

Angriffe auf die Netzwerksicherheit

1.kurzer Überblick über die Entstehung des Internet

2.Grundarten von Netzwerkangriffen

- Sniffing
- Denial–of–Service
- Spoofing
- Man–in–the–Middle–Attack

3.Sicherheitsschwächen der Internet– Protokolle und deren Implementationen

Überblick über Sicherheitsprobleme

1.kurzer Überblick über die Entstehung des Internet

- 1969: Gründung des ARPANET mit vier IMP's
- 1974: Beginn der Entwicklung von TCP (+IP)
- 1986: Gründung NSFNET → erster Backbone
- 1994: offiziell Entstehung des Internet ← Ablösung des NSFNET als Backbone
- 1996: kommerzielle Onlinedienste erhalten Gateways zum Internet

Zusammenfassung:

Internet früher: exklusiver Kreis von Benutzern (Wissenschaftler)
→ Durchsetzung von Strafen bei Verstößen möglich, abschreckend
Internet designed für Verfügbarkeit und Integrität

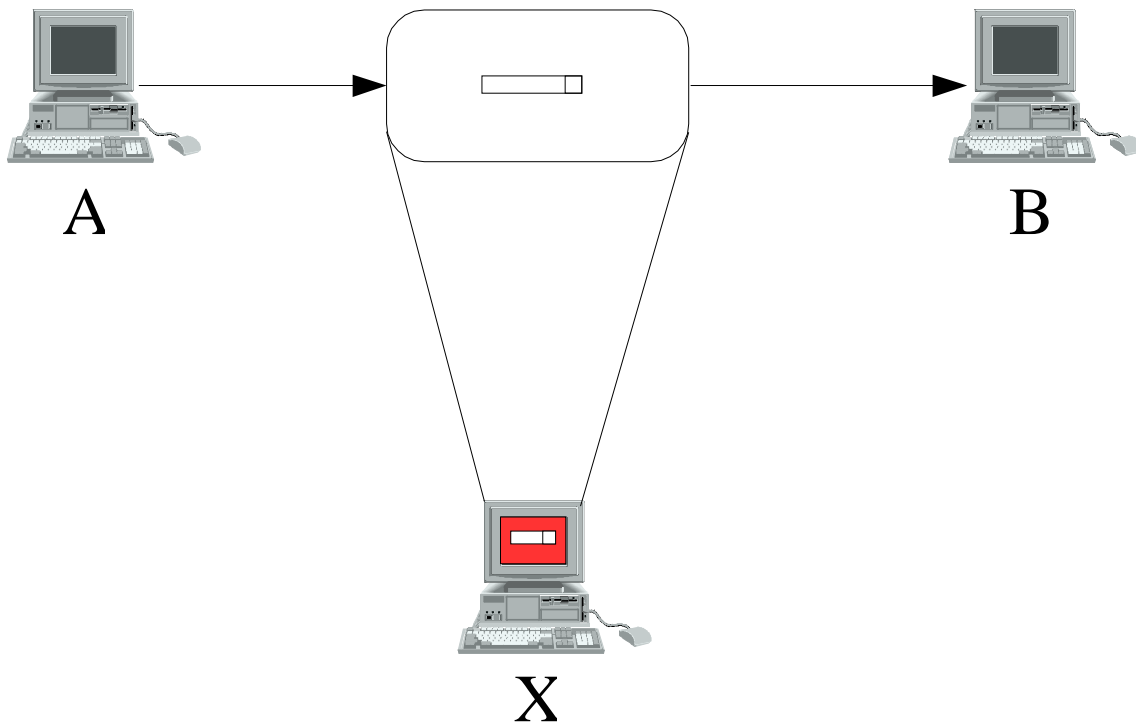
Internet heute: Nutzergruppe unüberschaubar in Vielfalt und Größe ; kommerzielle Dienste
→ Rückverfolgung durch die Menge an Servern und Clienten fast unmöglich

