Labeled NFS Review

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

The Goal

To provide a mechanism to allow for robust security mechanisms to be built with NFSv4 as the remote file system capability while leveraging network storage appliances

Documents

- Requirements document
    - draft-quigley-nfsv4-sec-label-requirements-02.txt
- MAC Attribute Specification Document
    - draft-quigley-nfsv4-sec-label-01.txt
- RPCSECGSSv3
    - draft-williams-rpcsecgssv3-00.txt
- Impact Study
    - draft-quigley-nfsv4-lnfs-impact-00.txt
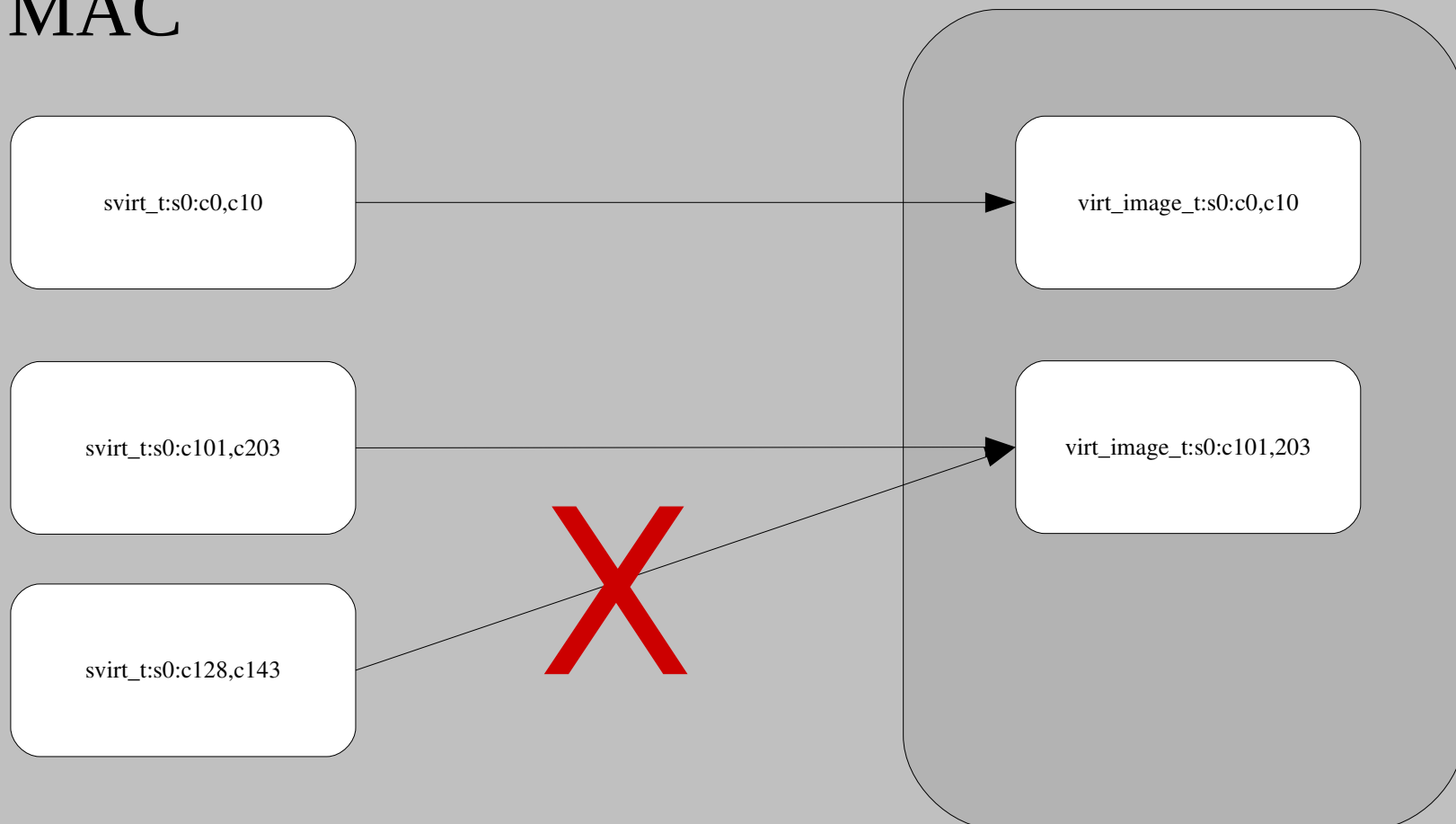
Impact Study
(Use Cases)

