SCAP Exchanges in Trusted Network Connect

IT Security Automation Conference 2012

Charles Schmidt

Overview

- This talk describes an ongoing specification development effort within the Trusted Computing Group
  - Authors: Kent Landfield, Paul Sangster, Charles Schmidt, and Steve Hanna
- Looking to bridge two security automation communities
  - Security Content Automation Protocol (SCAP)
  - Trusted Network Connect (TNC)

Trusted Network Connect

Open Architecture for Network Security

- Completely vendor-neutral
- Strong security through trusted computing
- Original focus on NAC, now expanded to Network Security

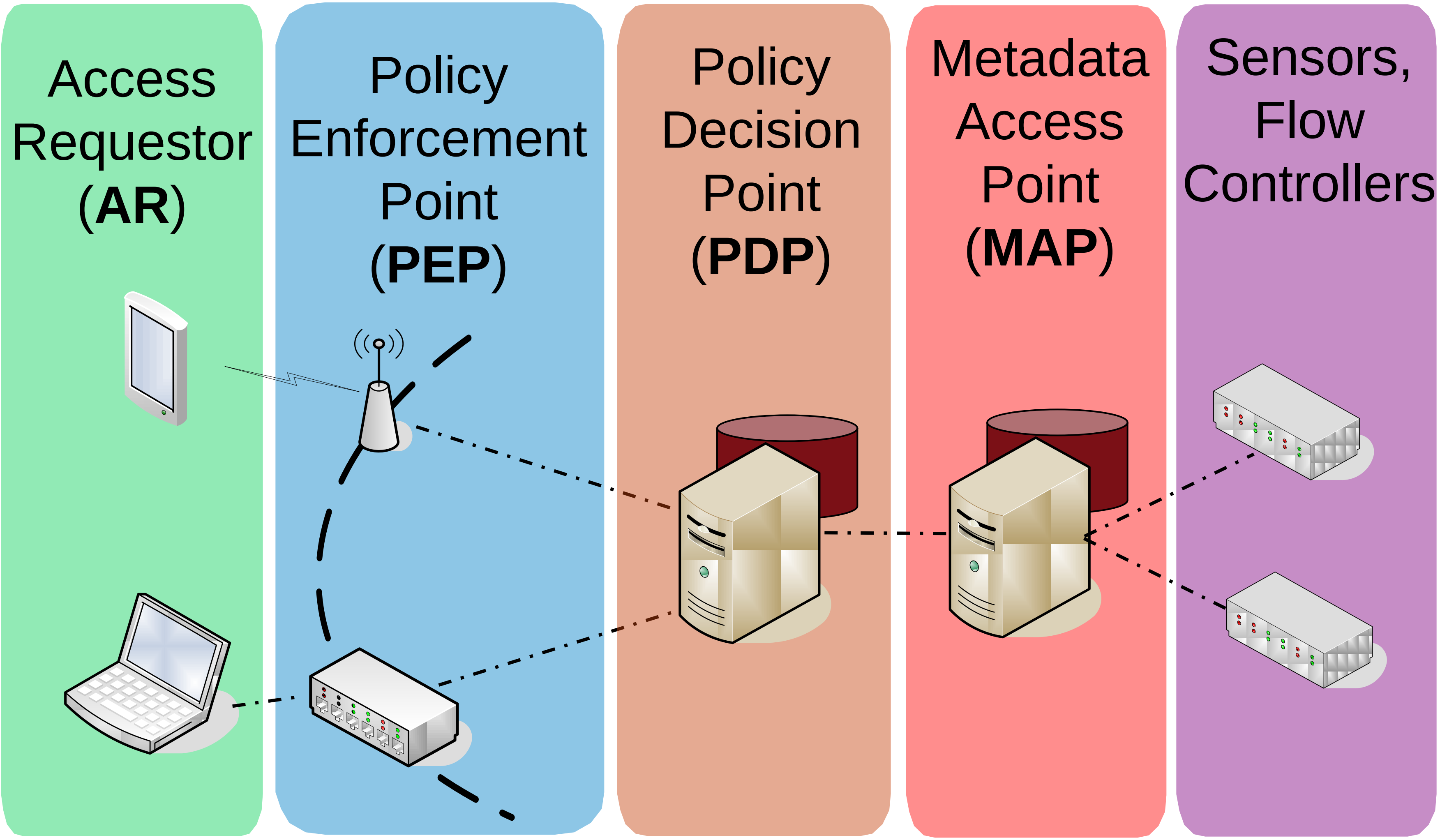
Open Standards for Network Security

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

Developed by Trusted Computing Group (TCG)

