



••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

# Netzwerksicherheit

# Angriffsmechanismen

Stephen Wolthusen





# Modus Operandi

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Gezielte Angriffe von außen sind eher selten
  - Erfahrene Angreifer suchen meist „weiche Ziele“ innen
  
- Die Mehrheit der Angriffe sind Gelegenheitsangriffe
  - „script kiddies“ verwenden vorgefertigte Angriffe
  - Automatische Werkzeuge für Scans auf verwundbare Opfer
  - Die Attraktivität des Ziels spielt nur nachgeordnete Rolle
  - Wichtig ist „Blut im Wasser“:
    - ♦ Erreichbarkeit gefährdeter Dienste
    - ♦ Erkennung von fehlerhafter Server-Software und Inhalten
  - Finanziell motivierte Angreifer (Botnets für Spam, etc.) sind meist ähnlich beschränkt qualifiziert – aber offenbar gibt es hier signifikante Ausnahmen





# Modus Operandi II

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

## ■ Fortgeschrittene Angreifer verwenden

### „Island Hopping“-Technik

- Kette von Verwundbarkeiten entlang adjazenten Netzwerken, Hosts
  - ◆ Erreichen von Host in DMZ
  - ◆ Einspielen von Datenmaterial in WWW-Server für Rücktransfer
  - ◆ WWW-Admin mit internem Konto führt Code aus...
- Falsche Annahmen und Nachlässigkeiten führen oft zu katastrophalen Verwundbarkeiten
  - ◆ Ein populärer SOHO-Router/“Firewall“ erlaubt Zugriff von internem Netz via Telnet
  - ◆ Einschleusen einer Telnet-Datenverbindung von außen via einem legitimen Browser-Datenkanal ist einigermaßen trivial





# Offenlegung von Verwundbarkeiten („Full Disclosure“)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Diskussion ist mindestens so alt wie BUGTRAQ (1993)
  - Wenn ausreichend Informationen zum Nachvollziehen einer Verwundbarkeit vorhanden ist, wird damit Angreifern geholfen
  - Vage Angaben lassen keine klare Identifikation, Reproduktion, oder Verifikation der Verwundbarkeit zu
  - Hersteller verschleppen häufig gemeldete Verwundbarkeiten (CERT-Vorgehensweise)
  - WIPO/WCT und Umsetzungen (DMCA, ZKDSG etc.) bieten rechtliche Handhabe zur Unterdrückung von unliebsamen Meldungen
  - Europarats-Konvention zu „Cybercrime“: Je nach Lesart ist hier durchaus bereits der Besitz von typischem Proof-of-Concept zur Demonstration von Sicherheitslücken potentiell strafbar





# Diverse Informationsquellen

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- BUGTRAQ
- NTBUGTRAQ
- VULN-DEV
- NMAP-HACKERS
- VULNWATCH
- Technotronic
- Firewall Wizards
- Incidents





# Code Red (I + II)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- IIS-Verwundbarkeit: Indexing Server
  - Patch war bekannt seit dem 18. Juni 2001
  - Dienst meist unnötig
- Code Red I: 12. Juli 2001
  - Wurm mit statischer Adreßverteilung
- Code Red II: 19. Juli 2001
  - Nutzt gleiche Verwundbarkeit, zufällige Weiterverbreitung
  - Kaum Gemeinsamkeiten im Code zwischen CRI und II
  - Mindestens 450,000 Hosts infiziert, LD50 erst nach 11 Tagen
- Plus ca change...: Blaster, Slammer, Nachi, Witty (2003/04)







# Blaster / Sapphire (MS03-026)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

Map source: [www.visualroute.com](http://www.visualroute.com)



Sat Jan 25 05:29:00 2003 (UTC)

Number of hosts infected with Sapphire: 0

<http://www.caida.org>

Copyright (C) 2003 UC Regents

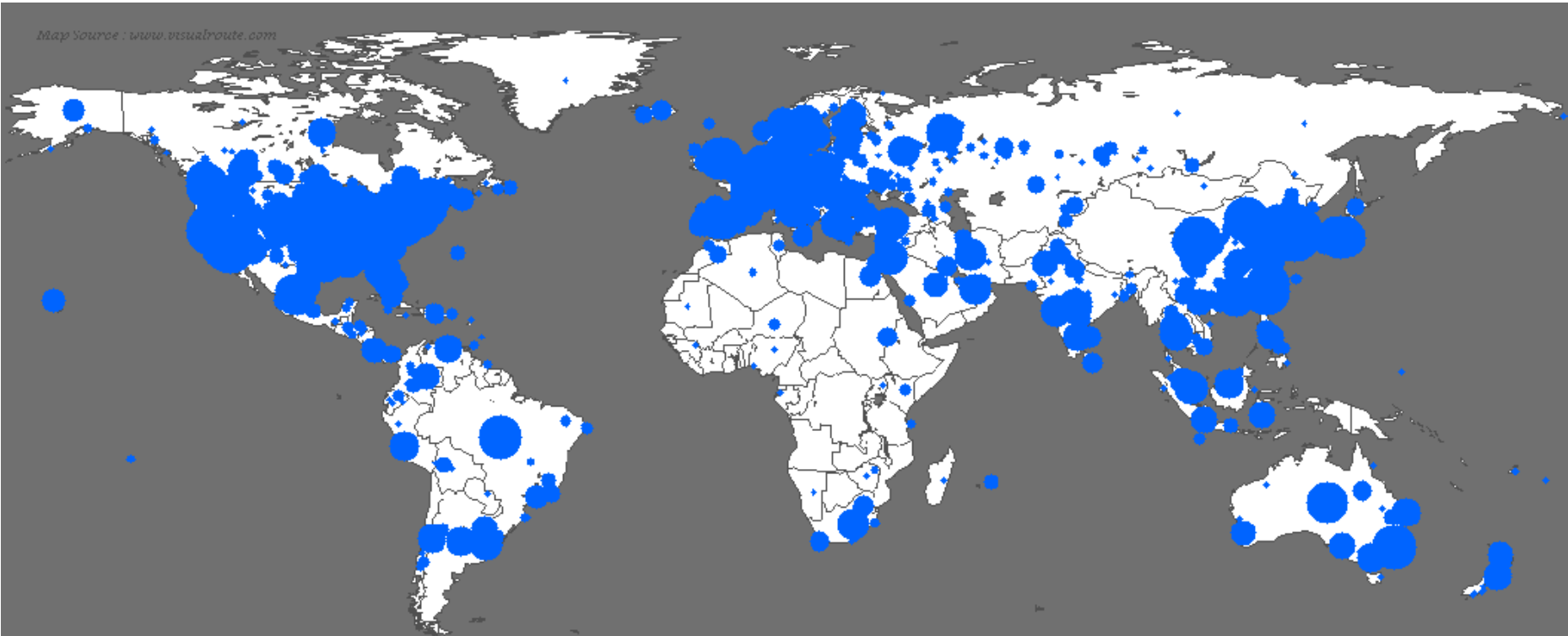




# Blaster / Sapphire (MS03-026)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

Map source: [www.visualroute.com](http://www.visualroute.com)



Sat Jan 25 06:00:00 2003 (UTC)

Number of hosts infected with Sapphire: 74855

<http://www.caida.org>

Copyright (C) 2003 UC Regents





# Project HoneyNet

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

## ■ Honeypot:

- Rechner mit für Angreifer vermutlich attraktiven (gefälschten) Inhalten, der vom eigentlichen Netz abhalten soll und rechtzeitige Vorwarnung ermöglicht

## ■ HoneyNet analog:

- (simulierte) Netzwerke, die von Angreifern kompromittiert werden sollen

## ■ Ziele:

- Beobachtung aktiver Hacks „in freier Wildbahn“
- Methoden, Werkzeuge, operatives Vorgehen





# Angriffe auf Authentisierungsverfahren

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Es werden immer noch häufig Klartext-Authentisierungsverfahren eingesetzt (telnet, Windows NTLM)
  - Abhören von Netzwerkverkehr
    - ◆ Schwierig in bridged networks, WANs
    - ◆ Dennoch: DNS Cache Poisoning, Routing-Injektion
    - ◆ Angreifer kann meist Authentisierung wiederverwenden
  - Man in the Middle-Angriff:
    - ◆ Angreifer gibt sich als Host aus
  
- Gefahrenmomente durch wiederverwendete Konten/Paßwörter unterschiedlicher Sicherheitsstufen





# „Sichere“ Authentisierungsverfahren

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- X.509-Zertifikate
  - Qualität der Registration Authority? Betrieb? Wer haftet?
- Zertifikate, öffentliche Schlüssel (SSH, PGP)
  - Wer prüft Angaben der Schlüssel gewissenhaft?
- Meist ist Man in the Middle Attack möglich, da die kryptographischen Mechanismen nicht bestimmungsgemäß eingesetzt werden
- Gelingt es einem Angreifer, z.B. eine WWW-Site zu kompromittieren oder umzulenken erhält er Authentisierungsdaten (von innen **und** außen)





# Angriffe mittels Datenmaterial

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

## ■ Häufigste Ursache kompromittierter Systeme

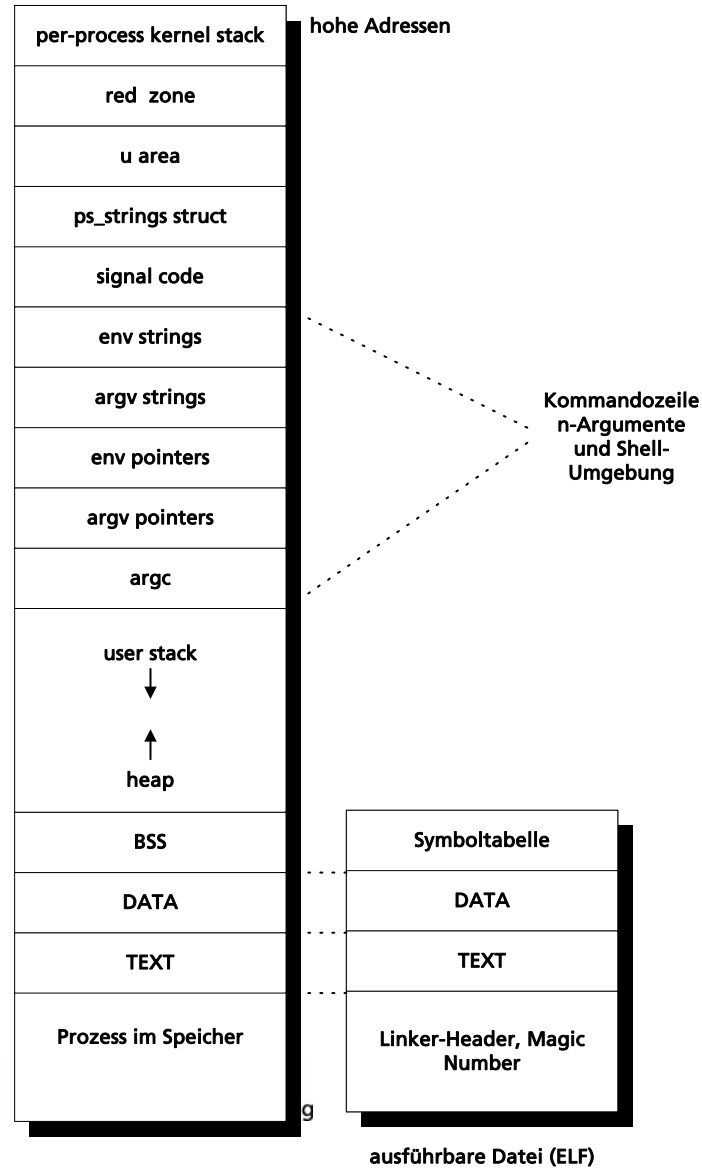
- Eingaben werden unzureichend überprüft
- Grundlegende Probleme: Buffer Overflows: Mehr dazu gleich
- Semantik von Eingabedaten
  - ◆ Unzureichende Überprüfung auf Escapes, Sonderzeichen
  - ◆ Evaluierung von Puffern in perl: Ausführung von Skripten
  - ◆ Der „...“-Bug: In NCSA HTTPD 1995 korrigiert... und 2001 in mehreren Inkarnationen (Unicode...) in Microsoft IIS 5.0 wieder aufgetreten
  - ◆ Alle Jahre wieder: Buffer Overflows in Microsoft MDAC (IIS und lokale Angriffe), MS02-065, MS03-033, MS04-003





