Grid Security and Identity Management

Mine Altunay

Security Officer, Open Science Grid, Fermilab

Grid Security in a nutshell

- Identity management: authN
- Access control: authZ
- Operational security
  - Monitoring/detecting suspicious behavior
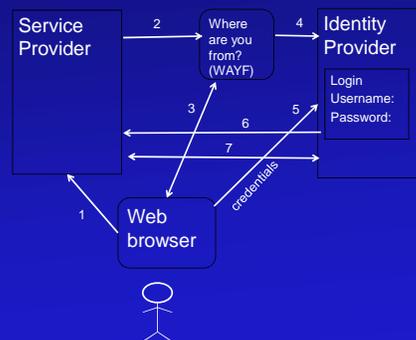 - Incident response
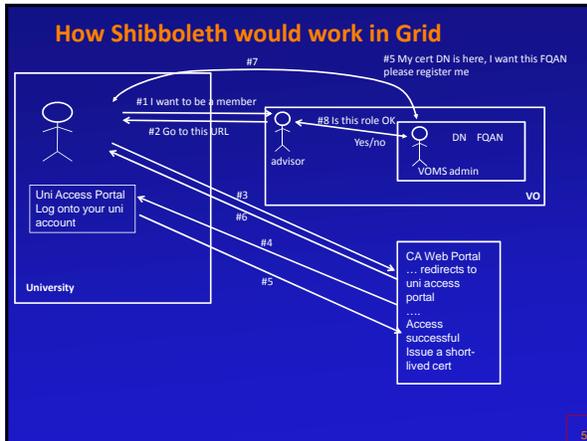
2

Identity Management

- Who are you?
- Currently PKI and X.509
  - Public-private key pairs
  - Users still not used to certificate management
  - Renewing, requesting, moving certs around.
- Is X.509 the only answer
  - Of course not
- Federation-based identity management springs up
- Proprietary tools: Microsoft infocards, IBM Higgins, etc

3

Federation-Based Identity Management: Shibboleth

Service Provider

2 → Where are you from? (WAYF) ← 4

Identity Provider

Login
Username:
Password:

3
5
6
7

credentials

1

Web browser

4

How Shibboleth would work in Grid

#7

#5 My cert DN is here, I want this FQAN please register me

#1 I want to be a member

#2 Go to this URL

#8 Is this role OK

Yes/no

advisor

DN   FQAN

VOMS admin

VO

Uni Access Portal
Log onto your uni account

#3
#6

#4

#5

CA Web Portal
… redirects to uni access portal
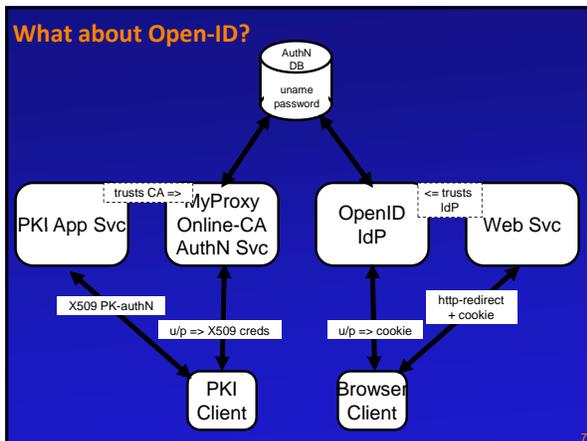….
Access successful
Issue a short-lived cert

University

5

Shib-CAs

- Federation-based CAs
- Identity vetting up to federation member institutions
- IGTF accredited
- Short lived certs (1 week)

6

What about Open-ID?

AuthN DB

uname password

trusts CA =>

PKI App Svc

MyProxy Online-CA AuthN Svc

OpenID IdP

<= trusts IdP

Web Svc

X509 PK-authN

http-redirect + cookie

u/p => X509 creds

u/p => cookie

PKI Client

Browser Client

7

Diversity

- Diversity in identity mgmt will continue
- Will increase
- NSF and NIH joined Shibboleth
- TG started a Shib test bed
- ESG uses OpenID
- …..
- The goal is to get diverse systems to talk to one another

8

Interoperability:

Can OSG users use web-based ESG services ?

• Right now no.
• if OSG user has another IdP that ESG can work with,
• or OSG can build and operate an IdP for OSG users

Can OSG users use non-web ESG services ?
• Yes. ESG should recognize the same CA OSG uses

Can ESG users use OSG services ?

• Yes. ESG users have certs. OSG would recognize the CA and authenticate ESG users

9

Authorization

- Standards have not emerged as in authentication
- It will happen
- Messaging layer has been worked on
- Diverse, home-grown tools used by grids
- Does not get a lot of attention but….
- Will be affected by changes in authN mechanisms

10

Operational Security

- Cares about authN/authZ
- Traceability, accountability, containment are dependent on authN/authZ
- Who did it? Can we suspend him/her? Can we re-instate his/her access after an incident?
- Inter-operation during incident response
  – Grids are connected via bridges, gateways
  – Incidents spread
  – EGEE-TG-OSG shares incident data for cross-incidents
  – Incident sharing community for HEP institutions

11

Operational Security

- Hard to teach and execute
  – NSF Large Facility CyberSecurity Workshop
  – NSF Small Facility Workshop to help small sites
- Hard to research and implement
- DOE Labs town-hall meetings on Security R&D
  – Incident response and intrusion detection
  – data provenance
  – Quantifying risk
  – Report sent to DOE

12

3