Systeme II

10. Vorlesungswoche
30.06. – 04.07.2008

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Christian Schindelhauer
Sommer 2008

1

Kapitel 7

Die Anwendungs-schicht

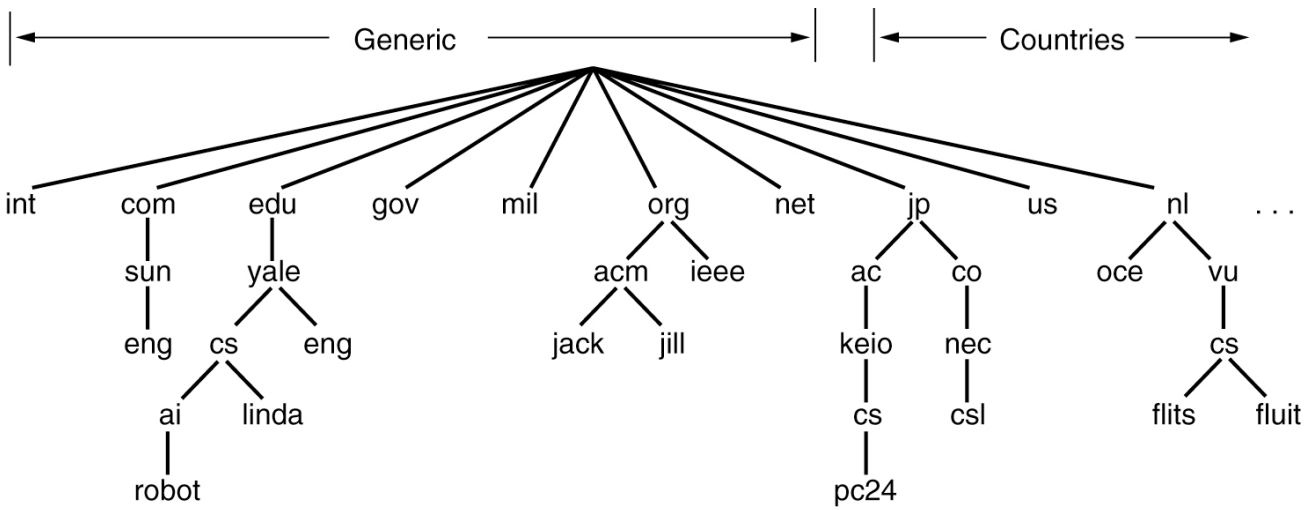
2

Domain Name System (DNS) – Motivation

- **Menschen kommen mit den 4byte IPv4-Adressen nicht zu Recht:**
  - 72.14.221.104 für Google
  - 132.230.2.100 für Uni Freiburg
  - Was bedeuten?
    - 80.67.17.75
    - 132.230.150.170
- **Besser: Natürliche Wörter für IP-Adressen**
  - Z.B. www.schiessmichtot.de
  - oder www.uni-freiburg.de
- **Das Domain Name System (DNS) übersetzt solche Adressen in IP-Adressen**

DNS – Architecture

- **DNS bildet Namen auf Adressen ab**
  - Eigentlich: Namen auf Ressourcen-Einträge
- **Namen sind hierarchisch strukturiert in einen Namensraum**
  - Max. 63 Zeichen pro Komponente, insgesamt 255 Zeichen
  - In jeder Domain kontrolliert der Domain-Besitzer den Namensraum darunter
- **Die Abbildung geschieht durch Name-Server**



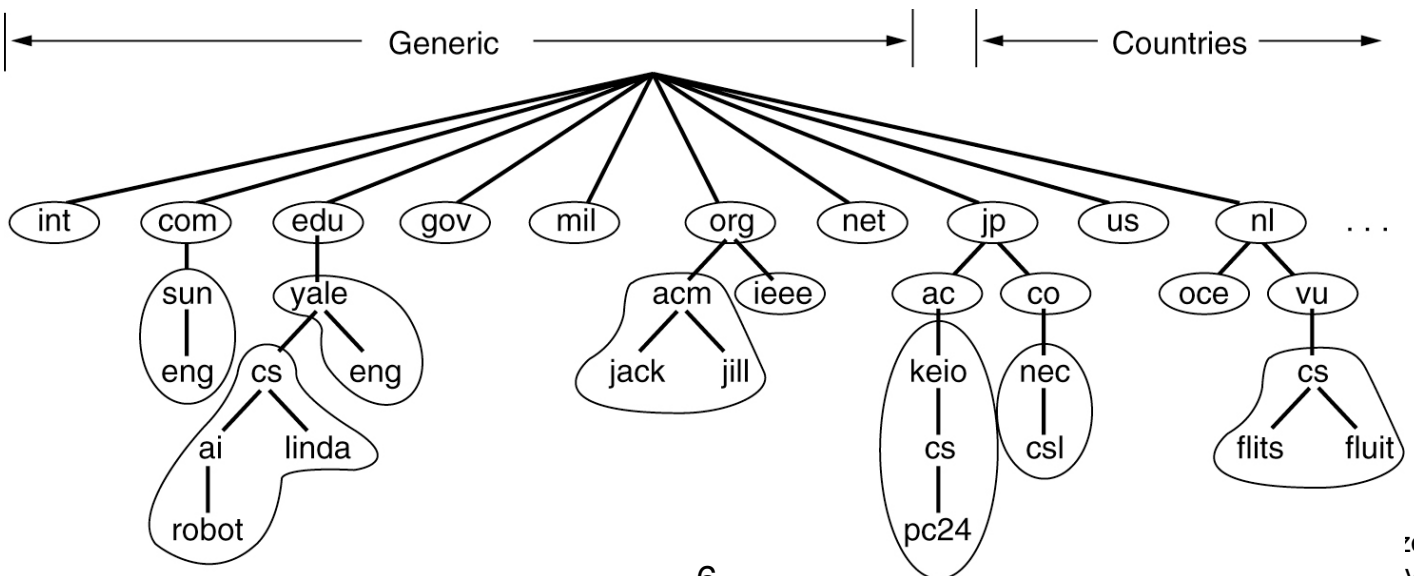
DNS Resource Record

- **Ressourcen-Einträge: Informationen über Domains, einzelne Hosts,...**
- **Inhalt**
  - Domain_name: Domain(s) des Eintrags
  - Time_to_live: Gültigkeit (in Sekunden)
  - Class: Im Internet immer “IN”
  - Type: Siehe Tabelle
  - Value: z.B. IP-Adresse

