

```
..$a3/.v%>login: root  
..$a3/.v%>password: gs$vm/13  
..$a3/.v%>sniffit ...  
..$a3/.v%>
```

> HACKER AM WERK

Von der öffentlichen Zugänglichkeit
privater Internetkommunikation

Hannes Federrath • TU Dresden

INTERNETKOMMUNIKATION

⌘ ANGREIFERSICHT

⊗ Interception / Hacken / Sniffen

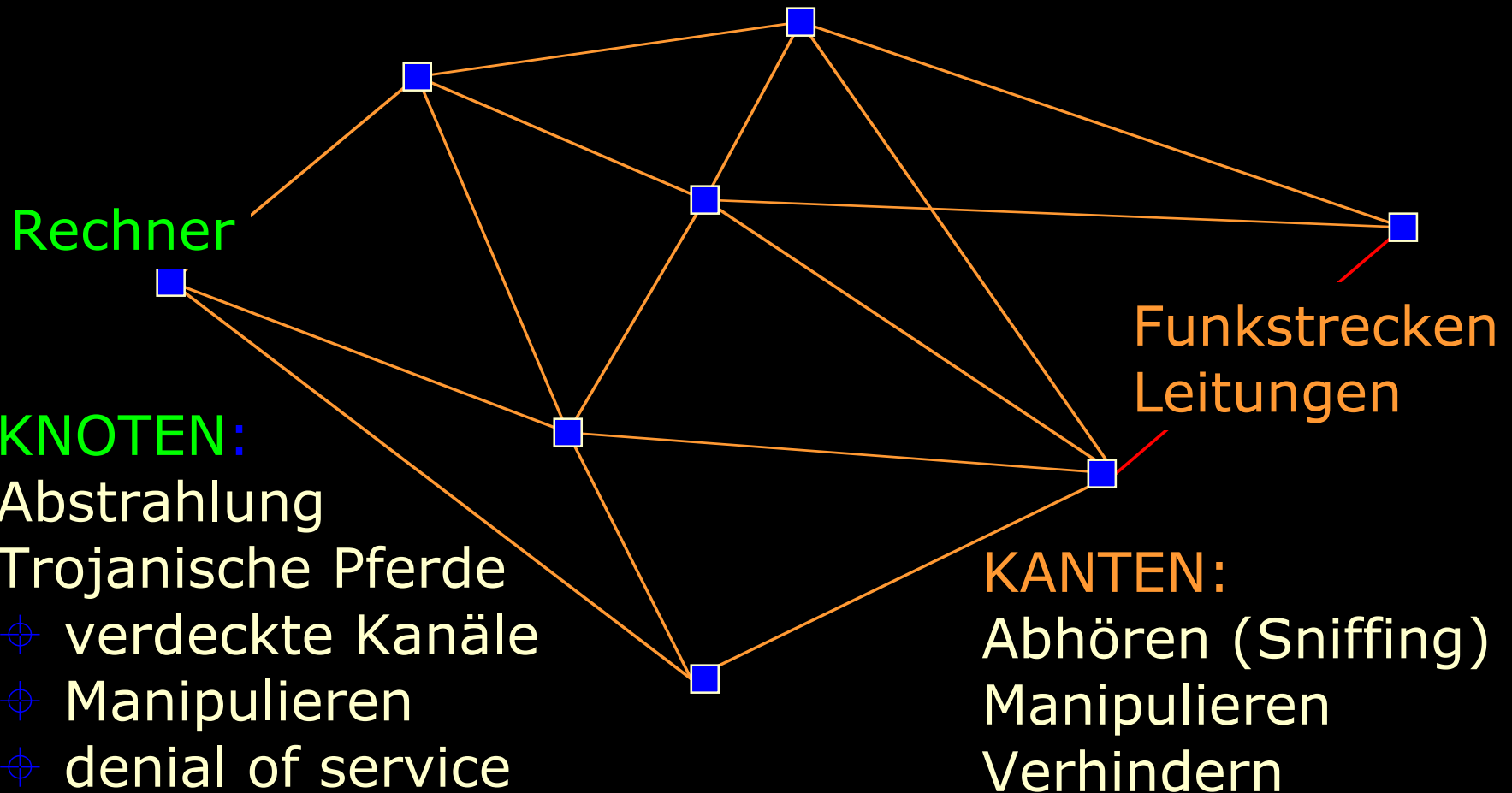
⌘ ÜBERWACHEN

⊗ in Echtzeit: **Sniffen**

⊗ spätere und / oder frühere Kommunikation:
Log-Dateien

⌘ WIE KOMMT MAN AN DIE DATEN?

