Schichtenübergreifendes Identitätsmanagement zwischen HIP und SAML

Ein Architekturkonzept

Marc Barisch, Alfredo Matos
marc.barisch@ikr.uni-stuttgart.de, alfredo.matos@av.it.pt
June 2009

Universität Stuttgart
Institute of Communication Networks
and Computer Engineering (IKR)
Prof. Dr.-Ing. Andreas Kirstädter
Outline

Introduction
- Identities on different layers

Motivation
- Combination of User IdM and HIP

Background
- Introduce User IdM and HIP

Architecture
- Overview of combined system

Message Flows
- Management of different identities

Summary and Future Work
Introduction

What is an identity?

Definition

An identity describes an entity represented by different attributes within a specific context.

Source: P. Windley, "Digital Identity", O'Reilly

Examples for Identities

Account with Amazon → User Identity
- Entity: User
- Attributes: Name, Credit Card, ...
- Context: Buying books

Mobile phone → Host Identity
- Entity: Cell phone (Host)
- Attributes: IP Address, IMEI, ...
- Context: Surfing the web

→ Can we benefit from an integrated identity concept?
Motivation for an Integrated Identity Concept

- Benefit from mutual advantages
  - User IdM System - SAML-based
    - Single Sign-On
    - Attribute Retrieval
  - Network Protocol - Host Identity Protocol
    - Mobility
    - Multihoming
- Avoid duplicate security functionality
  - User IdM System - SAML-based
    - TLS
  - Network Protocol - Host Identity Protocol
    - IPSec
- Provide new possibilities
  - Extension of trust concepts
  - Cross-Layer Attribute Exchange

→ Design an integrated architecture
Background

User Identity Management Systems – SAML-based

• Roles
  – User
  – Service Provider (Relying Party)
  – Identity Provider

• Message Flow
  1. User authenticates against IdP
  2. IdP creates tokens
  3. SP receives token
  4. User consumes service provided by SP
  5. SP retrieves attributes from IdP

• Advantages
  – Improves Security
  – Improves Usability
Background

Host Identity Protocol (RFC 4423, 5201-5206)

Characteristics

- Host is identified by Host Identifier (HI)
- Host Identifier is the public key of a corresponding asymmetric key pair
- Dynamic mapping of HI to IP addresses
- Additional control layer between network and transport layer
  - Mobility
  - Multihoming

Base Exchange to establish HIP association

- Four-way handshake
- Key Negotiation Protocol → IPSec channel
- Basis to enable host authentication
Requirements for Cross-Layer Attribute Exchange

Mapping between HIP namespace and IdM namespace

- HIP namespace is flat
- User identifier namespace is hierarchical
  - User part
  - Identity Provider part

→ Additional mapping mechanisms in IdM system required

Managing the relation between HI and user identifiers

- User has different hosts, i.e. assign host identity based on user identity
- Trust in HI requires secure mapping between host identity and user identity

→ Additional HI assignment/registration mechanism required
Architecture

User IdM Subsystem
- Authentication Service:
  - Authentication of users
  - Single Sign-On support
- Attribute Service
  - User and host attributes
  - Mapping of identifiers

HIP Subsystem
- HIP HI Manager
  - Assignment of HI
  - Registration of HI
- HIP Session Manager
  - Manage active HIP sessions
Attribute Retrieval

Mapping mechanism between HI and UI

Possible to exchange X.509 certificate in HIP Base Exchange

- **Trust**: Verify host identity
- **Attribute Retrieval**: Discover IdP with additional information

Access control framework

- **Static policies** based on existing HIP associations
- **Dynamic policies** based on HI of communication partner (i.e. Service Provider)
Host Identity Assignment/Registration

Two alternatives

Alt 1: Host Identity Assignment
  - Host has no identity before
  - IdP assigns identity

Alt 2: Host Identity Registration
  - Host has already an identity
  - IdP manages mapping to user id.

Process

• Successful user authentication with Authentication Service (AS)
• Host Identity Manager (HIMgr) responsible for assignment/registration of HI
• HIMgr creates **X.509 certificate** to attest host identity and as prerequisite for attribute retrieval
• Mapping between HI and UI is stored in Attribute Service (AttrS)
Summary and Future Work

Summary

- Motivated advantages of proposed solutions
  - Combine advantages of HIP and User IdM (mobility, trust, security)
  - Cross-Layer attribute retrieval
- Presented an architecture that integrates user and host identities
- Proposed protocol to assign/register host identities
  - Not considered by IETF, so far
  - Alternatives have different security properties
- Introduced solution to map HI to user identities based on extended X.509 certificates

Future Work

- Evaluation of privacy issues
- Support for multiple hosts and multiple identities (Virtual Identities)
- Work on proof-of-concept implementation started
- Integration into Liberty Alliance possible
- Extension towards other technologies (e.g. MIP, SHIM, ...) that have a notion of identity on the network layer
• Examination of privacy problem by several simultaneous HI
Backup Slides
## Identity Concepts on Different Layers

### Application Layer/ User Identity Management

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Identification and Authentication of users</td>
</tr>
<tr>
<td>– Improve Security (Reduce number of accounts)</td>
</tr>
<tr>
<td>– Single Sign-On and Single Bill</td>
</tr>
<tr>
<td>– Attribute Retrieval</td>
</tr>
</tbody>
</table>

### Network Layer/ Host Identity Management

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Support Mobility</td>
</tr>
<tr>
<td>– Support Multihoming</td>
</tr>
<tr>
<td>– Improve Security (e.g. Encryption, Network Endpoint Assessment)</td>
</tr>
</tbody>
</table>

### Solutions

- Windows CardSpace
- Liberty Alliance
- Shibboleth
- Security Assertion Markup Language (SAML) is often the basis

- Explicit Notion of Identity
  - Host Identity Protocol (HIP)
  - SHIM6
- Implicit Notion of Identity
  - Mobile IP (MIP)
  - Network Endpoint Assessment (NEA)

→ **Combine** both Identity Concepts at the example of **SAML** and **HIP**
Motivation for Integration of Identity Concepts

• **Differentiation** between user and device identities is hard
  – Devices are typically not shared between users
  – Which attribute belongs to the user and which to the device?

• **Benefit** from mutual advantages
  – **Security**: Avoid duplicate security functionality (Authentication, Encryption)
  – **Trust**: Use IdM systems to create trust between hosts
  – **Mobility**: HIP provides a mobility solution
  – **Attribute Exchange**: Retrieve user attributes based on the HI/HIT and vice versa

**Example Scenario**

Retrieve location information based on Host Identity