2. Grundarten von Netzwerkangriffen

aktiv: modifizierend

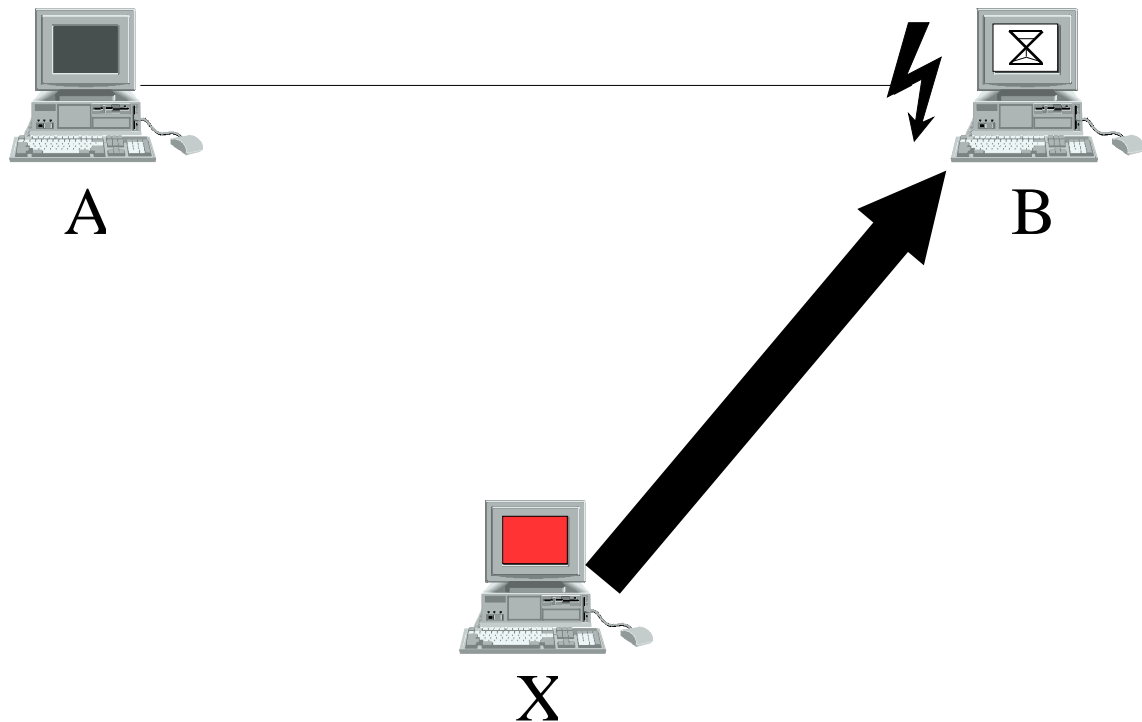
passiv: nicht modifizierend

Sniffing (passiv)



