XNET and NFS Security

Mike Kupfer

kupfer@Eng.Sun.COM

Connectathon 1998

Overview

- intro to XNET, XNFS
- MOUNT security issue

Who is XNET?

- X/Open + OSF → The Open Group (www.opengroup.org)
- XNET technical group: “communications and networking aspects of Open Systems”
- representatives from Digital, Fujitsu, HP, IBM, Sun, the Software Council...
- Specifications
  - APIs, e.g., Streams
  - protocols, e.g., (X)NFS
  - many on Web
- Test Suites, Branding

XNFS Specification

- more comprehensive than RFCs
- protocols: XDR, RPC, PORTMAP, NFS, MOUNT, NLM, NSM
  - WebNFS optional
- API deltas from UNIX (C and shell) (e.g., ESTALE, uid consistency)
- separate PCNFS spec

XNFS Test Suite

- API tests (e.g., unlink after open)
- protocol tests (e.g., CANCEL of non-existent LOCK)
- interpretations
  - bug in test suite
  - bug in spec
  - gray area in spec

MOUNT Security Issue

- client tries to mount non-existent directory. What should the server return?
- need to avoid security hole where client can probe server using `MOUNT` requests
- spec says:

MNT_EACCES	Indicates that the call failed because access ... was denied. Either no directory in the path... is exported, or the client system is not permitted to mount this directory.
MNT_ENOENT	Indicates that the call failed because the specified directory does not exist. If the server exports only **/a/b**, an attempt to mount **/a/b/c** will fail with ENOENT if the directory does not exist; on the other hand, an attempt to mount **/a/x** would fail with EACCES.

- not a hole if client can mount then do LOOKUPs

Issues

- what about `/a/b/protected/c`?
  - require `ENOENT`? `EACCES`?
  - allow both?
- Any clarifications to spec needed?