





Prof. Dr. Hans Peter Großmann mit M. Rabel sowie H. Hutschenreiter und T. Nau | Sommersemester 2012 | Institut für Organisation und Management von Informationssystemen

Lecture Computer Networks

Security / Firewall

Types of Attacks

- General Intrusion
- Compromise reputation
- Denial of service
- Information theft
- Corruption of data, deletion of files

Security Steps

- No security
- Security through obscurity
- Host security
- Network security

The Zone of Risk I

- All hosts on the LAN are directly accessible through the Internet
- Every host on the Internet can attack every host on the LAN



The Zone of Risk II

All hosts on the LAN are only indirectly accessible through the Internet via the Firewall system



- Forces people to enter at a controlled point
- Prevents attackers from getting in contact with all hosts
- Forces people to leave at a controlled point



Packet Filter



Proxy Server



Types of Proxy Servers

• circuit-level proxy



Types of Proxy Servers II

• application-level proxy



Firewall Architectures I

• Packet Filter Architecture



Firewall Architectures II

• Dual-homed Host Architecture



Firewall Architectures III

• Screened Host Architecture



Firewall Architectures IV

Screened Subnet Architecture



What a Firewall cannot do

A firewall cannot protect an intranet against

- insiders
- connections that do not go through it

(e.g. dial-up modem connections)

- completely new threats
- viruses