RPC-on-TLS

Next Steps

Chuck Lever
<chuck.lever@oracle.com>
Goals of RPC-on-TLS

• Increase the deployment rate of NFS with encryption

  • Make it significantly simpler for administrators to deploy NFS with privacy and data integrity

• Reduce the performance cost of using privacy

• Improve security of NFS with AUTH_SYS, which is still widely deployed
Primary Benefits

- **In-transit privacy** When a server possesses a certificate, clients can authenticate servers, and can enable transport layer encryption

- **Machine authentication** When each client possesses a certificate, servers can authenticate clients to determine whether:
  - A client may have access to an export, or
  - A client’s AUTH_SYS user identities are trustworthy
Secondary Benefits

- Channel security protects the whole data stream rather than a portion of each RPC message.
- Hardware offload of encryption is enabled.
- User identities can be administered independently of machine identities – combination of GSS, SYS, certs, etc.
- Eventually support transports that have in-built encryption and machine authentication capabilities; e.g., QUIC.
Current Prototypes

- DESY prototype of NFSv4 client and server (complete)
- Linux kernel NFS client and server prototype (in progress)
Future Work

• A new document that details of NFSv4 operation on RPC-on-TLS
  • Possibly bind the lease management credential with the transport credential

• A new document that specifies an RPC-on-QUIC transport
  • QUIC has TLS built into the transport
Next Steps

• Add a charter milestone including a delivery date target

• Review by other area experts or another SecDir review

• Further detail regarding machine authentication

• More text focusing on weaknesses of AUTH_SYS and how they are to be addressed

• Present a threat model and security analysis