A responsibility based model

EDG CA Managers Meeting

June 13, 2003

Trusts

- Authentication requires the following trusts:
  - Identity issued is unique
  - Identity is issued to the appropriate entity
  - Identity Signing Key is well protected
  - Compromised identities are revoked
  - Entity asserting the identity is authorized to hold the secret
  - Proxy has not been stolen

+

  - Authentication token has not been forged or stolen

Managing the Risks

The Pool of involved parties will grow, certainly in the near term, as the Grid grows. How will we manage the risks ?

- Reduce the threat
  - Improve private key management
- Reduce the impact of misuse
  - Restricted network connections
  - Validated executables
  - Throttled bandwidth
- Reduce the liability
  - Assign responsibilities clearly
  - Provide means for calling to task

Scenario

- A Grid job is submitted to a multiuser machine which contains a root escalation attack which takes all proxies from the attacked machines and copies all key files (private and public) from available user home areas.
- Who does what now ?

Walk through the responsibilities

- Cleanup requires:
  - Analysis of how the job was submitted and closing the hole.
    - Rogue user ?
    - Exploit of application hole on target resource ?
    - Stolen user identity ?
    - Stolen proxy ?
    - Hacked submitting machine ?
  - Replacement of hacked machine’s credentials
    - Pretty clearly responsibility of machine owner
  - Replacement of all stolen user credentials
  - Alert (?) of compromised proxies
    - This may be minimized by checks in code that proxies are used by the machine to which they have been delegated.

Walk through the responsibilities

- Identity Issued is Unique
  - Discovered by overlapping namespaces or duplicate identities
  - Resolution left to CAs and enforced by signing policies used by relying parties
- Identity is issued to the appropriate entity
  - How discovered ?
  - Resolved by CAs invalidating misissued credentials (and issuing correct replacements)
- Identity Signing Key is well protected
  - Discovered by report of unauthorized use of Signing Key or discovery of compromised storage
  - Fixed by CA (how and what standards?)
- Compromised identities are revoked
  - Compromises have to be reported (by whom to whom and how ?)
  - How to tell if a revocation has not happened ?
  - Fixed by CAs updating revocation lists
- Entity asserting the identity is authorized to hold the secret
  - Discovered by finding the secret exposed or in possession of unauthorized party
  - Resolution requires interaction with user and certificate issuer. Fixed by
- Proxy has not been stolen
  - Discovered by finding machine compromises or misused proxies.
  - Fixed by custodian of proxy fixing the access hole.