- SVirt

- Build Environments/Simple Storage

- Compliance

SVirt

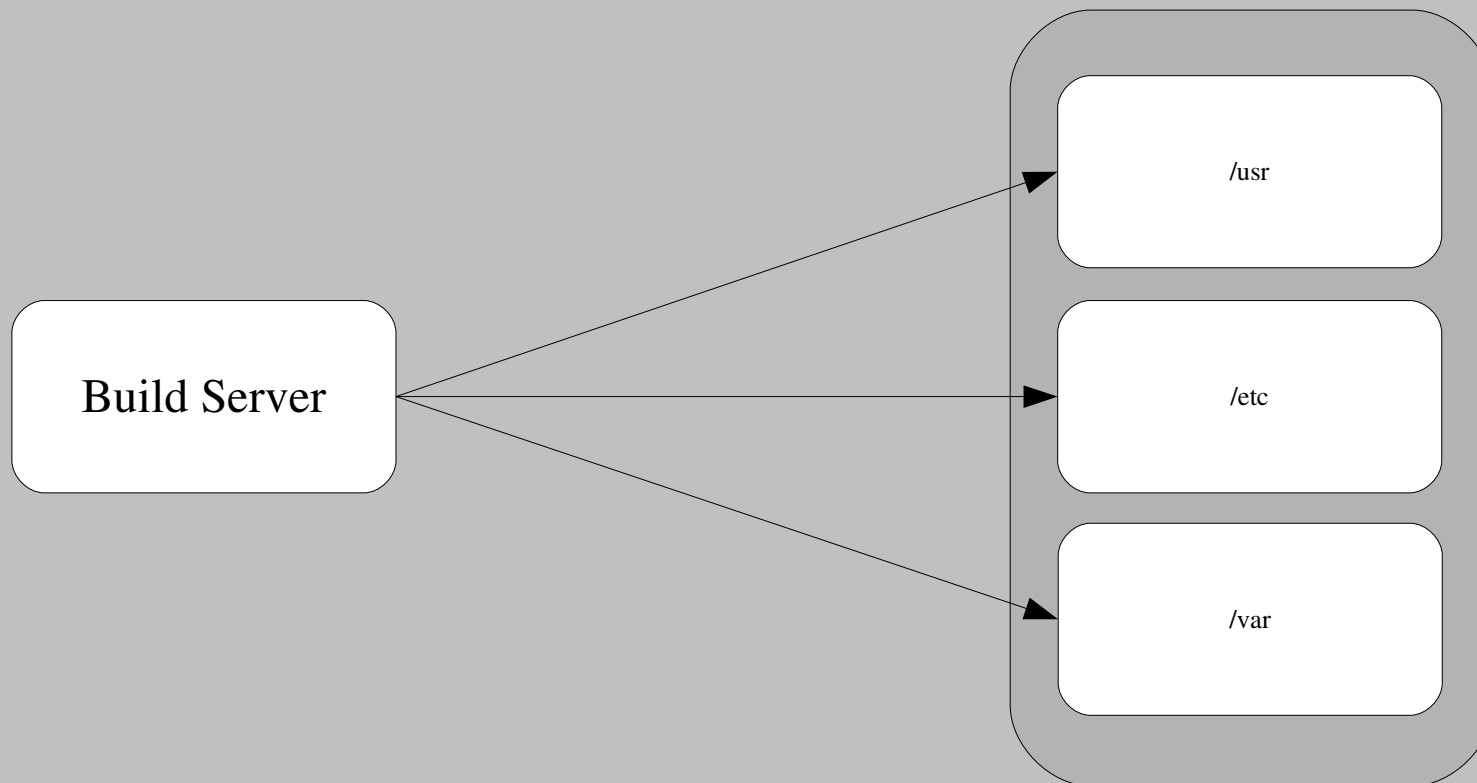- Enable isolation of VMs/Qemu instances using MAC

