Some security standards and how they might Grid-ify

stephen.farrell@cs.tcd.ie

"*Your favorite standards joke here"*

Contents

- What I was asked to chat about
- What I'm going to chat about
- Conclusions

Slide with acronyms only

- IETF
  - PKIX
    - CMP CMC
    - OCSP SCVP
    - AC
  - SACRED
    - BEEP
- OASIS
  - SAML
  - XrML
  - XACML
- W3C
  - XMLENC
  - XMLSIG
  - XKMS
    - X-KISS X-KRSS

What I'm going to talk about

- Grid AAA +
- Strawman

Disclaimer

- I've never really done any Grid stuff
- I've done PKI stuff for too loooong
- So beware combinations of naivety and skepticism

Grid AAA

- Authentication, Authorization and Accounting
  - RADIUS (Diameter)
- Maybe a better start for thinking about Grid security problems
  - Compared to “usual” security protocol approach (Kerberos/PKI)

Grid authentication

- Seems like a two-fold problem:
  - Who is the local individual?
  - Who is the foreign institution?
    - Modulo an accounting/audit identity
- Is there a need to tie key management to authentication?
  - Not sure – maybe unbound IPSec and SSL with tunneled authentication is ok?

Grid authorization

- Generally, authorization using token-passing systems (e.g. ACs, some SAML use-cases) have serious performance issues
  - Canadian DoD AC study: 109 certs per purchase!!!
- Keeping authorization information in a server with a query protocol is arguably much better

Grid accounting

- Audit/accounting confusion
  - I'll just add to the confusion!
- Accounting maybe not in monetary units
  - Potential new resource stealing attacks?
- Audit identity concept
  - Labour law/pseudonymity

Other security services

- (When) Are data integrity and confidentiality needed?
  - Field level or connection
    - Performance!!!
- Non-repudiation is non-sense

What to standardise

- Less than PKI did!
  - Too late to change the past
- Only standardise fields which are required for run-time interoperability
  - No policy-mappings!
  - With a server-based authorization approach, there's less need
    - Reminds one of XKMS too!

Security levels

- Insisting on the best (most expensive!) mechanisms everywhere is probably wrong
- Possible approach
  - Provision for ubiquitous use of highest level security (e.g. everyone gets a cert or two)
  - Only use the level of security required for this transaction/session

Ad break

- Two PKI workshops that this audience might be interested in:
  - Washington DC., April '04, http://middleware.internet2.edu/pki04/ papers due: end Jan
  - Greece, June '04, http://www.aegean.gr/EuroPKI2004 papers due: mid Feb

Grid Security Strawman

- Caveats
  - Product of an idle morning's typing!
  - Other people have done real work on this
- But (if its not too late) there may be benefits to making some changes
  - Maybe just at version n+1

Authentication Strawman

- Grid authentication should use:
  - Peer IP address/IPSec, or,
  - SACRED for remote credential storage, or,
  - Stronger PKI options where necessary/possible, or,
  - Even weird things like entity recognition (ER)
- Authentication checking could be via XKMS
  - A Grid specific XKMS server-server protocol may be required
  - Not hard, just name based re-direct really

Authentication Strawman (2)

- Delegation/proxying:
  - Allow sequences with different mechanisms on each hop (performance)
  - Maybe use SACRED (or X-KRSS) for cases where "strong" crypto authentication needed from intermediary
    - But always make up a new key
- Figure out how to include Kerberos/Win2k security

Authorization Strawman

- Grid authorization should use:
  - Mapping (from Grid authenticated ID or audit ID) to OS authorization where possible
    - Proprietary mappings are ok to start with – no need to standardise yet!
  - SAML for other cases where (direct!) checking with a foreign authority is needed
    - Should define a ***few*** Grid-wide authorization SAML attributes

Accounting Strawman

- ***All*** Grid uses should be accounted/audited
  - Even if no budgets/charging
  - Probably RADIUS based
  - Have to define an identifier
    - Sometimes calculated, not asserted!!!
- Allows use of weaker authentication and authorization mechanisms
  - Just spot what happened and prevent it recurring
    - Rather than spending upfront to prevent initial occurrence(s)

Other security services

- IPSec &/or TLS
  - Try to use by default
  - Keying issue during install
    - XKMS for locates (maybe)
  - Application awareness!
- Field level integrity/confidentiality
  - Leave that to the applications, but,
  - Provide some (source) examples using CMS and XMLENC/XMLSIG

Strawman Features

- COTS products and open source are available for all
  - Well...nearly :-)
- Flexibility in ramping up/down security as needed built in from the start
- Real delegation: allow axe-grinders to rule their own roost!

Conclusions

- PKI and all that stuff exists and (eventually) works
- Token passing authorization systems are bad performers
- Grid security can be re-thought a bit
  - Up to you to decide if that's worthwhile!