MAC Labeling and Enforcement in NFSv4

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

System Properties

NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

- MAC Policy Enforced
  - Client/Server
- MAC Security Attribute
  - Per File Object
  - Set on Create
- Process Label Transport
  - Provide secure channel between client and server
  - Compatible with existing flavors.

What's the problem?

NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

- No mechanism for file label transport
  - Inferred from zone (Solaris)
  - Coarsely assigned per mount (Linux)
- No mechanism for process label transport
  - Inferred from connection or zone (Solaris)
  - Uses label of kernel daemon (Linux)

File Label Transport Requirements

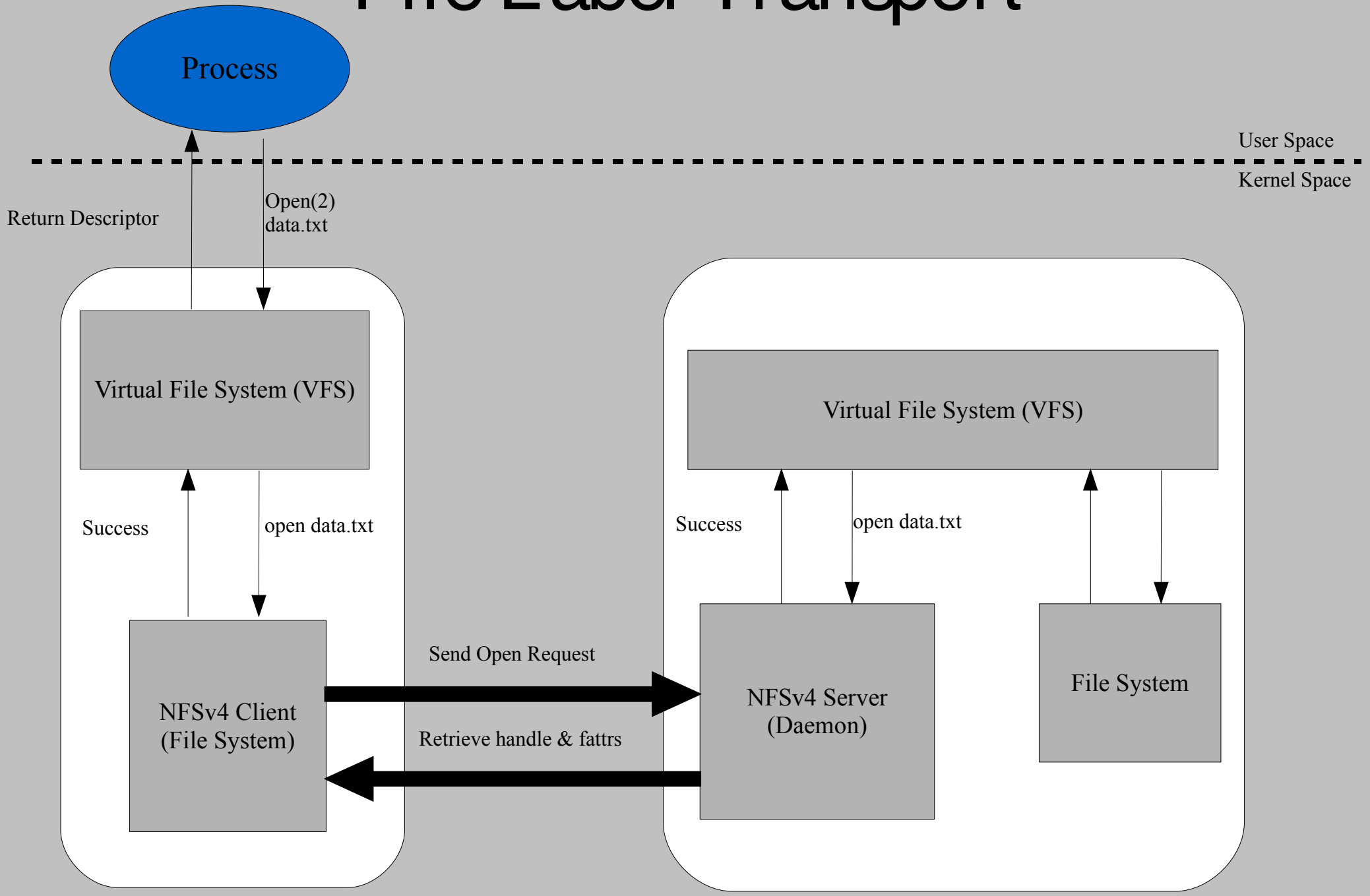
- Needs to
  - Atomically set label on file creation
  - Support setting and retrieving labels on server
  - Support multiple MAC models
  - Finely Grained
- Should
  - Be human readable
  - Support MAC model interoperability

