# *Systeme II*


**Albert-Ludwigs-Universität Freiburg**
**Rechnernetze und Telematik**
**Prof. Dr. Christian Schindelhauer**

**Christian Schindelhauer**

Sommersemester 2006

21. Vorlesung

19.07.2006

**schindel@informatik.uni-freiburg.de**

# Verschlüsselungs-methoden

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Symmetrische Verschlüsselungsverfahren**
  - z.B. 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)
  - Diffie-Helman
- **Digitale Unterschriften (Elektronische Signature)**
  - PGP (Phil Zimmermann), RSA

# Symmetrische Verschlüsselungsverfahren

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **z.B. Cäsars Code, DES, AES**
- **Es gibt Funktion f,g, so dass**
  - 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

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **z.B. SHA-1, SHA-2, MD5**

- **Ein kryptografische Hash-Funktion h bildet einen Text auf einen Code fester Länge so ab,**
  - h(text) = code
  - dass es unmöglich ist einen anderen Text zu finden mit:
    - h(text‘) = h(text) und text $\neq$ text‘
- **Mögliche Lösung:**
  - Verwendung einer symmetrischen Kryptografie-Methode

# Asymmetrische Verschlüsselungsverfahren

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **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

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **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

# Das RSA-Schema

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Geheimer Schlüssel:**
  - zwei große Primzahlen p,q
  - eine Zahl d , sodass
    - $e\ d = 1 \bmod \phi(n)$
    - mit $\phi(n) = (p-1)(q-1)$
- **Entschlüsselung:**
  - $\mathtt{message} = \mathtt{code}^{d} \bmod n$

- **Öffentlicher Schlüssel:**
  - $n = p\ q$
  - eine Zahl e
- **Verschlüsselung:**
  - $\mathtt{code} = \mathtt{message}^{e} \bmod n$

- **Kleiner Satz von Fermat:**
  - Für alle $m \neq 0$: $m^{\phi(n)} = 1 \bmod n$

- **Korrektheit:**

$$(\mathtt{message}^{e} \bmod n)^{d} \bmod n$$

$$= \mathtt{message}^{e\,d} \bmod n = \mathtt{message}^{e\,d \bmod \phi(n)} \bmod n$$

$$= \mathtt{message} \bmod n$$

# RSA Beispiel

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Geheimer Schlüssel:**
  - zwei große Primzahlen 7,11
  - eine Zahl d = 43, sodass
    - $e * d = 1 \bmod \phi(n)$
    - mit $\phi(n) = (p-1)(q-1) = 60$

- **Entschlüsselung:**
  - $\texttt{message} = \texttt{code}^{43} \bmod 77$

**$47^{43} \bmod 77 = \ldots = 5 = \text{message}$**

- **Öffentlicher Schlüssel:**
  - n = 77
  - eine Zahl e = 7

- **Verschlüsselung:**
  - $\texttt{code} = \texttt{message}^{7} \bmod 77$
  - message = 5
  - $\text{code} = 5^{7} \bmod 77 = 47$

# Elektronische Unterschriften

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **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 Entschüsselungsfunktion g
  - Kontrolleur
    - berechnet `h(text)`
    - und überprüft `f(offen, signatur)` = `h(text)`, für die asymmetrische Verschlüsselungsfunktion g

# IPsec (RFC 2401)

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Schutz für Replay-Attacken**
- **IKE (Internet Key Exchange) Protokoll**
  - Vereinbarung einer Security Association
    - Idientifikation, Festlegung von Schlüsseln, Netzwerke, Erneuerungszeiträume für Authentffizierung und IPsec Schlüssel
  - Erzeugung einer SA im Schnellmodus (Nach Etablieriung)
- **Encapsulating Security Payload (ESP)**
  - IP-Kopf unverschlüsselt, Nutzdaten verschlüsselt, mit Authentifizierung
- **IPsec im Transportmodus (für direkte Verbindungen)**
  - IPsec Header zwischen IP-Header und Nutzdaten
  - Überprüfung in den IP-Routern (dort muss IPsec vorhanden sein)
- **IPsec im Tunnelmodus (falls mindestens ein Router dazwischen ist)**
  - Das komplette IP-Paket wird verschlüsselt und mit dem IPsec-Header in einen neuen IP-Header verpackt
  - Nur an den Enden muss IPsec vorhanden sein.
- **IPsec ist Bestandteil von IPv6**
- **Rückportierungen nach IPv4 existieren**

# Firewalls

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **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
  - Bastion Host
  - Proxy

# Firewalls: Begriffe

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **(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

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Proxy (Stellvertreter)**
  - Spezieller Rechner, über den Anfragen umgeleitet werden
  - Anfragen und Antworten werden über den Proxy geleitet
  - Vorteil
    - Nur dort müssen Abwehrmaßnahmen getroffen werden
- **Network Address Translation (NAT):**
  - siehe folgende Folie

- **Perimeter Network:**
  - Ein Teilnetzwerk, das zwischen gesicherter und ungesichter Zone eine zusätzliche Schutzschicht bietet
  - Synonym demilitarisierte Zone (DMZ)