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

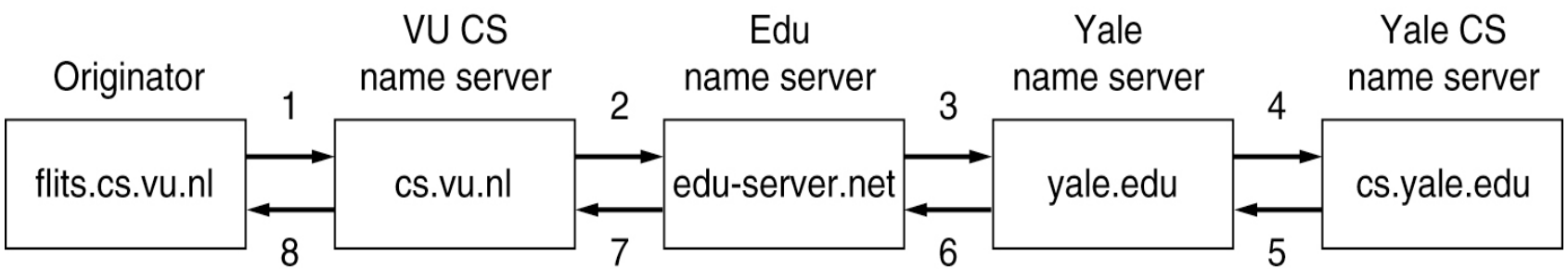
DNS Name Server

- **Der Namensraum ist in Zonen aufgeteilt**
- **Jede Zone hat einen *Primary Name Server* mit maßgeblicher Information**
  - Zusätzlich *Secondary Name Server* für Zuverlässigkeit
- **Jeder Name Server kennt**
  - seine eigene Zone
  - Name-Server der darunterliegenden Bereiche

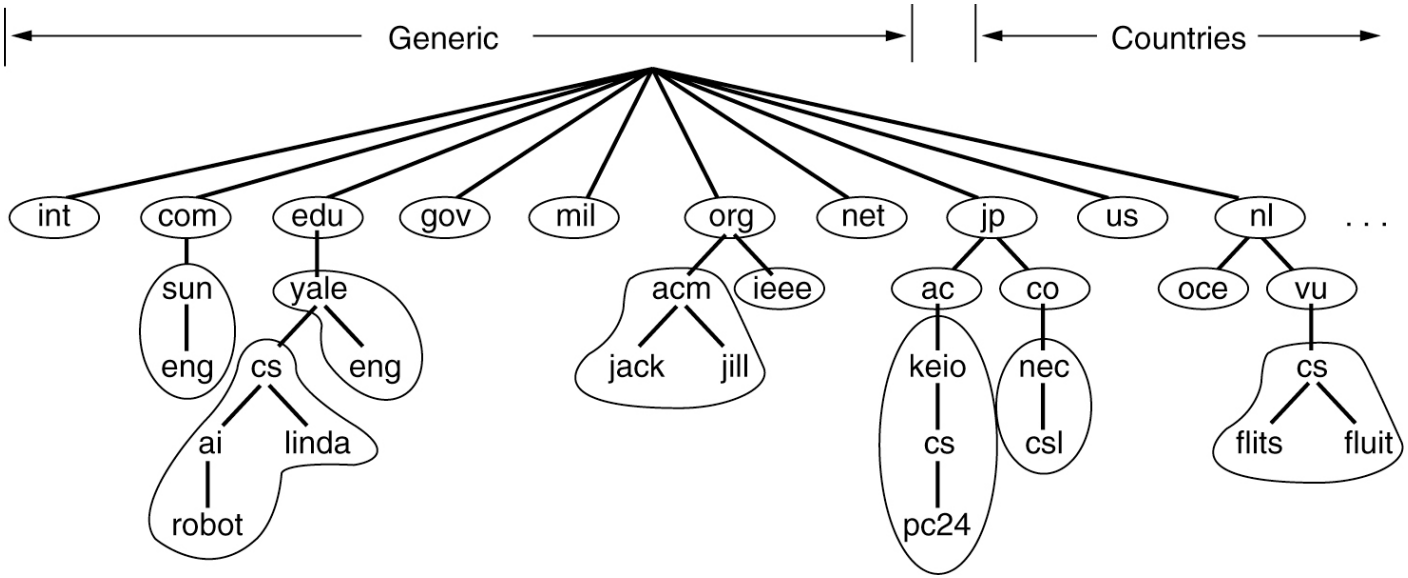


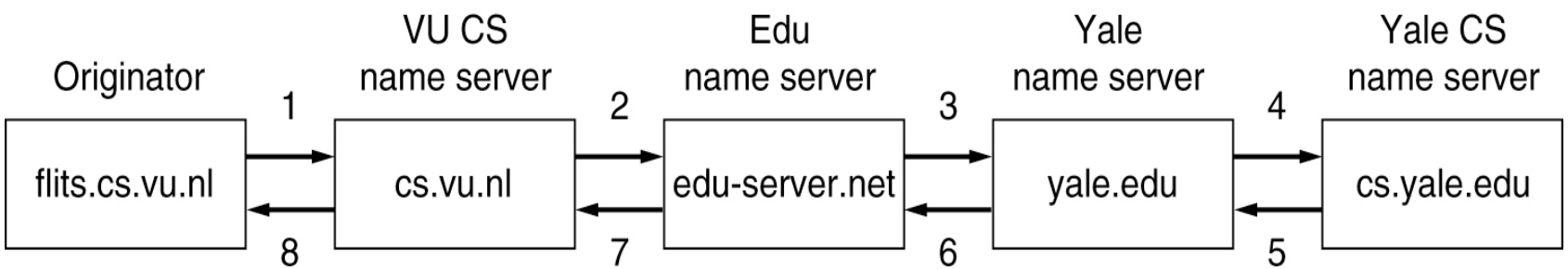
DNS Anfragebearbeitung

- **Anfragen von einem End-System werden zu den vorkonfigurierten Name-Server geschickt**
  - Soweit möglich, antwortet dieser Name-Server
  - Falls nicht, wird die Anfrage zu dem bestgeeigneten Name-Server weitergereicht
  - Die Antworten werden durch die Zwischen-Server zurückgeschickt
- **Server darf Antworten speichern (cachen)**
  - Aber nur für eine bestimmte Zeit



Beispiel


Generic
Countries
int
com
edu
gov
mil
org
net
jp
us
nl
. . .
sun
eng
yale
cs
eng
ai
linda
robot
acm
ieee
jack
jill
ac
co
keio
cs
pc24
nec
csl
oce
vu
cs
flits
fluit


Originator
VU CS name server
Edu name server
Yale name server
Yale CS name server
flits.cs.vu.nl
cs.vu.nl
edu-server.net
yale.edu
cs.yale.edu
1
2
3
4
5
6
7
8

