PKI and Shibboleth for Grids and IEs

JISC Core Middleware Meeting,
Windermere

14 November 2005
Mark Norman
This talk

- PKI with grids and the information environment
- How could Shibboleth help?
- Our work
  - DCOCE and ESP-GRID
- DCOCE main findings
  - The over-centralised security on the UK e-Science Grid

- ESP-GRID work so far
- An over-centralised security scenario
- ESP-GRID conclusions so far
- Next (final) steps
PKI and Grids and with the IE

- PKI and Grids (so far)
  - Need identity tying to ‘work’ or access
  - Identity/AuthN must be checked more rigorously
  - The middleware of choice had adopted PKI

- PKI generally seen as too hard for most end users
  - Apart from those who can script/implement/program
  - (and even some of those!)

- For those reasons, probably too heavyweight for the Information Environment (IE)
Can Shibboleth play a part?

- Shibboleth:
  - Allows ‘usual’ (and unusual) authentication methods
  - Based on machine to machine trust
    - (not end user/cert to machine)
  - Much better for most users in the IE (ease of use, and familiarity)
  - Not compatible with current grid middleware (e.g. Globus)
  - Not completely trusted by current grid users/owners
Our research

• DCOCE finished at the beginning of the year
• ESP-GRID ongoing
• Digital certificate Operation in a Complex Env.t, aims:
  – detailed implementation and evaluation report of 'real world' digital certificate services at the University of Oxford
  – development for, and implementation of, a public key infrastructure using digital certificates that will form a pilot project involving a selection of users within the University of Oxford
• Evaluation of Shibboleth and PKI for Grids, aims:
  – whether and how Shibboleth offers solutions to issues of grid authentication, authorization and security
DCOCE Main Findings

• PKI/client certificates *can* be usable and scalable
  – users *need* to understand only a few principles
• Cryptographic hardware devices *very* useful
  – and almost affordable
• Public/kiosk computers are a difficult case
  – but may be overcome by hardware tokens
• Separate AuthN and AuthZ as much as possible
  – Generally a good philosophy anyway
• PKI/client certificates *can* be usable and scalable
  – but they’re not!
14 November 2005

User visits RA

Signed certificate placed in cRA system

User downloads certificate

User encrypts certificate/private key and stores them in LICS

Certification Authority

Local Institution Certificate Store

User visits RA

Certificate request

Usual work PC

User

Private

1 or 2
Centralised Security with the UK Grid

Certification Authority
(A national ‘head of security’)

(Regional)
Registration Authorities

Organisations
(e.g. Universities)

Personnel
Officers etc.
(people at the end of the chain of trust!)
ESP-GRID work

• Project participants:
  – Mark Norman, Alun Edwards (Oxford)
  – Now some of the BRIDGES/DYVOSE team from NeSC@Glasgow

• Mostly requirements and devolved authentication ‘thinking’ so far
  – See http://wiki.oucs.ox.ac.uk/esp-grid/

• Some ‘grid people’ don’t like devolved AuthN
  – (but is it really DA?)
  – Lack of clear thinking on this subject!
Centralised security

• Recently gave a talk at NeSC on this
  – See http://www.nesc.ac.uk/talks/623/

• People want centralised security because it feels safe
  – It is usually unrecognised that the central people *have* to trust staff at the institutions (i.e. untrained, not RAs – personnel/registration)
  – By not recognising it, everything is less secure
  – No revocation or removal of privileges for *bad* users
A great new resource for researchers

Newman: What’s that? It looks great!
Oldman: That’s our new e-Science building. It’s got lots of cool stuff and any researcher can use it!
Newman: Oooh, I can’t wait! I think I’ll go there now!
Oldman: Ah, erm… You need a special security pass.
Newman: Eh?

14 November 2005
Newman: But I’ve got my University swipe card!
Oldman: That isn’t good enough! You need a high security card to get in – like this one. Chip and pin, you know!
Newman: OK, where do I get one of those?
Oldman: Because it’s such high security, these babies are issued nationally, via regional centres! As we work at Cotswolds University, we don’t have a centre here – you need to go to Oxford e-Science Centre.

Newman: Blinking heck! I’m only an ordinary biologist. Maybe I don’t need to use the building after all…
Oldman: No really – it’s fantastic in there. Free coffee too!
Newman: Oh… alright then.
Ha ha! They took everything away from me, apart from the highest security pass I had!

And it might be a year before anyone checks Newman’s security credentials!
Conclusions, so far…

• The grid *needs* devolved authentication [for it] to be secure
  – But is it DA?
  – Isn’t the status quo devolved/centralised identity management?
• Shibboleth *should* have a part to play with the Grid
  – But it can’t do everything:
    • There are some procedures that need to be tied to identity
      (or very strong trust)
    • Devolved rights – not a good fit with Shib unless all machines can be trusted
  – Shibboleth useful for ‘gateways’ to grid applications
    • e.g. portals etc.
  – Or a *Customer-Service* model would do just as well
    • Portals/Web services ideal
    • But Shibboleth fits well here too
Next steps

• Development of a prototype/demonstrator
  – BRIDGES/DYVOSE teams at NeSC@Glasgow doing this now
  – Shibboleth and Customer-Service model via a portal
    • Portal enables grid jobs to be run
    • The “Grid” trusts the portal machine (and its certificate)
    • Machine-machine trust!?!?
    • Fine for ?99%? of future users
      – who need grid power but not grid expertise

• The outcomes/findings may be less technical and really quite basic.
More information at

http://wiki.oucs.ox.ac.uk/esp-grid/

mark.norman@oucs.ox.ac.uk