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

Integrating Other Security Devices



Access Requestor **(AR)**

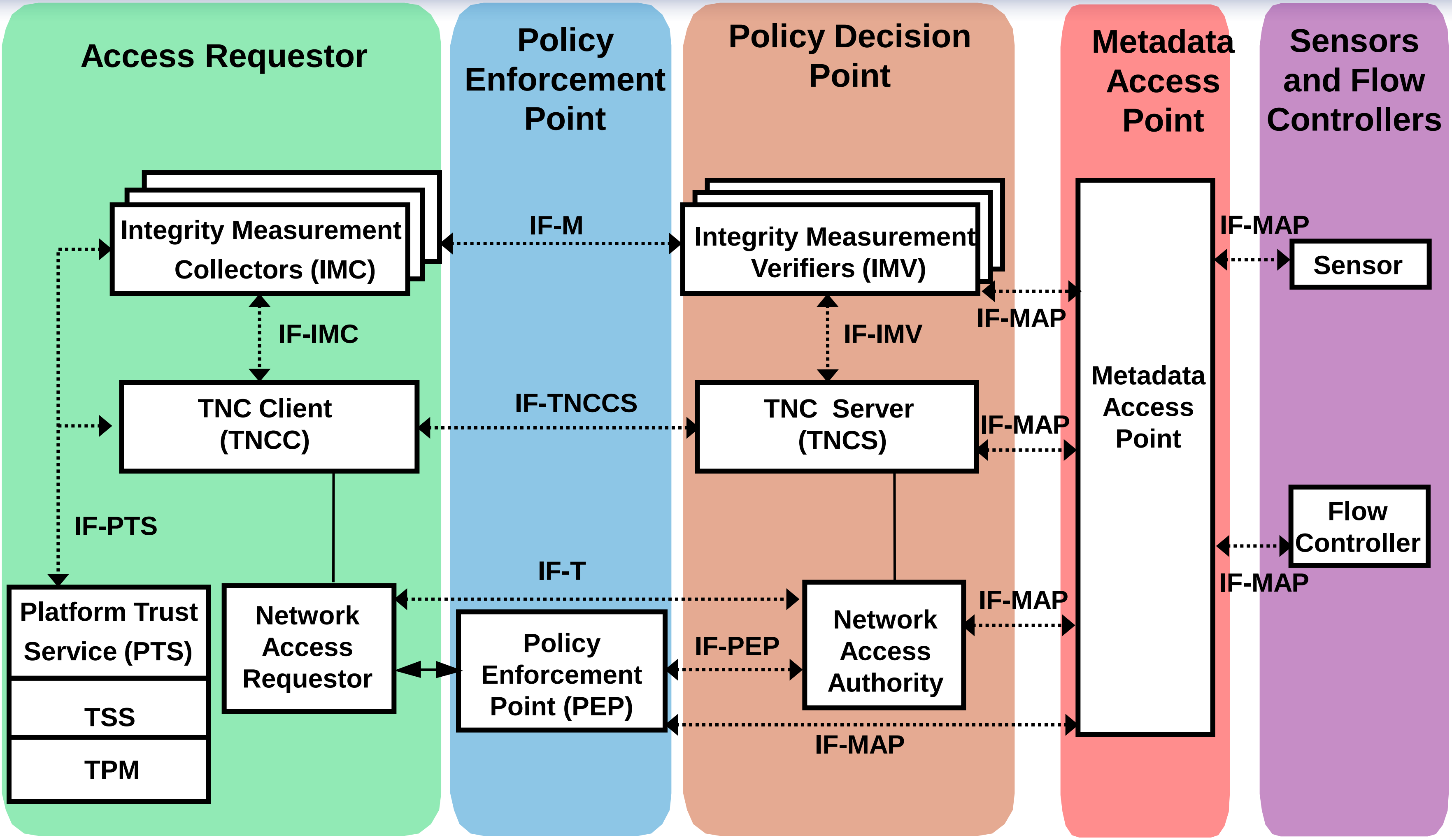
Policy Enforcement Point **(PEP)**

Policy Decision Point **(PDP)**

Metadata Access Point **(MAP)**

Sensors, Flow Controllers

TNC Architecture



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

Putting the Pieces Together

- Trusted Network Connect (TNC)
  - Defines a set of functional units and exchange protocols for endpoint assessment
  - Standardizes some message structures for reporting endpoint information
    - Currently, limited to basic information (software name, version, etc.)
    - To get more detailed information requires proprietary checks
- Security Content Automation Program (SCAP)
  - Structures and values to express policies and checks
  - No standardized SCAP architectures or exchange protocols
    - (But there are some people working on such things)