> NETZ = KNOTEN + KANTEN



> NETZ = KNOTEN + KANTEN

⌘ SNIFFING: Angriff auf Kanten

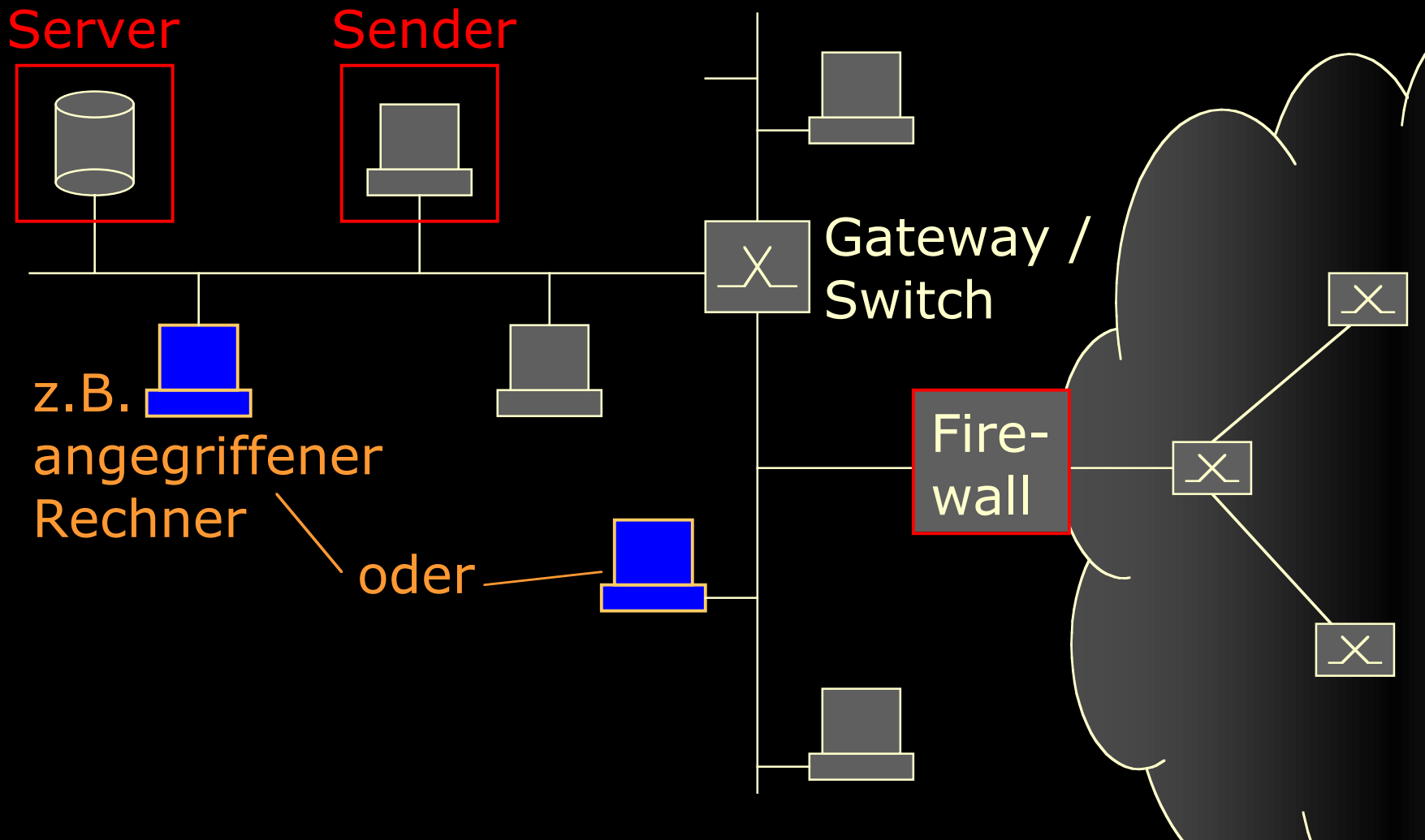
- ⊗ ECHELON
- ⊗ Lokales Netz
- ⊗ Telefonleitungen
- ⊗ Richtfunkstrecken

⌘ TROJANISCHE PFERDE:

Unberechtigter Zugriff auf Knoten

- ⊗ Verbindungsverschlüsselung hilft nichts
- ⊗ oft in Kombination mit Sniffing

> Szenario Daten abfangen



> Probleme des Angreifers?

⌘ Firewall überbrücken

- ⊗ Angriff verbergen in erlaubter Kommunikation, z.B. Web-Zugriff

⌘ Gateway / Switch überbrücken

- ⊗ Vortäuschen falscher (Absender)-Angaben (Spoofing)

⌘ Hacken / Cracken

- ⊗ meist nicht direkt beim Server oder Sender, sondern bei einem unauffälligen Rechner
- ⊗ Wie?

> Probleme des Angreifers?