- Mitlesen von Paketen
- Netzwerkanalyse
- > Angriff auf Vertraulichkeit

Denial-of-Service

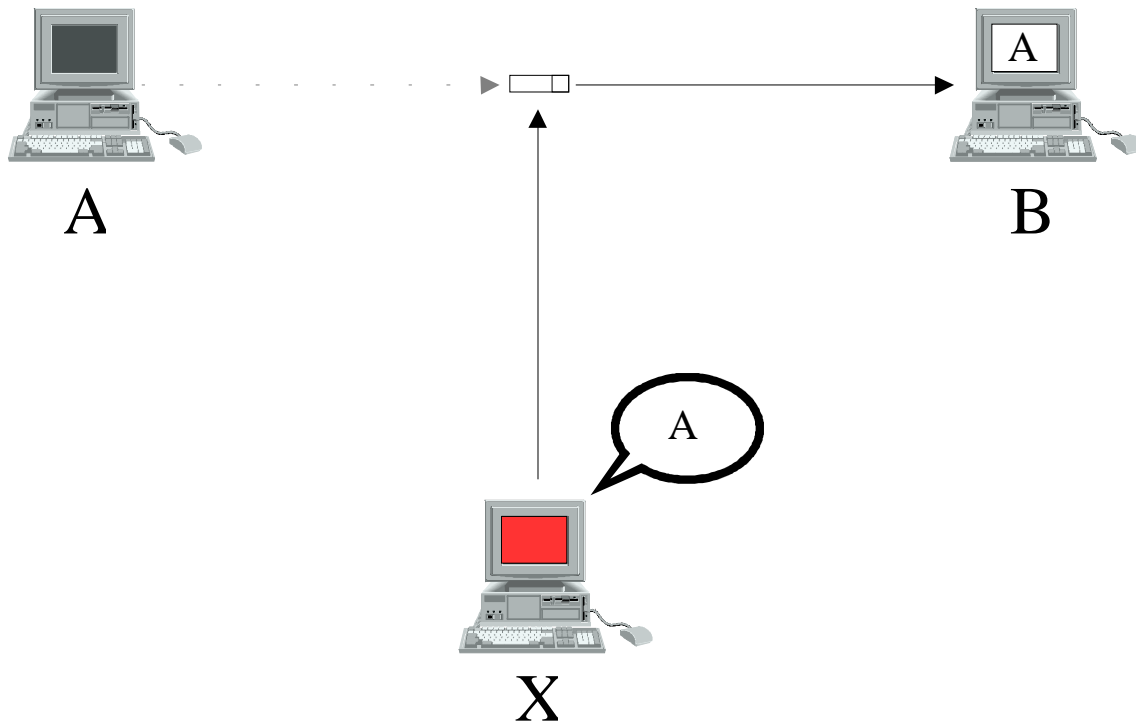


unrechtmäßiger Ge-/Verbrauch von Betriebsmitteln, so daß rechtmäßige Benutzung be-/verhindert wird