- There seems to be some opportunity for synergy

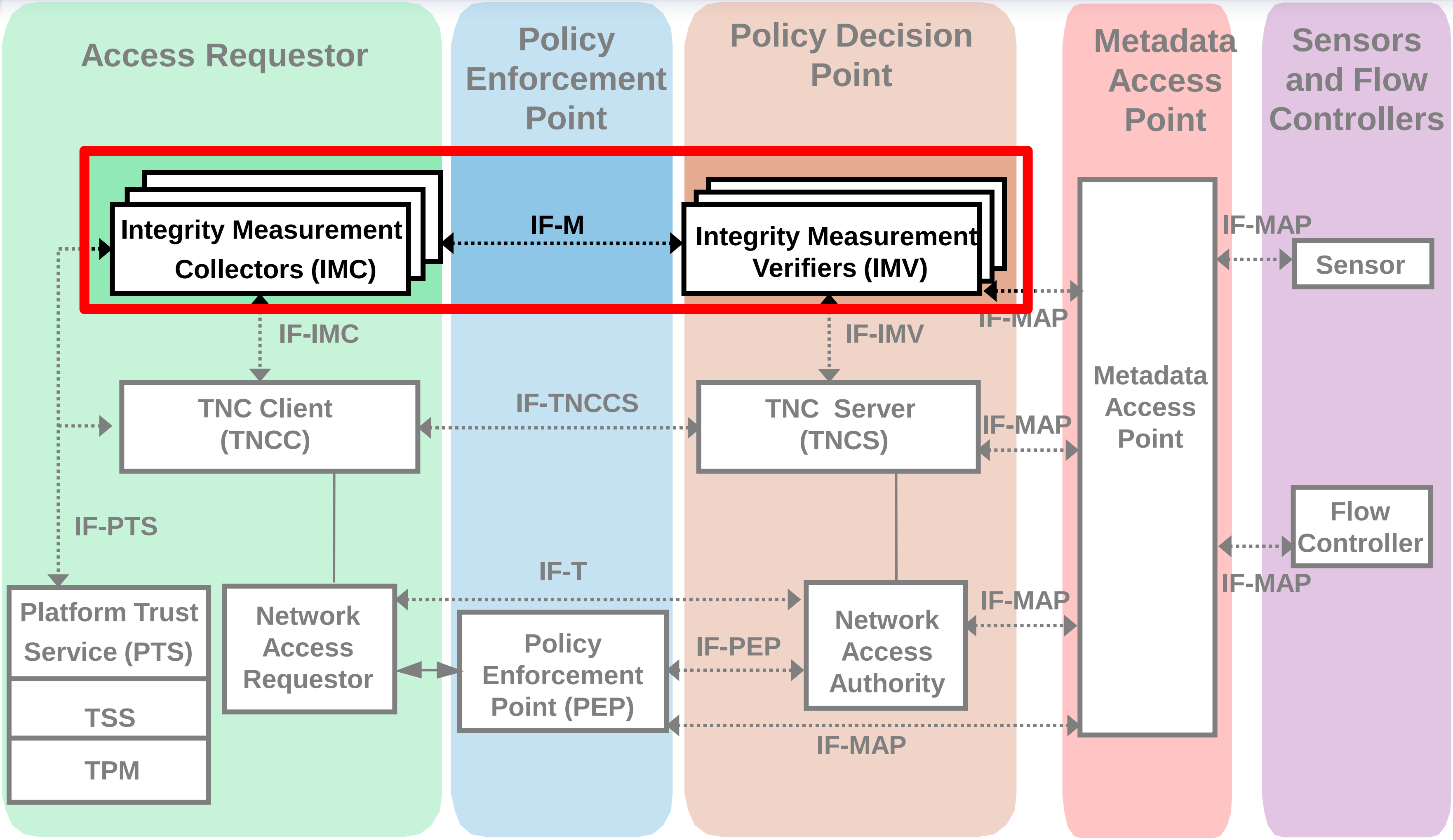
SCAP Messages for IF-M

- A TNC standard for using SCAP content to perform endpoint assessment within a TNC architecture
  - Allow SCAP assessments to be triggered over TNC exchanges
  - Allow SCAP results to feed into TNC-based access decisions
- Design objective – conform as much as possible to the conventions of both the TNC and SCAP communities
  - Do not want to create a new paradigm for SCAP use
  - Instead, provide a way to connect existing SCAP use conventions into TNC
- This is not the first attempt at this
