Authentication & Authorization Infrastructure (AAI) on the WN

GDB 2011-12-14

Maarten Litmaath, Steffen Schreiner

Introduction

- We are particularly concerned with protection against and investigations of malicious abuse
  - An attacker may use complex technologies and attempt to cover up the traces
  - Can we find out how an incident happened exactly?
  - Can we contain it in a sustainable way?
  - Can we find out which credentials (if any) were involved?
  - Can we reduce the probability of repetition?

- Can we devise a strategy for incremental improvements?
  - Short, medium, long term

Key concepts

- Traceability
  - See next pages
- Fine-grained control
  - For banning
- Proxy life time
  - Short life time vs. renewal complexity
- Use of general-purpose proxies
  - Safer technologies are advisable

Documentation

- We have a working document
  - https://twiki.cern.ch/twiki/bin/view/LCG/AAIWNSummaryDraft

- Sections
  - Introduction
    - Current summary of where we are
  - Rationale
    - More for the longer term
  - Policies
  - Various other key inputs to the discussion
  - Issues with X509 proxies
    - In particular affecting MUPJ
  - Desired properties of credentials
    - Longer term

Traceability (1)

- Goals
  - Help preventing security incidents from spreading or reoccurring
  - Ensure compliance with legal requirements, including due diligence
  - Provide deniability for users who were not involved with an incident
- OK for now to rely on the VO to provide details
  - We anyway (need to) trust the VO to a large degree
  - Long term: signing payloads may be possible

Traceability (2)

- User payloads should be separated on the WN
  - Avoid interference → allow for quick identification of involved DN
  - Otherwise need to rely on time-based circumstantial evidence
    - May need to ban multiple users
    - Need to be able to exclude Trojan horses or time bombs
    - Data ownership?

- Possible technologies
  - Glexec → currently needs a proxy
    - Investigate if that could be relaxed for the time being
    - ALICE plugin will check payload signature instead
  - Sudo → how to determine the target account?
  - Virtual machines → when will most sites be ready for that?
  - One account per job slot → only Condor supports it
  - SELinux → not evident

Legal issues

- Usually it will be very hard to prove that a particular user was responsible, but we need to prove which DN was involved
  - Allow for containment and resolution of the incident

- Sites may need proof of who was using a resource at a certain time
  - By default they only have the pilot DN for a MUPJ

- The VO ought not knowingly put its users (e.g. the pilot owner) at risk of getting accused of someone else's actions
  - Would you want to run anybody's stuff and have your name pop up in a police investigation?
    - Better pinpoint the involved DN convincingly

Longer term

- Use of general-purpose proxies on the WN is questionable
  - Cf. AliEn plans

- Relation between payload and user?
  - Payload may have been tampered with
  - Signed payloads would be verifiable
    - Cf. AliEn plans

- Data ownership, restrictions?
  - Cf. AliEn token model