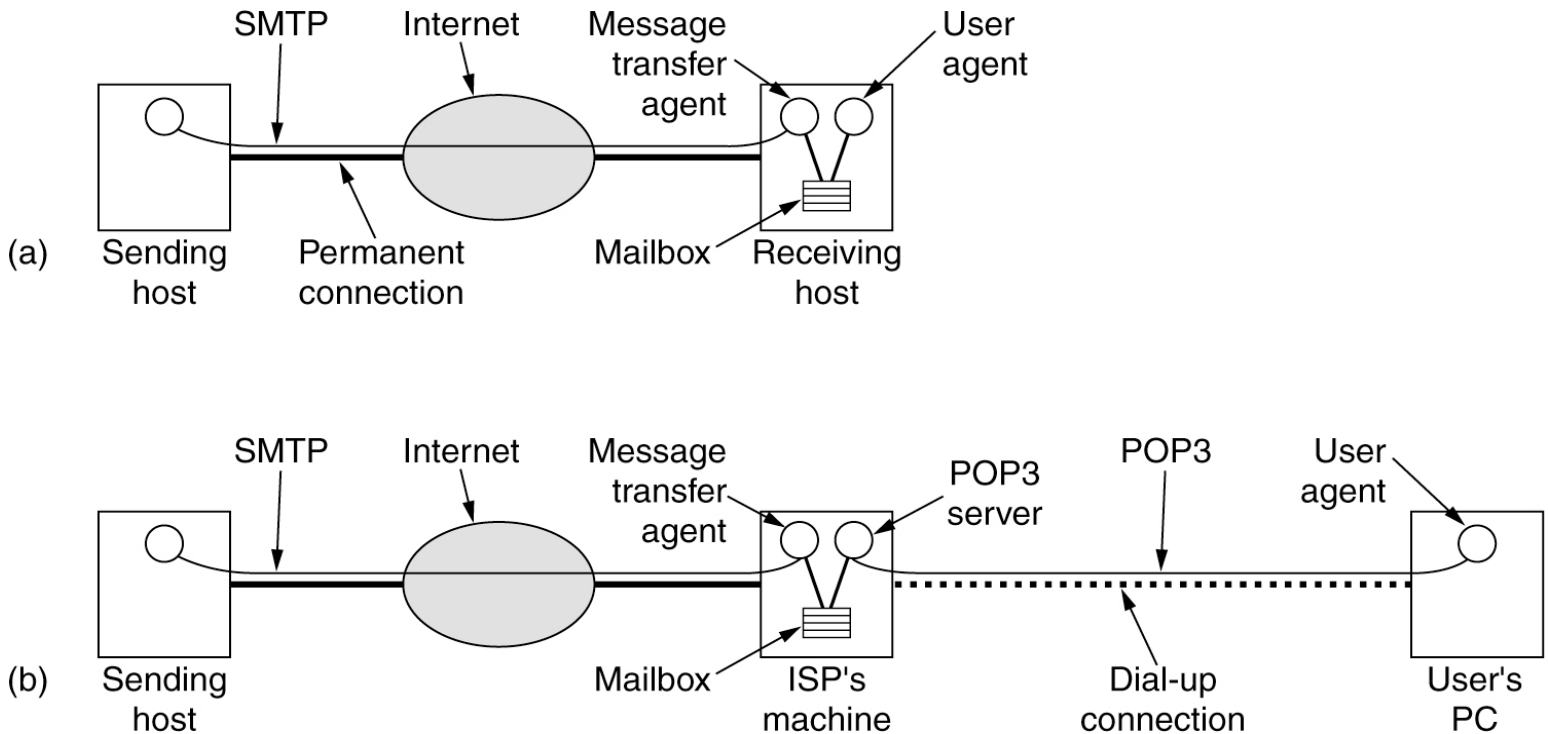
Dynamisches DNS

- **Problem**
  - Zeitlich zugewiesene IP-Adressen
  - z.B. durch DHCP
- **Dynamisches DNS**
  - Sobald ein Knoten eine neue IP-Adresse erhält, registriert dieser diese beim DNS-Server, der für diesen Namen zuständig ist
  - Kurze time-to-live-Einträge sorgen für eine zeitnahe Anpassung
    - da sonst bei Abwesenheit die Anfragen an falsche Rechner weitergeleitet werden
- **Anwendung**
  - Registrierung einer Domain für den Otto Normalverbraucher
  - Siehe www.dyndns.com

E-Mail

- **Beispiel: E-Mail aus RFC 821/822**
  - **User Agents (UA)**
  - **Message Transfer Agents (MTA)**
- **Dienste**
  - Entwurf
  - Beförderung
  - Berichtswesen
  - Anzeige
  - Lagerung
- **Zusatzdienste**
  - Weiterleitung, Automatische Antwort, Abwesenheitsfunktion, Mail-Listen, Blind Copy
- **Struktur einer E-Mail**
  - Umschlag mit Information für Transport (verwendet von MTA)
  - Inhalt
    - Header – Kontroll-Information für UA
    - Body – Eigentlicher Inhalt der E-Mail

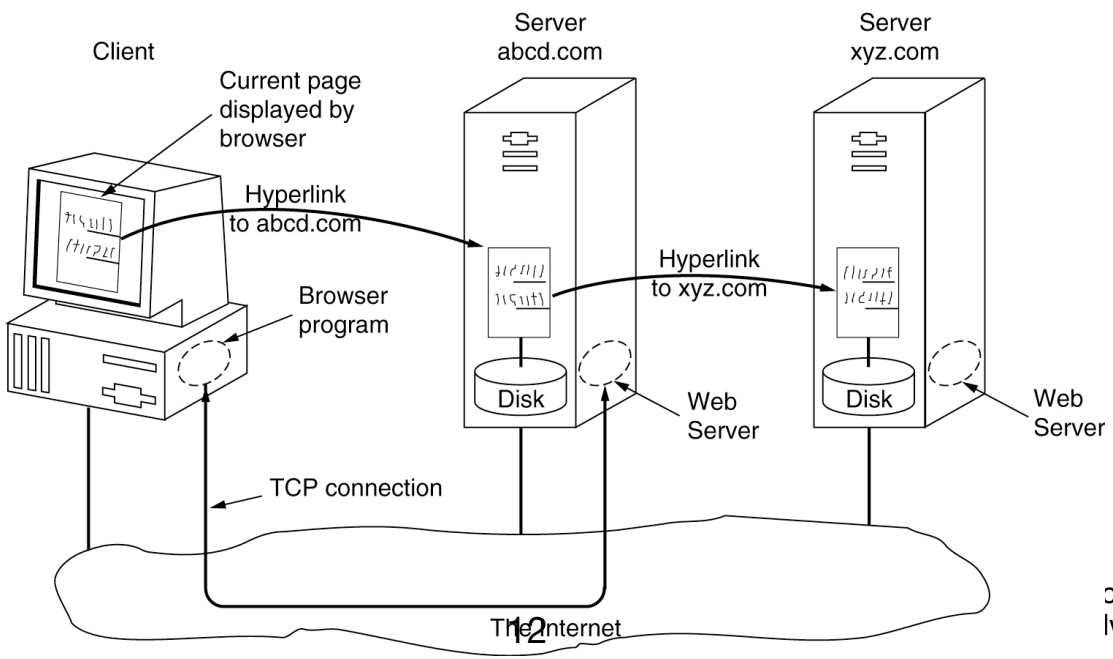
E-Mail: SMTP und POP



SMTP: Simple Mail Transfer Protocol
POP: Post Office Protocol
IMAP: Internet Message Access Protocol

