**Kerberos: System for mutual authentication**

**Background**
- Part of Windows XP.
- Network authentication protocol.
- Invented in the 60’s at MIT.
- Uses secret key cryptography.
- Encryption used by default is DES.
- **KDC** (Key Distribution Center) contains all the private keys for every user used for authentication and the encryption process.
- Consist of 2 parts, the **Authentication Server** and the **Ticket Granting Server**
- Mutual Authentication

**Versions**
- Currently on version 5, though very similar to version 4 in overall security and implementation. Corrects bugs found in earlier implementations.
- Version 5 has extra features such as delegation, which allows you to hand off access (let them be you) to another user for a certain time period and also post dated tickets for future transactions.
- Later versions rely on use of Universal Clock rather than use of nonces.
- Earlier versions were susceptible to bugs and various security holes.

**Kerberos:**

What should you use for a session key?

**Session Key Properties:**
1. Not sent over in the clear
2. Change each time

There are many possible ways to create a session key.
If Kab is the secret key and C the random challenge then as session key you could use Kab + C.
I want to talk to KDC1
Eka(ka,KDC2)

Auth Using KA KDC2
I want to talk to x
Eka(KaX)

EkaKDC2(Ka,KDC2)

KDC2

Auth
Talking

KDC1

A

X

Auth
I want to talk to
Eka(ka,KDC2)
Needham-Schroeder Protocol

- Suppose N1 was not there. Trudy gets hold of an old key of Bob. Impersonates KDC first and replays old #2. Then Trudy impersonates Bob using the old key.
- Why a ticket? To prevent Alice from blocking on the KDC talking to Bob.
- Why “Bob” in #2? Suppose there is no “Bob” in #2, then Trudy changes #1 to N1, “Alice”, “Trudy” so KDC sends ticket encrypted with KT instead of KB. Now Trudy impersonates Bob and she can because she can decrypt the ticket.
**Bug Discovered 10 years Later:**
Trudy uses an old key of Alice & old #2 to impersonate Alice. This works as long as B’s key has not changed.

To solve this problem use the following scheme.