IF-MAP in a Nutshell
Interface to Metadata Access Point

Ingo Bente
ingo.bente@fh-hannover.de

Trust@FHH Research Group
University of Applied Sciences and Arts in Hannover

March 15, 2011
MASSIF Meeting
Fraunhofer SIT Darmstadt

Trust@FHH
Fachhochschule Hannover
University of Applied Sciences and Arts
Trust@FHH Research Group

Figure: University Building

Figure: Trust@FHH Team
(slightly outdated)
# Trust@FHH Research Group

## Team
- chair: Prof. Dr. Josef von Helden
- 3 research associates
- 4 student assistants

## Research Fields
- Trusted Computing
- Network Security
- Mobile Security

## More Information
- [http://trust.inform.fh-hannover.de](http://trust.inform.fh-hannover.de)
IF-MAP Overview
Some IF-MAP Facts

IF-MAP is ...
- a protocol for sharing arbitrary (meta)data across arbitrary entities
- an open standard proposed by the Trusted Computing Group (more precisely: a part of their TNC framework)
- a pretty new technology (first release in 2008)

IF-MAP is not ...
- directly related to any Trusted Computing approaches (TPM)
- widely adopted yet
How is IF-MAP specified anyway?

Dedicated TCG Work Group

- TCG is organized in work groups that address several topics
- TNC work group is responsible for TNC framework
- dedicated MAP sub group of TNC work group addresses IF-MAP

The Set of IF-MAP Specifications

- one specification defines the base protocol
- N specifications define standard metadata for arbitrary use cases
- currently available: IF-MAP 2.0 + IF-MAP Metadata for Network Security
IF-MAP Background

Original Motivation

- improve TNC based Network Access Control
- share network security metadata (AAA, IDS events, addresses)
- make NAC solution leverage IF-MAP metadata when making decisions

Now

- IF-MAP (expected to be) useful for a more broader set of use cases
- goal: general purpose protocol for sharing data in real-time
IF-MAP Architecture

Entities
- central MAP Server (MAPS) as silo for metadata
- arbitrary MAP Clients (MAPC) send/receive metadata via MAPS
- request/response based communication: MAPC ← → MAPS
How does IF-MAP fit into the TNC Framework?

Figure: TNC Architecture Version 1.4
IF-MAP Protocol Details
# IF-MAP Protocol Details

## Technological Basis
- XML messages exchanged via SOAP/https

## Communication Protocol
- request-response protocol
- defines set of valid operations, their syntax and semantics

## Metadata Model
- extensible framework for metadata
- defined by XML schemata
## Metadata Model

### Components

- **identifier**: IP-Address, MAC-Address, Access-Request, Device, Identity
- **metadata**: AAA, Role, Layer2-Information, ... (basically `xsd:any`)
- **link**: relationship between two identifiers
- metadata can be placed both on identifiers and on links
Metadata Model

Components

- **identifier**: IP-Address, MAC-Address, Access-Request, Device, Identity
- **metadata**: AAA, Role, Layer2-Information, ... (basically `xsd:any`)
- **link**: relationship between two identifiers
- metadata can be placed both on identifiers and on links

```
access-request = request01
identity = bob
role = employee
layer2-information
VLAN = 96
Port = 12
device=switch01

device=aaa-server-01
authenticated-by

device=aaa-server-01
access-request-device

device = laptop01
access-request-device

ip-address = 10.0.0.99
ip-mac

ip-address = 10.0.0.99
access-request-ip

ip-mac

VLAN = 96
Port = ...
```
IF-MAP Communication Protocol

IF-MAP Operations

- publish: update/delete/notify MAPS metadata
- search: search for existing metadata in MAPS
- subscribe/poll: observe metadata in MAPS

Session Handling

- MAPC and MAPS establish a session
- session consists of two communication channels
- SSRC (mandatory): publish, search, subscribe
- ARC (optional): poll
IF-MAP Example Flow of Operations

 время

 SSRC1
 MAPC1 MAPS

 publish(A, B, C)
 publishReceived
 subscribe(B, C)
 subscribeReceived
 publish(D)
 publishReceived

 ARC1
 MAPC1 MAPS

 poll()
 pollResult(B, C)

 MAPC2 MAPS

 SSRC2

 MAPC2

 poll()

 pollResult(B')

 publish(B')
 publishReceived
IF-MAP Demo
IF-MAP Demo Software

MAP Server

- irond
- Apache License 2
- http://trust.inform.fh-hannover.de

MAP Clients

- irongui
  - Apache License 2
  - http://trust.inform.fh-hannover.de
- soapUI
  - LGPL 2.1
  - http://www.soapui.org
IF-MAP Experiences from Adoption

:-)

- quality of the specs
- approach seems reasonable and feasible
- MAP subgroup is very responsive
- level of interoperability
- commercial products and open source tools are available

:-(

- complexity (analysis, search expressions)
- some details are ambiguous (connection handling, size-calculation)
- the spec is a moving target
Thank You
Questions?