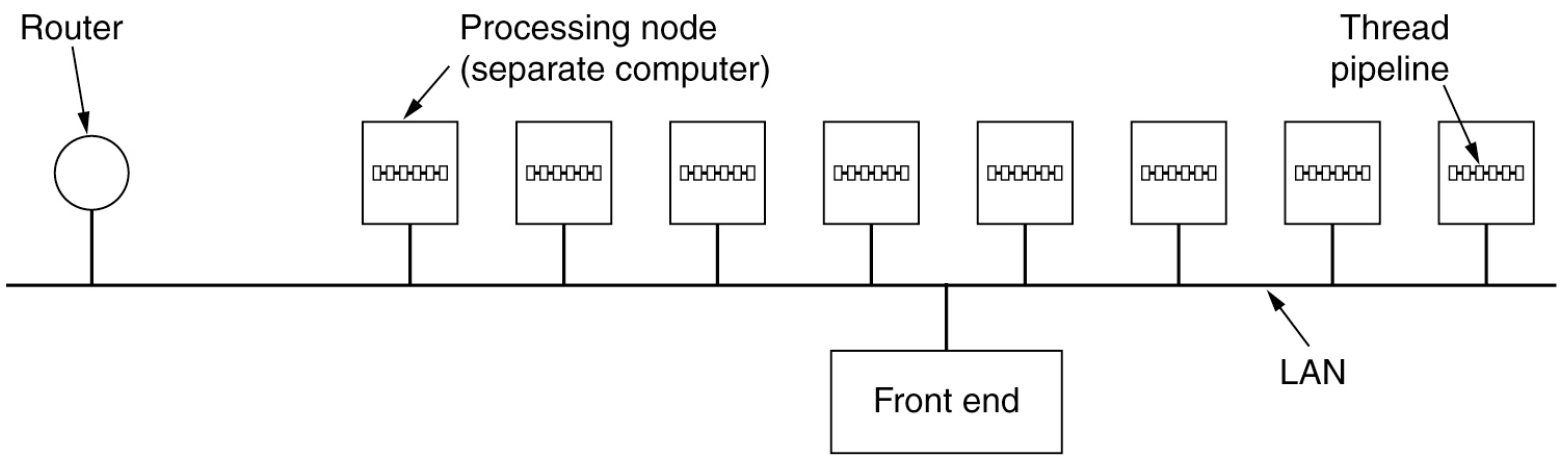
World Wide Web

- **Client-Server-Architektur**
  - ***Web-Server*** stellt Web-Seiten bereit
  - Format: ***Hyptertext Markup Language*** (HTML)
  - ***Web-Browser*** fragen Seiten vom Server ab
  - Server und Browser kommunizieren mittels ***Hypertext Transfer Protocol*** (HTTP)



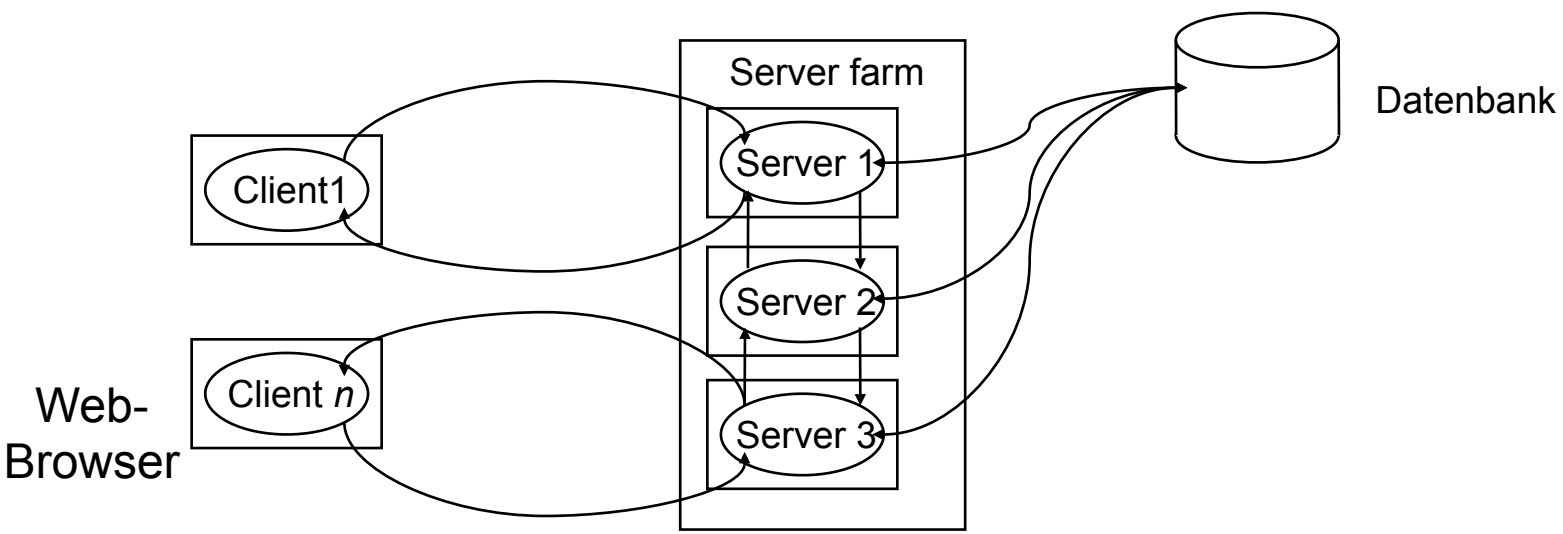
Server-Farm

- **Um die Leistungsfähigkeit auf der Server-Seite zu erhöhen**
  - wird eine Reihe von Web-Server eingesetzt
- **Front end**
  - nimmt Anfragen an
  - reicht sie an separaten Host zur Weiterbearbeitung weiter



Web-Servers und Datenbanken

- **Web-Server stellen nicht nur statische Web-Seiten zur Verfügung**
  - Web-Seiten werden auch automatisch erzeugt
  - Hierzu wird auf eine Datenbank zurückgegriffen
  - Diese ist nicht statisch und kann durch Interatkionen verändert werden
- **Problem:**
  - Konsistenz
- **Lösung**
  - Web-Service und Daten-Bank in einer 3-Stufen-Architektur



