SEAM - Windows 2000

Interoperability Testing

Ram Marti

Sun Microsystems, Inc

rammarti@eng.sun.com

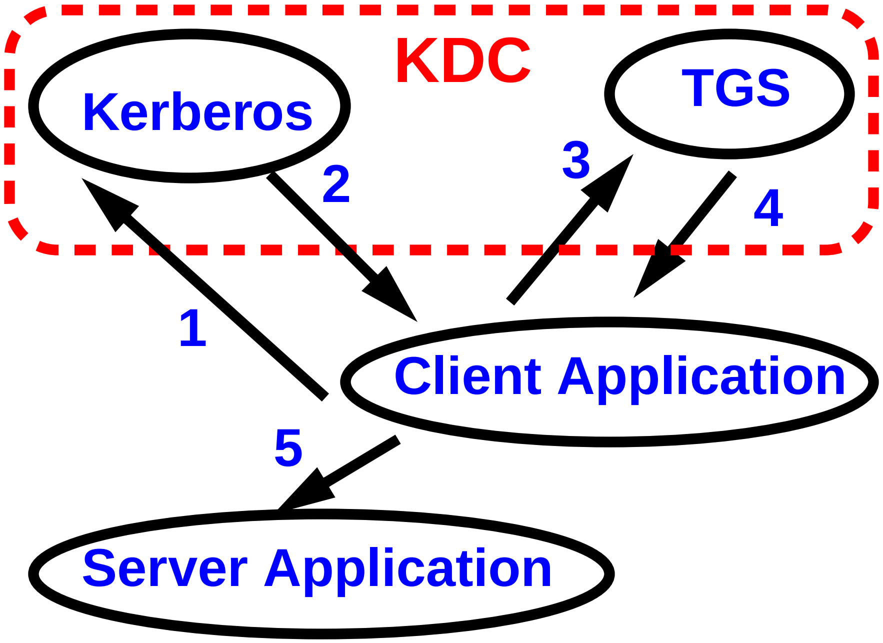
Goals

- Verify Kerberos V5 interoperability
  - Conformance to RFC 1510
- Verify GSS Interoperability
  - Conformance to RFC 2078 (now obsoleted by RFC2743)
- Verify Kerberos V5 plug-in for GSS
  - Conformance to RFC1964

Non Goals

- Active Directory Testing
- Windows 2000 proprietary extensions to Kerberos Protocols are not tested.
  - pkinit integrating Public Key with initial Kerberos authentication
  - KDC location using DNS SRV records
  - KDC “chaining”

Kerberos V5 Protocol



1. Request for Ticket Granting Ticket (in the clear) to Kerberos Authentication Server
2. Session Key (encrypted with client’s secret key) for client to TGS session plus TGT (encrypted with TGS’ secret key)
3. Request for service ticket: client id (encrypted with session key from step 2) plus encrypted TGT from step 2 plus server id
4. Key (encrypted with session key from step 2) for client/server session plus server ticket (encrypted with server’s secret key)
5. Request to server: client id (encrypted with session key from step 4) plus encrypted ticket from step 4