# Stack-Frame für Unix-Derivate

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





# C-Fragment für Stack-Betrieb (Linux x86)

... department security technology ... department security technology ... department security technology ... department security technology ...

```
■ void foo(int a, int b, int c)
  {
    char bar[5];
    char baz[10];
  }

■ int main(void)
  {
    foo(1, 2, 3);
    return 0;
  }
```





# Stack-Frame nach Aufruf

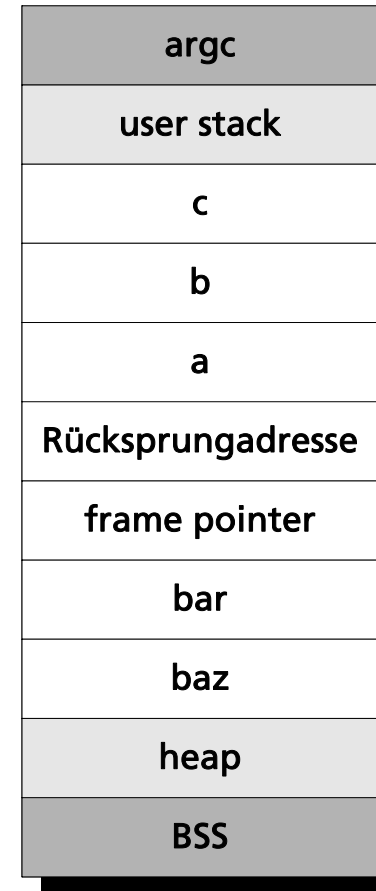
••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

```
pushl    $3
pushl    $2
pushl    $1
call     foo
```

## Assembler-Fragment für Beispiel

```
pushl    %ebp
movl     %esp, %ebp
subl    $20, %esp
```

## Anlegen des Stack-Frame



hohe  
Adressen





# C-Fragment für Stack-Overflow (Linux x86)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

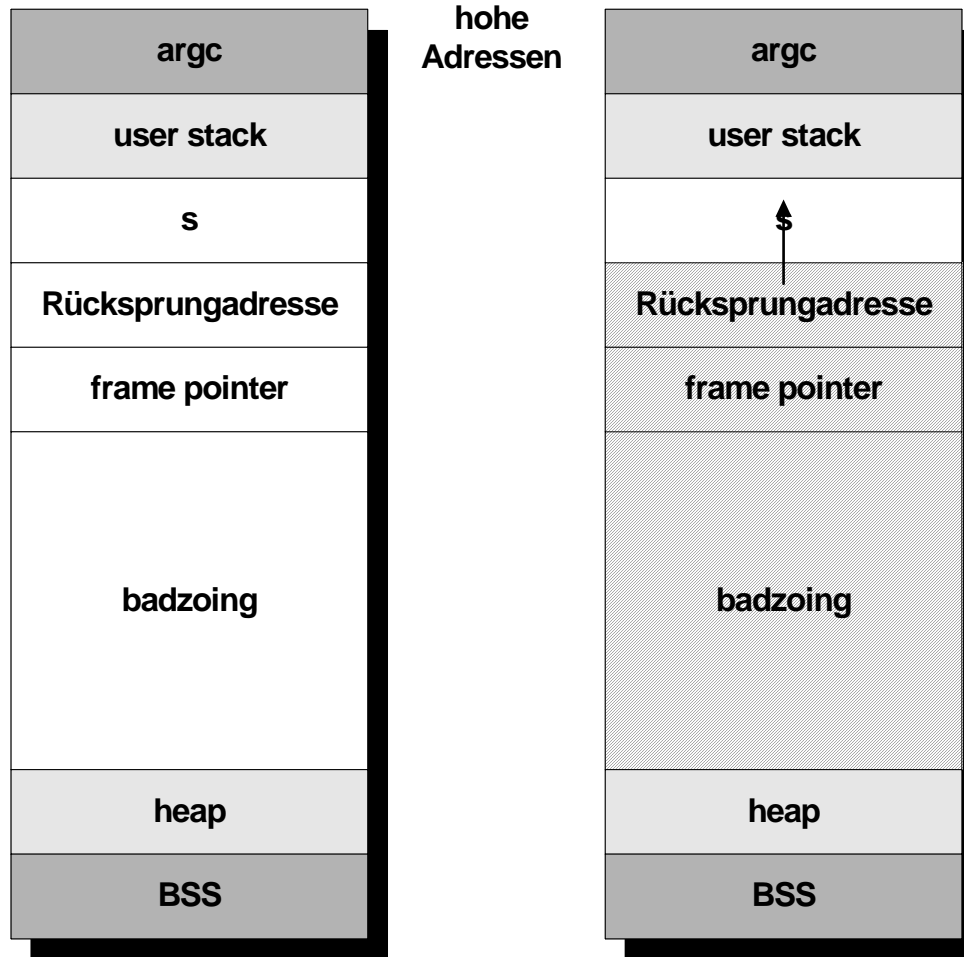
```
#include <strings.h>
void foobar(char *s)
{
    char badzoing[16];
    strcpy(badzoing,s);
}
int main(void)
{
    char bazooka[256];
    int i;
    for(i=0; i<256; i++)
        bazooka[i]=42;
    foobar(bazooka);
    return 0;
}
```





# Stack Frame nach Overflow

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





# Shell Code

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

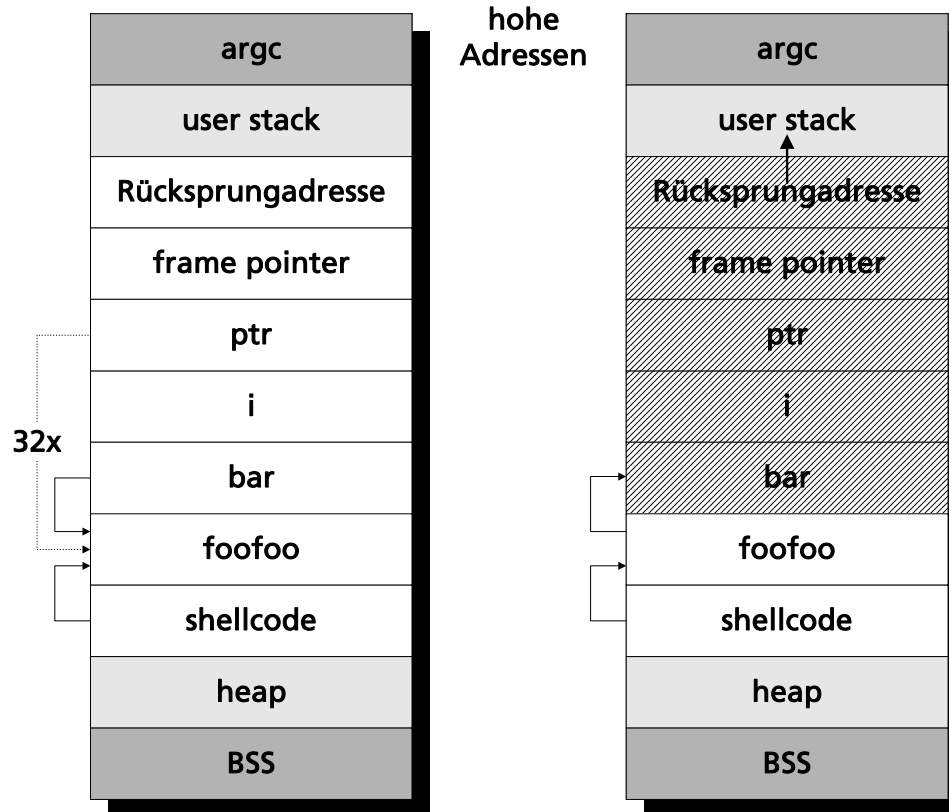
- Einfügen von ausführbarem Code bzw. eines Sprungs in existierenden Code anstelle der Rücksprungadresse einer Funktion
  - Ermöglicht Ausführung beliebigen Codes mit Privilegien des ausführenden Prozesses
  - Unter Unix: Traditionell Ausführen einer Shell für den Angreifer (mit root-Privilegien)
    - ♦ `execve(name[0], "/bin/sh", NULL);`
  - Shellcodes für verschiedene Architekturen, Betriebssysteme gibt es als fertige Sammlung (Phrack etc.)





# Stack Frame nach Aufruf mit Shellcode

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





# Alternativen zu Stack Overflows

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Gegenmaßnahmen:
  - Compiler-Maßnahmen, Stack-Guard-Mechanismen, W<sup>^</sup>X,...
    - ◆ Sind auch zu umgehen, wenn auch mit etwas mehr Aufwand
- „Return to libc“ und verwandte Angriffe
  - Ausnutzen bestehenden Codes durch Einschmuggeln von Argumenten
- Funktionszeiger-Manipulationen
  - Funktionszeiger, Exception Handler, VPTR-Tabellen
- Heap Overflows
  - Deutlich schwieriger als Stack Overflows





# Die Wahl des richtigen Werkzeugs...

... department security technology ... department security technology ... department security technology ... department security technology ...

Es gibt Programmiersprachen,  
in denen Buffer Overflows,  
Heap Overflows, Integer  
Overflows etc. nicht  
vorkommen können

C/C++/Java/C# gehören nicht  
(vollständig) dazu.





# Fragmentierungs-Angriffe

... department security technology ... department security technology ... department security technology ... department security technology ...