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

File Label Transport



Process Label Transport Requirements

- Needs to
  - Convey context of principal making the request
  - Assure context integrity
  - Bind Client and Host credentials together

Process Label Transport

NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

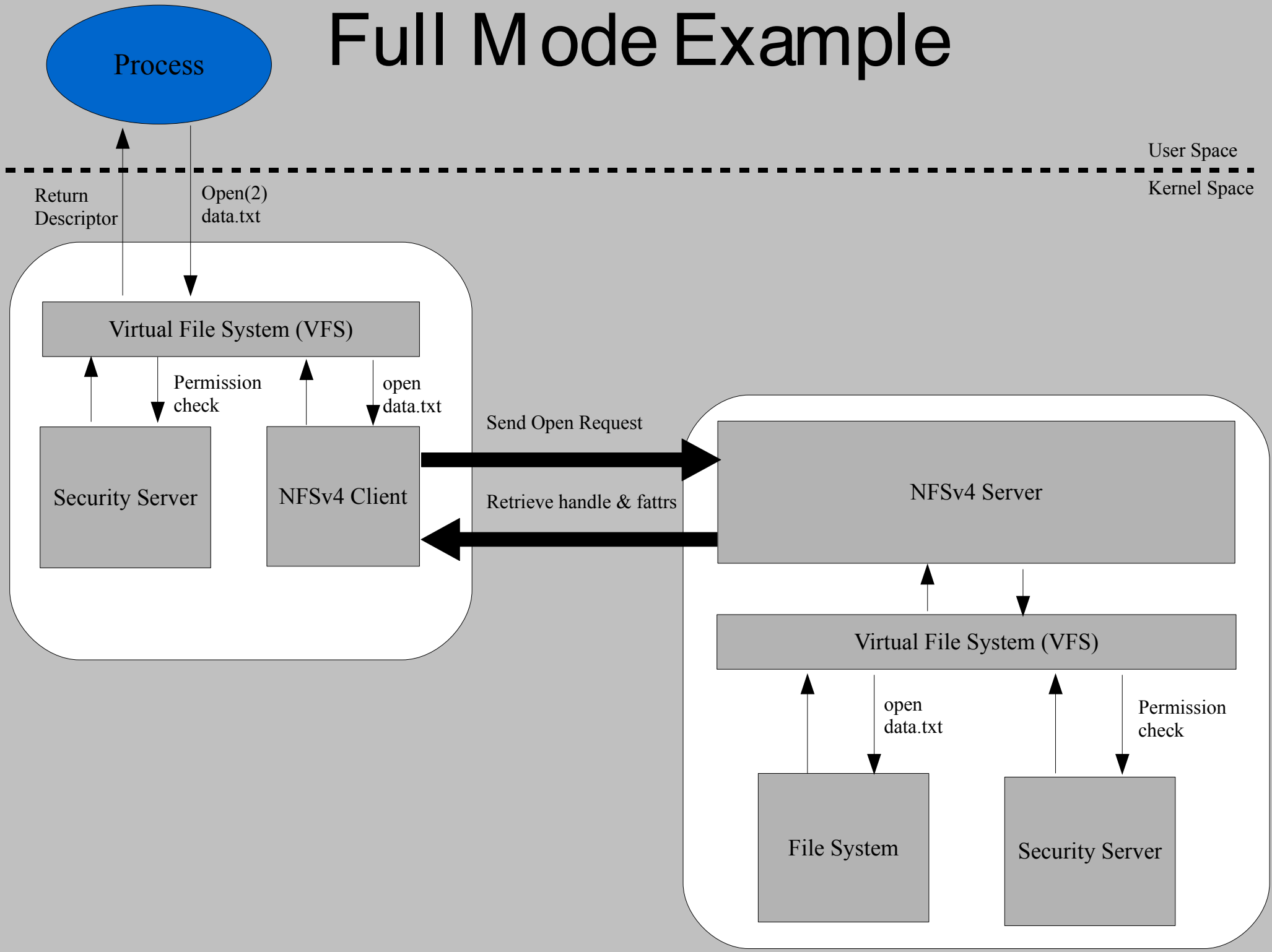
- Extension to RPCSECGSS (new v3)
  - Bind host and client credentials into new cred.
  - Doesn't require changes to underlying mechanisms
  - Eases channel binding
  - Provides access control information integrity
  - Prevents Kerberos MITM attack