→ Angriff auf Verfügbarkeit

Überblick über Sicherheitsprobleme

Spooftng

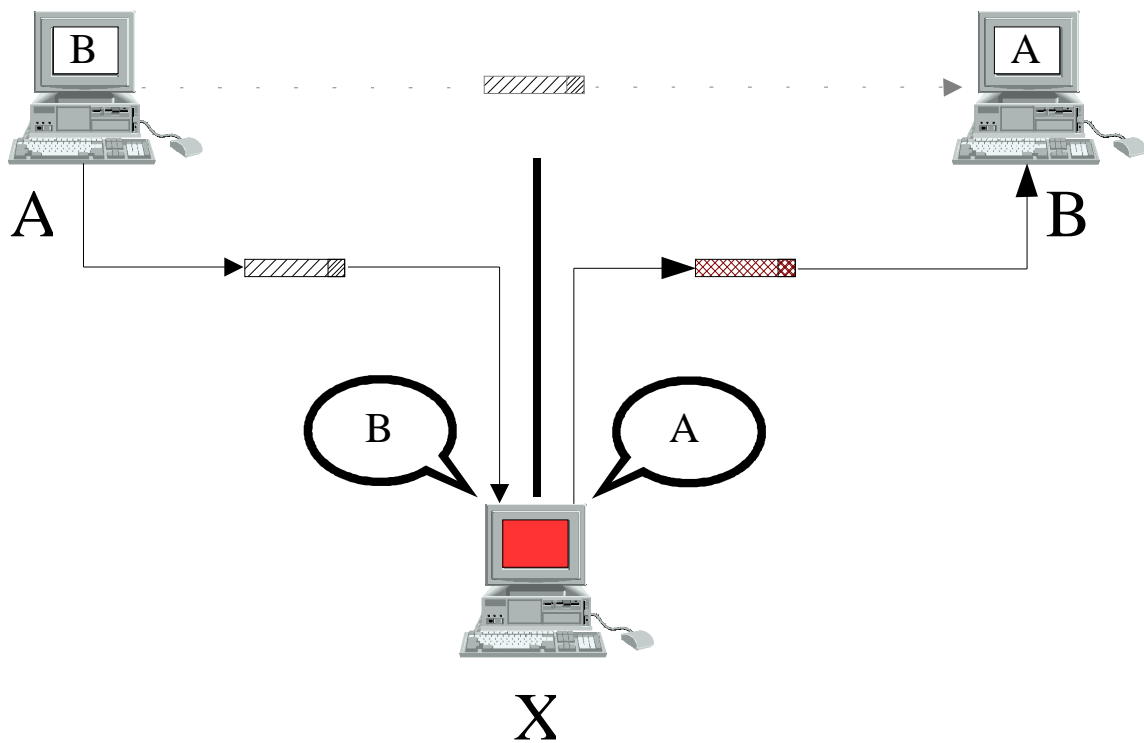


Fälschung von Daten, die zur Identifikation oder Authentikation verwendet werden

→ Angriff auf Identifikation / Authentikation

Überblick über Sicherheitsprobleme

Man-in-the-Middle



Modifikation, Umleitung, Unterbrechung der Kommunikation zwischen zwei Hosts ohne deren Wissen

→ Angriff auf Integrität

3. Sicherheitsschwächen der Internet-Protokolle und deren Implementation

1. ARP

- ARP-Sturm (DoS)
- ARP-Spoofing
- *ARP-Broadcast-Sturm (DoS)*

2. IP

- IP-Spoofing
- Source-Routing-Attack (MitM)
- Ping-of-death (DoS)
- *Tiny-Fragment-Attack*
- *Overlapping-Fragment-Attack*

3. ICMP

- Ping-Flooding (DoS)
- ICMP-Destination-Unreachable-attack (MitM)
- ICMP-Redirect-attack (MitM)
- *Smurf (DoS)*
- *ICMP-Fragmentation-Needed-And-DF-Set*
- *ICMP-Source-Quench-Attack (DoS)*

4. TCP

- Syn-Flooding (DoS)
- Sequencenumber-attack (Spoofing)
- TCP-Hijacking (MitM)
- TCP-Man-in-the-Middle-Attack
- *Land (DoS)*

5. DNS

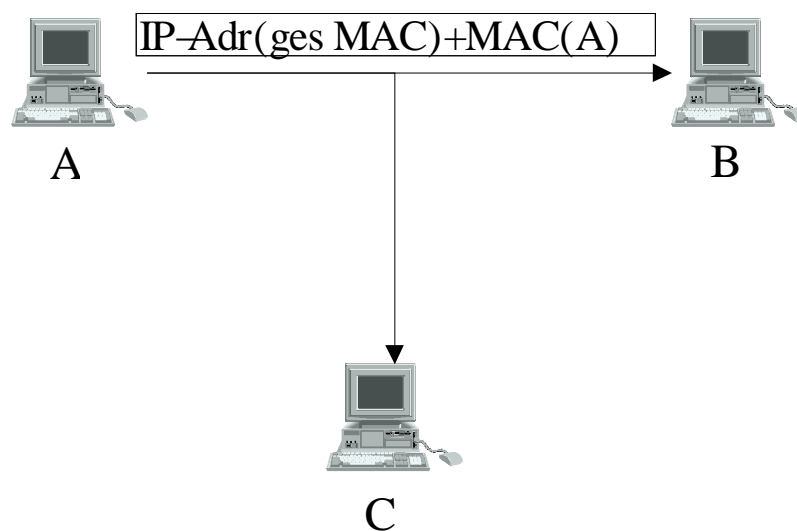
DNS-Spoofing (MitM)

