XDR / SECINFO / CCM
NFSv4 Interim WG Meeting
Ann Arbor

Mike Eisler
Network Appliance, Inc.
mike@eisler.com
June 4, 2003

XDR - draft-ietf-nfsv4-rfc1832bis-01.txt

- XDR is currently at Draft Standard
- Desire is advance to full Standard
- New I-D adds IANA Considerations and ISOC Copyright as prerequisites for advancement
- Currently in WG Last Call
  - Issues so far include a typo in intro and “int” not being listed as a reserved keyword

SECINFO - draft-ietf-nfsv4-secinfo-00.txt

- In NFSv4.0, SECINFO is used to negotiate security flavor (e.g. AUTH_SYS, krb5), but has issues, due to the calling convention of { filehandle, component name}
  - No way to negotiate the initial security to be used for mounting the root or public filehandles of the server
  - No way to negotiate the security used for accessing parent directory

SECINFO (continued)

- I-D proposes adding a SECINFO_NO_NAME operation that supplements SECINFO
- SECINFO_NO_NAME takes no component name, and instead refers to the current filehandle or the parent directory of the current filehandle (depending on a style discriminator)
- Next step: SECINFO extensions should be basis of NFSv4.1 document.

CCM - draft-ietf-nfsv4-ccm-01.txt

- CCM: Same abbreviation, but now stands for Channel Conjunction Mechanism for GSS
- Co-authored by Nico Williams & Mike Eisler

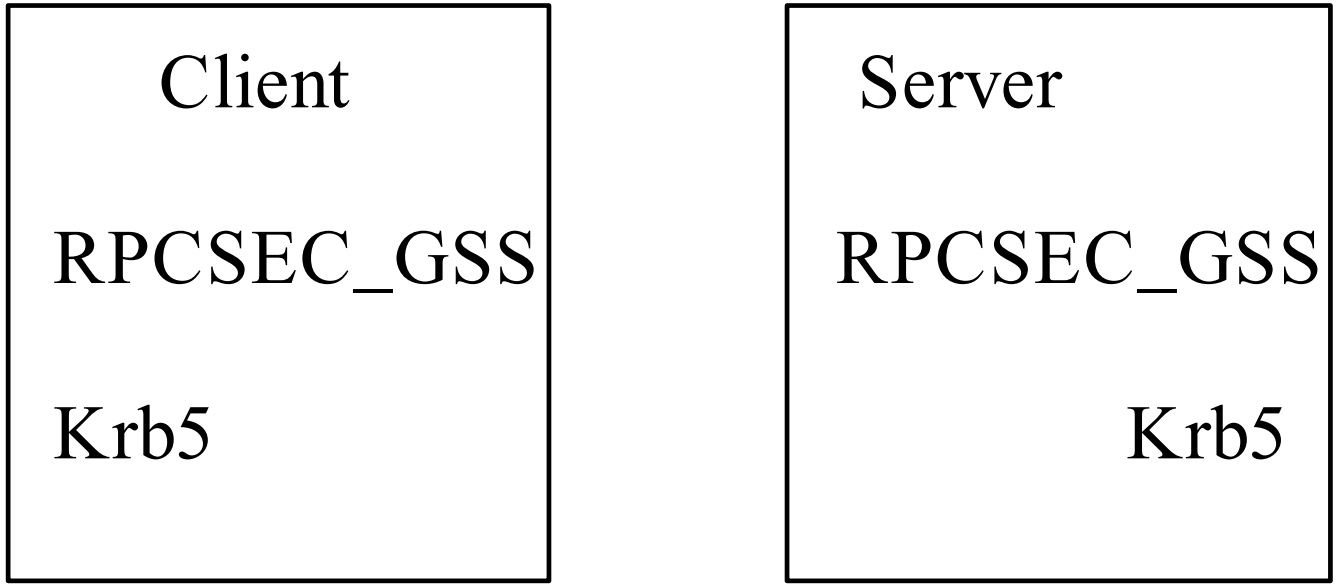
CCM: The Looming Problem

- The current NFS security model relies on RPC layer for data integrity, encryption, and authentication on each RPC round trip
- Encryption is fundamentally CPU bound
- Network media data speed accelerating faster than Moore's Law's acceleration of CPU speed

CCM: The Looming Problem (cont'd)

