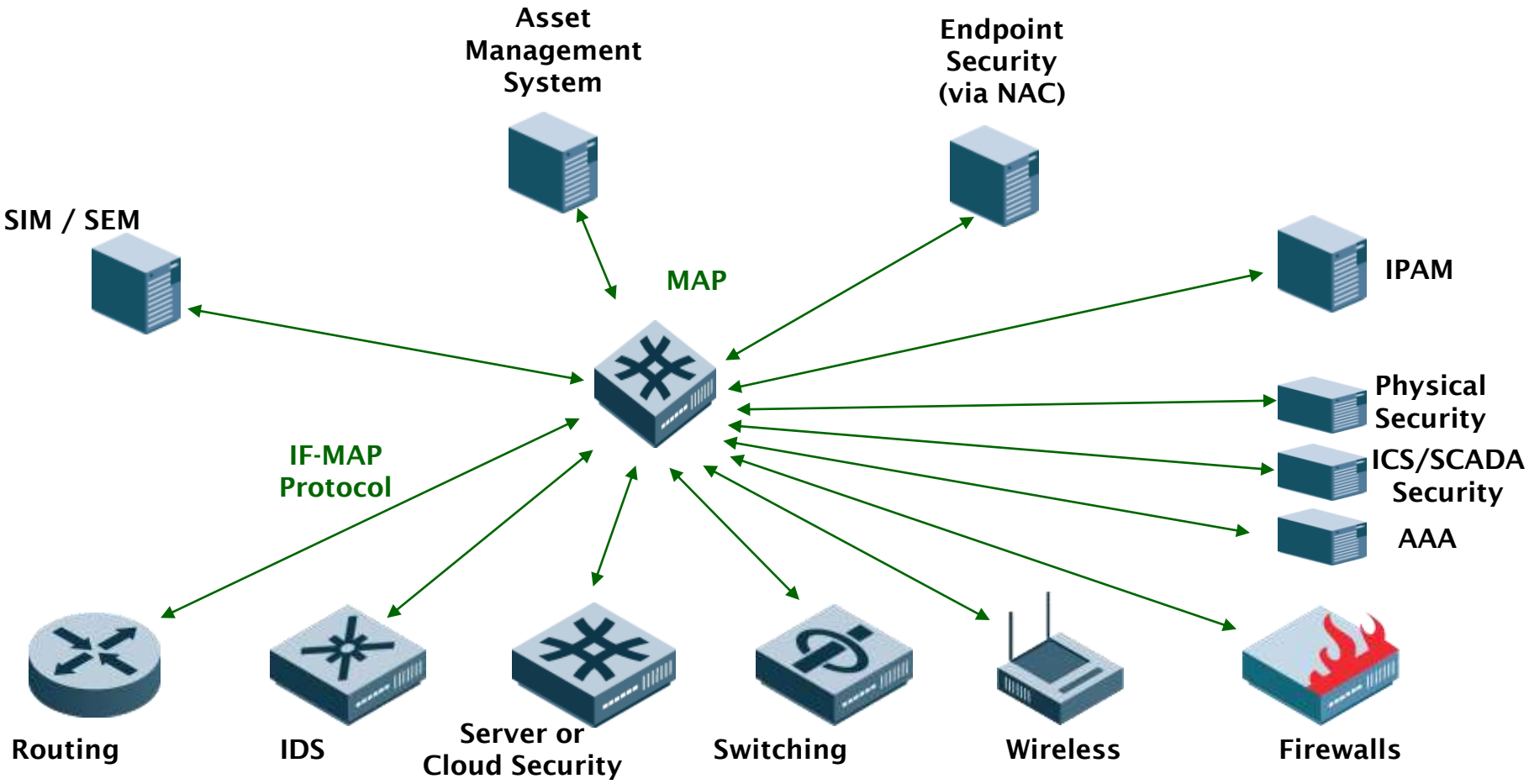
Aggregates real-time information from many different sources

- Both standard data types and vendor-specific extensions

Designed to scale for machine-to-machine coordination

Formal IF-MAP certification program will be available later this year

Coordinated Security with IF-MAP



Physical/Network Security Orchestration

Run Video

http://www.if-map.org/

IT/Business Challenges Addressed by IF-MAP

Network and Endpoint Visibility

- Situational Awareness - Who and what's on my network and what is the appropriate response to their presence?