Gross Over Simplification

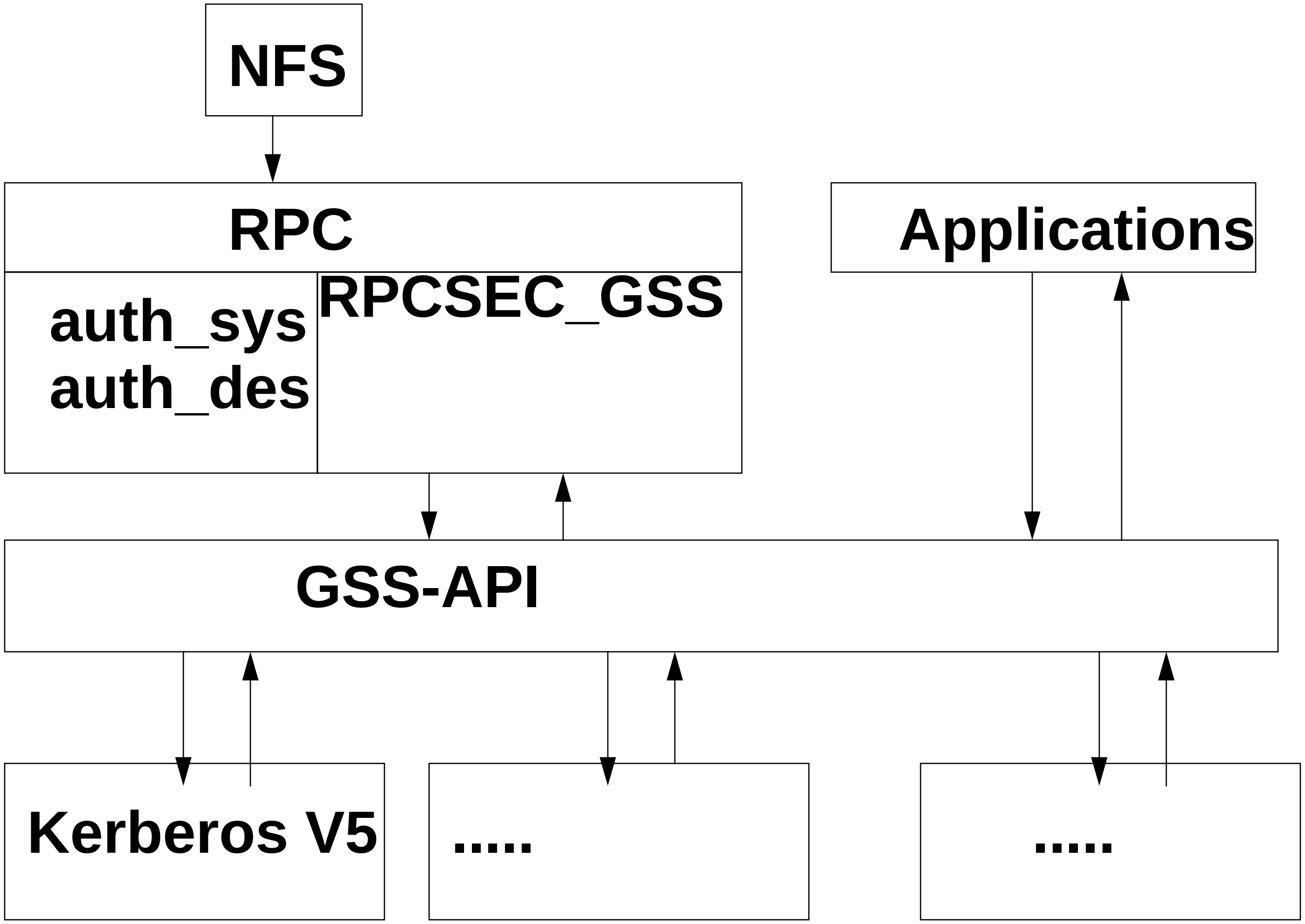
GSS-API in a Nutshell

- Stands for Generic Security Service API
- Applications using GSS-API can operate over a wide variety of security mechanisms - public-key based or shared private key
- Security identities are represented as credentials: servers and clients both have credentials
- Contexts are established between peers after handshake
- Integrity and privacy can be per message basis
- Each security mechanism defines token formats, protocols and procedures to implement GSS-API services

Sun Enterprise Authentication Mechanism (SEAM)

- **Sun's implementation of Kerberos V5, GSS-API and RPCSEC-GSS**
- **But that is not all - you also get the following:**
  - **Database administration programs (local and remote) and propagation software**
  - **Kerberized Applications: NFS, ftp, telnet, rlogin, rcp and rsh**
  - **Java Based GUI Admin tool**
  - **Kerberos integrated with PAM**
  - **Kernel modifications for better performance**
  - **gsscred utility and gssd daemon for mapping security principal names to uid and gid**
  - **Available for Solaris 2.6, Solaris 7 and Solaris 8**

