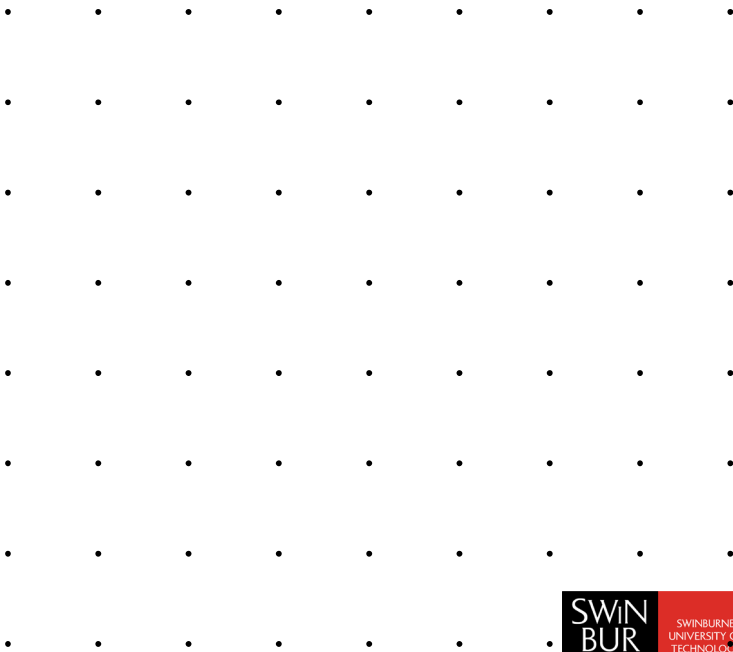


Kerberos



Kerberos

- **Kerberos** is an authentication protocol and a software suite implementing this protocol.
- uses symmetric cryptography to authenticate clients to services and vice versa.
- Windows servers use Kerberos as the primary authentication mechanism, working in conjunction with Active Directory to maintain centralized user information.

Kerberos

- Other possible uses of Kerberos include
 - log into other machines in a local-area network,
 - authentication for web services,
 - authenticating email client and servers,
 - authenticating the use of devices such as printers.

Kerberos

- Uses **tickets** as tokens that prove user identity.
- Tickets are digital documents that store session keys:
 - During authentication, a client receives two tickets:
 - A **ticket-granting ticket (TGT)**, (a global identifier)
 - A **service ticket**, which authenticates a user to a particular service (session ticket)

Kerberos

- Uses a **key distribution center (KDC)**, which contains:
 - An **authentication server (AS)**
 - A **ticket-granting server (TGS)**
- Keeps a database storing the secret keys.
- Centralises authentication for an entire network.
- Each transmission is encrypted.
- Compares password hashes (never sends password).

Advantages

- Timestamps tickets to prevent playback attacks.
- Uses a cache of previously used tickets to prevent replay attacks (sort of OTP).
- Tickets may be specific to IP addresses.
- Uses symmetric keys.
- Open source version available.

Disadvantages

- Single point of failure:

- If the KDC goes down, no-one can authenticate.

- Can have multiple KDCs, or backup KDCs

- If an attacker compromises the KDC, the authentication information of every client and server on the network would be revealed.

- Requires that all hosts have synchronized clocks.

- Used DES encryption - really out of date

- http://media.blackhat.com/bh-us-10/whitepapers/Stender_Engel_Hill/BlackHat-USA-2010-Stender-Engel-Hill-Attacking-Kerberos-Deployments-wp.pdf