Advanced Network Security Policy Enforcement

- Easily leverage attributes previously difficult to access to make real time access decisions
  - Location, role, device type, OS, device vulnerability status, physical security status, event logs, application information

Security Automation/Orchestration

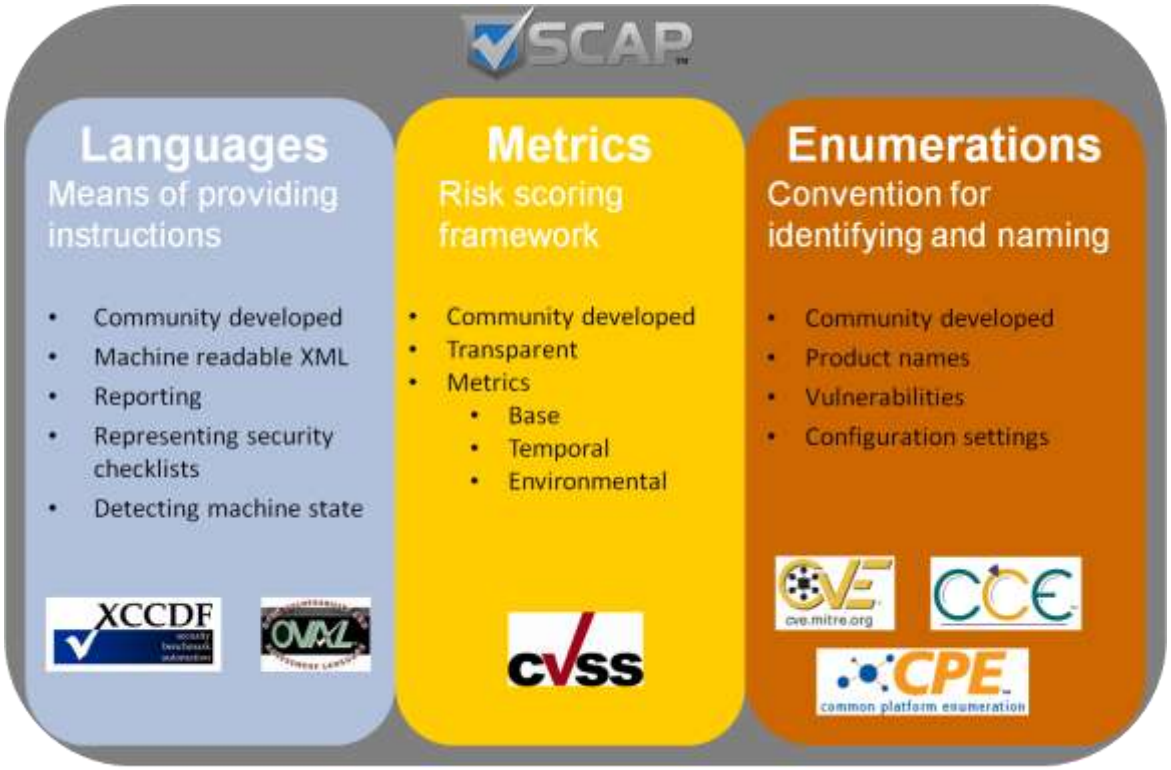
- Automate audit of security controls across a full suite of tools
- Validate remediation efforts

Systems Interoperability & Data Integration

- Accuracy of CMDB content for networked assets?
- Share real-time information about network events, users, devices, threats, etc.

Security Content Automation Protocol

SCAP combines a common set of standards that are used to enable automated identification, measurement and scoring of vulnerabilities to ultimately minimize endpoint attack surfaces…..



