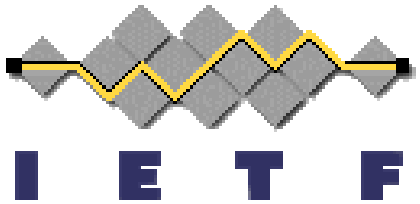
NFS Version 4 Security

Mike Eisler

mre@Eng.Sun.Com

43rd IETF
Orlando
December 7-11, 1998



NFS Version 4 Working Group

NFS Version 2 and Version 3 Security

Existing implementations of NFS provide inadequate security

- NFS relies on ONC RPC to provide security
- AUTH_SYS is trivial to exploit
- AUTH_DES is trivial to exploit by someone with a degree in Mathematics
- AUTH_KERB is better, but it isn't standard
    - No written specification to refer to.
    - Like AUTH_SYS, AUTH_DES, there is no integrity or privacy protection.

To address RPC security, IETF's ONCRPC working group developed RPCSEC_GSS:

- RFC 2203
- Proposed Standard
- Adds integrity and privacy in addition to authentication
- An abstraction over GSS-API

RPCSEC_GSS and NFS Version 2 and Version 3

Sun is modifying its NFS implementation to use RPCSEC_GSS

- First plug in is Kerberos V5
- Code is in beta test
- Published specification of NFS V2 and V3 over RPCSEC_GSS/GSS-API/Kerberos V5:
  - http://search.ietf.org/internet-drafts/draft-eisler-nfssec-02.txt
  - Proposed to IESG as an Informational RFC (decision due January, 1999)

Security for NFS Version 4

It is believed that IESG will not accept NFS V4 on the standards track unless it has a security model of NFS V4 that addresses:

- Mandatory set of security mechanisms
- Secure negotiation of security mechanisms
- Strong authentication, integrity, and privacy

The NFS V4 Straw Man and Requirements drafts propose:

- RPCSEC_GSS
- Kerberos V5 as one mandatory mechanism
- A secure negotiation scheme built into the protocol
- Strong authentication

Security for NFS Version 4 (continued)

The Straw Man/Requirements leave as open issues:

- Additional mandatory security mechanisms, i.e. public key certificate based
  - SPKM
  - Globus project (www.globus.org/security) has a GSS-API plug-in that uses the SSLeay code.

The Requirements document lists privacy and integrity as SHOULDs, not MUSTs.

- Given the ONC RPC experience with IESG, this seems doomed to fail.
- This needs to be addressed, either within the NFS V4 protocol, RPCSEC_GSS, some other external means, or mandate IPSEC.

Issues raised by the working group

Is RPCSEC_GSS a standard?

- RFC 2203 is a proposed standard. Very few RFCs are Standards, and there is nothing comparable to RPCSEC_GSS that is a Standard.

SSL should be *the* security method or *one* of the security methods.

- SSL won't work over connectionless protocols like UDP. The WG seems to want to use UDP.
- How does one design something that might use SSL authentication, and RPC authentication?

What's the user experience when using something like Kerberos V5 with NFS?

- Existence proof is AFS and www.connectathon.org/talks97/eisler1.ps

Meaning of "Required Security Mechanisms"

- NFS V4 clients and servers MUST provide them, though one would be free to configure something weaker.
- Negotiation MUST never use a weak mechanism.

Recommendations

- Pursue the Globus model for a public key solution
- State that integrity and privacy are requirements
- Decide if we are using RPCSEC_GSS or not
  - It can take years to construct security architectures for protocols (e.g. IPSEC, NFS V2/V3)
  - RPCSEC_GSS if anything is expedient
  - SSL protocol based security can be OPTIONAL if anyone can figure out how to do it.