  - Triumfant described a TNC-SCAP integration at the 2010 ITSAC
  - SCAP Messages for IF-M expands the Triumfant approach with the goal of creating a standard

We Need Your Input!

- The specification is complete, but it is not final
- The authors need input from the SCAP community
  - Our goal it to create a useful protocol that doesn’t force SCAP vendors to completely re-vamp their products – only you can tell us if we have succeeded
- Specification is available – please download and provide comments

TNC Architecture

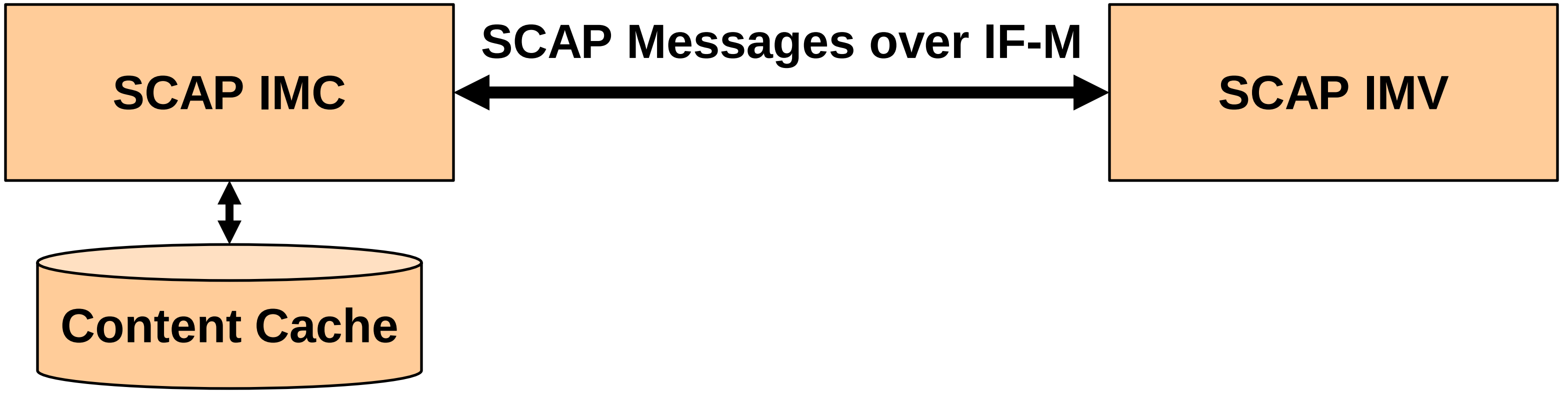


http://www.trustedcomputinggroup.org/developers/trusted_network_connect/specifications