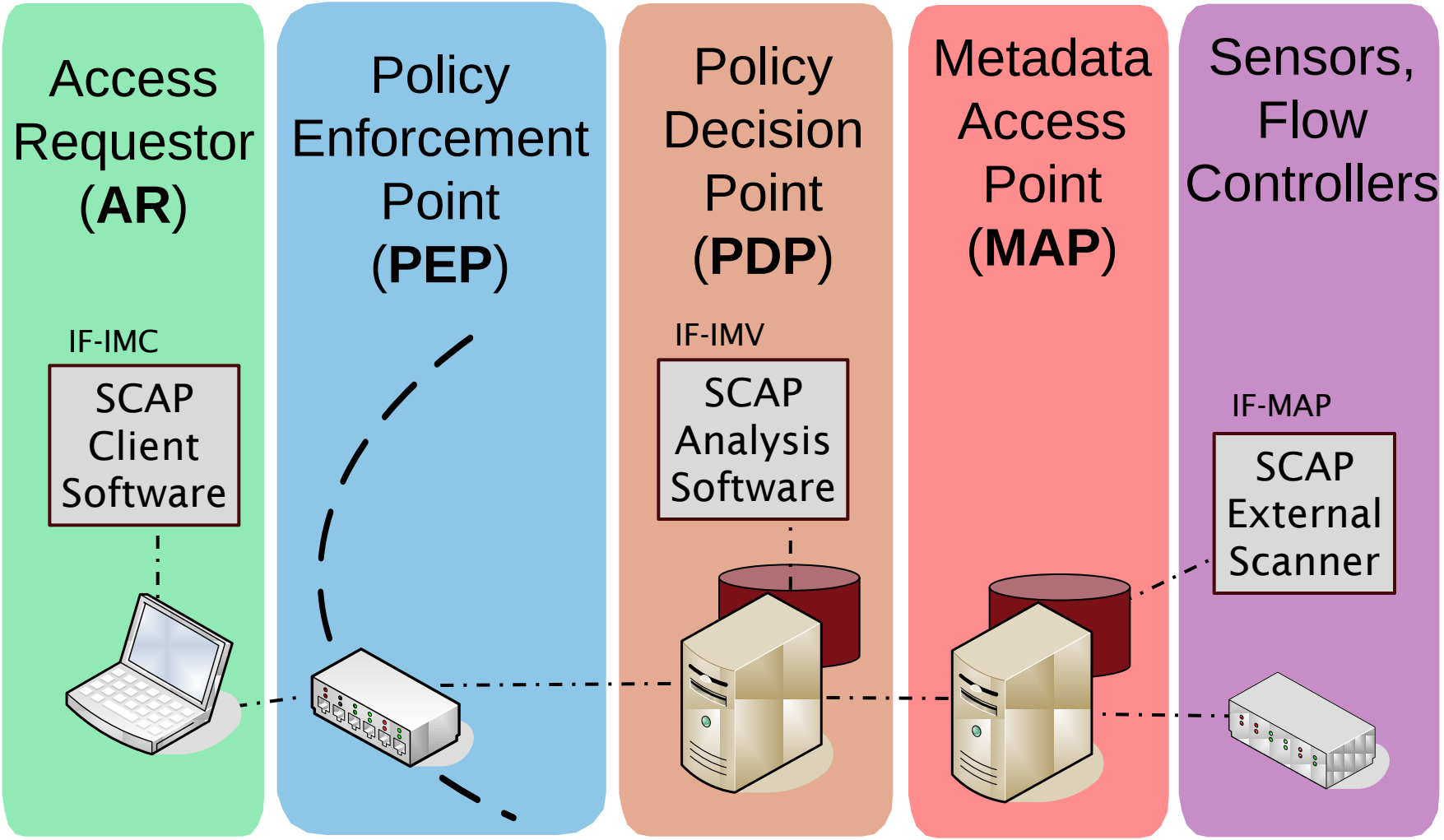
•Languages - The SCAP languages provide standard vocabularies and conventions for expressing security policy, technical check mechanisms, and assessment results.

•Enumerations- Each SCAP enumeration defines a standard nomenclature (naming format) and an official dictionary or list of items expressed using that nomenclature. For example, CVE provides a dictionary of publicly known information security vulnerabilities and exposures.

•Vulnerability measurement and scoring systems. In SCAP, this refers to evaluating specific characteristics of a vulnerability and, based on those characteristics, generating a score that reflects the vulnerability's severity.