svirt_t:s0:c0,c10 → virt_image_t:s0:c0,c10
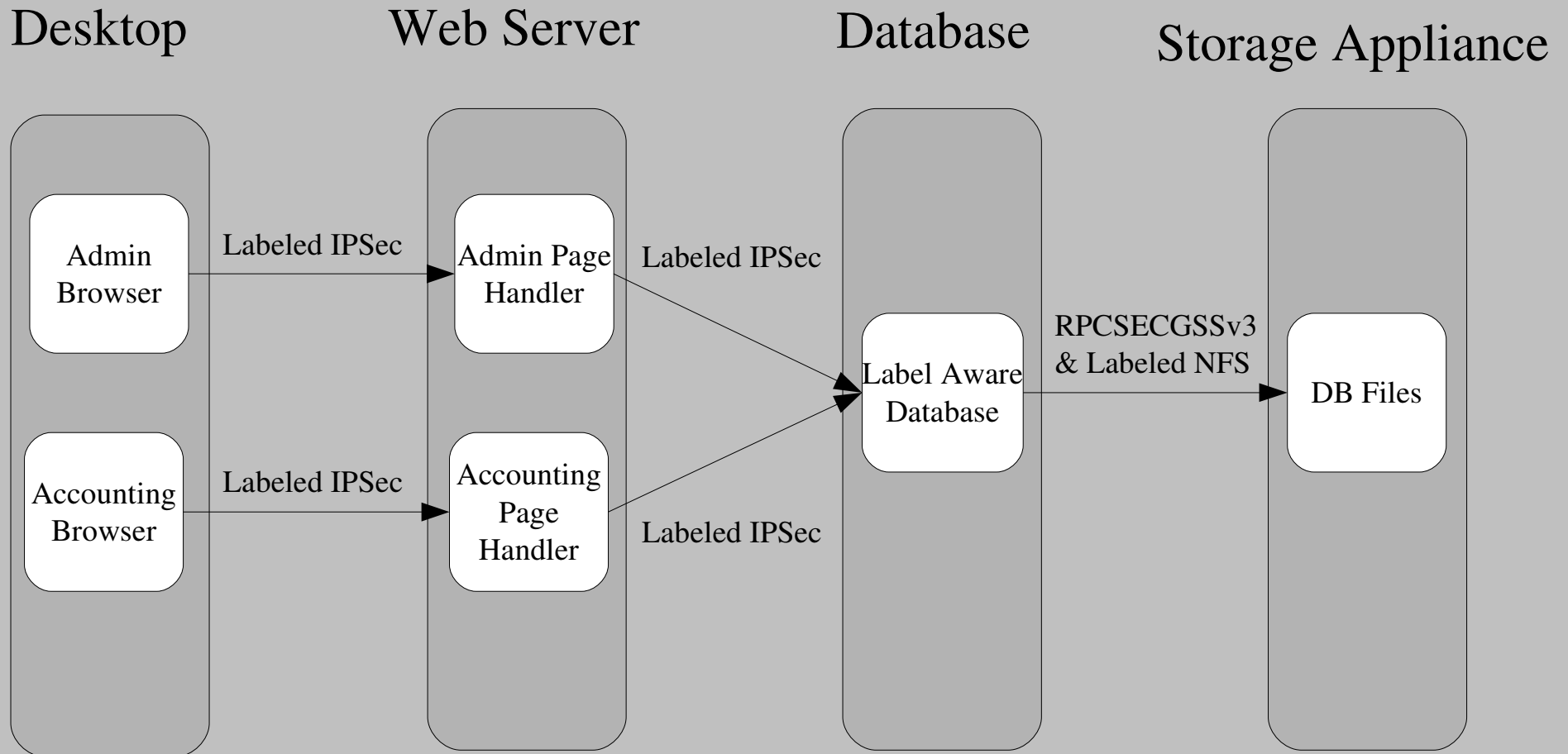
svirt_t:s0:c101,c203 → virt_image_t:s0:c101,203

svirt_t:s0:c128,c143 ✗ virt_image_t:s0:c101,203

Build Environments /Simple Storage

- Build server compiles and ensure proper labels
- Clients retrieve and set security labels

Compliance

Desktop	Web Server	Database	Storage Appliance

Admin Browser → Labeled IPSec → Admin Page Handler → Labeled IPSec → Label Aware Database → RPCSECGSSv3 & Labeled NFS → DB Files

Accounting Browser → Labeled IPSec → Accounting Page Handler → Labeled IPSec → Label Aware Database

Impact Study
(Protocol Impact)

- New Recommended Attribute

  – Per file attribute (sec_label)

  – Provides labeling on files

  – Consists of label format specifier & data

- RPCSECGSSv3

  – Uses existing RPCSECGSS version 1 and 2 implementations

  – Allows clients to assert security information for operations on each context

Impact Study (Dependencies)

- RPCSECGSSv3
  - Originally proposed by Nico Williams
  - Dave Quigley offered to Co-Author
  - Work on prototype will begin soon
- LFS Document
  - Originally proposed by Dave Quigley
  - Currently being written

Questions?