Data Integrity, Confidentiality, Audit, Non-Repudiation

Ron Burback

Lecture 9

Data Integrity

- Is this the same data?
- MD5 checksum, encrypted with the session key
- like a digital signature

Data Confidentiality

- Only the people who need to see the data can.
- DES encryption

Audit

- DCE keeps an audit trail of events
- Any application can send audit events
- DCE services have built in events
  - security
  - time
  - audit
- Need auditd running on same machine

Events, Event Classes

- Every event has a unique 32 bit number
- Events are grouped into classes
  - name
  - 32 bit number

Filters

- Who should be audited?
- What events should be audited?
- What outcome of events should be audited?
- Where will the information be placed?

Filters - Who?

- Principal, foreign principal
- Group, foreign_group
- Cell
- World

Filters - Outcomes

- success
- failure
- denial

Filter - Where

- Alarm
  - print message to the console
- Log
  - write message into the audit file
  - /dcelocal/var/audit/adm/central_trail
    - » file size then wrap
    - » file size then close and start new file
  - write back cache

Security Audit Events

- TGT, PTGT
- ACLs
- Accounts
- Policies
- Registry Master Key
- Secure RPC
- Change in state of the registry

DTS Audit Events

- Service changes
- clock readings
- cell service profiles
- service attributes

“Audit” audit events

- changes in filters
- changes in state

Display Audits

- dcecp> audtrail <*filename*>