Web-Cache

- **Trotz Server-Farm ist die Latenzzeit häufig kritisch**
- **Lösung:**
  - Cache (Proxy)
- **Ort**
  - Beim Client
  - Im lokalen Netzwerk (bei einem Proxy)
  - Beim Internet-Service-Provider
- **Fragen**
  - Plazierung, Größe, Aktualität
  - Entwertung durch Timeout

Content Distribution Networks (CDN)

- **Eine koordinierte Menge von Caches**
  - Die Last großer Web-Sites wird verteilt auf global verteilte Server-Farmen
  - Diese übernehmen Web-Seiten möglichst verschiedener Organisationen
    - z.B. News, Software-Hersteller, Regierungen
  - Beispiele: Akamai, Digital Island
  - Cache-Anfragen werden auf die regional und lastmäßig bestgeeigneten Server umgeleitet
- **Beispiel Akamai:**
  - Durch verteilte Hash-Tabellen ist die Verteilung effizient und lokal möglich

Sicherheit

Kapitel VIII

Sicherheit in Rechnernetzwerken

- **Spielt eine Rolle in den Schichten**
  - Bitübertragungsschicht
  - Sicherungsschicht
  - Vermittlungsschicht
  - Transportschicht
  - Anwendungsschicht
- **Was ist eine Bedrohung (oder ein Angriff)?**
- **Welche Methoden gibt es?**
  - Kryptographie
- **Wie wehrt man Angriffe ab?**
  - Beispiel: Firewalls

Was ist eine Bedrohung?

- **Definition:**
  - Eine Bedrohung eines Rechnernetzwerks ist jedes mögliche Ereignis oder eine Folge von Aktionen, die zu einer Verletzung von Sicherheitszielen führen kann
  - Die Realisierung einer Bedrohung ist ein Angriff
- **Beispiel:**
  - Ein Hacker erhält Zugang zu einem geschlossenen Netzwerk
  - Veröffentlichung von durchlaufenden E-Mails
  - Fremder Zugriff zu einem Online-Bankkonto
  - Ein Hacker bringt ein System zum Absturz
  - Jemand agiert unautorisiert im Namen anderer (Identity Theft)

Sicherheitsziele

- **Vertraulichkeit:**
  - Übertragene oder gespeicherte Daten können nur vom vorbestimmten Publikum gelesen oder geschrieben werden
  - Vertraulichkeit der Identität der Teilnehmer: Anonymität
- **Datenintegrität**
  - Veränderungen von Daten sollten entdeckt werden
  - Der Autor von Daten sollte erkennbar sein
- **Verantwortlichkeit**
  - Jedem Kommunikationsereignis muss ein Verursacher zugeordnet werden können
- **Verfügbarkeit**
  - Dienste sollten verfügbar sein und korrekt arbeiten
- **Zugriffskontrolle**
  - Dienste und Informationen sollten nur autorisierten Benutzern zugänglich sein

Angriffe

- **Maskierung (Masquerade)**
  - Jemand gibt sich als ein anderer aus
- **Abhören (Eavesdropping)**
  - Jemand liest Informationen, die nicht für ihn bestimmt sind
- **Zugriffsverletzung (Authorization Violation)**
  - Jemand benutzt einen Dienst oder eine Resource, die nicht für ihn bestimmt ist
- **Verlust oder Veränderung (übertragener) Information**
  - Daten werden verändert oder zerstört
- **Verleugnung der Kommunikation**
  - Jemand behauptet (fälschlicherweise) nicht der Verursacher von Kommunikation zu sein
- **Fälschen von Information**
  - Jemand erzeugt (verändert) Nachrichten im Namen anderer
- **Sabotage**
  - Jede Aktion, die die Verfügbarkeit oder das korrekte Funktionieren der Dienste oder des Systems reduziert

Bedrohungen und Sicherheitsziele

Sicherheits-ziele	Bedrohungen						
	Mas-kierung	Abhören	Zugriffs-ver-letzung	Verlust oder Verän-derung (über-tragener) information	Verleug-nung der Kommuni-kation	Fäl-schen von Infor-mation	Sabotage (z.B. Überlast)
Vertraulichkeit	x	x	x				
Datenintegrität	x		x	x		x	
Verantwort-lichkeit	x		x		x	x	
Verfügbarkeit	x		x	x			x
Zugriffs-kontrolle	x		x			x	

Terminologie der Kommunikationssicherheit

- **Sicherheitsdienst**
  - Ein abstrakter Dienst, der eine Sicherheitseigenschaft zur erreichen sucht
  - Kann mit (oder ohne) Hilfe kryptografischer Algorithmen und Protokolle realisiert werden, z.B.
    - Verschlüsselung von Daten auf einer Festplatte
    - CD im Safe
- **Kryptografischer Algorithmus**
  - Mathematische Transformationen
  - werden in kryptografischen Protokollen verwendet
- **Kryptografisches Protokoll**
  - Folge von Schritten und auszutauschenden Nachrichten um ein

Sicherheitsdienste

- **Authentisierung**
  - Digitale Unterschift: Das Datum ist nachweislich vom Verursacher
- **Integrität**
  - Sichert ab, dass ein Datum nicht unbemerkt verändert wird
- **Vertraulichkeit**
  - Das Datum kann nur vom Empfänger verstanden werden
- **Zugriffskontrolle**
  - kontrolliert, dass nur Berechtigte Zugang zu Diensten und Information besitzen
- **Unleugbarkeit**
  - beweist, dass die Nachricht unleugbar vom Verursacher ist

Kryptologie

- **Kryptologie**
  - Wissenschaft der geheimen Kommunikation
  - Von griechisch kryptós (versteckt) und lógos (Wort)
  - Kryptologie beinhaltet:
    - Kryptografie (gráphein = schreiben): die Lehre des Erzeugens von geheimer Kommunikation
    - Krypto-Analyse (analýein = lösen, entwirren): die Lehre des Entschüsselns geheimer Information

Verschlüsselungs-methoden

- **Symmetrische Verschlüsselungsverfahren**
  - Cäsars Code
  - Enigma
  - DES (Digital Encryption Standard)
  - AES (Advanced Encryption Standard)
- **Kryptografische Hash-Funktion**
  - SHA-1, SHA-2
  - MD5
- **Asymmetrische Verschlüsselungsverfahren**
  - RSA (Rivest, Shamir, Adleman)
  - El-Gamal
- **Digitale Unterschriften (Elektronische Signatur)**
  - PGP (Phil Zimmermann), RSA

Symmetrische Verschlüsselungsverfahren

- **z.B. Cäsars Code, DES, AES**
- **Es gibt Funktionen f und g, sodass**
  - Verschlüsselung:
    - f(schlüssel,text) = code
  - Entschlüsselung:
    - g(schlüssel,code) = text
- **Der Schlüssel**
  - muss geheim bleiben
  - dem Sender und Empfänger zur Verfügung stehen