⌘ Hacken / Cracken

- ⊗ Trivialmethoden

- ⊗ Schwächen / Programmierfehler ausnutzen

- ⊗ Einschleusen / Einbauen von Trojanischen Pferden

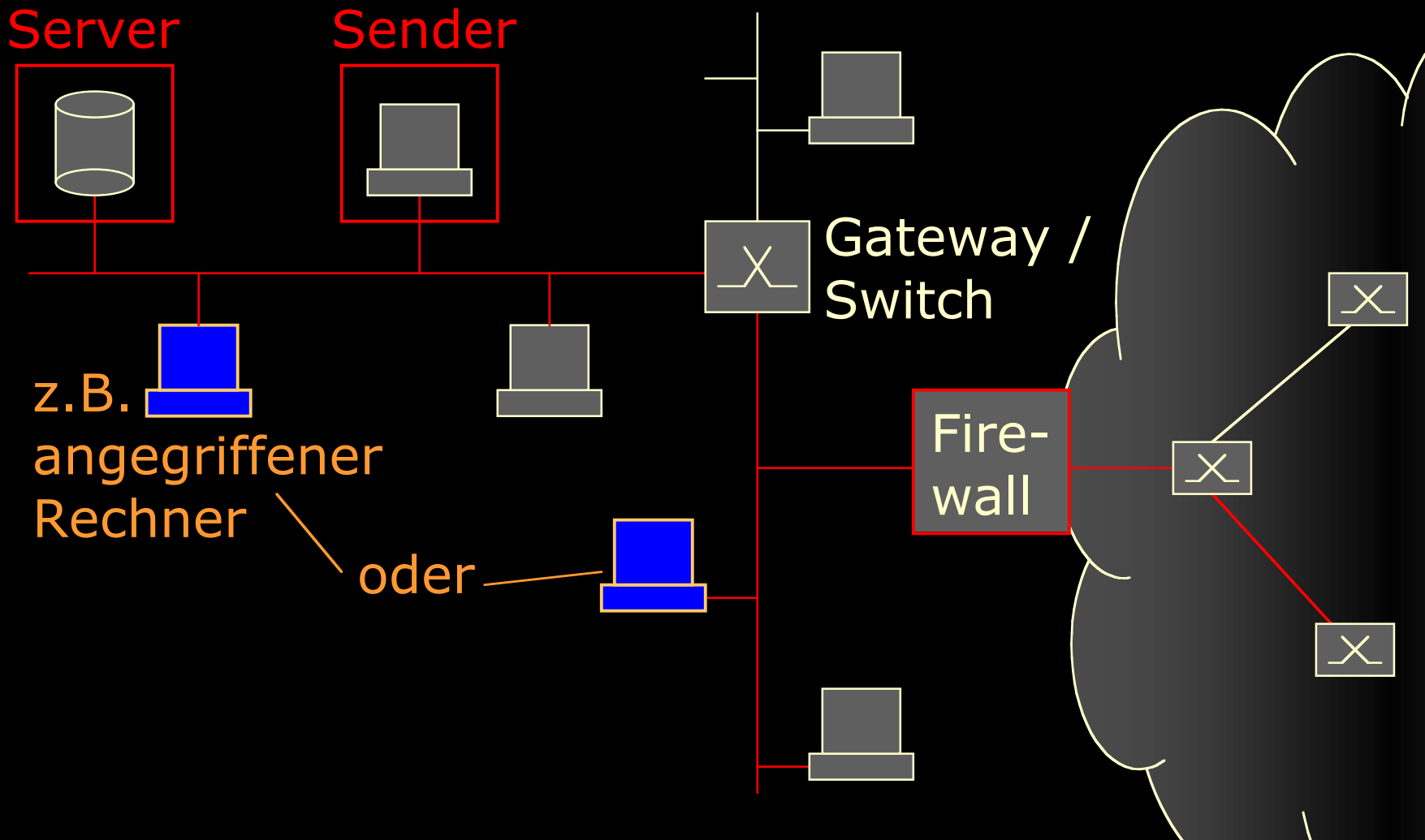
⌘ **JETZT:** Warten, bis etwas interessantes geschieht: z.B.