*http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf

TNC/IF-MAP and SCAP Together

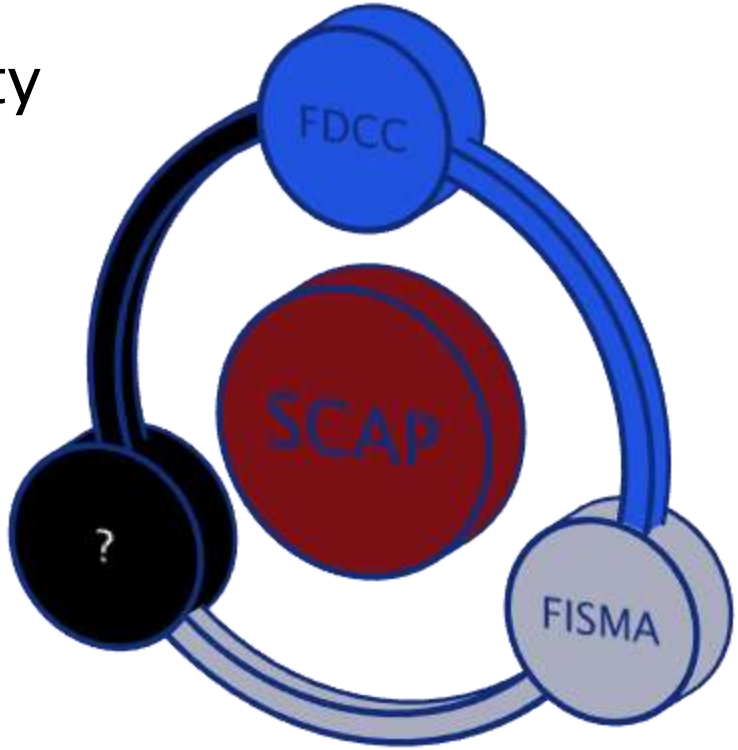


TNC handles the networking and network integration and SCAP handles compliance

---IF-IMC & IF-IMV designed for adding new device checks into TNC…

SCAP Implementations

- Federal Desktop Core Configuration
- Federal Information Security Management Act
- ?



Why Consider IF-MAP Standardization & Adoption?

Agencies & Vendors benefit from Security Automation in multi-vendor environments

- Agencies leverage existing IT investments with interoperability; improve information sharing with standardized data
- Procurement & Gov't IT Leadership drive standards adoption among vendors
- Product integration costs & time greatly reduces through standards-based interoperability

Many New Applications are Emerging

Cyber/Physical (CyPhy) Convergence	IT Automation	Cloud Computing
•Don't allow users to connect to the network if they haven't badged into the building	•Track the location and status of all IT assets (IPs, MACs, devices, hardware, VMs, apps, users, etc.) in real time	•Federate authentication and authorization status across private & public clouds
•Don't allow a wireless device to connect if its located outside of the building	•Allocate assets on the fly, dynamically re-provision data centers	•Move computing workloads to the cloud when prices drop

Use Case – Quarantine a Leaking Device

Challenges:

- Manage network change
- Fight insider threats
- Ensure security policy compliance
- Enforce network segmentation

