Authentication Protocols

Wednesday, July 17, 2013
9:12 AM

Protocol

Method of communication

Basic Protocols

Simple Protocol

User sends PIN/password/etc to server auth channel
If correct, allowed access
Issues:
Plain text transmissions can be intercepted, stored & replayed
Solutions
Switch to encryption (e.g. https)
Frequently change password/PIN/etc.
Encrypted transmissions can also be intercepted
- weak encryption can be broken (e.g. WEP & WPA)
Solution
Use better algorithms (e.g. WPA2 with AES)

Challenge-Response

Server issues a challenge
User (or user's computer) has to come up w/ correct response to log in
Two-factor authentication
combines simple & challenge-response (usually)
Attacks on Challenge-Response
Man-in-the-middle
attacker tricks user into going through attacker instead of directly to server

Ways to guard against this:
use digital certificates for server identity
use digital certificate for client too (mutual authentication)

General Attacks
- Eavesdropping
- Key Logger
- Session Hyjacker
  - Solutions
    - Don't allow tabbed browsing
    - Physical / logical separation
- Manipulate the message
- Change the environment