Kryptografische Hash-Funktion

- **z.B. SHA-1, SHA-2, MD5**
- **Ein kryptografische Hash-Funktion h bildet einen Text auf einen Code fester Länge ab, sodass**
  - h(text) = code
  - es unmöglich ist einen anderen Text zu finden mit:
    - h(text‘) = h(text) und text ≠ text‘
- **Mögliche Lösung:**
  - Verwendung einer symmetrischen Kryptografie-Methode

Asymmetrische Verschlüsselungsverfahren

- **z.B. RSA, Ronald Rivest, Adi Shamir, Lenard Adleman, 1977**
  - Diffie-Hellman, PGP
- **Geheimer Schlüssel `privat`**
  - kennt nur der Empfänger der Nachricht
- **Öffentlichen Schlüssel `offen`**
  - Ist allen Teilnehmern bekannt
  - Wird erzeugt durch Funktion
    - keygen(`privat`) = `offen`
- **Verschlüsselungsfunktion f und Entschlüsselungsfunktion g**
  - sind auch allen bekannt
- **Verschlüsselung**
  - f(`offen`,`text`) = `code`
  - kann jeder berechnen
- **Entschlüsselung**
  - g(`privat`,`code`) = `text`
  - nur vom Empfänger

Beispiel: RSA

- **Verfahren beruht auf der Schwierigkeit der Primfaktorzerlegung**
- **1. Beispiel: 15 = ? * ?**
  - 15 = 3 * 5
- **2. Beispiel:**

3865818645841127319129567277348359557447904102899335864835520474 43 =

12345678901234567890123456789002 09 * 3131313131313131313131313131300227

- **Bis heute ist kein effizientes Verfahren zur Primfaktorzerlegung bekannt**
  - Aber das Produkt von Primzahlen kann effizent bestimmt werden
  - Primzahlen können ebenfalls effizient bestimmt werden
  - Primzahlen kommen sehr häufig vor

Elektronische Unterschriften

- **auch bekannt als digitale Signaturen**
  - Unterzeichner besitzt einen geheimen Schlüssel
  - Dokument wird mit geheimen Schlüssel unterschrieben
  - und kann mit einem öffentlichen Schlüssel verifiziert werden
  - Öffentlicher Schlüssel ist allen bekannt
- **Beispiel eines Signaturschemas**
  - m: Nachricht
  - Unterzeichner
    - berechnet `h(text)` mit kryptographischer Hashfunktion
    - und veröffentlicht m und `signatur` = g(`privat`, `h(text)`), für die Entschülsselungsfunktion g
  - Kontrolleur
    - berechnet `h(text)`
    - und überprüft `f(offen, signatur)` = `h(text)`, für die asymmetrische Verschlüsselungsfunktion g

Motivation

Symantec Internet Security Threat Report 2007

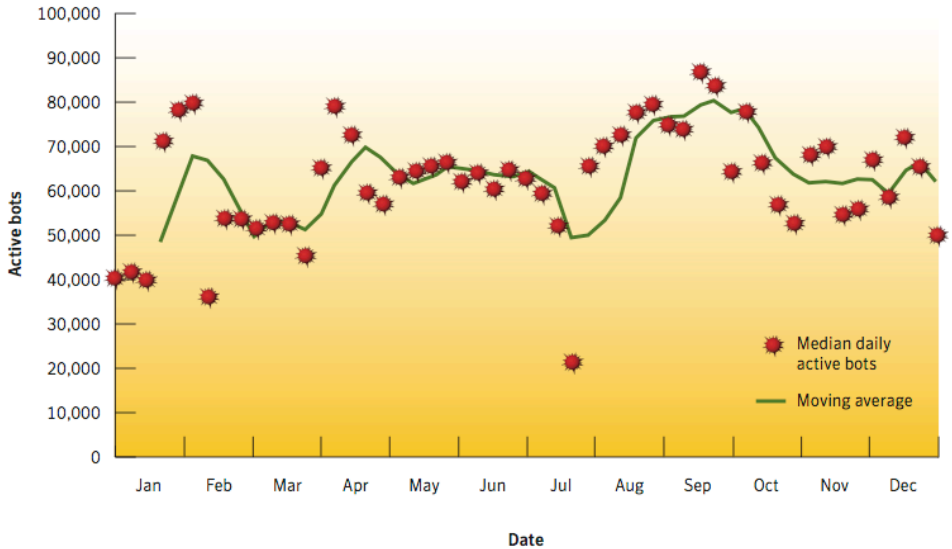


Figure 11. Active bot-infected computers per day
Source: Symantec Corporation

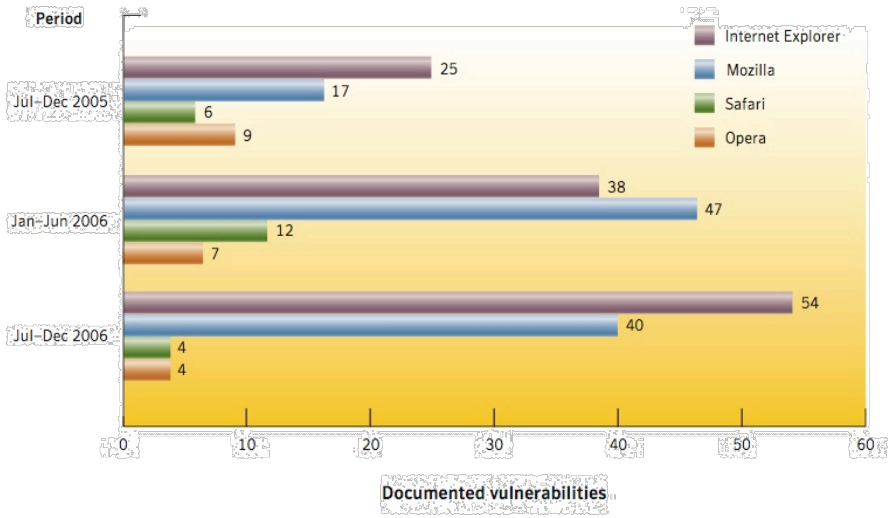


Figure 15. Web browser vulnerabilities
Source: Symantec Corporation

Overall Rank	Country	Overall Proportion	Malicious Code Rank	Spam Host Rank	Command and Control Server Rank	Phishing Host Rank	Bot Rank	Attack Rank
1	United States	31%	1	1	1	1	2	1
2	China	10%	3	2	4	8	1	2
3	Germany	7%	7	3	3	2	4	3
4	France	4%	9	4	14	4	3	4
5	United Kingdom	4%	4	13	9	3	6	6
6	South Korea	4%	12	9	2	9	11	9
7	Canada	3%	5	23	5	7	10	5
8	Spain	3%	13	5	15	16	5	7
9	Taiwan	3%	8	11	6	6	7	11
10	Italy	3%	2	8	10	14	12	10