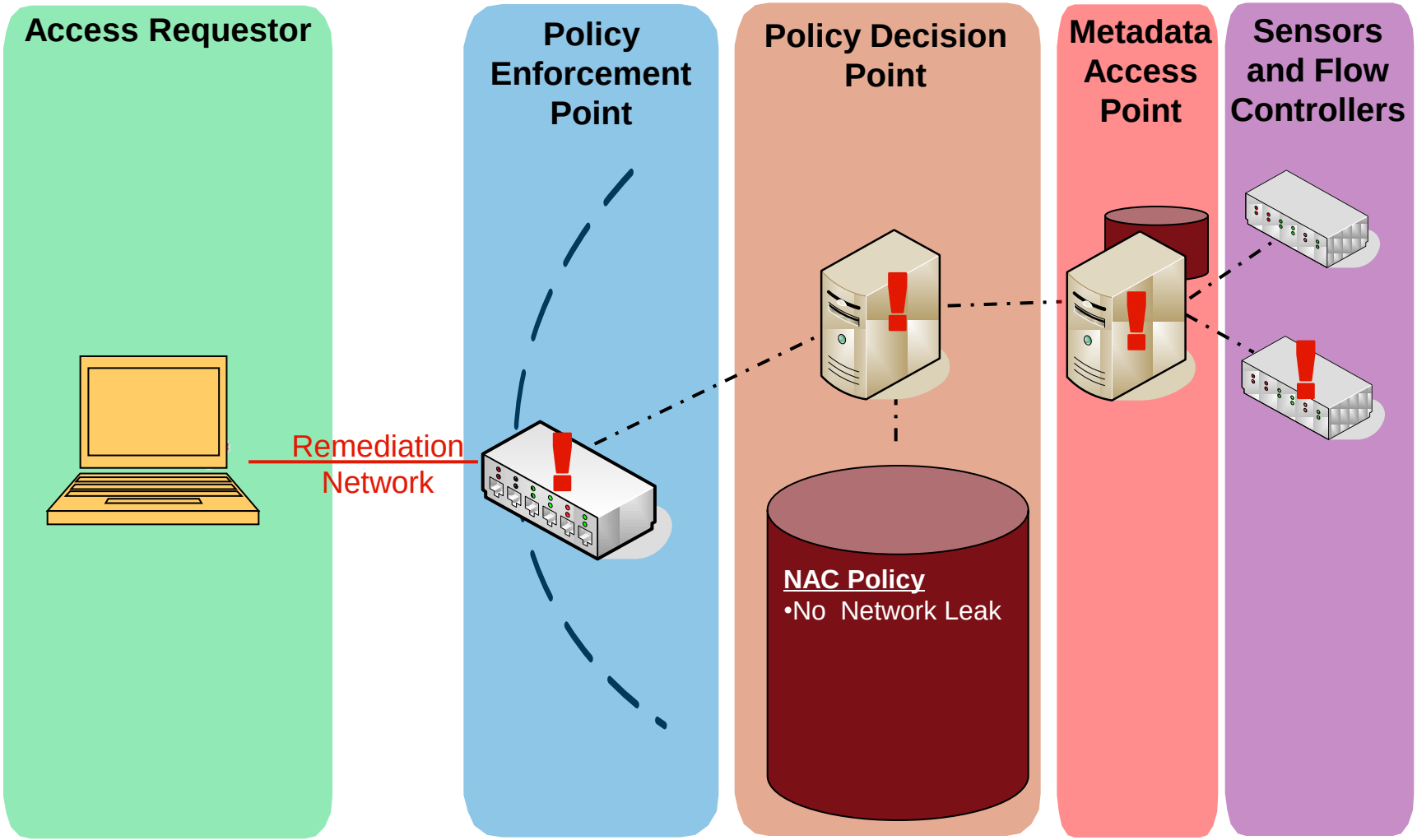
Consequences:

- Policy violations
- Unauthorized, unsecure network connections
- Worms, viruses, hackers, insider threat
- Inhibited situational awareness

Solution:

- Lumeta IPsonar's Network Leak Discovery
  - Enable organizations to detect unknown, unauthorized and unsecure network connections
- Juniper Networks Unified Access Control
  - Automatically and securely remediate the situation
- Integrated network defense via TNC

Policy Violation – Leaking Device



Lumeta's IF-MAP Client

Lumeta is currently a contributing member of TNC

- Participate in TNC and IF-MAP specification development
- Co-chair TNC adoption sub-group