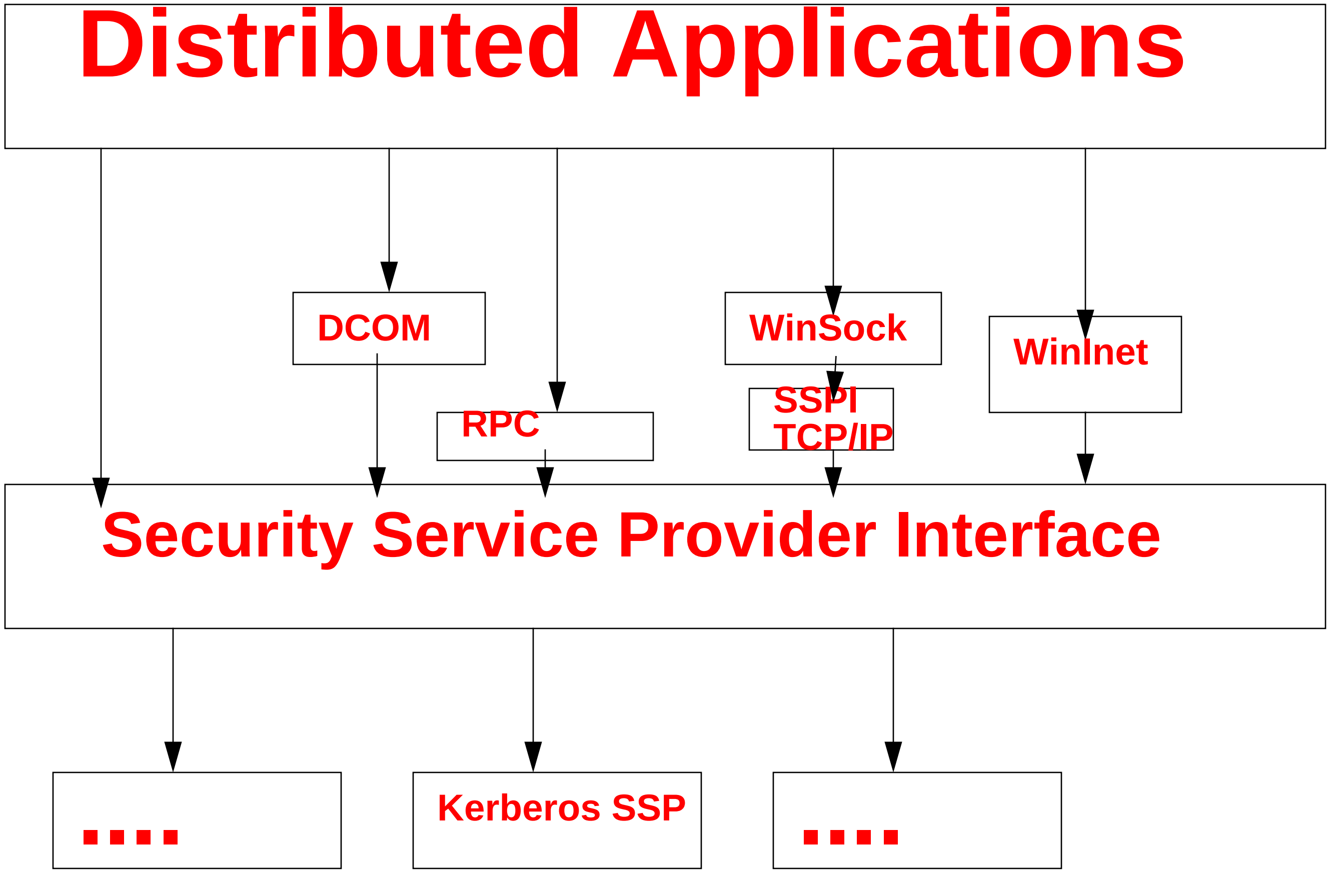
SEAM Overview



Overview of SSPI

- **Security Service Provider Interface (SSPI) is Windows interface between transport level applications and network security service providers**
- **Supports GSS-API wire protocol**
- **Does not provide GSS-API**
- **Instead SSPI APIs are to be used**
- **Supports mutual authentication, replay detection, message integrity and confidentiality**
- **Servers can impersonate a client**
  - **ImpersonateSecurityContext,RevertSecurityContext**

Overview of SSPI (cont)



Overview of Kerberos on W2K

- **Implemented as an SSPI plug-in**
- **RFC1510 and RFC1964 compliant**
- **Kerberos Realm = DNS Domain = NT Domain**
- **KDC located on every domain controller**
- **Client can determine KDC by querying DNS for SRV resource records**
- **Windows 2000 DC can be a KDC for RFC1510 compliant clients**
- **Windows 2000 Clients can use RFC1510 compliant server with single sign-on to Windows 2000 workstation account**

Overview of Kerberos on W2K (Cont)

- **Command line tools provided for configuration:**
  - **ksetup -> For a Win2000 machine to locate non-Windows KDC**
  - **ktpass -> For generating keytab files for services that will use Windows 2000 KDC**
  - **netdom -> For establishing/managing trust of the Win2000 half of the interoperable Kerberos realm**
  - **klist -> for listing Kerberos tickets**
- **These tools are part of Windows 2000 Resource Kit**

