SEAM: Sun Enterprise Authentication Mechanism (Kerberos V5 for Solaris and Solaris NFS)

Mike Eisler
Sun Microsystems
mre@eng.sun.com

Connectathon, 1999
San Jose, CA

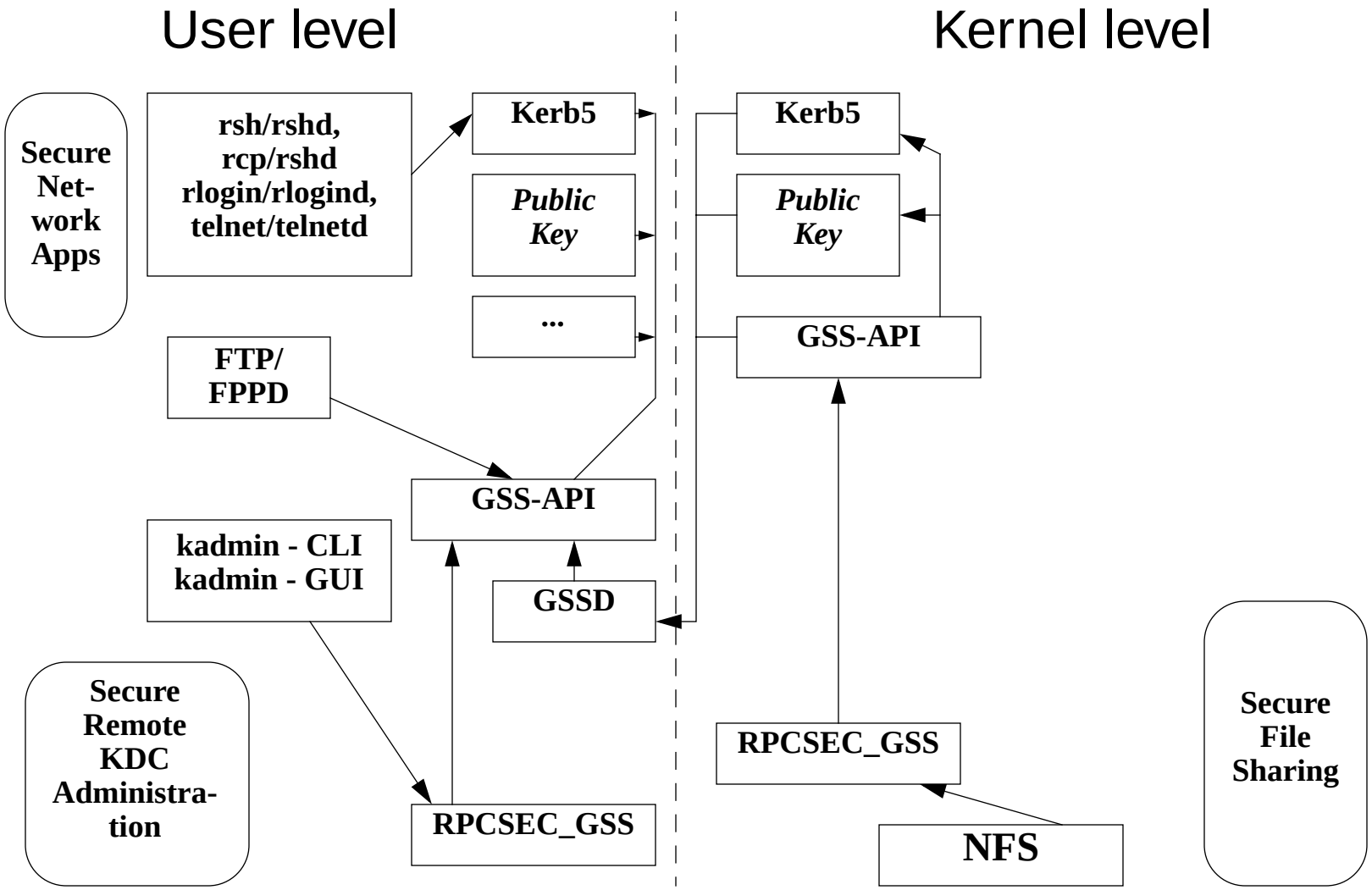
Overview

- Description of SEAM
- Multi-vendor support for the security architecture behind SEAM
- Export Control Update
- Performance Update
- How to get started

