IETF GEOPRIV Authorization Policies:

Hannes Tschofenig, Nokia Siemens Networks
Alissa Cooper, Center for Democracy and Technology,
Richard Barnes, BBN

W3C Access Control Workshop
17-18 November 2009, Luxembourg

Martin Euchner
Nokia Siemens Networks GmbH & Co KG
CTO RTP RT SWS SER
Tel: +49 89 5159 15667
Martin.Euchner@nsn.com

Nokia Siemens Networks

Conclusions

- The work in the IETF GEOPRIV WG on the location privacy led to the development of a more generic authorization policy mechanism (RFC 4745) that can be extended by other application specific contexts.
- Interoperability was the main reason for standardizing a policy language.
  - Allow authorization policies to travel with the data: this is still a very novel idea that has to find acceptance in the deployment community.
- Approach:
  - Define a basic authorization policy framework;
  - Define how the identities of specific communication protocols fit into identities used by the authorization policy framework;
  - Define how the data model used by the communication protocol maps to the conditions of the access control policies;
  - Important: application-specific extensions need to define the semantics of potential actions and transformations.
- Experiences:
  - The GEOPRIV architecture defined a lightweight version of these privacy policies (RFC 4745) that are more deployment friendly than the full-size authorization policies based on Common Policy.
  - The basic functionality of the authorization policy mechanism defined in the GEOPRIV working group could certainly be mapped to other authorization policy languages, such as XACML.
  - Standardization approach takes time to complete the work.
- Opportunity due to standardization:
  - allowing communication service providers (CSP) to actually develop their proprietary authorization policies as they have better means to innovate.
  - CSPs can offer a specialist user interface, typically controlled via a web browser, to allow the users to control their privacy preferences and the access to their data (better user experience).
- Outlook:
  - interesting challenge is the need to define incentives for various parties to actually deploy standardized solutions (in comparison to their preferred approach) given that new usage scenarios require a certain amount of standardization overhead in order to accomplish interoperability.

Introduction
IETF GEOPRIV WG background

- The IETF GEOPRIV working group was set up to develop privacy-preserving mechanisms for the distribution of location information on the Internet.
- RFC 4745 “Common Policy: A Document Format for Expressing Privacy Preferences”
  - defines an **XML-based access control language**
  - is not tied to a specific application,
  - it can later be used in other contexts as well (beyond location distribution).

- The GEOPRIV architecture has the need to specify such a policy language to allow authorization policies to be attached to data (in the form of sticky policies) when it leaves the Location Server towards the Location Recipient.
- GEOPRIV architecture use the presence architecture (RFC2776) as a foundation.

Nokia Siemens Networks

Common Policy (RFC 4745) "Common Policy: A Document Format for Expressing Privacy Preferences"

- Is a framework for authorization policies controlling access to application-specific data: combines common location- and presence-specific authorization aspects.
- Was used as a starting point for a minimal authorization policy baseline.
- Defines a format for XML documents that contain **access control rules**.
- Single rule has three parts:
  - Conditions:
    - identity condition: (sip:, tel:) URI of requestor, **"identity-based authorization"**
    - time-based validity condition: possibility to limit the lifetime of a specific rule
    - an abstract "sphere" condition: offers an easy way to switch named policies (e.g., 'home' to 'work').
  - Actions, and
  - Transformations: a set of transformations that allow access to various presence based information elements (aka access rules).
- A new conflict resolution mechanism:
  offers minimal disclosure in case that parts of the authorization policy are not understood, for example unknown extensions.

- Observations:
  - Common Policy mechanism alone is not sufficient to provide a complete authorization policy mechanism for most applications.
  - it needs to be extended to apply to a specific context.
    To deal with application-specific semantics, further specifications are necessary, such as described with the presence authorization policy or the geolocation authorization policy.

Access Control for SIMPLE

- SIMPLE = usage of SIP for instant messaging and presence.
- SIMPLE presence system instantiates the Common Profile for Presence (CPP) framework as its baseline architecture.
- Common Profile for Presence (CPP) (RFC 3859) defines a set of logical operations for delivery of presence information.
  These primarily consist of subscription operations and notification operations

- The Extensible Markup Language (XML) Configuration Access Protocol (XCAP) (RFC4825) is the SIMPLE protocol for provisioning access control and authorization policies in to a presence or a location server.

Authorization Policies

- Specifications provides a detailed description on how to use the identities in SIP with Common Policy rules.
- describes how the sphere element of Common Policy is utilized in the SIP presence context.
- The geolocation authorization policy defines
  - authorization policies with location-based conditions
  - and transformations that allow the rule change the returned location object. include the ability to set certain usage policies for the data and to control the granularity of location information being exposed to third parties (e.g., ”city level granularity”).

Nokia Siemens Networks

Standardization needs

- Use case/scenario:
  OpenID used for applications that are browser-based and these authorization policies are instead uploaded to the OpenID Provider (OP; IdP)

- Technical work is necessary that requires a description of the type of identities being used in the HTTP context to allow the OP to make decisions about which RP they provide what information, and the type of information that may be exchanged.

- The following might be researched for standardization?
  - Something similar like “Creative Commons License” for attaching to transaction data.

Nokia Siemens Networks