MIT Project Athena, Interop '88

Kerberos:

An Authentication Service for Open Network Systems

Attacks

- Impersonating a User
- Impersonating a Server
- Reading Sensitive Data Off the Network

The Goal

- Authentication of Client and Server
- Secure Exchange of Encryption Key

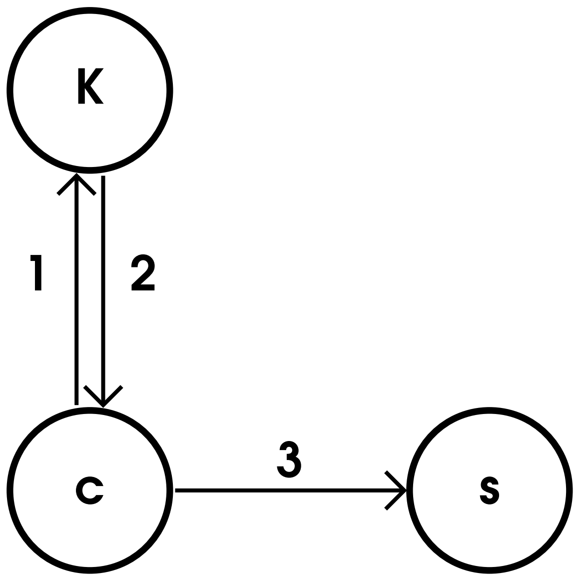
Definitions

- client
- server
- private key --> K_x
- session key --> $K_{c,s}$
- encryption --> $\{abc\}K_x$

The Model

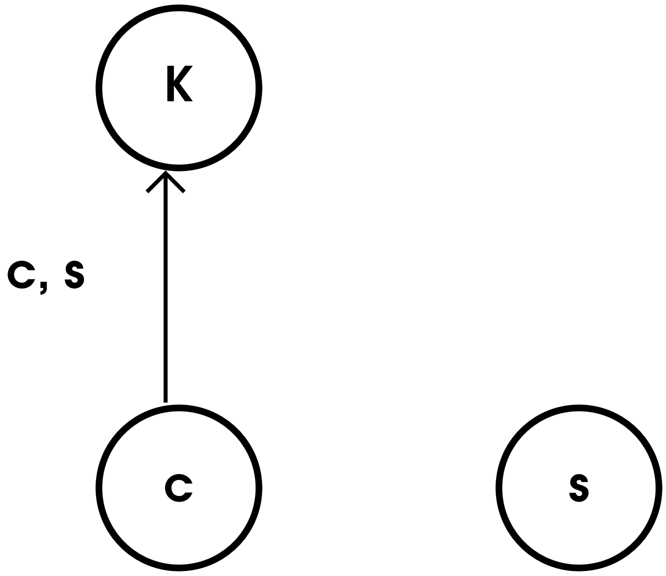
Needham and Schroeder, 1978

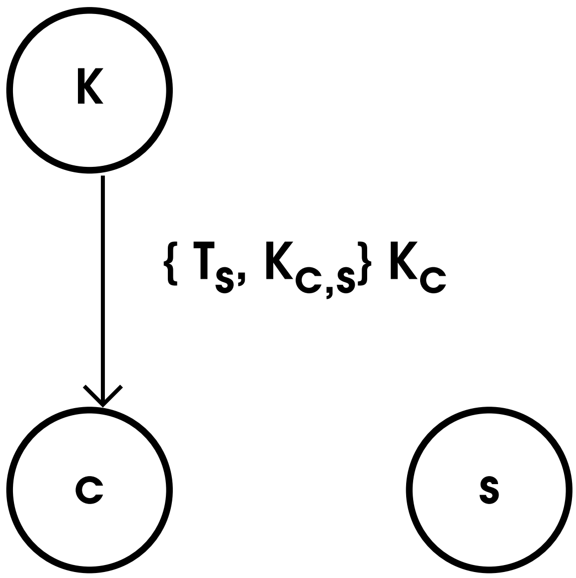
- Trusted Third Party Network Authentication Service
- Key Distribution Center
- Private Key Encryption (Two parties share a secret)

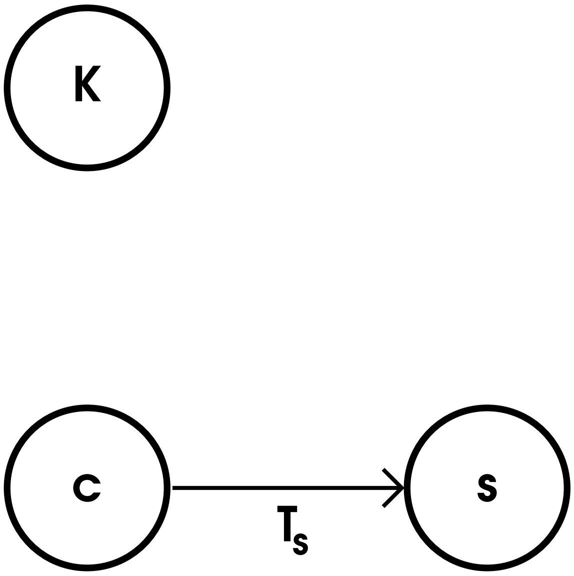

K
1
2
C
3
S

The Ticket

$$T_s = \{ s, c, addr, time, life, K_{c,s} \} K_s$$


K
C, S
C
S


K
$\{ T_S, K_{C,S} \} K_C$
C
S



$$T_s = \{\ s,\ c,\ addr,\ time,\ life,\ K_{c,s}\ \}\ K_s$$

The End Result

- Authentication of Client and Server
- Secure Exchange of Encryption Key

Applications

- Mail retrieval
- rlogin, rsh, rcmd
- Encrypted rcp, rlogin
- Network File System
- Remote Virtual Disk
- tftp
- Zephyr
- SMS