Authentication

1

Authentication

- Weak - Trusts the network
- Strong - Relies on protocols that do not require transmitting secrets over the network
- Any authentication worth using should be able to resist an attacker even if the attacker can monitor the entire login
- Passwords are obsolete

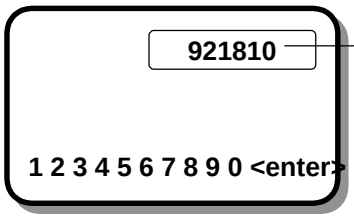
2

Authentication: Tradeoffs

- Strong authentication
  - Often requires extra steps
  - Often requires extra software or hardware
  - May require modification of applications base
  - Requires additional management
- Weak authentication
  - Cheap, easy, insecure

3

Authentication: Time Tokens



Username: mjr
Password: 921810

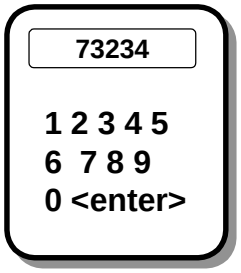
Encrypted value used instead of password

Secret key contained in card
Key used to encrypt clock within card
Encrypted clock value displayed on LED

Server software performs same encryption and permits access if values match

4

Authentication: Challenge/Response



Username: mjr
Challenge: 29381

User enters PIN to “unlock” calculator
User enters challenge into calculator

Calculator displays challenge encrypted with secret key

Response: 73234

Secret key contained in calculator

Server software performs same encryption and permits access if values match

5

Authentication: Software

Username: mjr
Challenge:key #430

User consults challenge response list
Selects requested response number

Response returned from list

Response: CAT LAMP

Printed challenge/response list stored in user’s wallet

Server software permits access if values match
Next challenge is #429

6

Authentication: Kerberos

- Trusted third party authentication system
- Requires secure server on network
- Requires software modification or support
- Permits use of plaintext passwords without compromising security

7