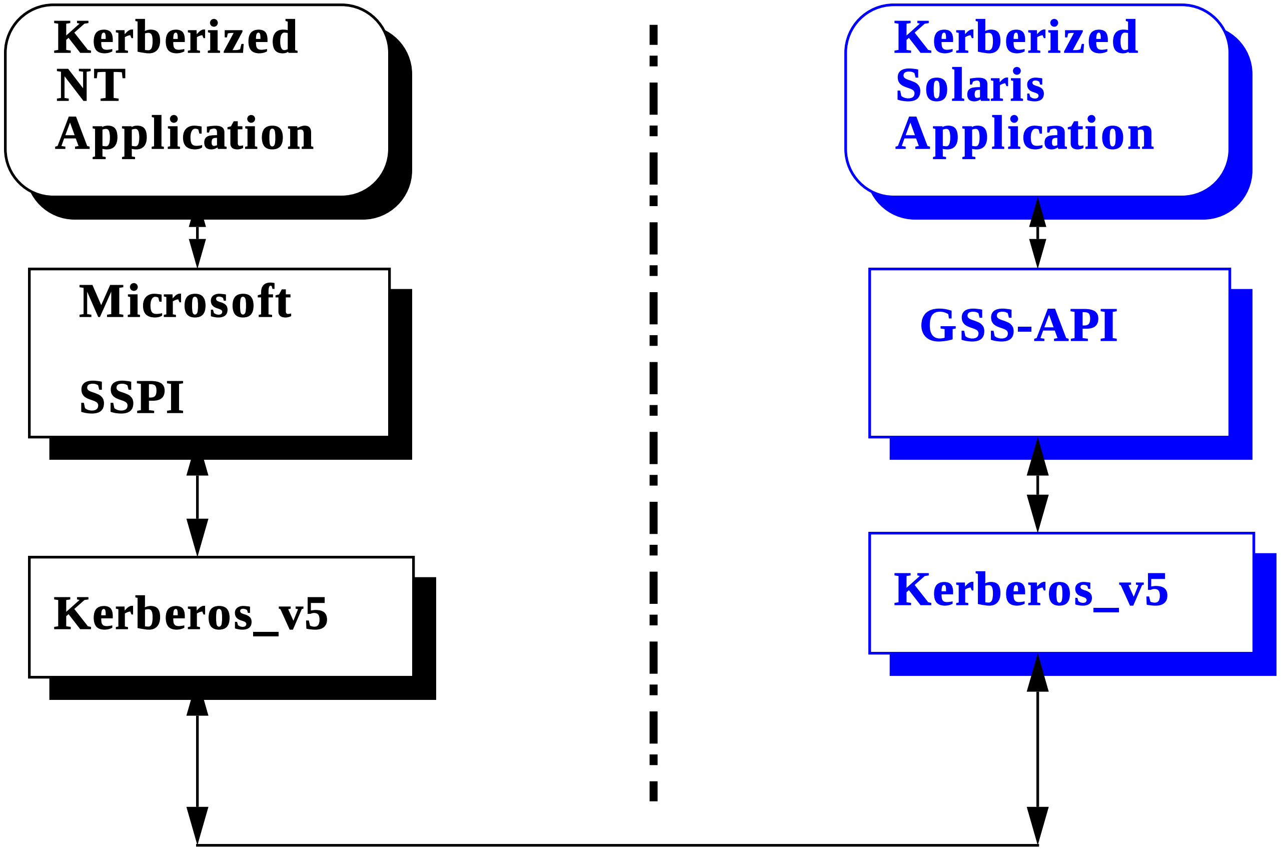
Windows 2000 Kerberos Limitations

- Uses Authorization header to return a list of Security Identifiers (SIDs)
  - SIDs are returned in AS Reply, TGT
  - Used in Service ticket so that the server can implement access controls.
  - Not compatible with OSF-DCE’s Privilege Attribute Certificates
  - Not understood by non-Windows clients
- Hierarchical realm support for non-Windows Kerberos realms is not supported
- Only DES-CBC-MD5 and DES-CBC-CRC supported
- kpasswd does not work with non-Windows KDC

Tests

- Active Directory is the only Kerberized application on Windows 2000
- NFS, ftp, telnet and r* are the only Kerberized applications on SEAM
- So we have to use sample gss-client and gss-server programs to verify interoperability
- Sample SSPI Client and SSPI server are available in Microsoft's Windows 2000 SDK
- SSPI Client and Server programs have the GSS-API calls replaced by equivalent SSPI calls

GSS Application Interoperability



References

[1] The Kerberos Network Authentication Service (V5)
ftp://ftp.isi.edu/in-notes/rfc1510.txt
[2] Generic Security Service Application Program Interface, Version 2
ftp://ftp.isi.edu/in-notes/rfc2743.txt
[3] The Kerberos Version 5 GSS-API Mechanism
ftp://ftp.isi.edu/in-notes/rfc1964.txt
[4] RPCSEC_GSS Protocol Specification
ftp://ftp.isi.edu/in-notes/rfc2203.txt
[5] Sun Enterprise Authentication Mechanism Guide
http://docs.sun.com:80/ab2/coll.384.1/SEAM
[6] Sun Enterprise Authentication Mechanism 1.0 Interoperability Notes
http://www.connectathon.org/seam1.0
[7] Windows 2000 Kerberos Authentication
http://www.microsoft.com/windows2000/library/howitworks/security/kerberos.asp
[8] Windows 2000 Kerberos Interoperability
http://www.microsoft.com/windows2000/library/howitworks/security/kerbint.asp
[9] Microsoft "embraces and extends" Kerberos V5 by Theodore Ts’o
http://www.usenix.org/publications/login/1997-11/embraces.html