Beta IF-MAP client fall 2008

- No significant development time or costs

IPsonar versions 4.5 and on contain IF-MAP client

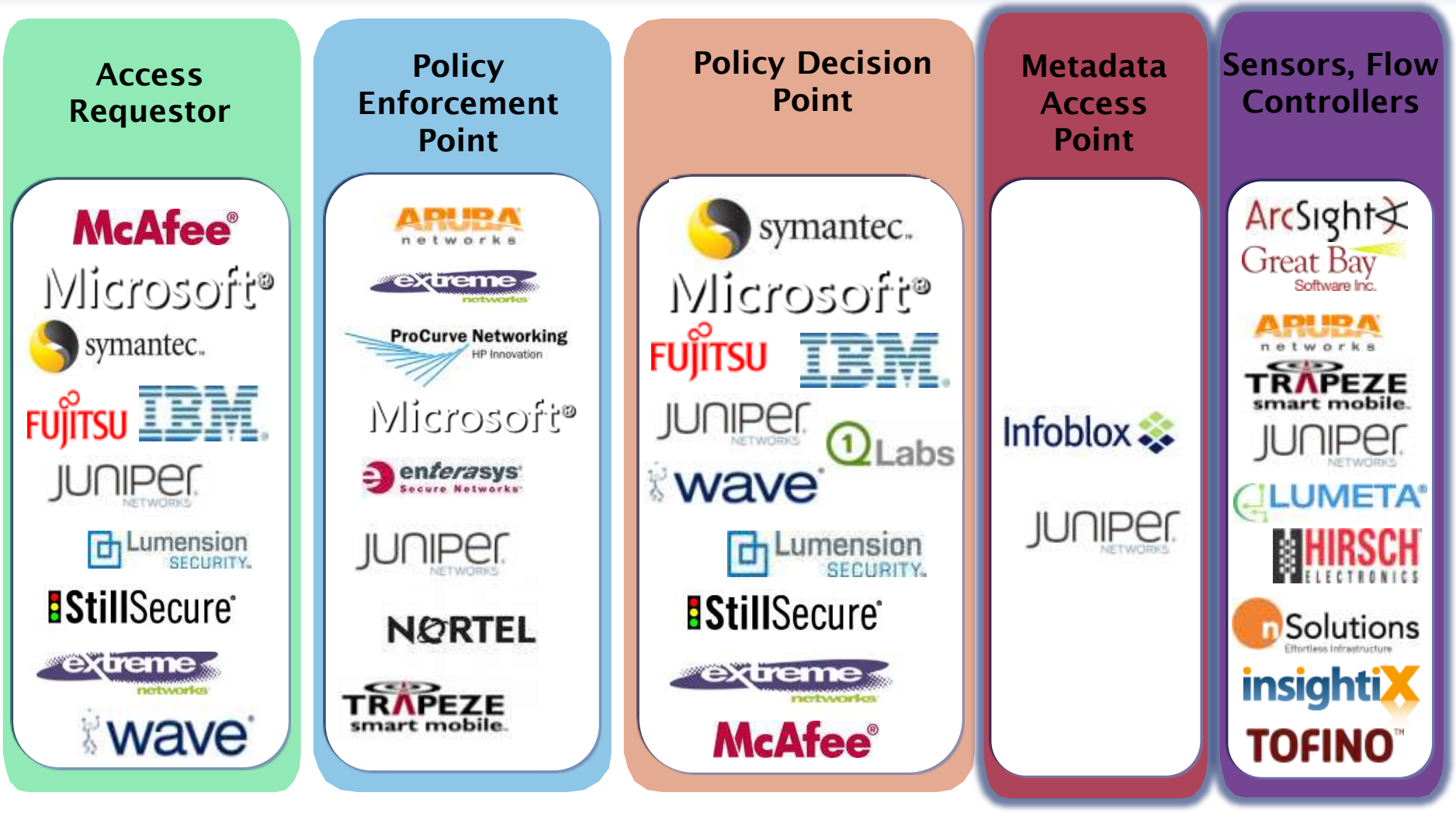
- GA in August of 2009

Enables delivery of IPsonar Discovery events for automated remediation

Significant interest with Government Clients

Integrated network defense solution with Juniper Networks

IF-MAP Adoption



TRUSTED COMPUTING GROUP™

What About Open Source?

Lots of open source support for TNC

- University of Applied Arts and Sciences in Hannover, Germany (FHH)

  http://trust.inform.fh-hannover.de

  - tnc@fhh - the open source TNC implementation.
  - ISC DHCP - the open source DHCP implementation.
  - Nagios - the industry standard in IT infrastructure monitoring.
  - Snort - the open source network intrusion prevention and detection system.
  - netfilter/iptables - the packet filtering framework inside the Linux 2.4.x and 2.6.x kernel series.
- omapd IF-MAP Server

  http://code.google.com/p/omapd
- IF-MAP Client Code

  http://ifmapdev.com/

For More Information

TNC Web Site

Technical

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

Business

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

TNC-WG Co-Chairs

Steve Hanna

Distinguished Engineer, Juniper Networks

shanna@juniper.net

Paul Sangster

Chief Security Standards Officer, Symantec

Paul_Sangster@symantec.com

Thank you!