Introduction to Computer Security

Lecture 8
Key Management
Nov 1, 2005

Issues

- Authentication and distribution of keys
  - Session key
  - Key exchange protocols
  - Kerberos
- Mechanisms to bind an identity to a key
- Generation, maintenance and revoking of keys

Notation

- $X \rightarrow Y : \{ Z \,||\, W \} k_{X,Y}$
  - X sends Y the message produced by concatenating Z and W enciphered by key $k_{X,Y}$, which is shared by users X and Y
- $A \rightarrow T : \{ Z \} k_A \,||\, \{ W \} k_{A,T}$
  - A sends T a message consisting of the concatenation of Z enciphered using k_A, A's key, and W enciphered using $k_{A,T}$, the key shared by A and T
- r_1, r_2 nonces (nonrepeating random numbers)