Network Services, VU 2.0

Security 2

Dipl.-Ing. Johann Oberleiter
Institute for Informationsystems, Distributed
Systems Group

Agenda

- Security Terms
- Security Threats
- Security Attacks
- Firewall Placement

Security - Terms

- Confidentiality
  - Prevent unauthorized access
  - Encryption
- Integrity
  - Prevent unauthorized changes
  - Message authentication codes (MACs)
- Availability
  - Uninterrupted service
  - prevent denial-of-service attacks
- Authenticity
  - Prove origin of data
  - Digital signatures

Security Attacks / 1

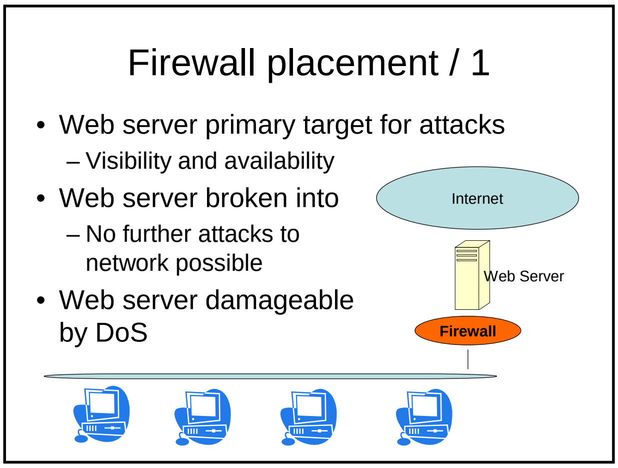
- Eavesdropping
  - Unauthorized intruder reads information which is sent over network or stored in memory
  - Difficult to detect
- Masquerading
  - Intruder tries to use someone else's identity to gain access to a system
- Message tampering
  - Unauthorized changes of network messages
- Replaying
  - Network packages stored and resent at a later time

Security Attacks / 2

- Denial of service
  - Make parts of system unuseable for other users
- Social engineering
  - Intruder gains access to system by playing the role of someone else
  - Convinces the user to change or revail password
- Exploits
  - Use security holes in operating systems and software to gain access to a system
- Data driven
  - Virus
  - Worm
  - Trojan Horse

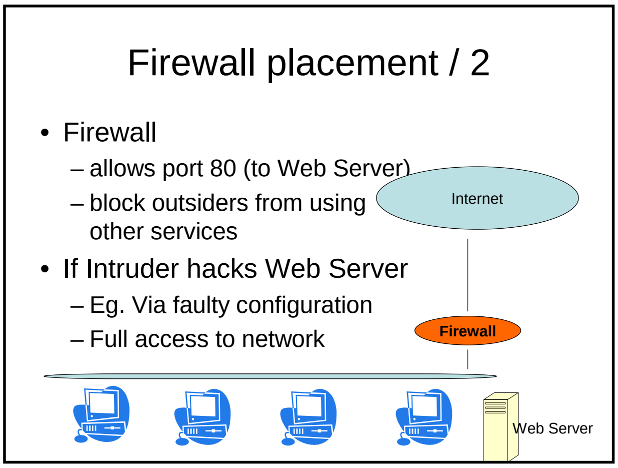
Firewalls

- Isolates network from Internet
- Allows certain connections and blocks others
- Firewall <> Security
  - Does not solve all problems
  - Attacks by frustrated/former employees



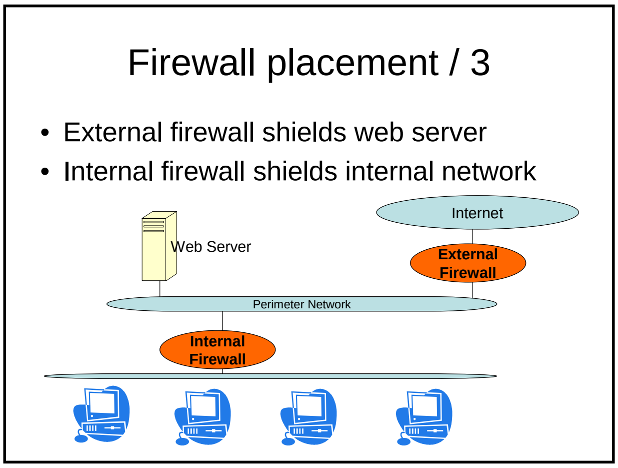
Firewall placement / 1

- Web server primary target for attacks
  - Visibility and availability
- Web server broken into
  - No further attacks to network possible
- Web server damageable by DoS



Firewall placement / 2

- Firewall
  - allows port 80 (to Web Server)
  - block outsiders from using other services
- If Intruder hacks Web Server
  - Eg. Via faulty configuration
  - Full access to network



Firewall placement / 3

- External firewall shields web server
- Internal firewall shields internal network