Limitation of Kerberos

Dharani S Vijayakumar
Graduate Student, CSE Dept.
vijayaku@cse.psu.edu
Main components of Kerberos Authentication

- Ticket - Given for the verifier to the principal who wants to be authenticated.

- Authenticator- Given by the principal to be authenticated to the verifier.

NONCE!
REUSE OF AUTHENTICATOR

- Timestamps
- Nonce-Identifier
Password Guessing Attacks

• Calculating Kc by making a guess at the password
• Why not use key exchange algorithms like Diffie Hellman?
One time passcode

• A version of this is obtained by encryption using a \{R\}Kc
Session Key

- Is is multi-session key really fine?
Cut and Paste

• A portion of the encrypted message being used
• A standard encoding scheme is used to validate the protocol.
Hardware

• The hosts need random keys for sessions. A key store?
• Support for encryption
Encryption

• A CBC encryption is used instead of PCBC encryption
• Checksum is used to detect message modification
Extension?

• Things change with time!
A higher version!

- Ultimate solution?