Überblick über Sicherheitsprobleme

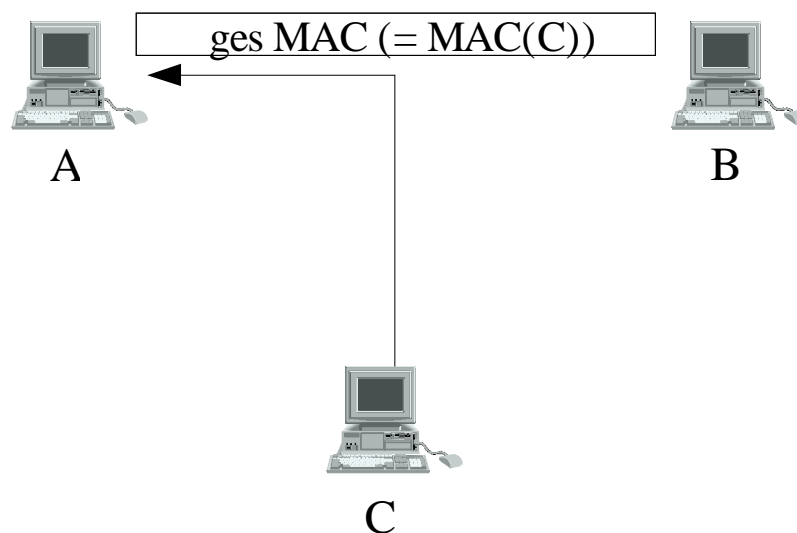
ARP

Zuordnung einer physikalischen Adresse (MAC) zu IP-Adresse

ARP Request :

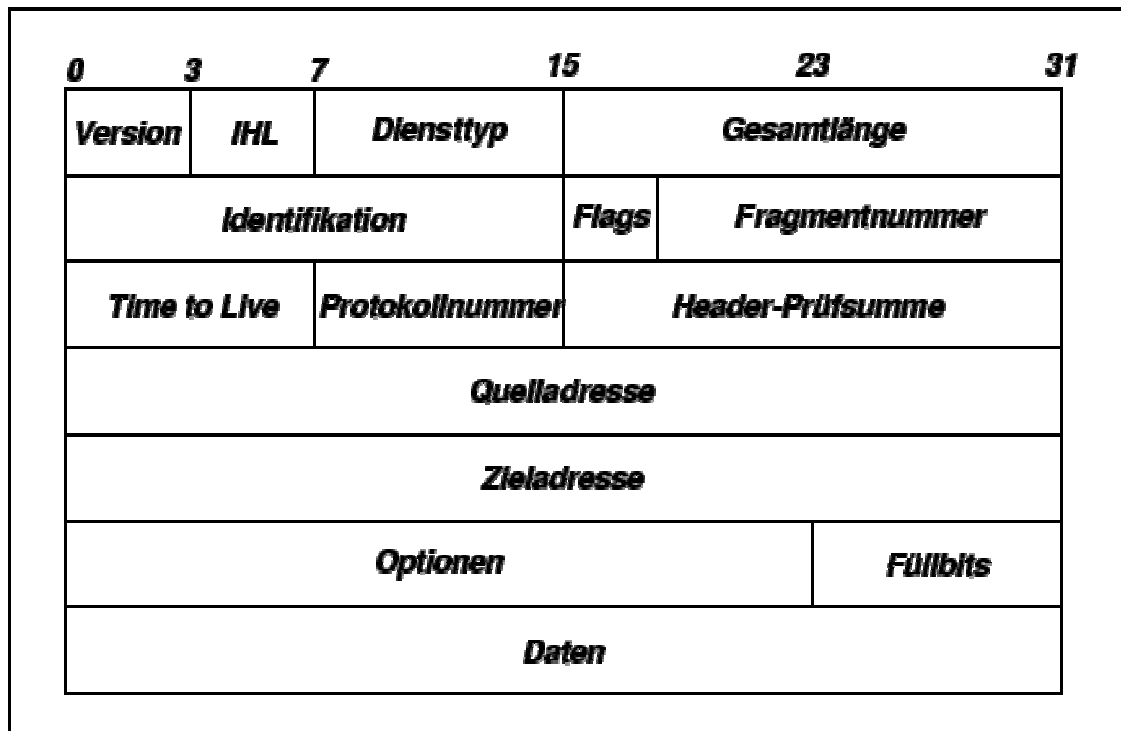


ARP Reply :