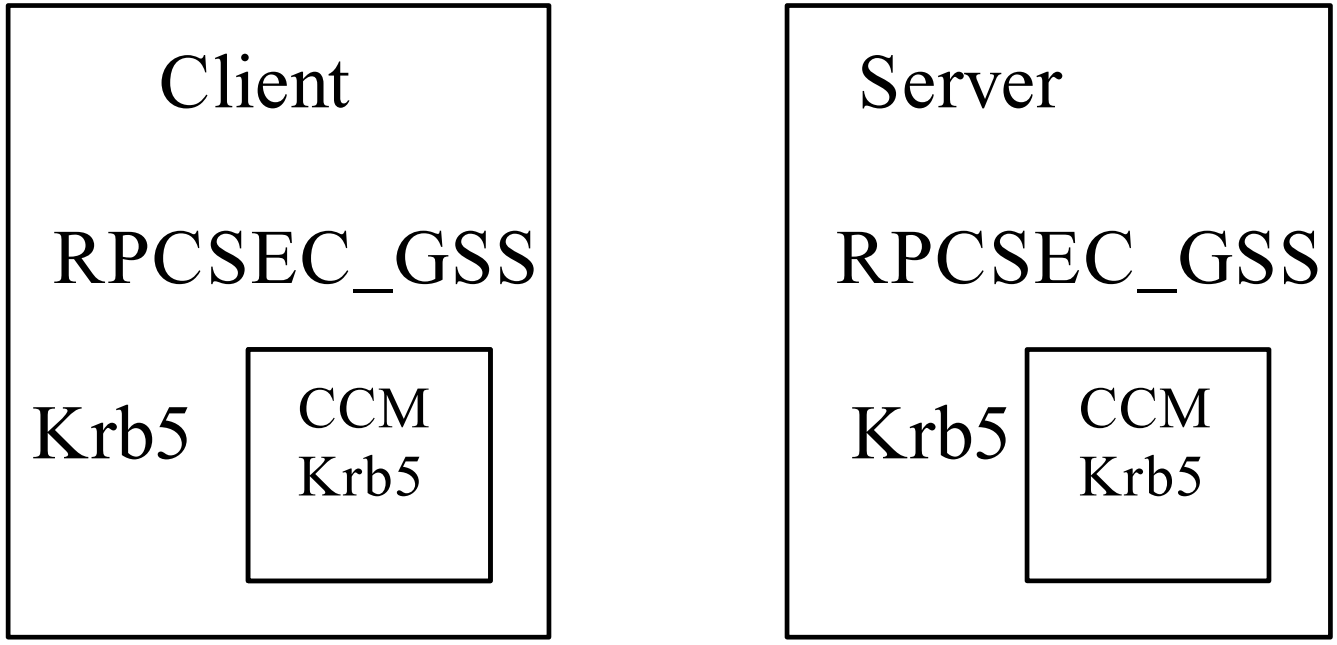
- Therefore, software crypto and fast network media are mutually exclusive
- Hardware-accelerated crypto for RPC layer is possible but not likely
- Whereas, hardware accelerated crypto for IPsec and TLS is becoming off the shelf

CCM Explained - Conventional NFS Security



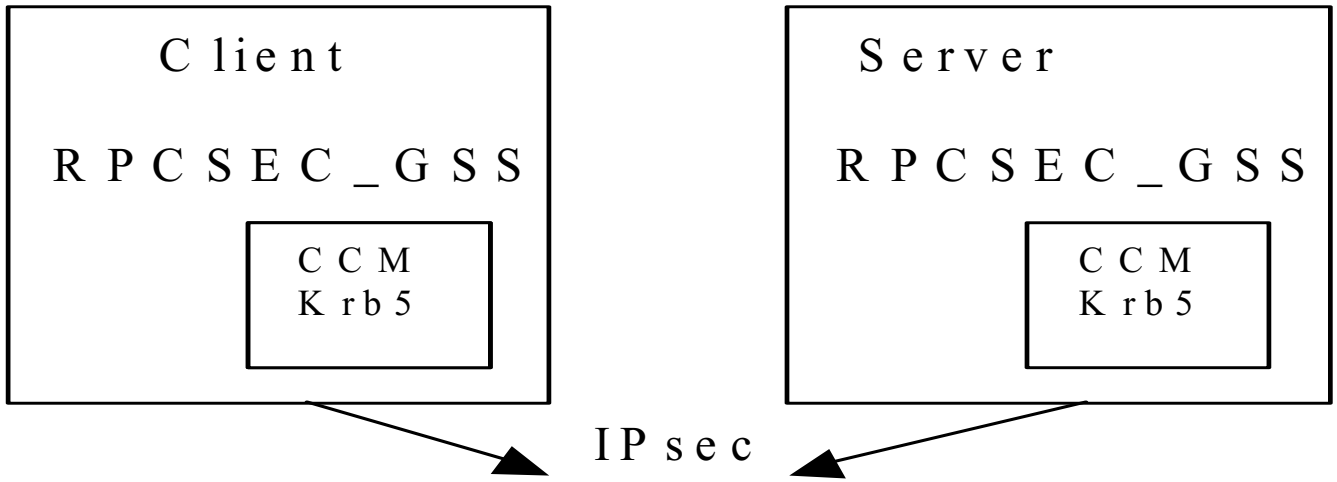
Conventional NFS/RPCSEC_GSS with Kerberos V5 – crypto penalty per round trip