Table 1. Malicious activity by country
Source: Symantec Corporation

Firewalls

- **Typen von Firewalls**
  - Host-Firewall
  - Netzwerk-Firewall
- **Netzwerk-Firewall**
  - unterscheidet
    - Externes Netz
      (Internet - feindselig)
    - Internes Netz
      (LAN - vertrauenswürdig)
    - Demilitarisierte Zone
      (vom externen Netz erreichbare Server)
- **Host-Firewall**
  - z.B. Personal Firewall
  - kontrolliert den gesamten Datenverkehr eines Rechners
  - Schutz vor Attacken von außerhalb und von innen (Trojanern)

- **Methoden**
  - Paketfilter
    - Sperren von Ports oder IP-Adressen
  - Content-Filter
    - Filtern von SPAM-Mails, Viren, ActiveX oder JavaScript aus HTML-Seiten
  - Proxy
    - Transparente (extern sichtbare) Hosts
    - Kanalisierung der Kommunikation und möglicher Attacken auf gesicherte Rechner
  - NAT, PAT
    - Network Address Translation
    - Port Address Translation
  - Bastion Host
    - Proxy

Firewalls: Begriffe

- **(Network) Firewall**
  - beschränkt den Zugriff auf ein geschütztes Netzwerk aus dem Internet
- **Paket-Filter**
  - wählen Pakete aus dem Datenfluss in oder aus dem Netzwerk aus
  - Zweck des Eingangsfilter:
    - z.B. Verletzung der Zugriffskontrolle
  - Zweck des Ausgangsfilter:
    - z.B. Trojaner
- **Bastion Host**
  - ist ein Rechner an der Peripherie, der besonderen Gefahren ausgesetzt ist
  - und daher besonders geschützt ist
- **Dual-homed host**
  - Normaler Rechner mit zwei Interfaces (verbindet zwei Netzwerke)

Firewalls: Begriffe

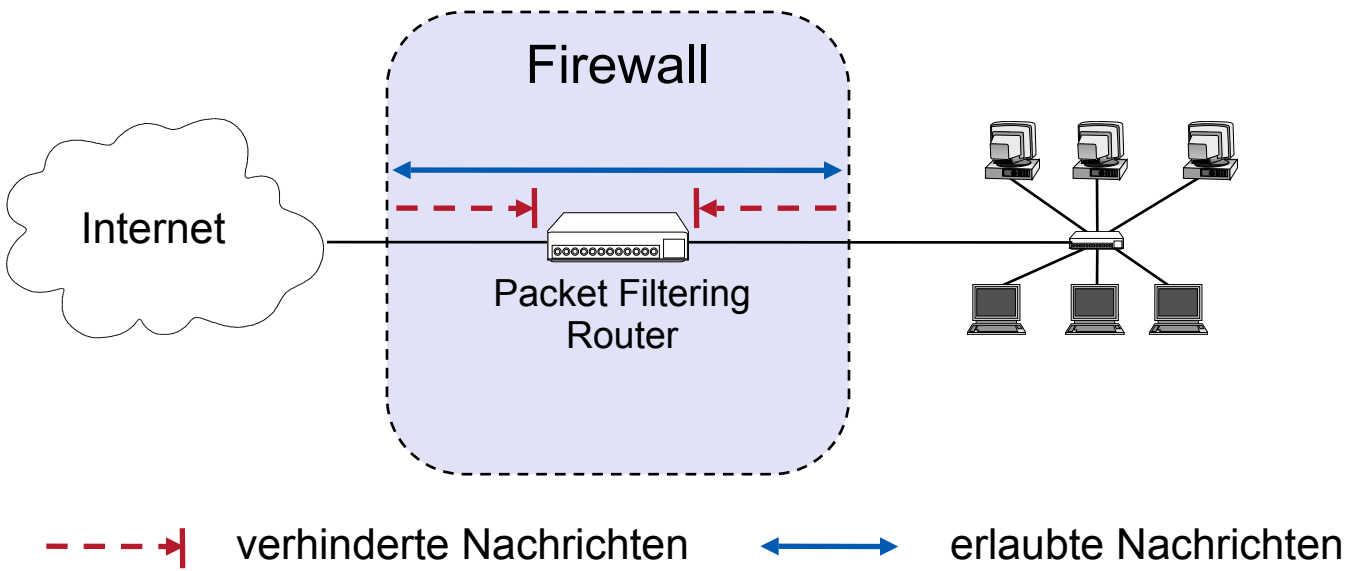
- **Proxy (Stellvertreter)**
  - Spezieller Rechner, über den Anfragen umgeleitet werden
  - Anfragen und Antworten werden über den Proxy geleitet
  - Vorteil
    - Nur dort müssen Abwehrmaßnahmen getroffen werden
- **Perimeter Network:**
  - Ein Teilnetzwerk, das zwischen gesicherter und ungesichter Zone eine zusätzliche Schutzschicht bietet
  - Synonym demilitarisierte Zone (DMZ)

NAT und PAT

- **NAT (Network Address Translation)**
- **Basic NAT (Static NAT)**
  - Jede interne IP wird durch eine externe IP ersetzt
- **Hiding NAT = PAT (Port Address Translation) = NAPT (Network Address Port Translation)**
  - Das Socket-Paar (IP-Addresse und Port-Nummer) wird umkodiert
- **Verfahren**
  - Die verschiedenen lokalen Rechner werden in den Ports kodiert
  - Diese werden im Router an der Verbindung zum WAN dann geeignet kodiert
  - Bei ausgehenden Paketen wird die LAN-IP-Adresse und ein kodierter Port als Quelle angegeben
  - Bei eingehenden Paketen (mit der LAN-IP-Adresse als Ziel), kann dann aus dem kodierten Port der lokale Rechner und der passende Port aus einer Tabelle zurückgerechnet werden
- **Sicherheitsvorteile**
  - Rechner im lokalen Netzwerk können nicht direkt angesprochen werden
  - Löst auch das Problem knapper IPv4-Adressen
  - Lokale Rechner können nicht als Server dienen
- **DHCP (Dynamic Host Configuration Protocol)**
  - bringt ähnliche Vorteile

