z/OS V1R9
Network Authentication Service Update

Session 09

Prepared by Patrick Kappeler
IBM Consulting IT Specialist
kappeler@fr.ibm.com

Redbooks
International Technical Support Organization

z Security Update

Trademarks

See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- A Few Words On Kerberos
- A Few Words On GSS-API
- Kerberos AES 128 And 256 Support
- z/OS V1R9 SPKM-3 And LIPKEY Support

z/OS V1R9 – Network Authentication Service

Network Authentication Service

- A z/OS component since OS/390 V2R10
  - Provides Kerberos support for applications with the GSS-API or krb5 API
  - Supports a KDC (Key Distribution Center) on z/OS
  - Currently support DES, derived-DES and Triple-DES as encryption/decryption algorithm

- z/OS V1R9 provides
  - AES 128 and 256 support for Kerberos
  - An implementation of the SPKM-3/LIPKEY protocols for applications that use the GSS-API

A Few Words On Kerberos

What Is Kerberos ?

- A distributed authentication service developed by MIT based on symmetric encryption - Today at Version 5

- Allows user authentication over a physically untrusted network
  (at the intranet/extranet level)

- Tickets are issued by a Kerberos authentication server
  - Users and servers are required to have symmetric keys registered with Kerberos server

- Flows to and from Kerberos server establish a symmetric session key
  - used in a direct exchange between a user and a service

- V5 implemented today in many platforms: z/OS, AIX, AS/400, Win2K/XP, Solaris
  With DES, derived-DES, Triple-DES or AES support, depending on the implementation

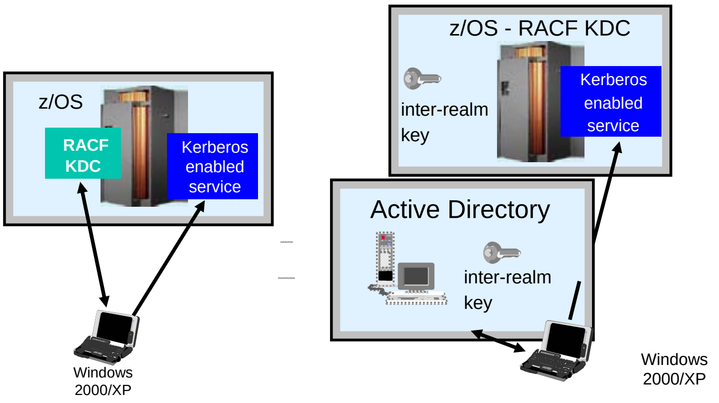
Kerberos on z/OS

Kerberos enabled z/OS servers

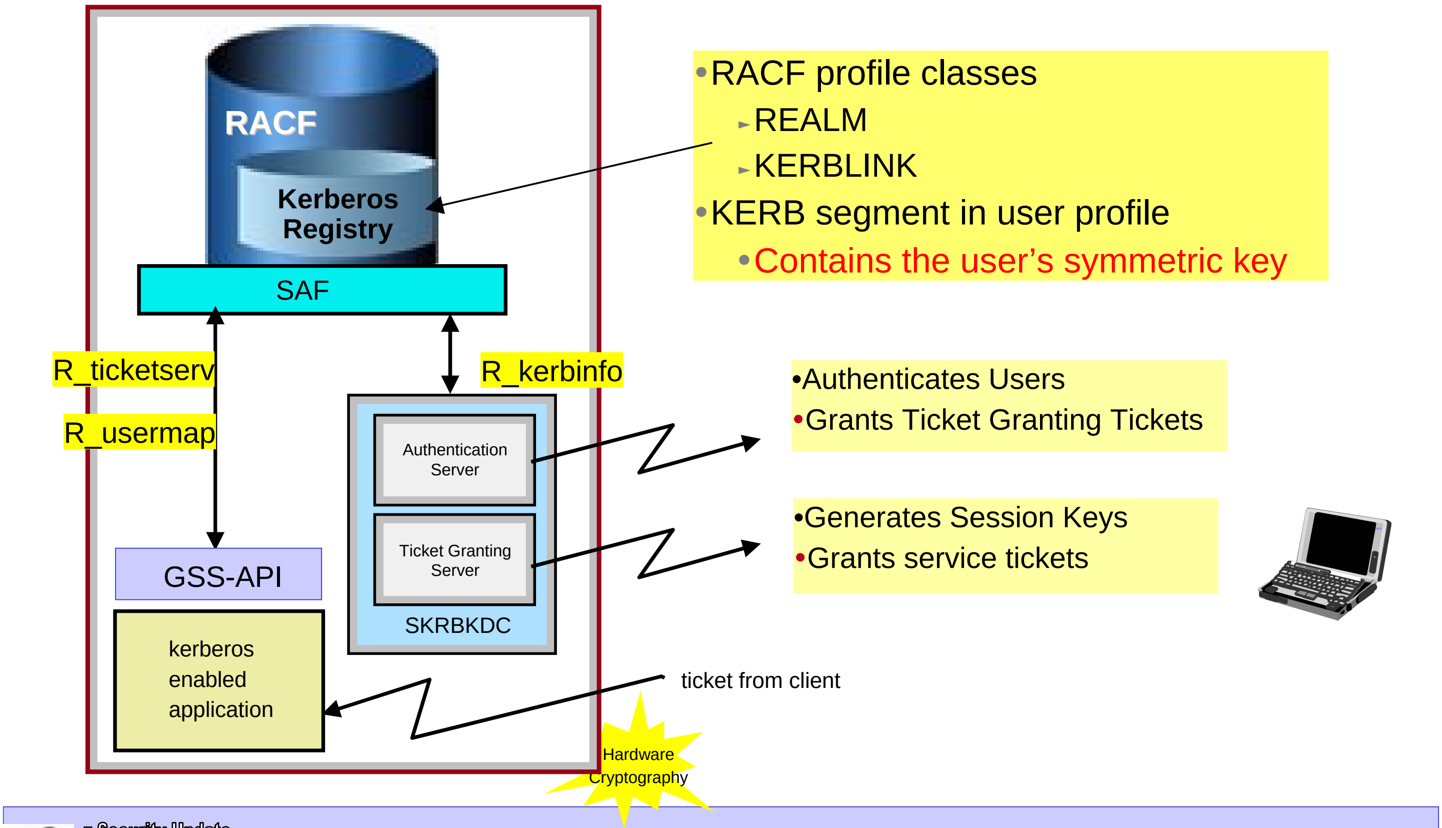
- **DB2** V7 and above (authentication)
- **WebSphere Application Server** (authentication)
- **FTP** client and server (authentication, optional encryption)
- **Telnet server** (authentication, optional encryption)
- **LDAP** client and server (authentication)
- **rshd** server (authentication, optional encryption)