- Angriffe auf IP Fragment Reassembly
  - Teardrop (Oktober 1997): Fragmente negativer Länge
  - Bonk: Wenige Monate später (April 1998)
    - ◆ Offset des 2. Fragments gewählt, sodaß dieses größer ist als Header-Länge
- Überprüfung von Eingabedaten ist zeitaufwendig, schwierig, und zwingend notwendig
- Ping of Death (ca. 1996)
  - Länge des ICMP Echo durch weiteres Fragment größer 65507 Bytes für Pakete ohne sonstige Optionen





# IP Spoofing TCP Session Hijacking

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

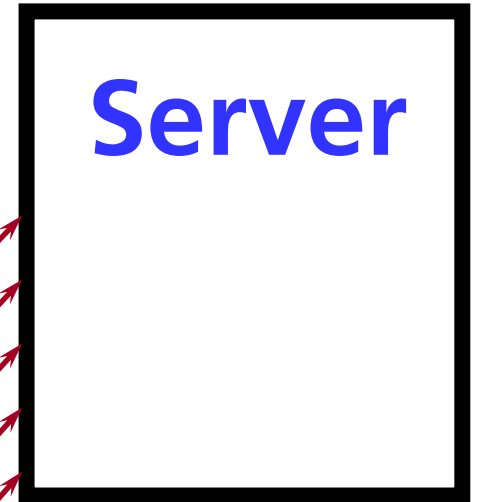
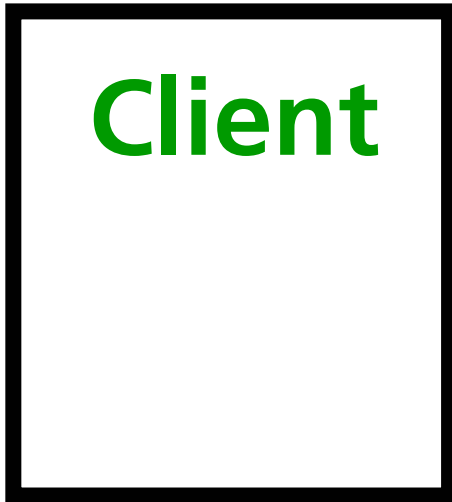
- DoS-Angriffe können Selbstzweck sein, sind aber oft nur Präludium zur eigentlichen Attacke
- IPv4 bietet keine Möglichkeit zur Authentisierung der Adressen, die Felder können beliebig belegt werden - „Spoofing“
- TCP Session Hijacking
  - Übernahme einer in Aufbau oder im Betrieb befindlichen TCP-Verbindung
  - Meist genutzt zum Einschmuggeln von Kommandos zur Kompromittierung eines Hosts





# Spoofing: Bestimme wahrscheinliche $SEQ_0$

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





# (Temporäres) Ausschalten des Clients

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

**Client**

**Server**

“Killer Packet” /  
SYN-Flood

**Angreifer**





# Vertrauenswürdiger Client reagiert nicht mehr

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

~~Client~~

Server

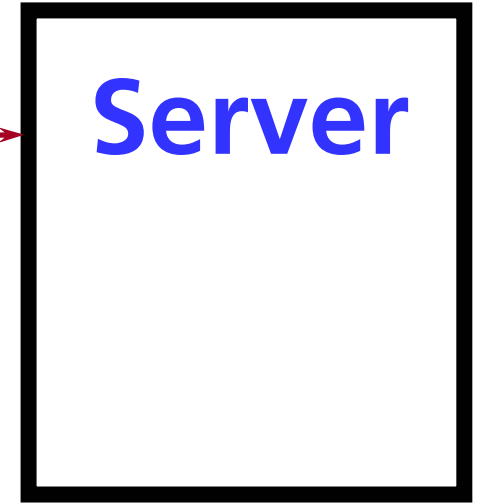
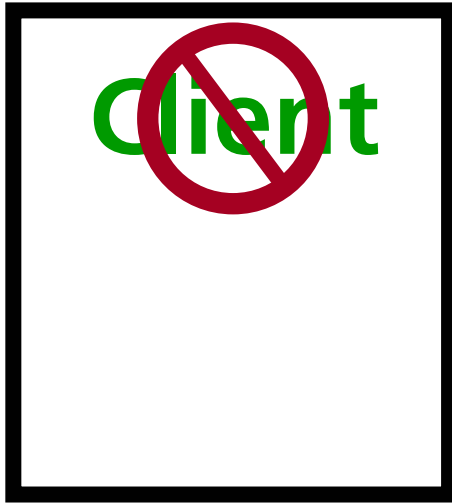
Angreifer



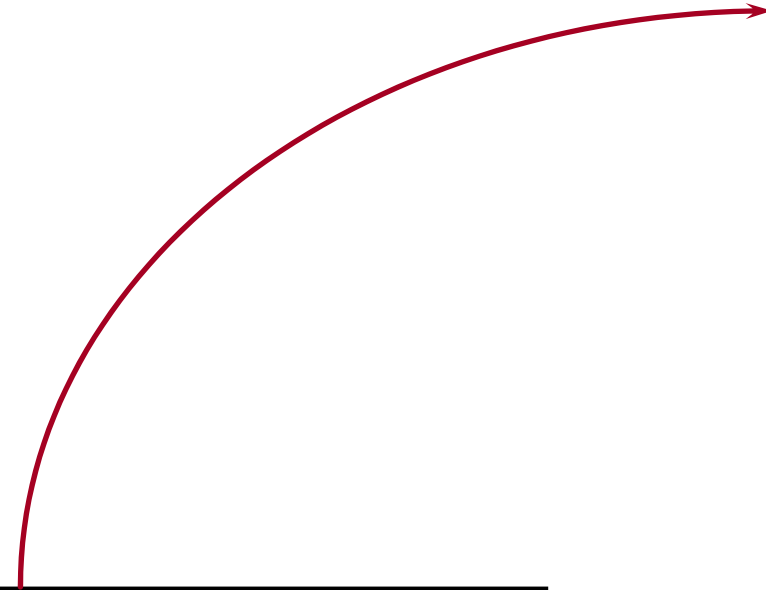


# Angreifer sendet Paket von „Client“

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••



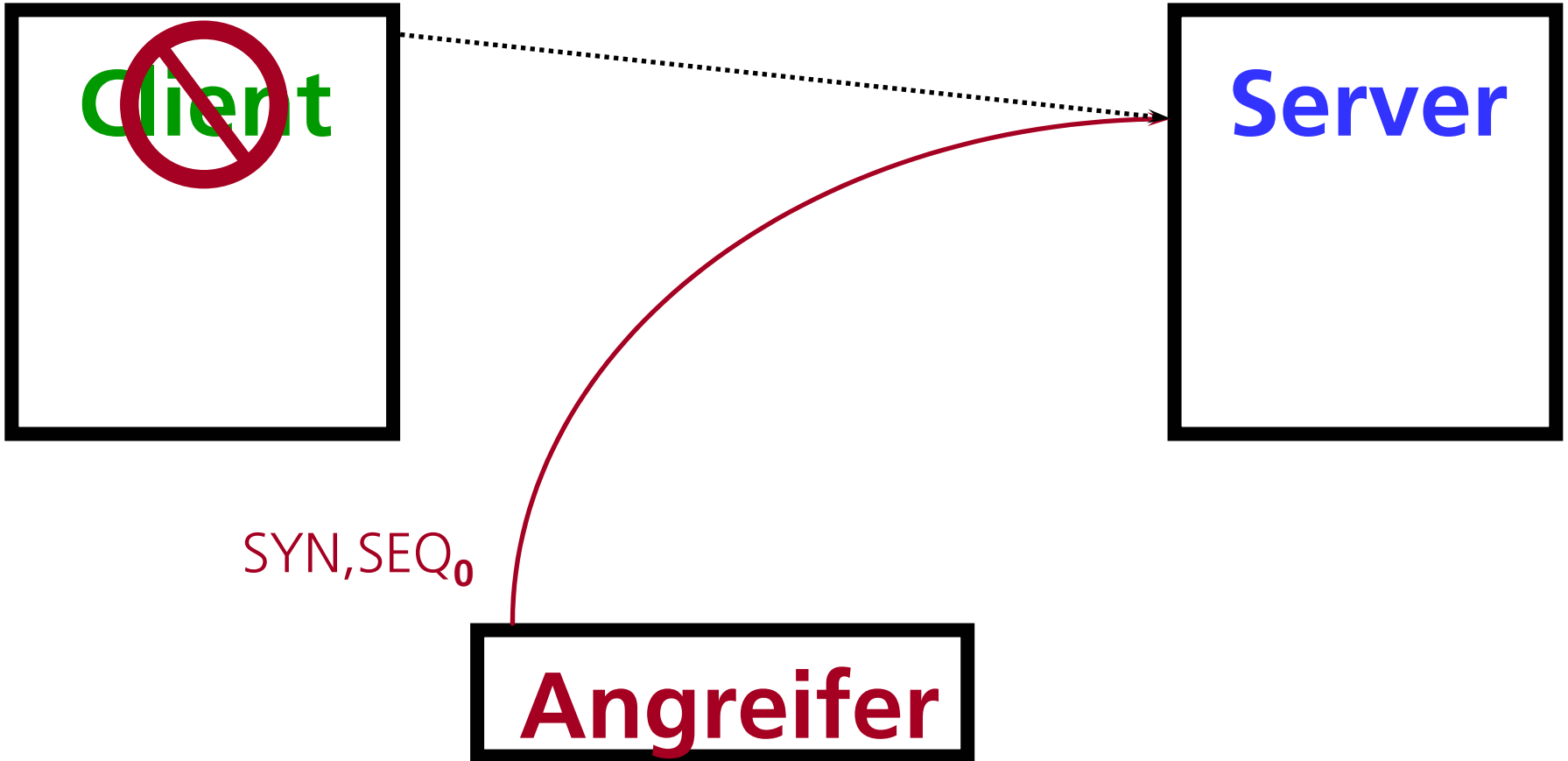
SYN,SEQ<sub>0</sub>





# Server sieht Verbindung von bekanntem Client

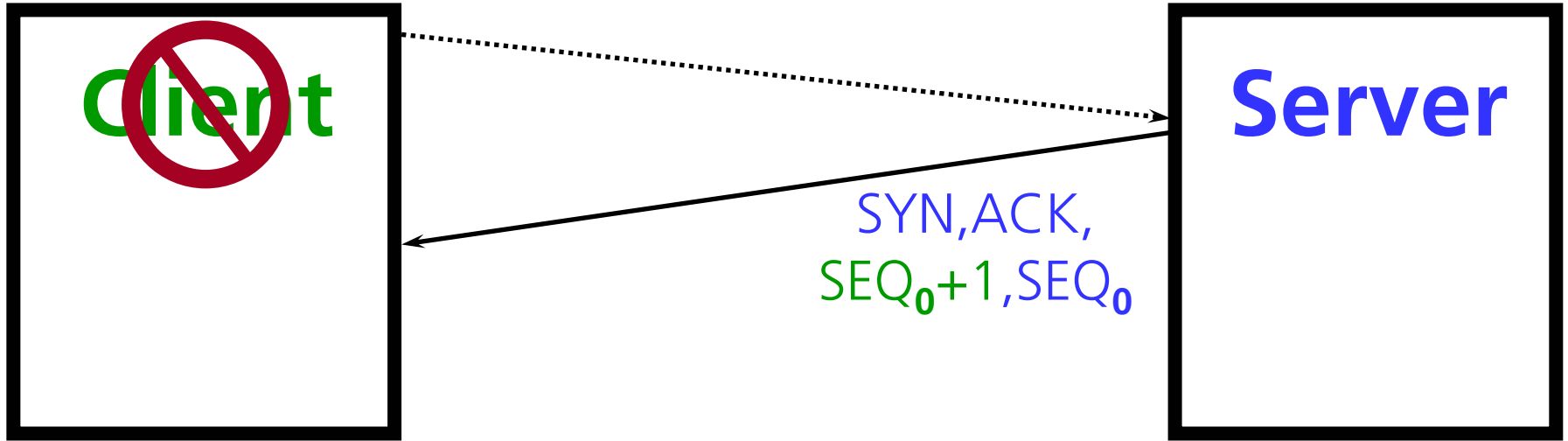
••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





