VOMS Attribute Authorities

Michael Helm

ESnet/LBNL

23 Feb 2007

Goals

- Better understanding
- Support authorization services
- Exchange information
- *Discuss questions about security, trust, and basic assumptions*
- *Source of Authority and management*
- *Clarify / rework existing practices*

Recap

VOMS AA server – surprise!

In Dec 06 learned several interesting things….

1. OSG very interested in VOMS as focus of attribute/role/authorization information
2. Proposal to make widespread use of VOMS AA, like in EU
3. Proposal to deprecate other types of proxy certs, use only VOMS-based proxies

---

- Very important activity – shows maturation of authorization efforts?
- Knew little about this activity
- Puzzled by Attribute Authorities themselves – what are they & how are they trusted?

How Does It Work?

VOMS as Attribute Authority

1. User authenticates to VOMS server, over a TLS-(or GSS-) secured connection
2. VOMS server finds appropriate attributes for this user
3. (Inner transaction) VOMS server private key signs these attributes (creating an attribute cert (VOMS AC))
4. User generates new key pair (proxy key pair)
5. (Outer transaction) User (software) bundles public key, authentication cert attributes, and VOMS AC, and signs the bundle, creating proxy cert
6. New proxy private key & cert moved to wherever needed
7. Combines some of the better features of delegation and a bearer credential

What could be bad about this?

Red Flags

VOMS as Attribute Authority

- What is the Attribute Authority?

Ans: It's the VOMS server, specifically the host or service certificate key pair.

- How do relying parties & users trust this AA?

Ans: It's the IGTF cert chain – the VOMS server is signed by an IGTF CA, so the trust works both paths – for the authentication cert, and for the AC

- How are is the information about attribute authorities managed?

Ans: A configuration file is distributed to relying parties, with the certificate of the AA (VOMS host cert). But this is awkward, so it is proposed to drop the certificate distribution, and only distribute the subject name (DN) of the AA.

- How are the configurations managed? How do AAs get listed/delisted?

Ans: ….

- When a security incident happens, where do the trust paths terminate, and who gets the blame?

Ans: (Me) In OSG, that's going to be DOEGrids CA

- How is the scope/value of VOMS attributes controlled? [From VOMS worker]

Ans: …

Work Through Problem Areas

- Server certificate is not appropriate for an AA
  - AAs are a type of CA
  - IGTF CAs have issues with host and service identification
  - IGTF CAs do not guarantee unique host certs
  - The identification is wrong – the host is an object, not the authority
- The trust answer, is the answer to a different question
  - The trust should be about the AA, and the organization behind it, not the IGTF CA
  - Inappropriate trust relationships endanger Grid security (& the PKI)
  - Source of Authority (SOA)?
- Management of AA information looks vulnerable to various kinds of attacks
  - Configuration files can be changed in transit or in place
  - Inappropriate services on same host can steal AA ID
  - Single point of failure (host cert)

What Can Be Done?

- Better understanding of VOMS, particularly security constraints
  - Some issues may have acceptable risks, constraints I don't know about &c
  - What is acceptable to security workers?
- ➢ AC's must point to responsible party – not IGTF CA
  - Must be clear to naïve user/adminstrator/relying party
  - See "VOMS Attribute Certificate Format", Ciaschini &al, OGSA-AUTHZ WG in OGF
- Maybe it is time to specify how abstract services can be "identified" and certified
  - AA is not the only service of this type
  - Perhaps only security-related services need this much attention?
- Software engineering
  - Hosts as SPF
  - Security of configurations / distributions

Discussion

Some references:

1. RFC 3281 (Attribute Certificate format)
2. VOMS Attribute Certificate Format”, Ciaschini &al, OGSA-AUTHZ WG in OGF
3. X.509 (as part of “The Directory”); in particular section 3, chapter 13 (on which RFC 3281 is based, in part)
4. Appendix: Short version of these slides, at EUGridPMA 9 (RAL, Jan 2007)

VOMS Attribute Authority

Michael Helm / ESnet / 17 Jan 2007

- Proposal in OSG to replace conventional proxy cert use with voms-proxy-init
- Technology: signed attributes (another kind of certificate) embedded in user's proxy cert
- Attribute authorities: voms server – host cert signs
- Trust anchors are Grid ID certification authorities

VOMS AA's

- **Trust – accountability terminates at Grid ID CA**

This means, in OSG, both the user & attribute trust is DOEGrids. We don't certify "attribute authorities". We certify something like SSL servers.

- **CA identifies hosts or services. We don't identify AA's.**

We could do this. But we don't have a category like this.

- **Relying parties are asked to trust the wrong thing**

Imagine we ran our id CAs this way – we would sign id assertions with the SSL server certs that the portals use for CSR submission &c.

- **Controls to prevent duplicate certificates for hosts don't take this scenario into account**

How easy is it to create an illegitimate AA?

- **How to distribute the ID's of the AA's**

What if a host cert needs to be replaced, a new one added to the infrastructure

- **What mechanisms exist to persuade people to trust these AA's?**
- **VOMS attributes**

Are the attributes signed consistently understood? VOMS developers not sure.

- **Why do you care? What I do with my cert is none of your business.**

That may be true in some hypothetical PKI, but of course there are usages we can't support. Obviously illegal activity is one of these. But more realistically, things like encryption have to be disclaimed, because the proper controls aren't in place.

- **Why is identity over-engineered (our process), and authorization under engineered (above process)?**

From security point of view isn't the balance wrong?