Operating Modes (Full)

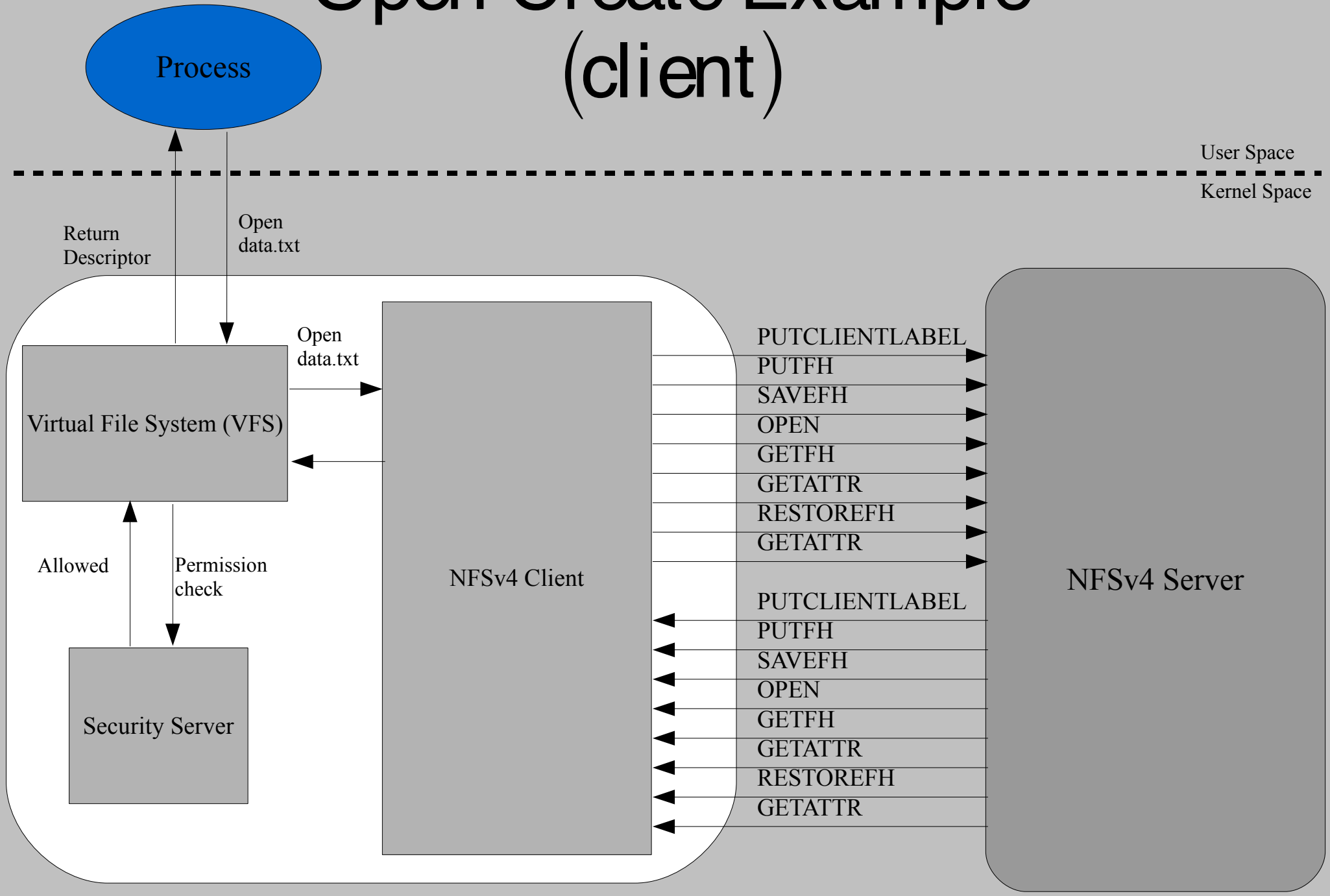
NATIONAL INFORMATION ASSURANCE RESEARCH LABORATORY

- Full Mode
  - Server & client are MAC enabled.
  - Server & client each enforce a local policy.
  - Requesting principal credentials used in server access decisions.

Full Mode Example



Open Create Example (client)



Open Create Example (server)