# Server antwortet inaktivem Client

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••



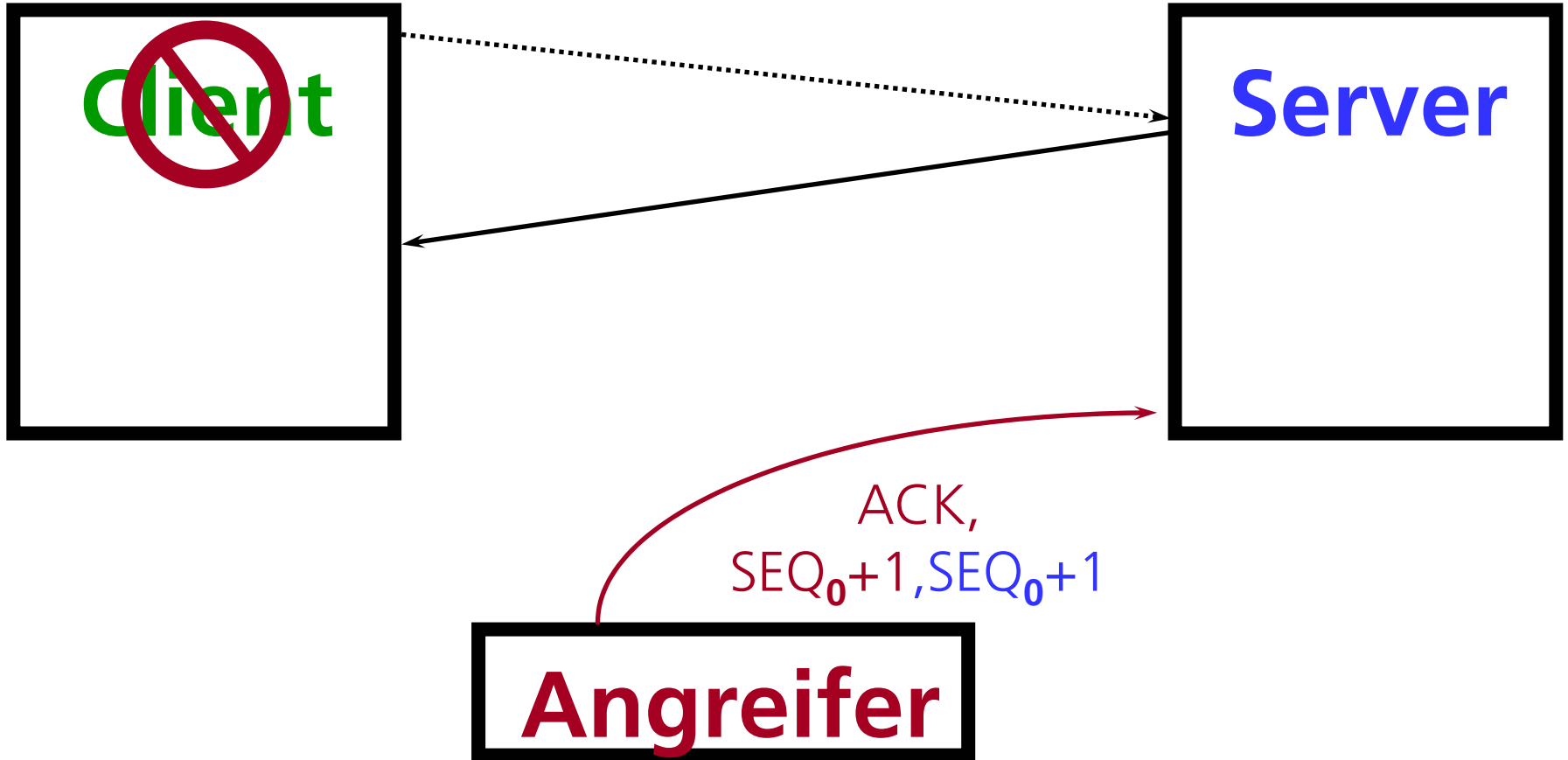
**Angreifer**





# Angreifer beendet Handshake mit Spoof-Paket

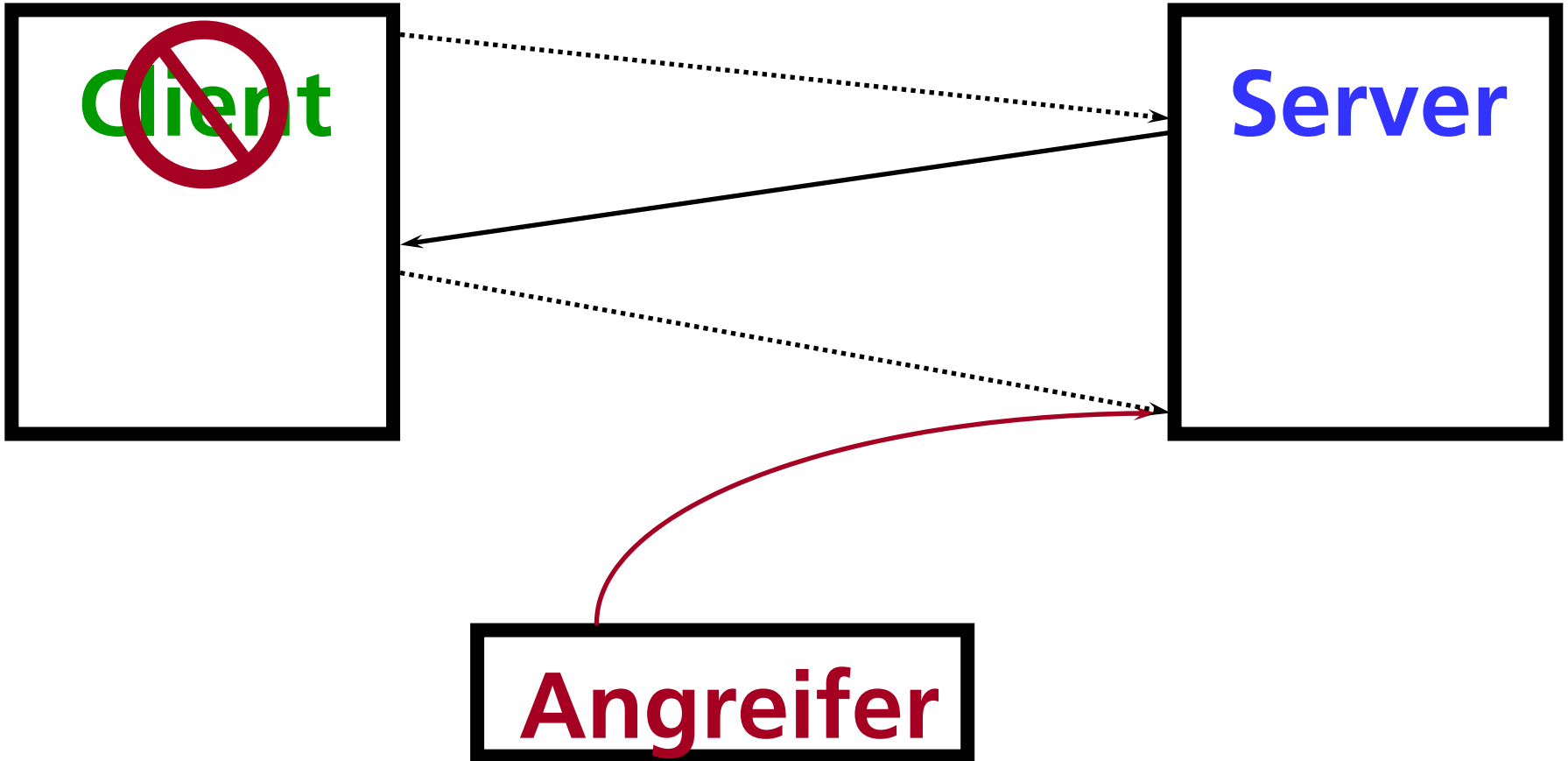
... department security technology ... department security technology ... department security technology ... department security technology ...





# TCP-Verbindung zu „Client“ ist damit aufgebaut

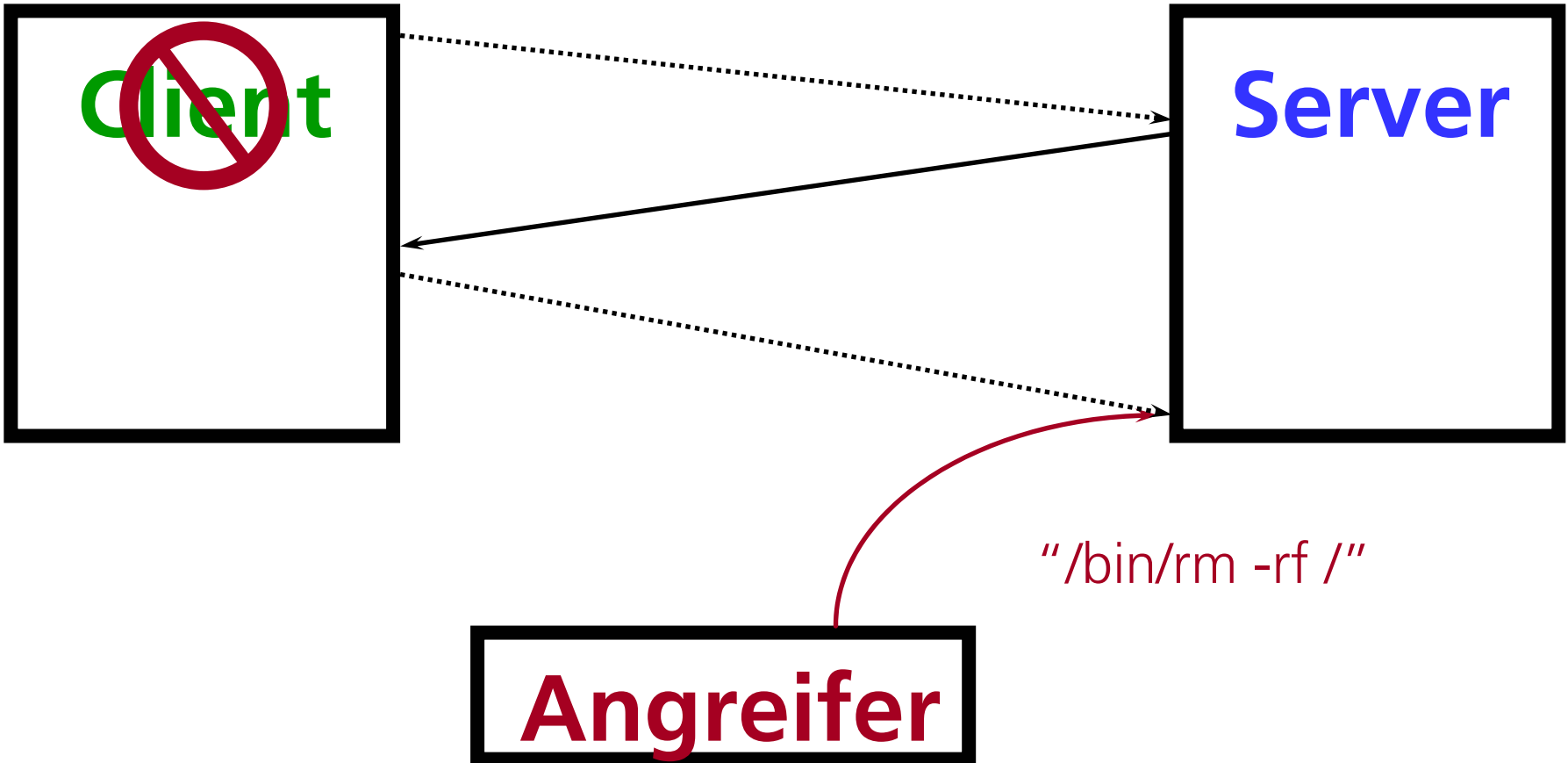
••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





# Angreifer kann nun z.B. Kommandos absetzen

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





# Gekaperte Sitzung aus Sicht des legitimen Nutzers

... department security technology ... department security technology ... department security technology ... department security technology ...

```
login: test
s/key 70 me33827
(s/key required)
Password:
Last login: Fri Aug 10 22:02:38 from baltimore.ftc.igd.fhg.de
Sun Microsystems Inc.      SunOS 5.8          Generic February 2000
[cle-te: /spac] pwd
Mail/           mbox          src/
elm*            resize*      traceroute*
/space/home/test
[cle-te: /spac] history
1 22:02 ls ; pwd
2 22:02 history
[cle-te: /spac] logout
Connection closed by foreign host.
```





# IP-Spoofing / Session Hijacking

... department security technology ... department security technology ... department security technology ... department security technology ...