The Big Challenge: Bandwidth

- TNC supports endpoint assessment prior to its joining the network (in addition to assessments after connection)
  - This is done through an 802.1x exchange
  - The total data bandwidth available for this exchange is approximately 20KB
  - USGCB Win7 OVAL is 1.3MB
- The punt:
  - "Only use SCAP over established connections"
  - We wanted to try to do more than this
- Our approach:
  - Provision Access Requestor when bandwidth is plentiful
  - Trigger pre-connection assessment by reference
  - Return summarized results
  - Still support full, traditional SCAP exchanges as well when bandwidth allows

Proposed Architecture and Exchanges



- The exchange protocol has 3 parts:
  - Capabilities exchange – IMV learns what the IMC can do
  - Content exchange – IMV provides the IMC with SCAP assessment instructions; added to IMC cache
  - Assessment exchange – IMV asks for assessment results; IMC provides the IMC with results
- A given assessment may not involve all three exchanges
  - Vendor defined exchanges can replace any of the above exchanges

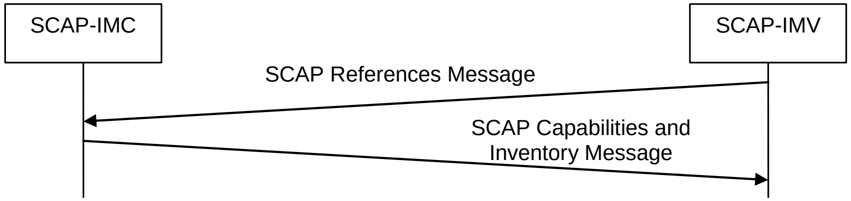
Content Management

- The use of a cache on the IMC means that content management is critical
- The key components used in this protocol are *documents* and *URIs*
  - Document represents a valid SCAP XML document
    - Something that could be handed to an appropriate tool and be interpreted
  - URI is a handle for that document
- Does NOT restrict how IMCs or IMVs store and manage their content internally
  - Can store all OVAL definitions in a database, etc.
  - Just need to be able to associate a valid SCAP document with a URI
    - "USGCB-Windows7-OVAL-1.2.7.1.xml" → a valid SCAP document
- Should not be a new concept – SCAP content does this itself

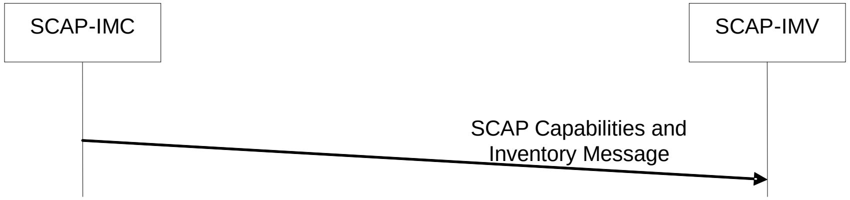
The Capabilities Exchange

- IMV learns
  - IMC's supported version of SCAP
  - Specific SCAP languages supported
  - Receives an inventory of cached content
    - URI – hash value pairs

- IMV-initiated
  - IMV indicates important content
  - IMC indicates the subset of that content present in cache

