

Date 02/14/06

Review

- Controlling access to objects from security domains.
- Controlling peoples access to a computer

Authentication

- Map a user to a domain
- Identify user
- Somehow prove user is who they claim to be.

✓ 4 important factors to worry about while communicating with the server – user, terminal, wire, and server. One or more of these might create security issues.

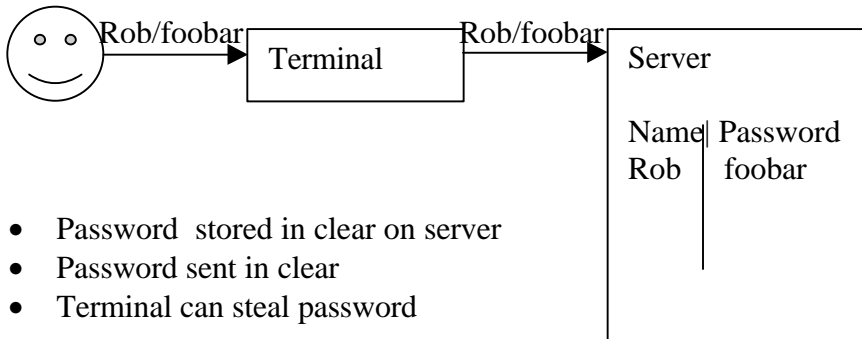
Threats

- Wire tapping (sniffing, spoofing)
- Terminal (key logging, other covert channels, spoofing)
- Server attacks (attacker may break into the server)

✓ Three kinds of authentication

- Something you know (password)
- Something you have (key, id)
- Something you are (biometrics)

Simple authentication system



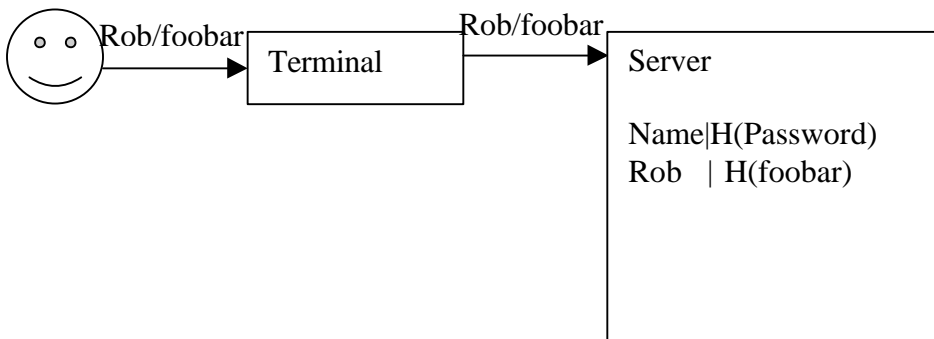
- Human factors in password
 - Easy to guess
 - shareable
 - stealable

- Password stored in clear on server
- Password sent in clear
- Terminal can steal password

Definition: A hash function H is a pre-image resistant if, given $Y=H(x)$, it is extremely difficult for an attacker to find x^1 s.t. $H(x^1)=Y$

EX: SHA – 1, SHA = 256

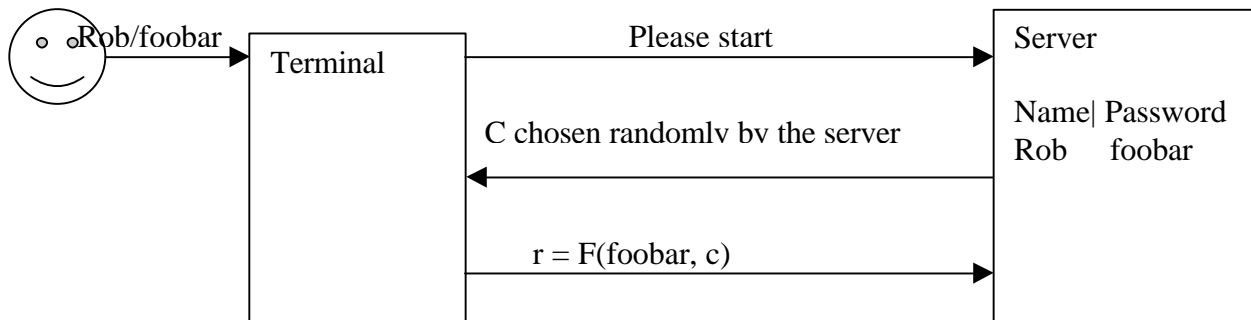
This tackles server problem but doesn't solve wire problem.



How to protect data on the wire?

Encryption – encrypt & mac all data sent between the terminal and the server.

Challenge Response protocol



Security Property of F

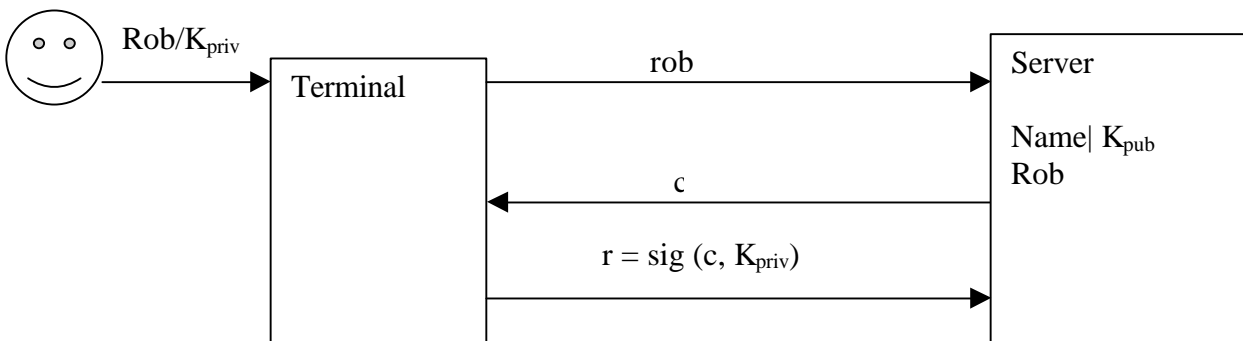
- Given $F(P, c_1), F(P, c_2), \dots, F(P, c_n)$ for c_1, c_2, \dots, c_n of the attacker's choosing, it is extremely difficult for the attacker to produce a pair of c, r , s.t. $r = F(P, c)$ and $c \neq c_1, c_2, \dots, c_n$

Properties of the protocol

- Attacker
 - Pass c to the terminal
 - Grab response and stop it
 - Let user try again and succeed
 - Later, present the original response to the server.

Digital Signature

- User possesses a private key K_{priv} , only the user knows K_{priv} .
- World can know a corresponding public key K_{pub}
- Extremely difficult to compute K_{priv} from K_{pub}
- A signature scheme is two functions sig and ver s.t. $ver(K_{pub}, M, sig(K_{priv}, M)) = valid$.
But an attacker cannot construct any value x s.t. $ver(K_{pub}, M, x) = valid$



- No binding between initial authentication and subsequent communications.
- Sign all subsequent messages too, include c for freshness.

For real password protocols see

- Encrypted key exchange (EKE)
- Diff Hellman EKE (DHEKE)
- Secure remote password protocol (SRP)