- Angriffe von außen sind leicht abzufangen
  - Filterungsregel, die interne Adressen als Quelle angeben, verbieten
  - Abgrenzung von Netzwerksegmenten unterschiedlichen Vertrauensgrades
- Gegen Angriffe von innen hilft nur eine starke Authentisierung
- Adreßbasierte Authentisierung (rhosts...) ist keine





# Denial of Service

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

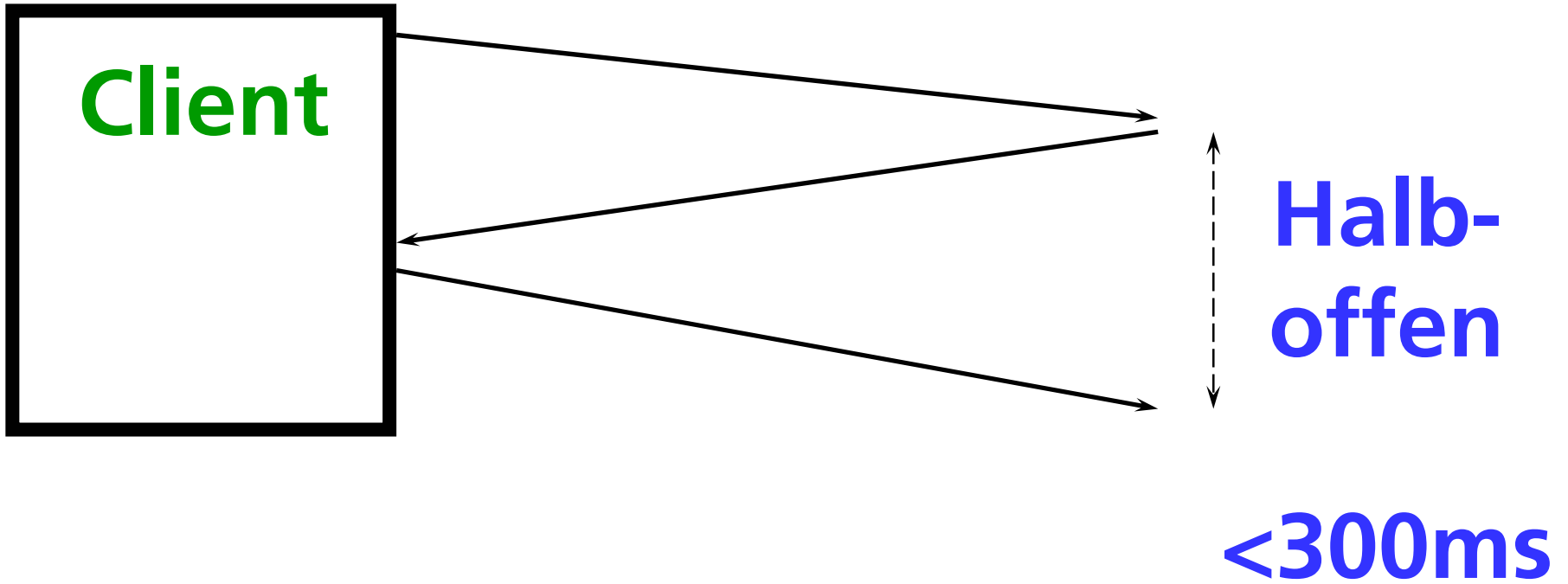
- Nutzung von Diensten oder Verfügbarkeit von Ressourcen wird legitimen Nutzern verweigert.
- Die Legitime Nutzung kann dabei nur temporär verlangsamt, verhindert, oder durch Zerstörung von Ressourcen permanent unmöglich werden





# SYN Flooding

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





# SYN Flooding

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

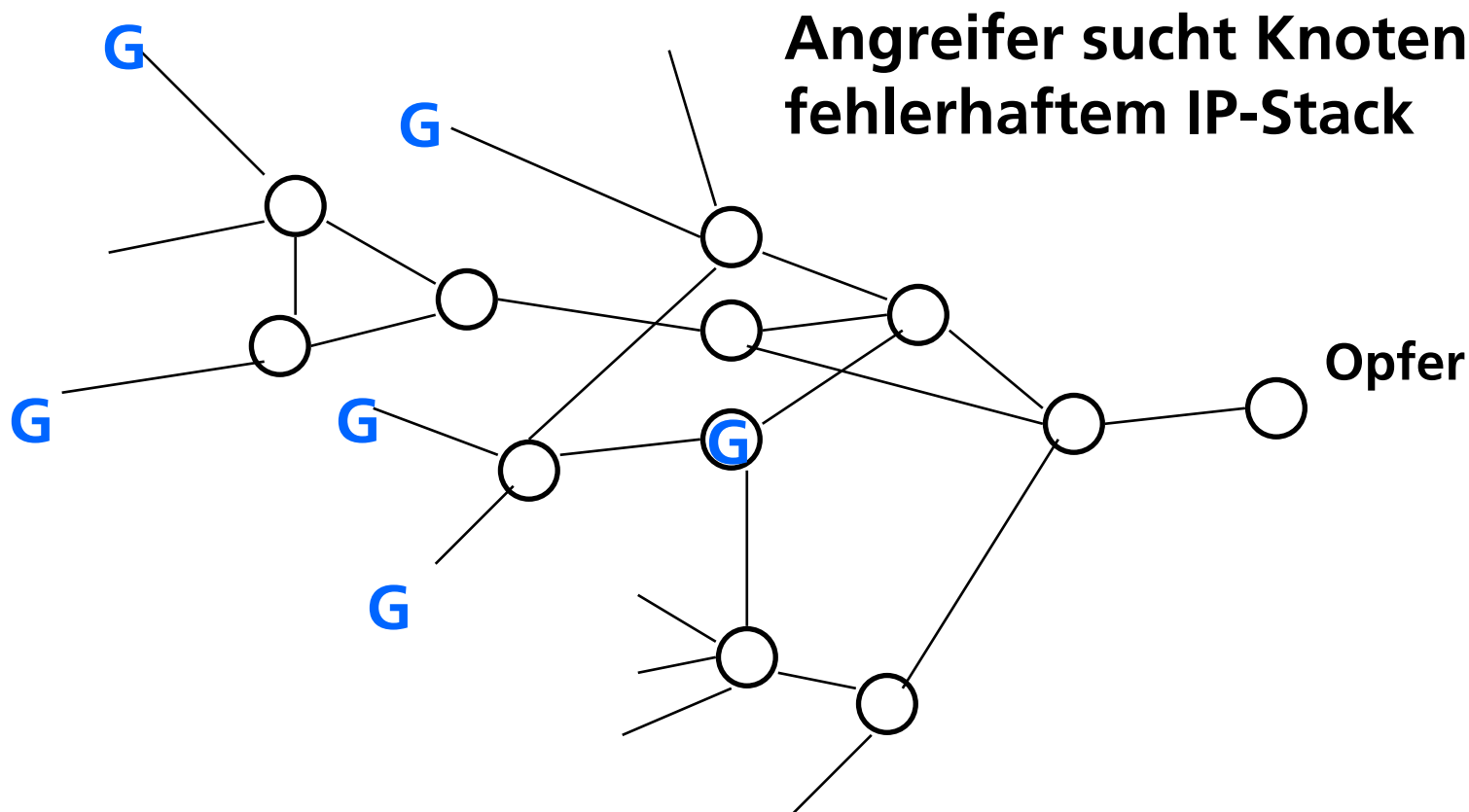
- Ziel wird mit SYN-Paketen bombardiert
  - Große Anzahl halboffener Verbindungen
    - ◆ Ressourcenverbrauch auf Gegenseite
    - ◆ Einige Implementierungen haben ungünstige Algorithmen in Open-Handhabung
  - Ungewöhnliche Adreßfelder und Optionen verwirren einige Implementierungen
  - Opfer ist eine Zeit lang „mit sich selbst beschäftigt“ oder TCP/IP-Stack / System bricht zusammen





# Denial of Service: Smurf...

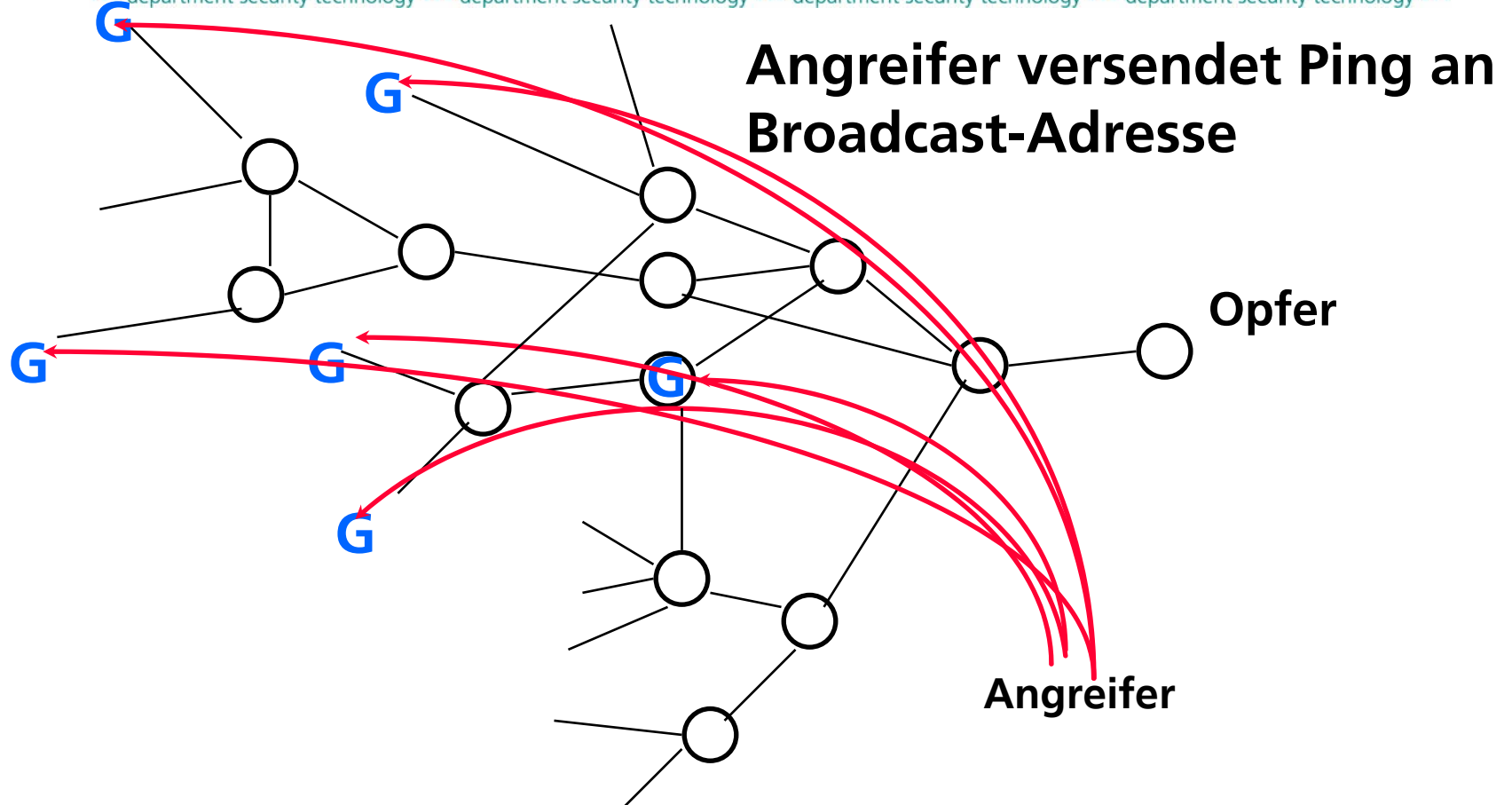
... department security technology ... department security technology ... department security technology ... department security technology ...