CCM Explained - Add CCM Mechanism



NFS/RPCSEC_GSS with Kerberos V5 and CCM wrapper

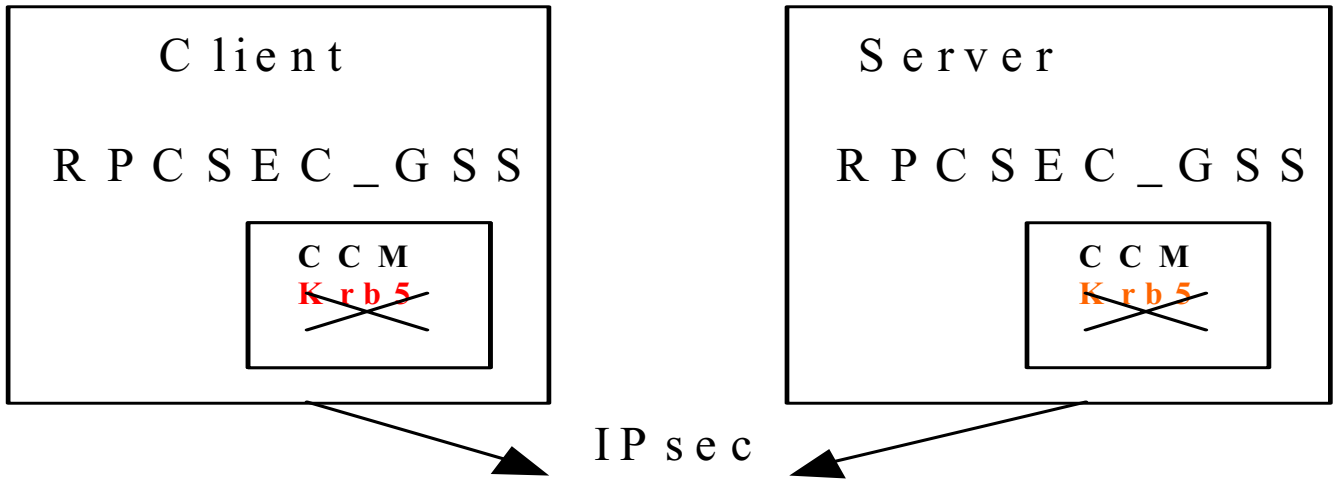
CCM Explained - Authentication Step



Step 1: Client and server agree that per-RPC crypto not needed (e.g. connection protected with IPsec).

Step 2: Client and server invoke CCM which invokes Krb5 GSS mechanism to create Kerberos V5 context (RPCSEC_GSS context creation phase). User on client now authenticated to NFS server (and vice versa).

CCM Explained - Steady State



Step 3. RPCSEC_GSS invokes CCM's GSS_GetMIC() (digital signing) routine to checksum RPC header.

Step 4. CCM's GSS_GetMIC sidesteps Kerberos V5 in favor of a null operation.

Step 5. IPsec below RPC/TCP integrity protects traffic, so security is as good (better since entire payload is protected) than with conventional RPCSEC_GSS

CCM: Changes from version -00

- Channel bindings formalized as part of specification
  - Channel bindings are a way to prevent man in the middle (MITM) attacks
  - In GSS, channel bindings are created by the client and server, which exchange ***signed*** information about the channel. E.g.
    - source and destination IP address
    - one way hash of IPsec session key

CCM: Channel Bindings

- Channel bindings expressed as three separate CCM mechanisms: CCM-NULL, CCM-ADDR, CCM-KEY
- CCM-KEY requires extensions to existing socket APIs
- CCM-ADDR useless in environments with Network Address Translation
- CCM-NULL is thus the least common denominator: no channel bindings

CCM and NFSv4.1

- WG consensus is that CCM security is a work item for NFSv4.1
- WG consensus appears to be for NFSv4.1 to RECOMMEND CCM-KEY and CCM-NULL
- Decision for making promoting CCM-KEY to MUST deferred to NFSv4.2

CCM: Next Steps

- Finalize TLS, SSH, and IPsec channel bindings (get input from domain experts)
- Interested implementers should start talking to their IPsec stack implementers to plan for CCM integration
- Fix I-D to address issues raised by Martin Rex (CCM as specified is not quite GSS compliant, but is easily fixed)
- Specify the use of CCM in NFSv4.1