MAC Labeling and Enforcement in NFSv4

David P. Quigley
dpquigl@tycho.nsa.gov
National Security Agency
National Information Assurance Research Laboratory
(NIARL)

What's the problem?

- NFSv4 doesn't support MAC labeling
  - Doesn't support fine grained MAC Labels.
  - Can't retrieve underlying labels from server.
  - Can't set underlying labels on server.
  - Can't convey process label on client to server.
  - Overly coarse labeling used to compensate.
- Request from SELinux users for use of SELinux with NFS file servers.

What's the Goal?

NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

- Provide secure labeling functionality for NFSv4.
- Provide mechanisms for managing and spanning DOIs (Domains of Interpretation).
- IETF standardization.
- Adoption by network storage appliances.
- Allow Interoperability with existing NFSv4 clients and servers.
- Support MAC Model and Policy flexibility.

File Label Transport

NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

- New recommended attribute
  - security_attribute
  - Named attributes don't provide necessary semantics.
- UTF-8 encoded string.
- Per file object attribute
- RA format
  - <opaque>@doi
  - Define structure for the opaque blob.

Process Label Transport

NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

- Server needs to know client's process context.
- `PUTCLIENTLABEL_OP` not the answer
- Bind process credentials to RPC session
  - rpcsecgss (v2? Possibly influence v3?)
- Options
  - Create new RPCSECGSS flavors (currently `AUTH_UNIX`)
  - Replicate all existing flavors adding label transport
  - Possibly revive kitten (v3) stackable security pseudo flavors

Label Translation

NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

- Client and server may have different DOIs.
  - different MAC models
  - different policy versions
  - different policy semantic
- Similar to ID -> {g,u}id mapping.
- Administration issues
- Similar model to DNS queries
- Central DOI authority
  - Private range for testing.

Operating Modes (Full)

NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

- Full Mode
  - Server & client are MAC enabled.
  - Server & client each enforce a local policy.
  - Client process credentials used in server access decisions.
  - Initial file labeling
    - Client calculates initial label and sends to server.
    - Server takes calculated label and process label and makes access decision.

Operating Modes (Server Guest)

NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

- Legacy Support
  - No server label support at all.
  - Client enforces local policy.
  - Treats server as a standard NFSv4 server.
  - Uses alternate labeling method (per-mount/per-server).
- Server Guest
  - Server strips doi and stores label.
    - Restricts network configurations.
  - Client enforces local policy.
  - Client may override labeling if server is untrusted.

Operating Modes (Client Guest)

- Client Guest
  - Server enforces local policy.
  - Server may offer services based on certain client properties.
    - Auth credentials
    - Network attributes

Path to Standardization

NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

- Working with IETF NFSv4 Working Group(WG)
  - Published Internet Draft containing requirements.
- Engaging individual WG Members
  - Sun (FMAC & TX)
  - Netapp (Govt Requirements, Linux Implementation)
- Drum up more interest.
- Presenting work at IETF Conferences

What's left to do?

- Continue work on Linux prototype.
  - Mainline kernel integration.
- Start FMAC Implementation
  - Waiting on file-object labeling.
- Work on userspace infrastructure.
  - DOI management and translation infrastructure.
- Work with working group on design document.
- Engage network storage companies.