8.2.6 Single Sign-on Facts

Enterprise environments frequently implement single sign-on (SSO) authentication. SSO is a distributed access method that allows a subject to log in (sign on) to a network once and access all authorized resources on the network. This reduces the number of credentials a user has inside an organization because he doesn't have multiple user names and passwords for various accounts.

When the user logs in to a domain, the SSO system authenticates the subject against a master system. This service shares authenticated sessions between crossed systems. An organization may also define a time limit for how long this authentication is granted. When authenticated, the user can access resources without additional login credentials or passwords. An SSO system is commonly used in directory systems and some types of scripted access.

Advantages of SSO include:

- Access to all authorized resources with a single instance of authentication through a single set of user credentials.
- A more efficient logon process. Users only need to type their user ID and password once.
- No need for multiple passwords or change synchronization.
- The user can create stronger passwords because there aren't so many passwords to remember.
- Inactivity timeout and attempt thresholds are applied closer to the user point of entry.
- The ability to disable all network and computer accounts for terminated users via a centralized database and one user interface.

Disadvantages of SSO include:

- Once a user's ID and password are compromised in the system, an intruder can access all of the resources authorized for the user without constraint.
- The system security policy must be followed to ensure access is granted and/or limited to appropriate users.
- Implementation with microcomputer systems is difficult and can prevent full implementation.
- Ticket schemes do not scale very well.
- SSO presents a single point of failure.

You should be aware of the following SSO solutions:

Solution	Description
Kerberos	Kerberos is an open system that can be used on Macintosh and Unix systems. It is built into Windows 2000 Active Directory. Kerberos: ▪ Uses symmetric key cryptography to provide end-to-end security. ▪ Uses DES encryption. ▪ Authenticates subjects to entities on a network. ▪ Supports mutual authentication. ▪ Provides authentication only. It does not provide data integrity or confidentiality. Kerberos authentication includes three entities: the subject who logs in to the network, the object or resources the subject wants to access, and a trusted authentication server. The collection of subjects and objects is known as the Kerberos realm. Kerberos weaknesses include: ▪ Passwords for authentication. ▪ Tickets that are temporarily stored on the user's workstation and could be compromised. ▪ Initial authentication that is vulnerable to password guessing (the KDC cannot know if an attack is in progress). ▪ When a user changes a password, it changes the secret ke, so the KDC database must be updated. ▪ The KDC must handle many requests in a timely manner.
Secure European System for Applications in a Multi-Vendor Environment (SESAME)	SESAME is an SSO technology that uses asymmetric cryptography. The following process is used with SESAME: 1. The user authenticates to an authentication server. The server grants the user a token that proves identity. 2. The user presents the token to a privilege attribute server, which gives the user a privilege attribute certificate (PAC). The PAC contains security attributes and access rights that have been granted to the user. The token is digitally signed to prove its integrity. 3. When the user attempts to access an application or a resource, the PAC is presented. The application uses the information in the PAC along with an access control list to allow or deny access. 4. Dialog keys are used to provide data integrity and confidentiality in communications (if desired). Because SESAME is similar to Kerberos, SESAME designers have supported some Kerberos data structures. SESAME goes beyond the functionality of Kerberos by supporting access control through access control lists, asymmetric keys, PKI systems, and auditing.

Directory Services	Directory services implement single sign-on for resources on the network. Examples are: ▪ Active Directory on a Microsoft network ▪ eDirectory on a Novell network ▪ LDAP Directory Services Single sign-on can be implemented between directory services of different systems--for example, between Microsoft and Linux systems, if the directory services are compatible. In this case, a user logging into a Linux system would be authenticated to access resources on the Microsoft network that the user has permissions to access. Directory services users sign on using a domain user account and password to gain access to resources available on the domain.