# Denial of Service: Smurf...

... department security technology ... department security technology ... department security technology ... department security technology ...

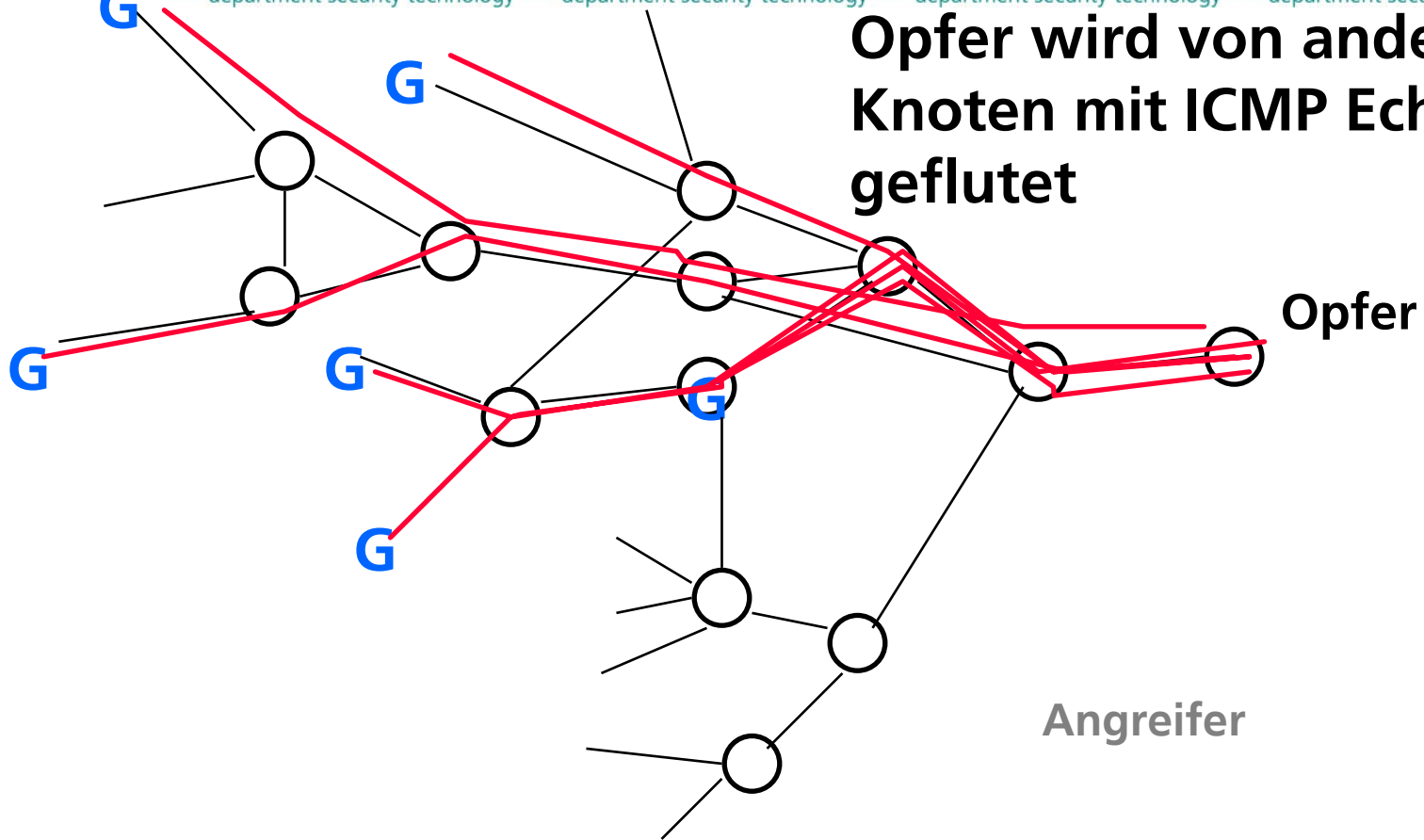




# Denial of Service: Smurf...

... department security technology ... department security technology ... department security technology ... department security technology ...

**Opfer wird von anderen Knoten mit ICMP Echo Reply geflutet**





# Smurf/Fraggle

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Smurf versendet ICMP Echo Requests an Broadcast-Adresse
  - Eigentlich darf keine ICMP Echo Reply generiert werden...
- Fraggle versendet UDP-Pakete an Broadcast-Adresse
  - Dafür kann es legitime Gründe geben
- Ziel des Angriffs ist weitgehend machtlos
  - Seine Bandbreite ist in jedem Fall verloren
- Beseitigung nur durch Kooperation potentieller Opfer/ISPs
  - Abfangen von Smurfs an Site/ISP-Boundaries





# Botnets

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

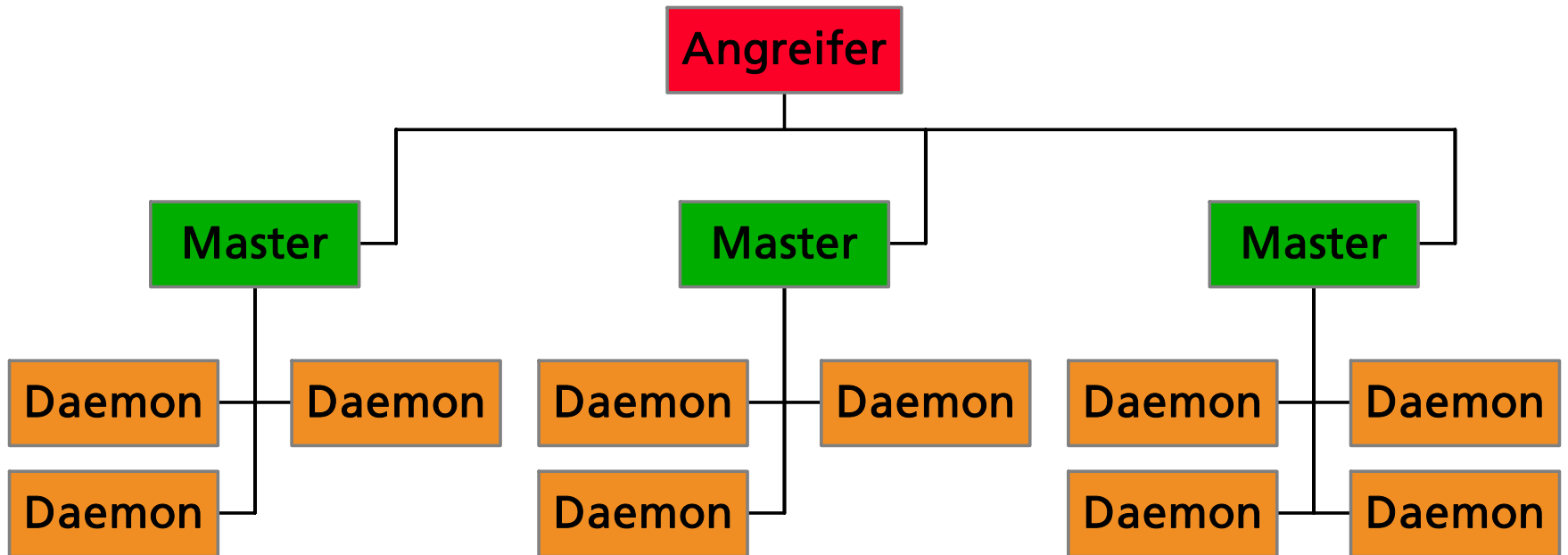
- **TFN / Trinoo / Stacheldraht**
  - Ursache für Medienecho im Februar 2000
  - Im Untergrund davor im Einsatz seit Anfang 1999
  - Weiterentwicklung von Smurf/Fraggle
  - Setzen auf kompromittierte Hosts, die auf Befehl DoS-Angriffe fahren
  
- **Komplexes hierarchisches Netzwerk**
  - Hilft Spuren zu verwischen
  - Erlaubt Nutzung von tausenden von Hosts für DoS-Paketerzeugung
  - Art der Pakete ist hier egal (z.B. legitime HTTP-Requests)
  
- **Mittlerweile im Routineeinsatz auch durch OK**
  - Leichtes Spiel durch breitbandig angebundene Heimanwender





# TFN / Trinoo / Stacheldraht: Mehrschichtiges Protokoll

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





# TFN / Trinoo / Stacheldraht

... department security technology ... department security technology ... department security technology ... department security technology ...

- Angreifer / Master / Daemon kommunizieren über Pseudo-Shell
  - UDP-basiert
  - Paßwort-geschützt
  - Erlaubt komfortable Bedienung des Flood-Netzes
- Angriff erfolgt durch Versand von UDP-Paketen an zufällige Ports
  - Angriffsdauer konfigurierbar
- Erfordert große Anzahl Hosts oder hochwertige Hosts mit schneller Internet-Anbindung
  - davon gibt es anscheinend genug (CNN etc: über 1000 Hosts)





# Gegenmaßnahmen

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Nicht nur für Firewalls - eigentlich sollten alle Hosts diese Maßnahmen ergreifen
  - ICMP Bandwidth Limiting
    - ♦ Server begrenzt Geschwindigkeit, mit der er ICMP-Fehlermeldungen generiert auf tatsächliche Netzwerk-Bandbreite
  - TCP Random Early Drop
    - ♦ Mechanismen zur Bandbreitenbegrenzung: Verbindungen werden zufällig aus Verbindungsaufbau-Tabellen entfernt
    - ♦ Legitime Clients sehen zwischenzeitlich Fehler bei Aufbau
    - ♦ Server kann weiterhin mit begrenzter Leistung operieren
  
- Microsoft Windows XP SP 2
  - Begrenzung der ausgehenden unvollständigen TCP-Verbindungen
  - Anders als obige Vorgehensweisen existieren eine Reihe legitimer Anwendungen, die durch dieses Verhalten beeinträchtigt werden





# Weitere Angriffe

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- **Wiedereinspielung (Replay)**
  - Nicht idempotente Transaktionen ohne Erkennung von Wiederholung (kryptographische Mechanismen)
  - Können von Firewalls nicht abgefangen werden
  - Erfordern VPN-Mechanismen zum Integritätsschutz
  
- **Einfügen/Verändern von Daten in legitimen Verbindungen**
  - Quelle von IP-Datagrammen ist nicht festzustellen
  - Spoofing, Cache Poisoning
  - Angreifer muß allerdings in WAN-Situationen „blind“ modifizieren





# Angriffe auf Befehlskanäle

... department security technology ... department security technology ... department security technology ... department security technology ...