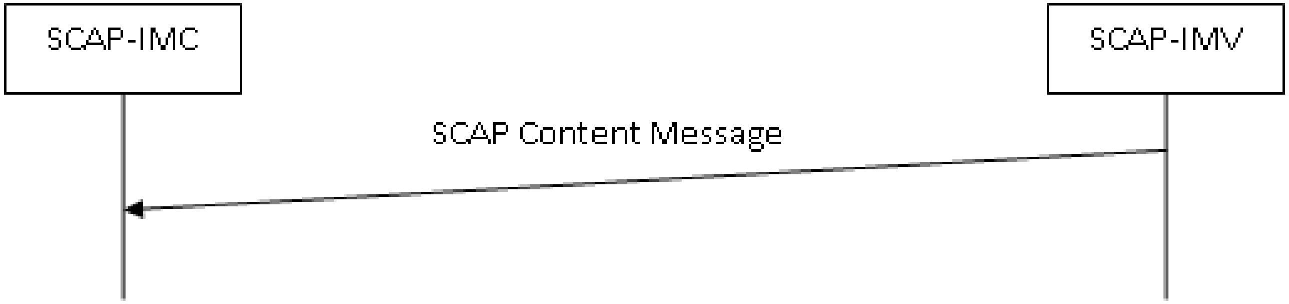


- IMC-initiated
  - IMC volunteers all information



The Content Exchange

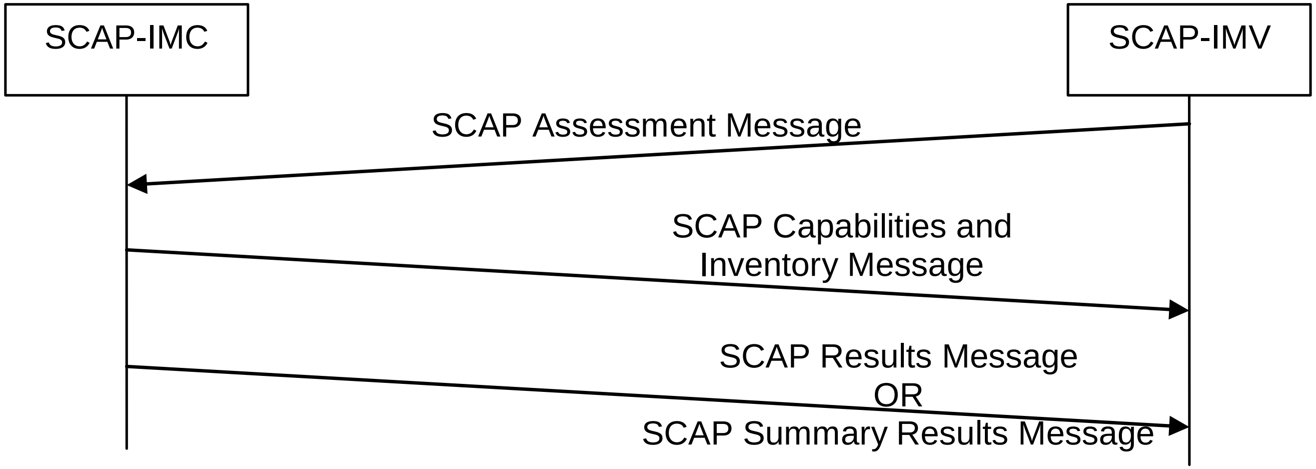
- IMC receives SCAP assessment instructions
  - IMV also provides a URI for each document for tracking



- This is probably the exchange most likely to be replaced by vendor proprietary exchanges
  - SCAP-IMC implementations SHOULD support it, but may choose not to
- Protocol takes the view that, as long as the IMC has content with a known handle, assessment can proceed

The Assessment Exchange

- IMV indicates what SCAP results it wants
- The IMC gathers the results (might be cached results)
- The IMC sends the IMV a list of the SCAP documents it used in the assessment
  - All content documents, variable documents, etc.
- The IMC sends results – full or summary


SCAP-IMC
SCAP-IMV
SCAP Assessment Message
SCAP Capabilities and Inventory Message
SCAP Results Message OR SCAP Summary Results Message

- Also a variant for spontaneous IMC self-assessment

What Next?

- Document is just entering public review
  - Download the spec at http://www.trustedcomputinggroup.org/placeholder
  - Document will remain in public review until November 30
- We need your feedback
  - Goal is a bridge to facilitate connection between the SCAP and TNC communities of practice
  - SCAP Vendors – could you see your products operating in this architecture? If not, why?
- Please send feedback to placeholder@trustedcomputinggroup.org

Questions?