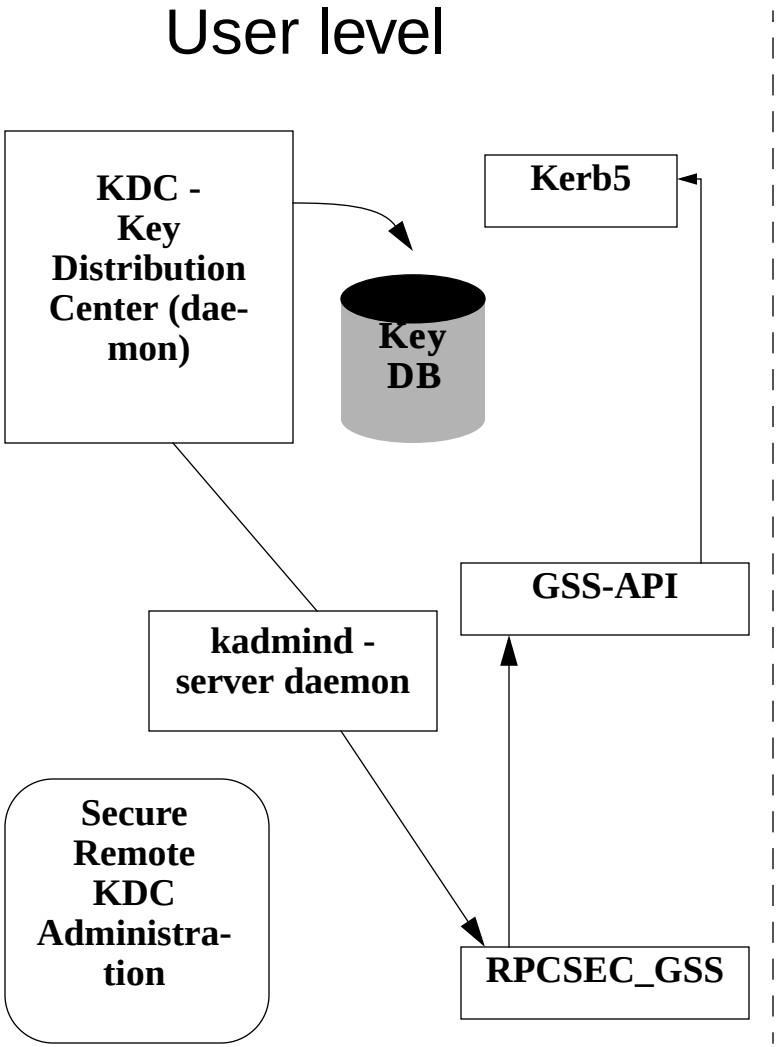
Description of SEAM

- **At previous Connectathons - 1995, 1996, 1997, 1998 - we've presented an architecture for Kerberos V5 security for NFS using the Generic Security Services API (GSS-API).**
  - SEAM is the productization of the 1998 Solaris NFS Security talk
  - http://www.connectathon.org/talks98/security.html
  - it also includes Kerberized:
    - **rlogin/rlogind**
    - **rsh/rshd**
    - **rcp/rshd**
    - **telnet/telnetd**
  - includes GSS-API-ized:
    - **ftp/ftpd**

SEAM Architecture - Client node



SEAM Architecture - KDC node



Multi-vendor Support

- **At the 1999 NFS Vendors' Conference two NFS vendors voiced their intent to interoperate with SEAM.**

Export Control Update

- **On December 31, 1998, Clinton Administration announced new regulations that relaxed controls of 56 bit DES encryption used for privacy.**
  - Exportable to all but the 7 countries identified as terrorist regimes
  - These rules do not require reporting (MASS MARKET - TSU classification).
- **SEAM is now approved for export under the MASS MARKET TSU countries.**

Performance Update

Last year:

- CLIENT - single CPU 170 Mhz Ultra
- SERVER - two CPU 200 Mhz Ultra/2
- Network - 10baseT

50MB NFS copy (mkfile command) to server degradation relative to AUTH_SYS:

authentication	integrity	privacy
0%	1.89%	27.4%

MD5 for integrity
DES 56 bit for privacy
NFS Version 3
NFS over TCP

Performance Update

This year:

- CLIENT - single CPU 270 Mhz Ultra 5, 128 MB RAM
- SERVER - single CPU 270 Mhz Ultra 5, 128 MB RAM
- Network - 100baseT
- 200MB NFS copy (mkfile command) to server's tmpfs file system
- NFS Version 3
- NFS over TCP

Performance Update

Security Flavor	Throughput (megabytes per second)	Throughput degradation relative to AUTH_SYS	CPU utilization on server (percentage used)
AUTH_SYS	5.40	N/A	69%
Kerberos V5 - just authentication	5.26	2.6%	70%
Kerberos V5 - with integrity (MD5)	4.44	17.7%	77%
Kerberos V5 - with privacy & integrity (56 bit DES/MD5)	1.45	73.1%	99% (more likely 100% pegged)

Implementors: How to Get Started

Technology	Specification	Source Code
NFS over RPCSEC_GSS	http://www.ietf.org/internet-drafts/draft-ietf-nfsv4-nfssec-00.txt	ONC+ source product
RPCSEC_GSS	RFC 2203	• **ONC+ source product** • **AUTH_GSSAPI code in MIT Kerberos V5 1.0 source code can be used as a hint to convert to RFC 2203. http://web.mit.edu/network/kerberos-form.html**
GSS-API	RFC 2078	MIT Kerberos V5 1.0 source code
Kerberos V5	RFC 1510 RFC 1964	MIT Kerberos V5 1.0 source code