- Einfügung, Replays etc. sind auch auf Befehlskanälen möglich
- Beispiel Firewall-1 4.0-SP4 (korrigiert im März 2000)
  - Zustandsbasierter Paketfilter mit partiellem Proxying
  - Nach Aufbau einer FTP-Kontrollverbindung wurde auf Antworten eines internen Clients gewartet um den Code 227 zu erkennen
  - Adresse, Portnummer sollten extrahiert werden um gezielt Verbindung zu gestatten
  - Tauchte die 227 zu Beginn eines beliebigen Paketes auf (z.B. durch langen, fehlerhaften Pfad), wurde Verbindung geöffnet
  - Angreifer kann sich somit an beliebigen Host, Port via TCP in DMZ verbinden





# Systemprofile

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- „Security by Obscurity“ ist wirkungslos, dennoch:
- Jede Information, die einem Angreifer über ein potentielles Opfer zur Verfügung steht kann dieser ausnutzen
  - Betriebssystem, Version
  - Netzwerktopologie
  - Nutzerverhalten, Aktivitätsmuster
- Manchem Angreifer genügen bereits derartige Informationen um an ihr Ziel zu gelangen
- Für die Auswahl von geeigneten Werkzeugen sind Profile wichtig





# Zur Profilierung nutzbare Eigenschaften (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- **FIN-Verhalten**
  - Nach RFC793 bei FIN ohne vorher SYN, ACK: Ignorieren
  - Windows, IOS, HP-UX, MVS, IRIX: versenden RST
  
- **Handhabung illegaler Flags**
  - Werden illegale Flags/Kombinationen zurückgesandt?
  
- **ISN-Analyse**
  - Welche Strategie verfolgt das System bei der Inkrementierung der ISNs von aufeinander folgenden Verbindungen?





# Zur Profilierung nutzbare Eigenschaften (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Don't Fragment-Bit
  - Setzen von DF in Datagrammen?
- Größe der TCP Initial Window Size
- Rückgabe von ACK-Segmenten
  - Sende Segment mit FIN,PSH,URG-Flags an geschlossenen Port
  - Soll: ACK mit SEQ=x. Windows: ACK mit SEQ=x+1
- ICMP-Fehlermeldungen
  - Häufigkeit mit der Fehlermeldungen versandt werden („rate throttling“)





# Zur Profilierung nutzbare Eigenschaften (3)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

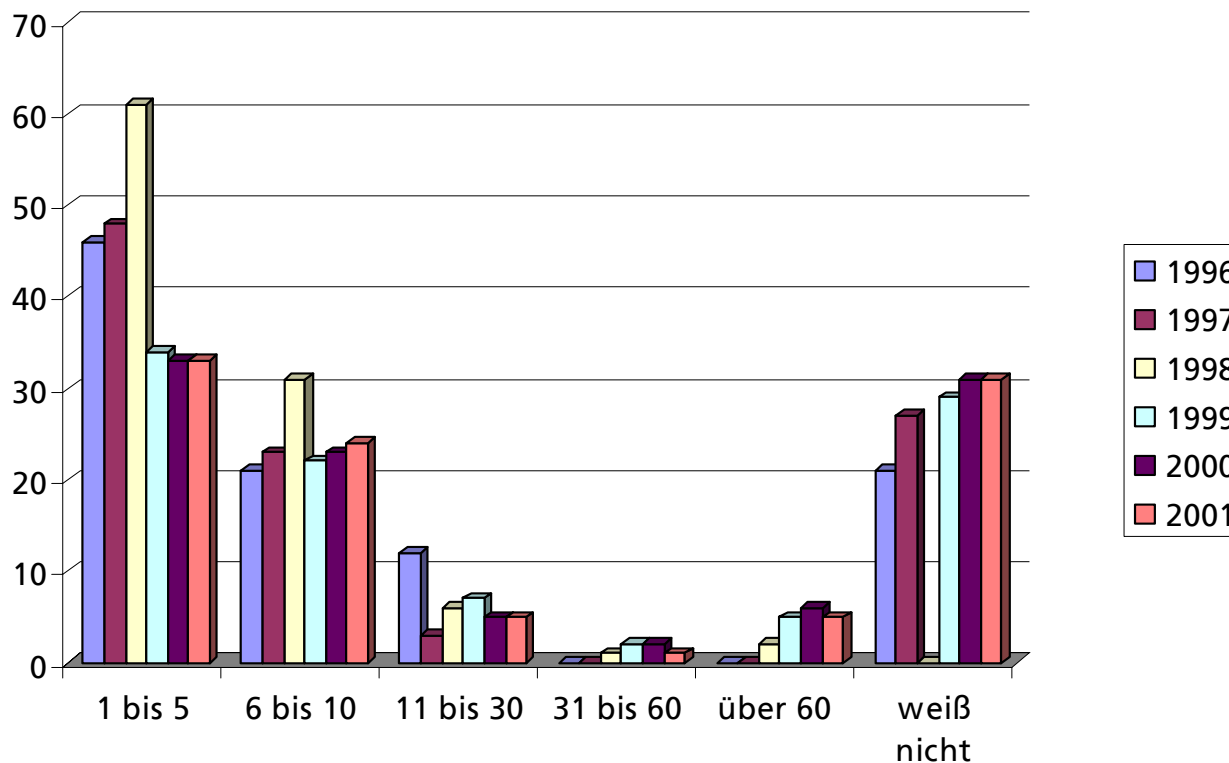
- ICMP-Rückmeldungen
  - Wieviel des verursachenden Datagramms wird zurück geschickt?
- Inhalt von ICMP-Rückmeldungen
  - Nicht-konforme Änderungen am Inhalt der Rücksendungen
- Type of Service: Linux setzt TOS bei ICMP Typ 3 auf 0xC0 statt 0x00
- Fragmentierung
  - Implementierungsabhängige Zusammensetzung von Fragmenten
- Unterstützung von TCP-Optionen
  - Werden Optionen bearbeitet?
  - Reihenfolge der Bearbeitung?





# Anzahl von sicherheitsrelevanten Vorfällen

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••



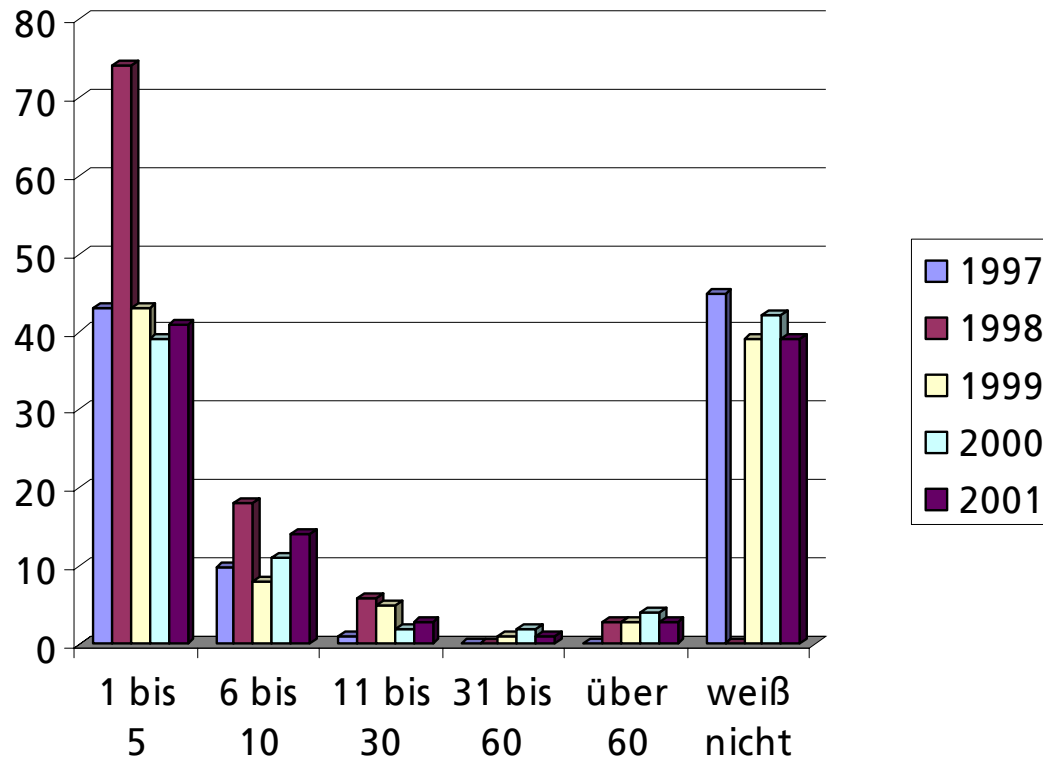
Quelle: CSI/FBI Computer Crime and Security Survey 2001





# Anzahl sicherheitsrelevanter Vorfälle von außen

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••



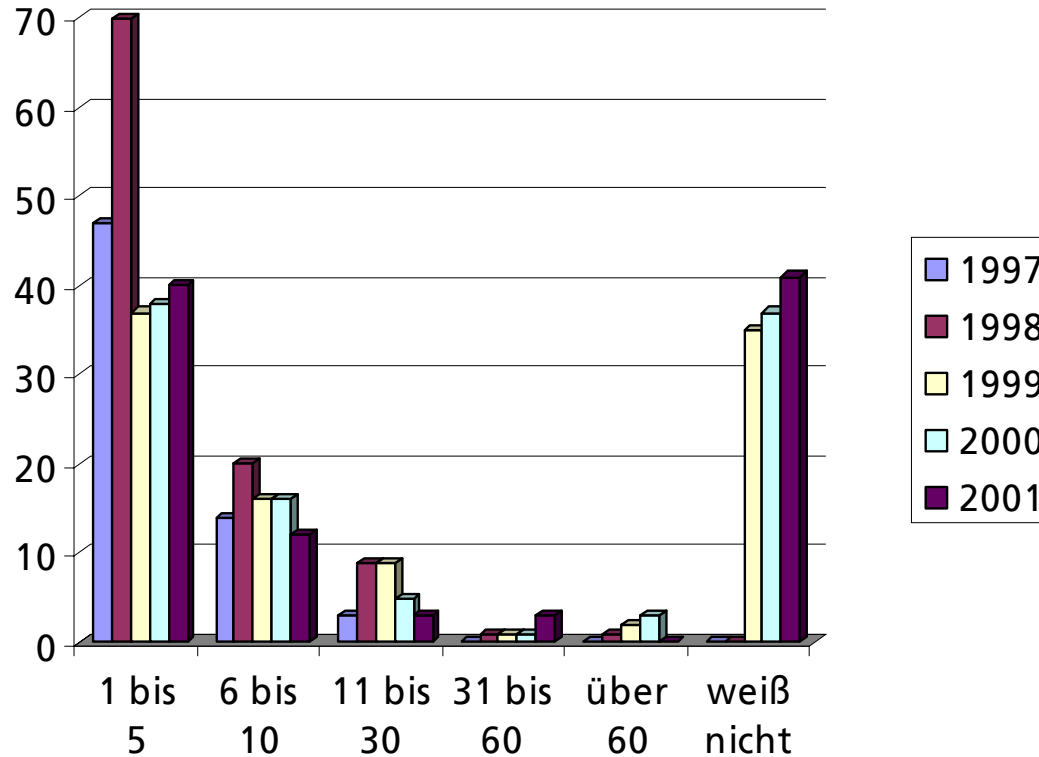
Quelle: CSI/FBI Computer Crime and Security Survey 2001