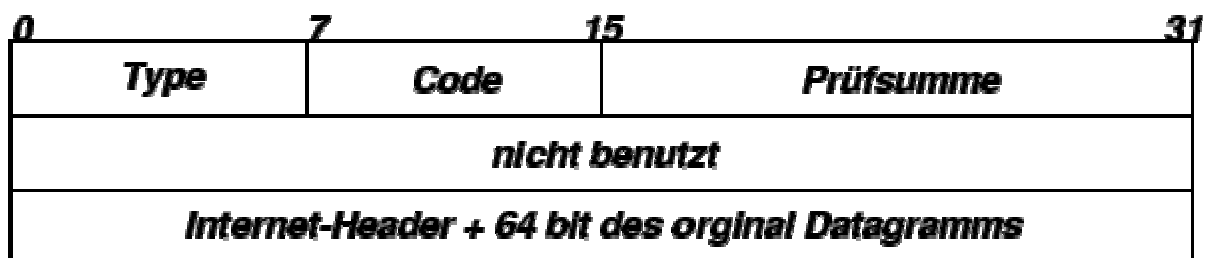
Überblick über Sicherheitsprobleme

IP-Header



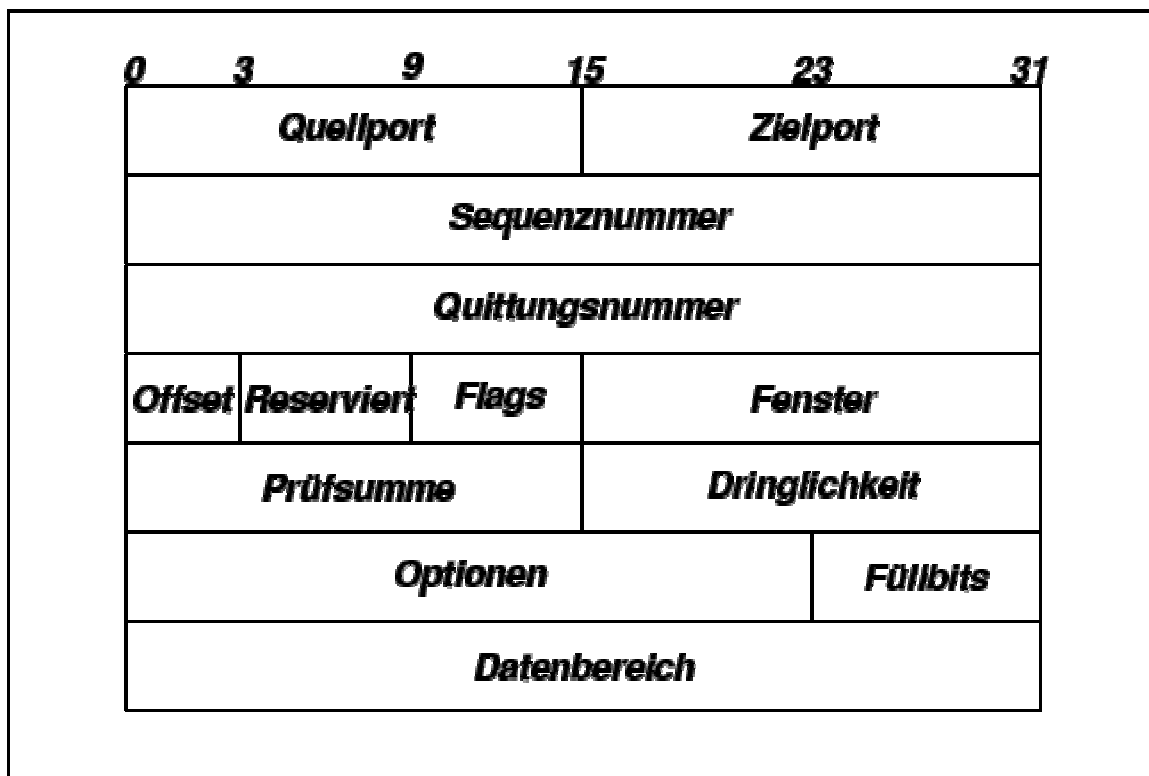
Überblick über Sicherheitsprobleme

