Key Distribution Center

- What is Key Distribution Center?
- KDC Concept & Architecture
- KDC Application
What is Key Distribution Center?

- symmetric schemes require both parties to share a common secret key
- issue is how to securely distribute this key
- often secure system failure due to a break in the key distribution scheme

What is Key Distribution Center?

- given parties A and B have various key distribution alternatives:
  1. A can select key and physically deliver to B
  2. third party can select & deliver key to A & B
  3. if A & B have communicated previously can use previous key to encrypt a new key
  4. if A & B have secure communications with a third party C, C can relay key between A & B
What is Key Distribution Center?

- typically have a hierarchy of keys
- session key
  - temporary key
  - used for encryption of data between users
  - for one logical session then discarded
- master key
  - used to encrypt session keys
  - shared by user & key distribution center

Key Distribution Center

- What is Key Distribution Center?
- KDC Concept & Architecture
- KDC Application
KDC Concept & Architecture

- hierarchies of KDC’s required for large networks, but must trust each other
- session key lifetimes should be limited for greater security
- use of automatic key distribution on behalf of users, but must trust system
- use of decentralized key distribution
- controlling key usage
KDC Concept & Architecture

Kerberos

- Kerberos is an authentication service developed at MIT that uses symmetric key encryption techniques and a Key Distribution Center.
- Kerberos is framed in the language of users who want to access network services (servers) using application-level network programs such as Telnet (for remote login) and NFS (for access to remote files), rather than human-to-human conversant.
- The most recent version of Kerberos (V5) provides support for multiple Authentication Servers, delegation of access rights, and renewable tickets.
KDC Concept & Architecture

- Kerberos

1. Log on to realm and obtain referral ticket
2. Get ticket for SSH server using referral ticket
3. Log on to SSH server, authenticate using ticket

KDC Concept & Architecture

- Kerberos (IIS)
Key Distribution Center

- What is Key Distribution Center?
- KDC Concept & Architecture
- KDC Application

KDC Application

- Key Distribution Center Configuration
- Use
  - The Kerberos authentication process uses a Key Distribution Center (KDC) to authenticate a client and to issue the Kerberos Client/Server Session Ticket, which is used for the communication between the Web client and the AS Java. For this reason, the KDC maintains a directory of the users that can access AS Java resources for a Kerberos Realm.
  - You can use this topic for information about the KDC configuration requirements that have to be in place to use SPNego for Kerberos authentication with the AS Java.
KDC Application

• **Features**
  
  • The configuration steps are specific to the KDC that you use. For more information, see the documentation provided by your KDC vendor.
  
  • If you use a Sun JDK to run the J2EE Engine and the KDC is a Windows 2000 Domain Controller with ADS, you also have to disable delegation in the ADS to avoid errors during ticket verification.

KDC Application

• **Example**
  
  The following example shows the configuration steps when the KDC is a Microsoft Windows 2000 Domain Controller (DC) that uses an Active Directory Server (ADS) for a user store.

• **Assumptions**
  
  For the purpose of this example we assume that:
  
  • The KDC is a Microsoft Windows 2000 Active Directory Server
  
  • The Windows Domain Name is IT.CUSTOMER.DE
  
  • The fully qualified host name of the AS Java is hades.customer.de.
  
  • The AS Java has an additional alias su3x24.customer.de.
**KDC Application**

- **Configuration steps on the DC**
  1. Create a service user `j2ee-jdi-hades` with a password for this example `secret12`. Enable the Password Never Expire option for this user.
  2. In the options for the user account, choose the option *Use DES encryption types for this account*.
  3. From a command line, enter the following command to register service principal names (SPNs) for the AS Java host name and alias and map them to the service user `j2ee-jdi-hades`.

```
setspn -A HTTP/hades.customer.de j2ee-jdi-hades
setspn -A HTTP/su3x24.customer.de j2ee-jdi-hades
```

- **Result**
  1. To check the result of the configuration, enter the following command line for each SPN you registered:

```
ldap -r
serviceprincipalname=HTTP/hades.customer.de -f
out.ldf
```
  2. The output of this command is one entry which points to the previously created service user.
Reference

- http://rnd.feide.no/doc/resources/feide-ssh/kerberos-1.png @ 28 OCT 2008