# Anzahl sicherheitsrelevanter Vorfälle von innen

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••



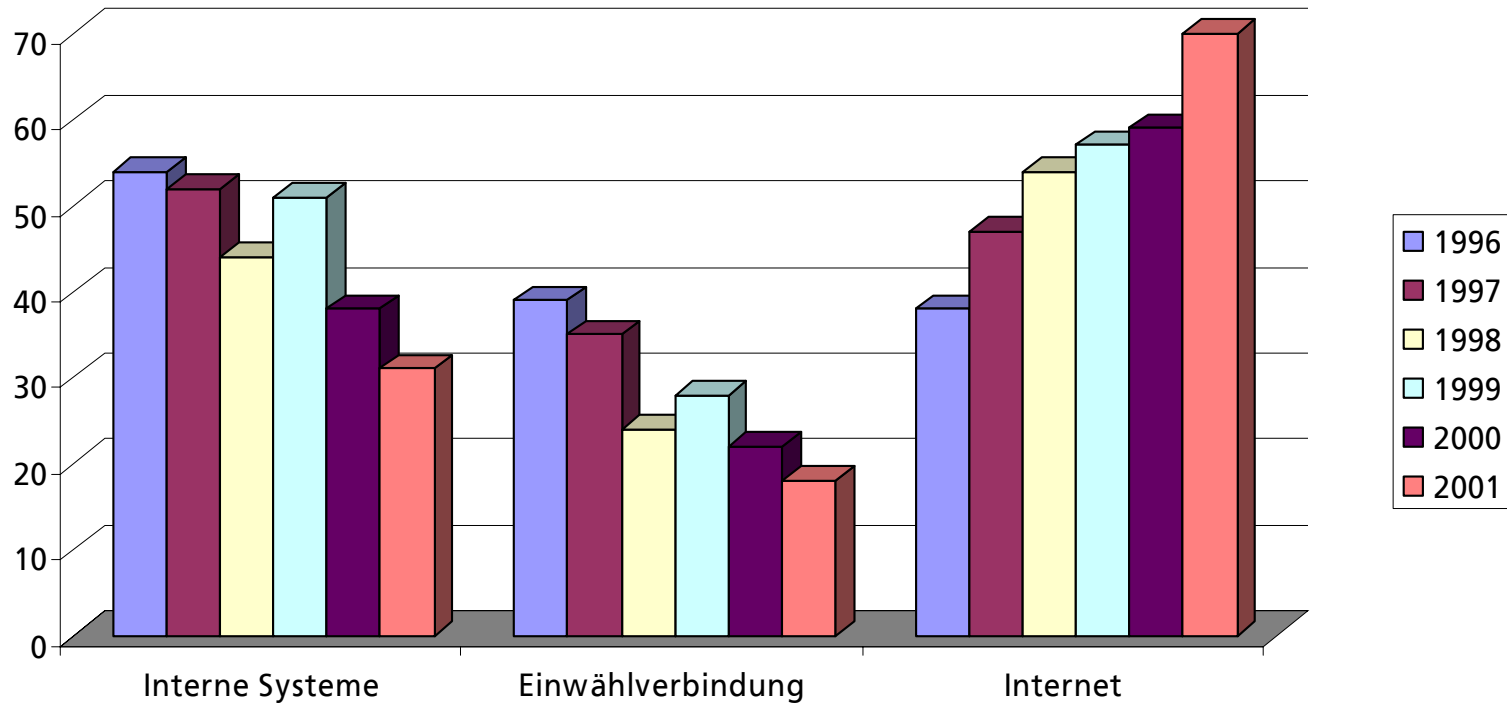
Quelle: CSI/FBI Computer Crime and Security Survey 2001





# Häufigste Quelle von Angriffen

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••



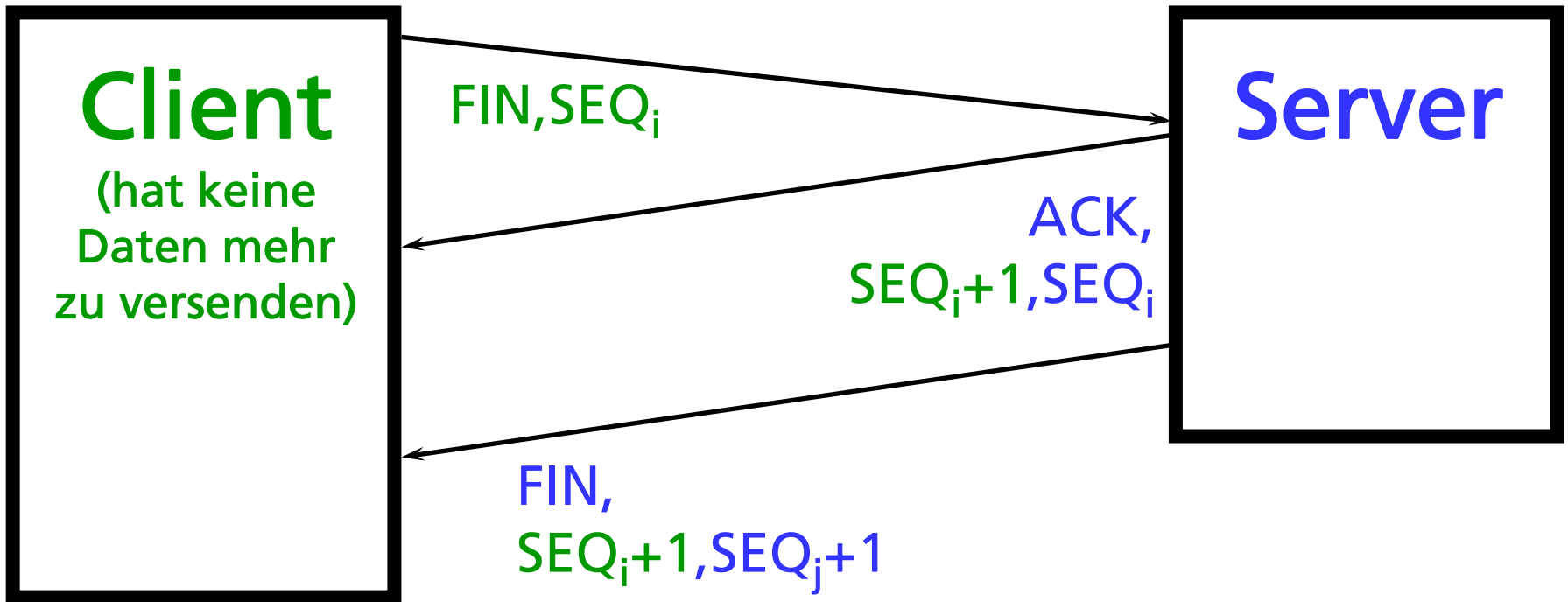
Quelle: CSI/FBI Computer Crime and Security Survey 2001





# Verbindungsabbau

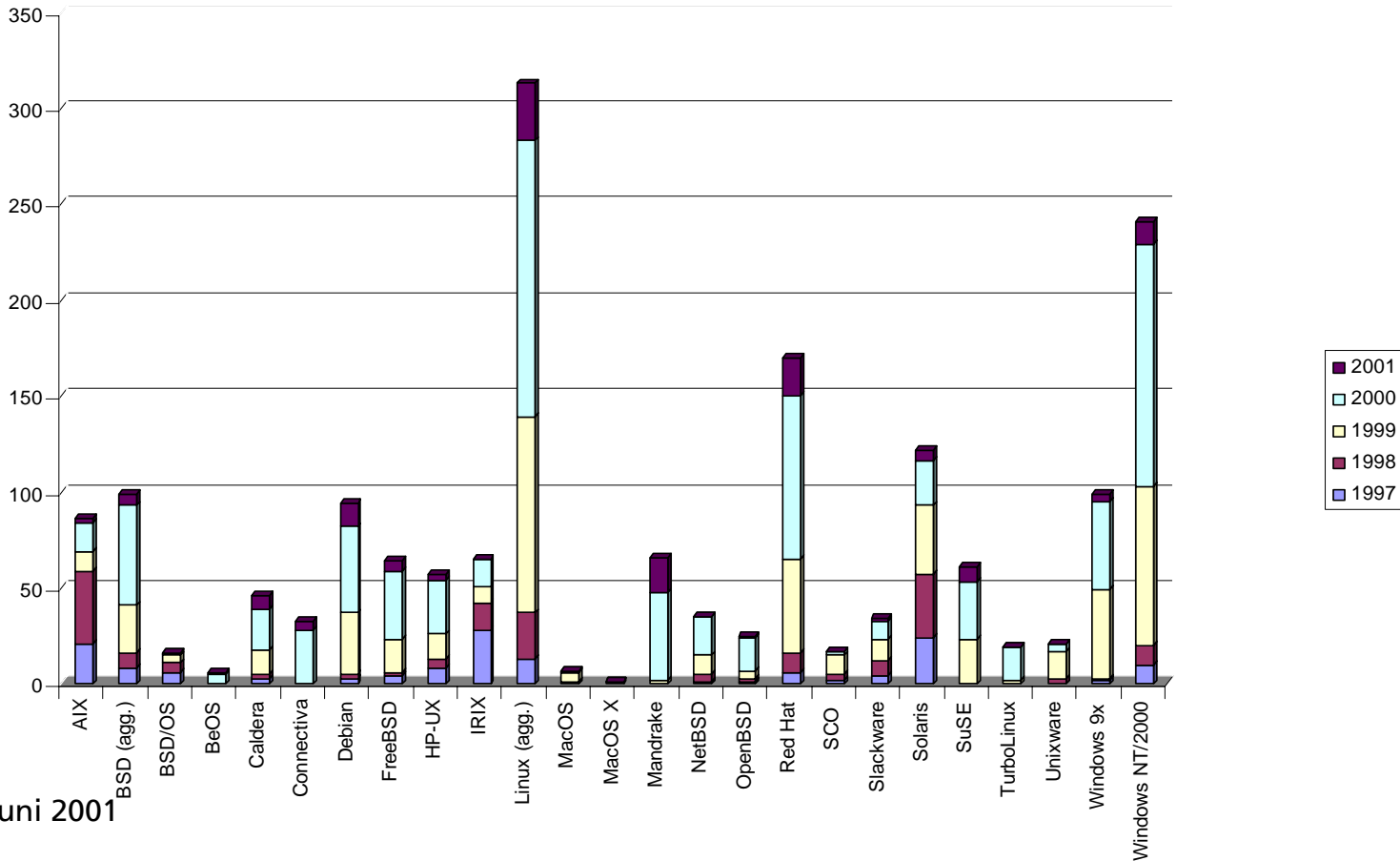
••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





# Extern nutzbare Verwundbarkeiten verschiedener Betriebssysteme

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••



Quelle: SecurityFocus, Juni 2001