Using tickets issued by the Active Directory KDC

Using tickets issued by the z/OS KDC



Kerberos on z/OS



- RACF profile classes
  - REALM
  - KERBLINK
- KERB segment in user profile
  - Contains the user’s symmetric key

- Authenticates Users
- Grants Ticket Granting Tickets

- Generates Session Keys
- Grants service tickets

A Few Words On GSS-API

Generic Security Services API (GSS-API)

- Provides security services to applications using peer-to-peer communications at an abstracted level
  - Using GSS-API routines, an application can determine another application’s user identity and verify authentication credentials
  - Enable an application to delegate access rights to another application
  - Apply security services, such as confidentiality and integrity, on a per-message basis
- The application specifies the security mechanism that GSS-API should drive at the lower level
  - Kerberos (OS/390 V2R10)
  - SPKM (Simple Public Key Mechanism) (z/OS V1R9)
  - LIPKEY (Low Infrastructure Public Key Mechanism) (z/OS V1R9)
  - Others on other platforms
- The z/OS GSS-API is available to C/C++ applications
- Non-LE applications have access to a subset of the GSS-API functions with the R_GenSec (IRRSGS00 or IRRSGS64) RACF callable service

Kerberos
AES 128 And 256
Support

z/OS V1R9 – Changes For Kerberos AES Support

- Use of AES keys can be enabled in the z/OS Network Authentication Services configuration file
- Commands, panels, utilities, and SAF callable services which support Kerberos encryption types are enhanced to also support 128-bit and 256-bit AES

```
ADDUSER RONTOMS KERB(KERBNAME(raeburn) ENCRYPT(NOAES256))

LISTUSER RONTOMS NORACF KERB
 USER=RONTOMS

 KERB INFORMATION
 ----------------
 KERBNAME= raeburn
 KEY ENCRYPTION TYPE= DES DES3 DESD AES128 NOAES256
```

- Note that using a command or panel to enable use of AES keys, does not generate new keys…a password change is also required!

See the appendix for migration considerations

z/OS V1R9
SPKM-3 And LIPKEY Support

z/OS V1R9 – Simple Public Key Mechanism Support

SPKM-3

- The Simple Public-Key GSS-API Mechanism (SPKM) is based on a public key infrastructure, not the Kerberos symmetric-key infrastructure
  - – SSL-like mechanism for authentication and encrypted data channel
  - – Client and Server use certificates for authentication
  - – Can exploit the same certificate infrastructure as SSL/TLS
  - – Data formats and procedures are designed to be as similar to the Kerberos mechanism as possible for ease of implementation by applications which are already Kerberos enabled via GSS-API
- Documented in RFC 2025
- No IBM exploiter as of today

z/OS V1R9 – Low Infrastructure Public Key Mechanism

LIPKEY

- A GSS-API security mechanism where the server uses a certificate and the client uses userID and password for authentication
- Based on SPKM, establishes an encrypted channel between server and client
- The server must have access to a user ID/password repository
  - the __passwd() function is used in z/OS (password verification through SAF)
- Documented in RFC 2847
- No IBM exploiter as of today

Thank You

Any Questions ?

Appendix

- **RFC archives : http://www.faqs.org/rfcs/**
  - RFC 2025 - The Simple Public-Key GSS-API Mechanism (SPKM)
  - RFC 2847 - LIPKEY - A low infrastructure mechanism Using SPKM
  - RFC 3962 - Advanced Encryption Standard (AES) Encryption for Kerberos
  - RFC 4121 - The Kerberos V5 GSSAPI Mechanism: Version 2

- **SC24-5926 z/OS Network Authentication Service Administration**
- **SC24-5927 z/OS Network Authentication Service Programming**

- SC24-5901 Cryptographic Services System Secure Sockets Layer Programming
- GA22-7800 z/OS Unix System Services Planning
- SA22-7803 z/OS Unix System Services Programming: Assembler Callable Services Reference

z/OS V1R9 – SPKM-3 And LIPKEY Support

- New z/OS Network Authentication Service environment variables

  e.g. GSS_KEYRING_NAME : specifies the name of the key database HFS file or the SAF key ring

- New messages

- GSS-API new parameters to support the new mechanisms

  e.g. desired_mech parameter of the gss_acquire_cred function now supports

  gss_mech_krb5_old
  gss_mech_krb5
  gss_mech_spkm3
  gss_mech_lipkey

z/OS V1R9 – Migration Considerations

A problem can occur when RACF is the Kerberos registry and the database is shared between z/OS V1R9 and lower-level systems

- As always, administration should be done on the higher level system

- The fix for RACF APAR OA20304 must be applied in order for Kerberos to use **triple DES** and **DES with derivation** correctly on the lower-level systems