Preliminary Conclusions

VO Box Task Force

GDB Meeting

5 april 2006

VO boxes, services, software, & security

Jeff Templon

2015.01.14

J. Templon
Nikhef
Amsterdam
Physics Data Processing Group

Why this talk

- We made a big fuss about this in 2006
- Good example of why
- Some implications for vo sw security
- As well as VO traceability
  (cf current discussion)

J. Templon
Nikhef
Amsterdam
Physics Data Processing Group

Classification of VO Services

- Class 1:
  - Can access site's services (and work correctly) from a private network. (I.e. does not need to live within the trusted subnet of a farm.) Uses only service APIs/interfaces which are exposed to the external world past their firewall.
- Class 2:
  - Uses 'private' interfaces to access information/services at the site (i.e. not exposed to those beyond the site's firewall). Essentially this is anything which is not a Class 1 service.

J. Templon
Nikhef
Amsterdam
Physics Data Processing Group

Heart of the problem

- VO service authors write, install, maintain services. No site control or overview
- If box can live in separate network, no problem. Hacked?
  - Wipe the box
  - Reinstall from scratch
  - Say "here ya go" to the VO
- If box has to live inside trusted subnet, huge forensic task to see whether a breach has occurred

J. Templon
Nikhef
Amsterdam
Physics Data Processing Group

VO Box

- Used to have a class 2 service
- Not anymore .. Moved to vobox network
- Port scan revealed vulnerable service listening
- Because we had it in class 1 network:
  - Limit exposure through firewalling, but leave functional and running for a while
  - Once fixed: wipe box & return to VO

J. Templon
Nikhef
Amsterdam
Physics Data Processing Group

Counterexample: ATLAS N2N service

- Is class 2 by design … has to see SE namespace
- Vulnerability found: service immediately shut down
- Restarted only when fix was provided

J. Templon
Nikhef
Amsterdam
Physics Data Processing Group

Who checks VO sw?

- How many people potentially can add software to CVMFS repos?
- What security measures are there (also in checking / patching sw in CVMFS)?
- If VO deploys software for which trust is relevant beyond "VO boundaries", some rigor is needed. Should be well-defined what is, and is not, covered or assured.

J. Templon
Nikhef
Amsterdam
Physics Data Processing Group

Moving Traceability to VO

- Discussion about dropping glexec et al and mapping all VO activities at site to a single "VO user" since "the VO knows who the real users are"
- If VOs distribute vulnerable software providing network services, can we really trust them to handle all user traceability?
- Suggest any new services requiring substantial trust at site level be audited.

J. Templon
Nikhef
Amsterdam
Physics Data Processing Group