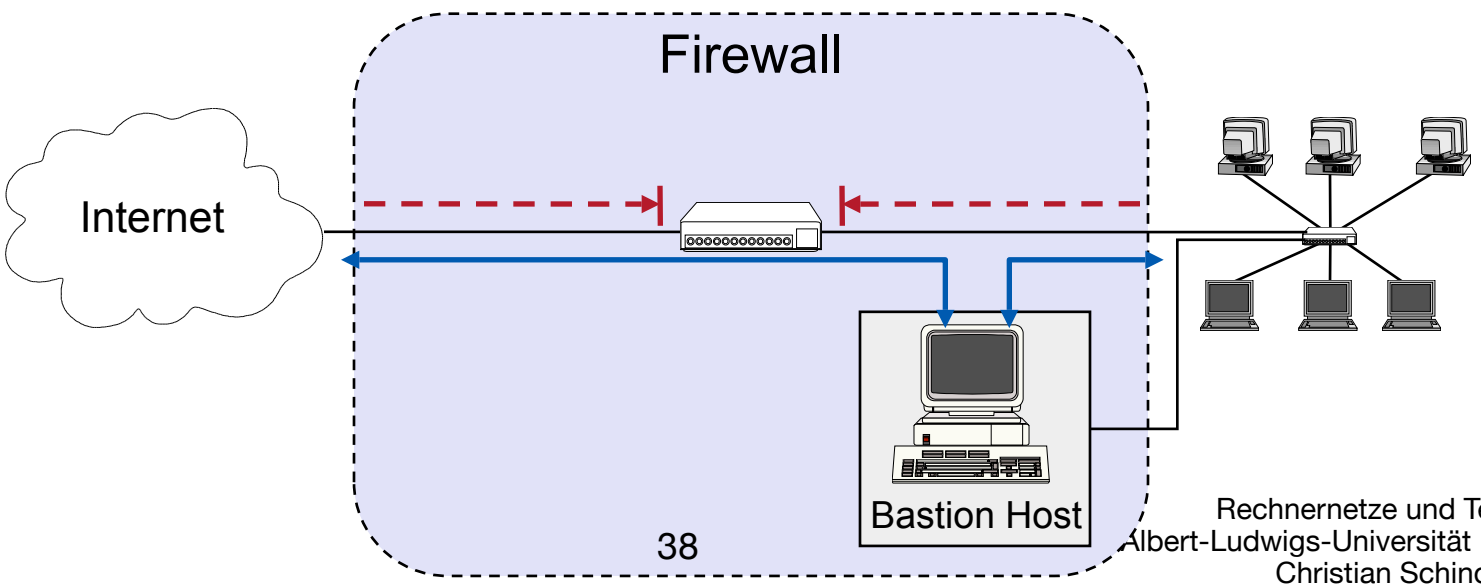
Firewall-Architektur Einfacher Paketfilter

- **Realisiert durch**
  - Eine Standard-Workstation (e.g. Linux PC) mit zwei Netzwerk-Interfaces und Filter-Software oder
  - Spezielles Router-Gerät mit Filterfähigkeiten



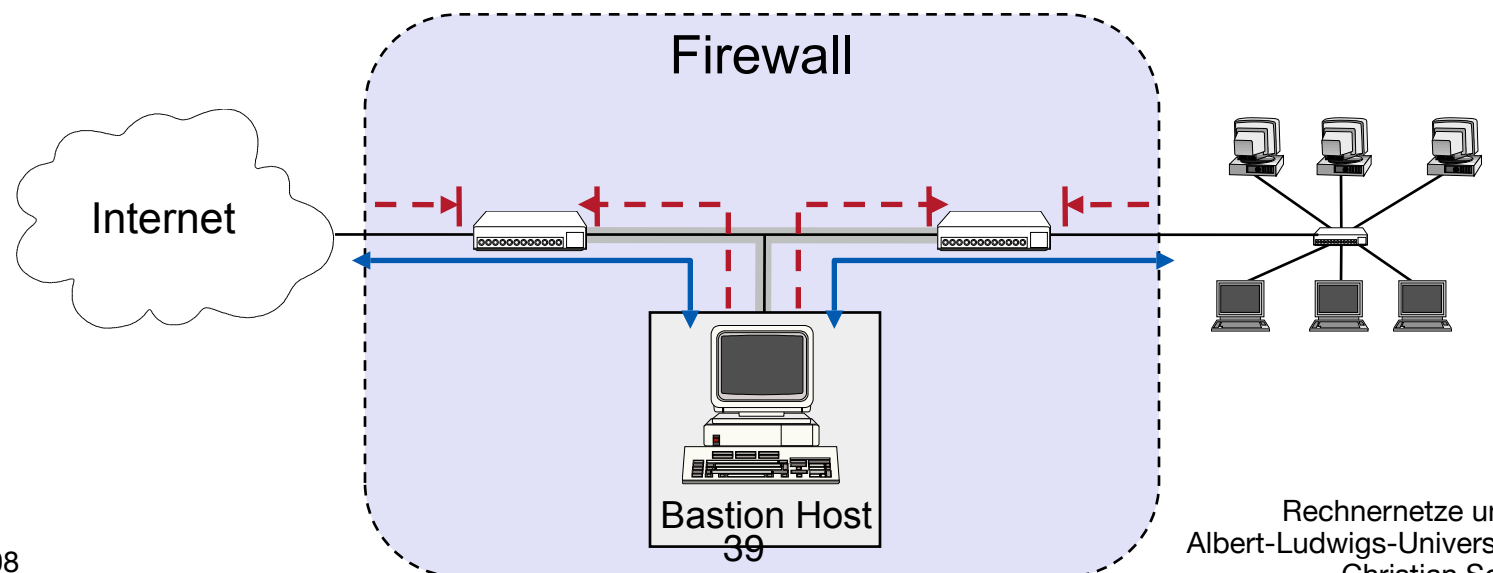
Firewall-Architektur Screened Host

- **Screened Host**
- **Der Paketfilter**
  - erlaubt nur Verkehr zwischen Internet und dem Bastion Host und
  - Bastion Host und geschützten Netzwerk
- **Der Screened Host bietet sich als Proxy an**
  - Der Proxy Host hat die Fähigkeiten selbst Angriffe abzuwehren



Firewall-Architektur Screened Subnet

- **Perimeter network zwischen Paketfiltern**
- **Der innere Paketfilter schützt das innere Netzwerk, falls das Perimeter-Network in Schwierigkeiten kommt**
  - Ein gehackter Bastion Host kann so das Netzwerk nicht ausspionieren
- **Perimeter Netzwerke sind besonders geeignet für die Bereitstellung öffentlicher Dienste, z.B. FTP, oder WWW-Server**



Firewall und Paketfilter

- **Fähigkeiten von Paketfilter**
  - Erkennung von Typ möglich (Demultiplexing-Information)
- **Verkehrskontrolle durch**
  - Source IP Address
  - Destination IP Address
  - Transport protocol
  - Source/destination application port
- **Grenzen von Paketfiltern (und Firewalls)**
  - Tunnel-Algorithmen sind aber mitunter nicht erkennbar
  - Möglich ist aber auch Eindringen über andere Verbindungen
    - z.B. Laptops, UMTS, GSM, Memory Sticks

Systeme II

Ende der 10. Vorlesungswoche

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Christian Schindelhauer
Sommer 2008

41