ICMP-Header



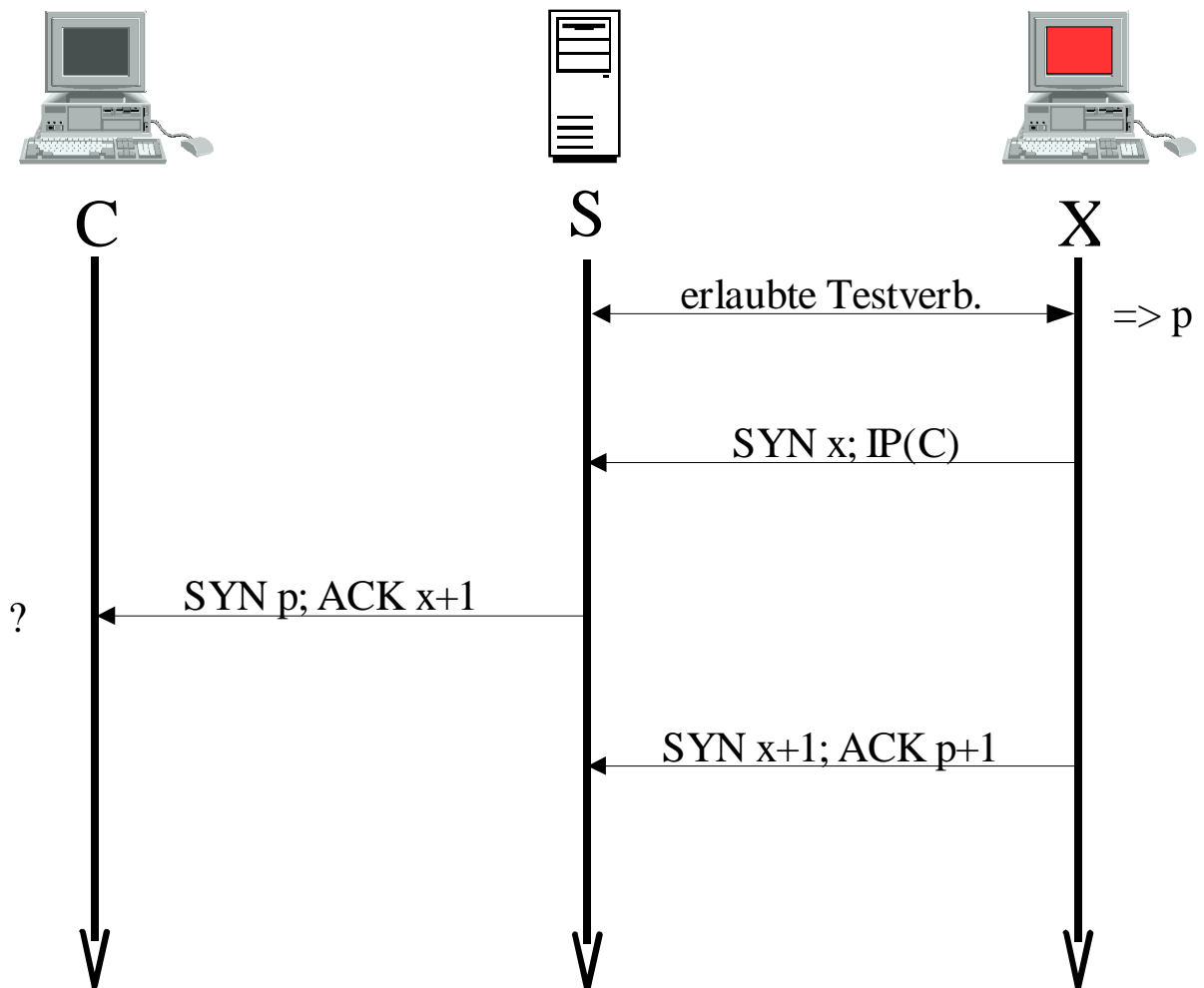
Überblick über Sicherheitsprobleme

TCP-Header



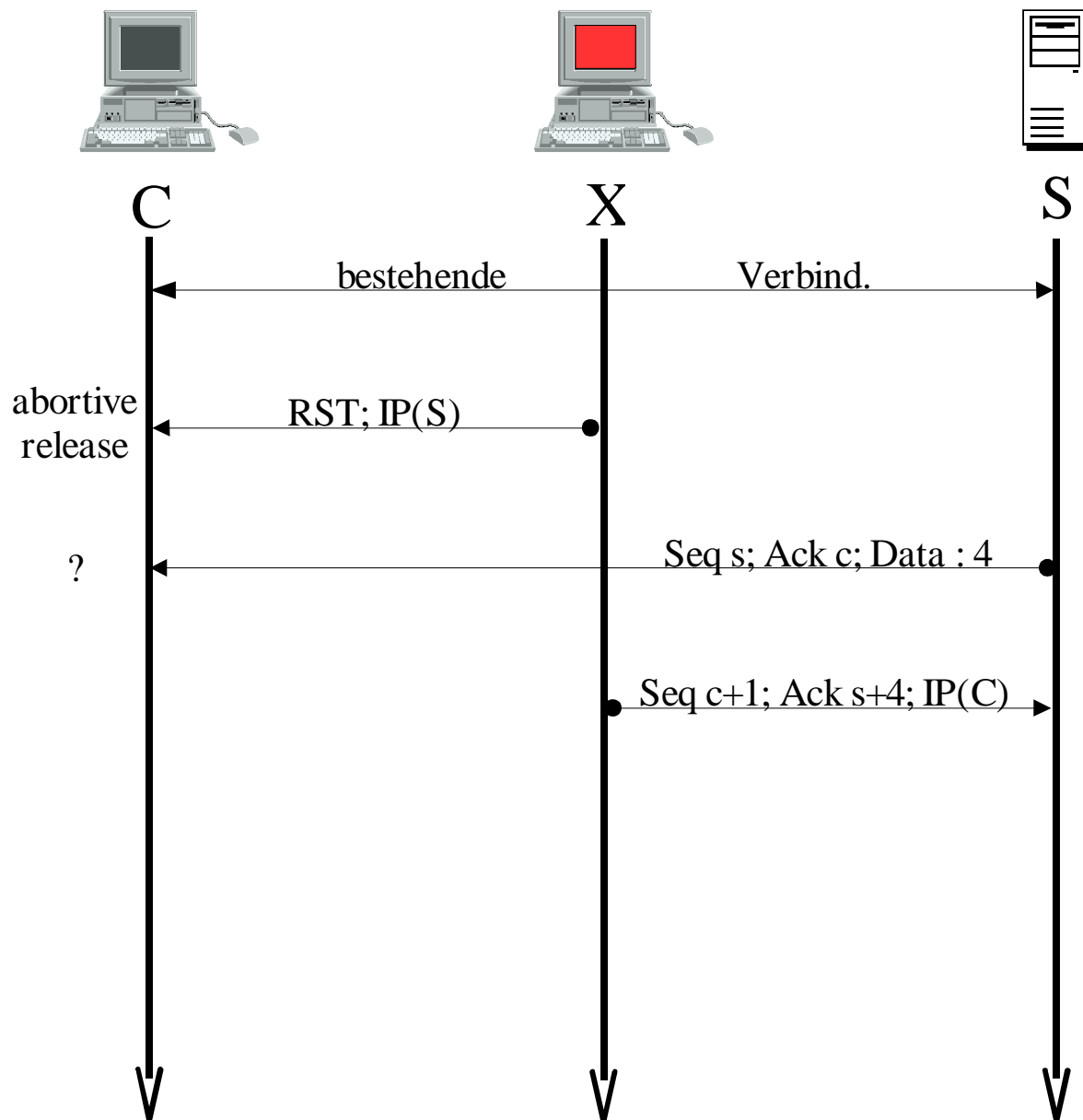
Überblick über Sicherheitsprobleme

TCP-Sequenznummer-Attack



Überblick über Sicherheitsprobleme

TCP-Hijacking



Überblick über Sicherheitsprobleme

TCP – Man-in-the-Middle – Attack