- ⊗ Passwörter vorbeikommen

- ⊗ E-Mails vorbeikommen

- ⊗ URLs vorbeikommen

> Szenario Daten abfangen



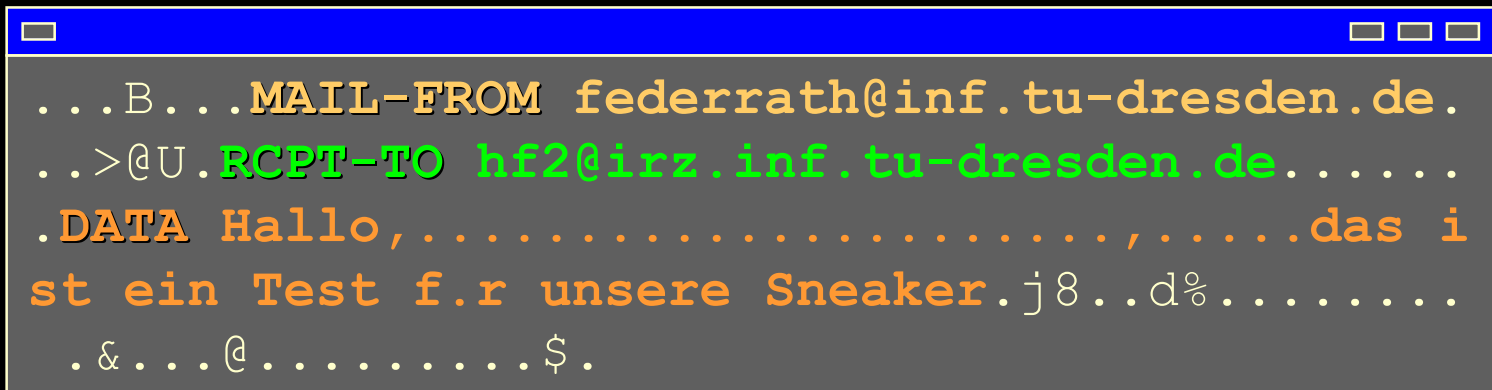
> Beobachtung im Internet?

- ⌘ E-MAIL: Log-Dateien zeigen Kommunikationsbeziehungen

```
>tail syslog
Oct 15 16:32:06 from=<feder@tcs.inf.tu-
dresden.de>, size=1150
Oct 15 16:32:06 to=<hf2@irz.inf.tu-
dresden.de>
```

> Beobachtung im Internet?

⌘ SNIFFER: Inhalte können mitgelesen werden



```
...B...MAIL-FROM federrath@inf.tu-dresden.de.  
..>@U.RCPT-TO hf2@irz.inf.tu-dresden.de.....  
.DATA Hallo,.....,.....das i  
st ein Test f.r unsere Sneaker.j8..d%.....  
.&...@.....$.
```

> Anonymität im Internet?

⌘ WORLD WIDE WEB: Log-Dateien zeigen Interessensdaten

```
wwwtcs.inf.tu-dresden.de>tail access_log
amadeus.inf.tu-dresden.de - -
[15/Oct/1997:11:50:01] "GET
/lvbeschr/winter/TechnDS.html HTTP/1.0" -
"http://wwwtcs.inf.tu-dresden.de/IKT/"
"Mozilla/3.01 (X11; I; SunOS 5.5.1 sun4u)"
```

> Anonymität im Internet?

⌘ FINGER: Die Ermittlung eines Rechnerbenutzers ist kein Problem

```
ithif19 logs 17 >finger @amadeus.inf.tu-dresden.de  
[amadeus.inf.tu-dresden.de]  
Login      Name          TTY          Idle         When  
feder      Hannes Federrath  console      Wed 11:56
```

> Was macht den Hacker ...

...zum Hacker? Oder: Was macht den unbescholtenen und spielfreudigen User zum Hacker?

⌘ Beispiel **Datenschutz-CD**

⊗ Immer wieder neue Auflagen, da die meisten Hackertools auf der Ausnutzung von Programmierfehlern beruhen

⌘ **Sniffing**: zunächst kein Einbruch ins System, jedoch strafbar; kaum Schutz

> Wie sich schützen?

- ⌘ INHALTE: Wirkungsvollste Methode:
ENDE-ZU-ENDE-VERSCHLÜSSELN
 - ⊗ Ohnmachtserfahrung des Hackers?
 - ⊗ Ja und nein: Verstärkt dort angreifen, wo Daten (noch) unverschlüsselt vorliegen
 - ⊗ LOKALER RECHNER / TROJANISCHE PFERDE
- ⌘ STEGANOGRAPHIE hilft auch

> Wie sich schützen?

- ⌘ Schutz vor TRAFFIC ANALYSIS:
 - ⊗ Techniken zum Schutz des SENDENS /
 - ⊗ des EMPFANGENS /
 - ⊗ und Schutz der
KOMMUNIKATIONSBEZIEHUNG
- ⌘ BROADCAST / DUMMY TRAFFIC /
PROXIES / MIXES / PSEUDONYME
- ⌘ STEGANOGRAPHIE hilft auch hier

> FAZIT

⌘ Ohnmachtserfahrung des klassischen abhörenden Angriffs (**interception**):
passiv

- ⊗ Ausweichen auf kompliziertere, aber im Endeffekt wirkungsvollere Methoden (z.B. Trojanische Pferde): **aktiv**
- ⊗ nur noch »TAMPERING OF PRIVATE DATA« möglich → **PHYSISCHE SICHERHEIT**, aber wie?
- ⊗ Analogie: Kryptoverbot → Steganographie