# NAT und PAT

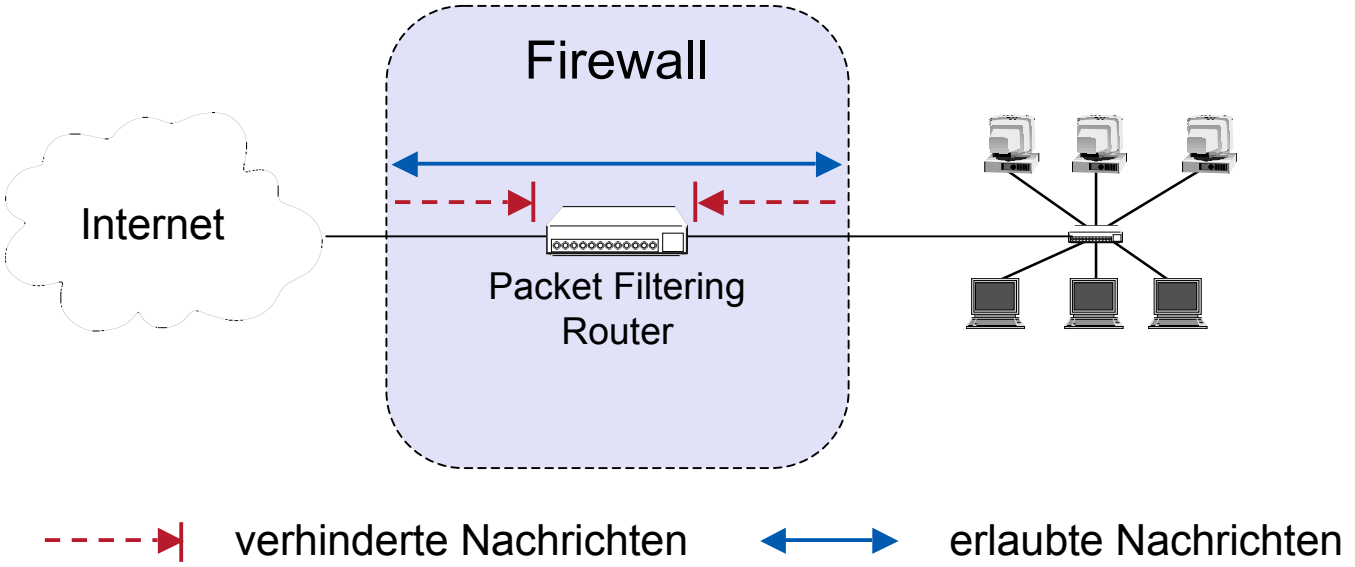
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **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

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

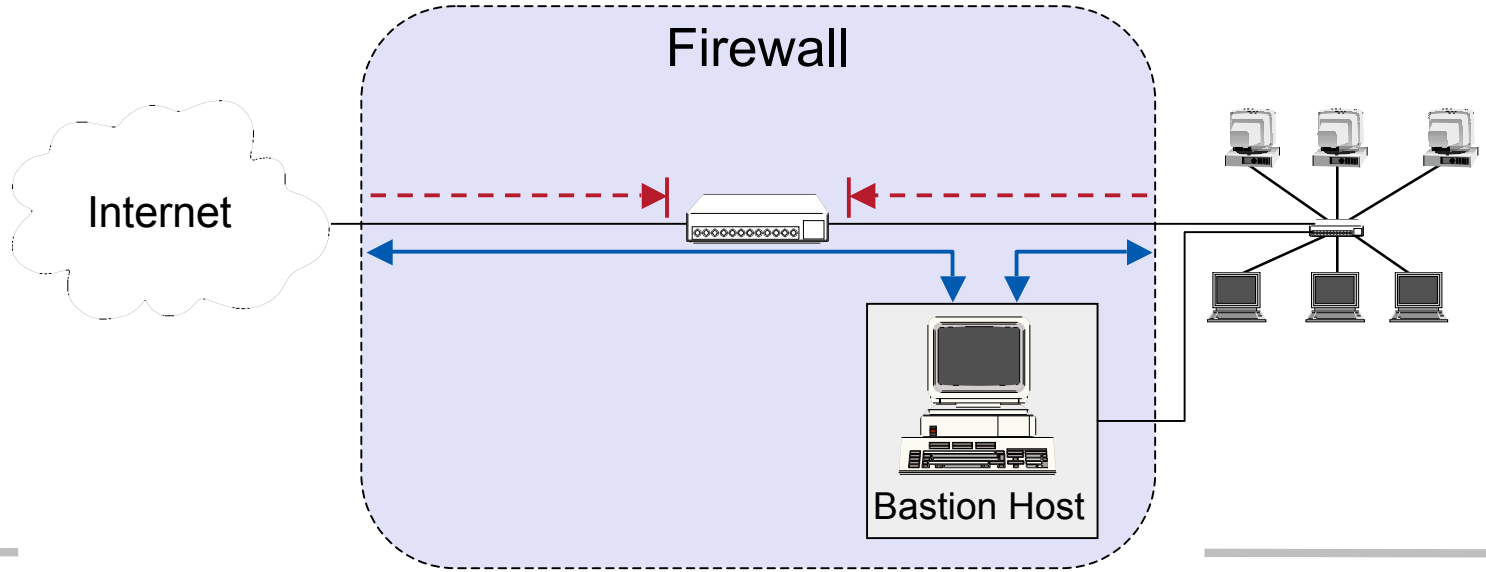
- **Realisiert durch**
  - Eine Standard-Workstation (e.g. Linux PC) mit zwei Netzwerk-Interfaces und Filter-Software oder
  - Spezielles Router-Gerät mit Filterfähigkeiten



# Firewall-Architektur
# Screened Host

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

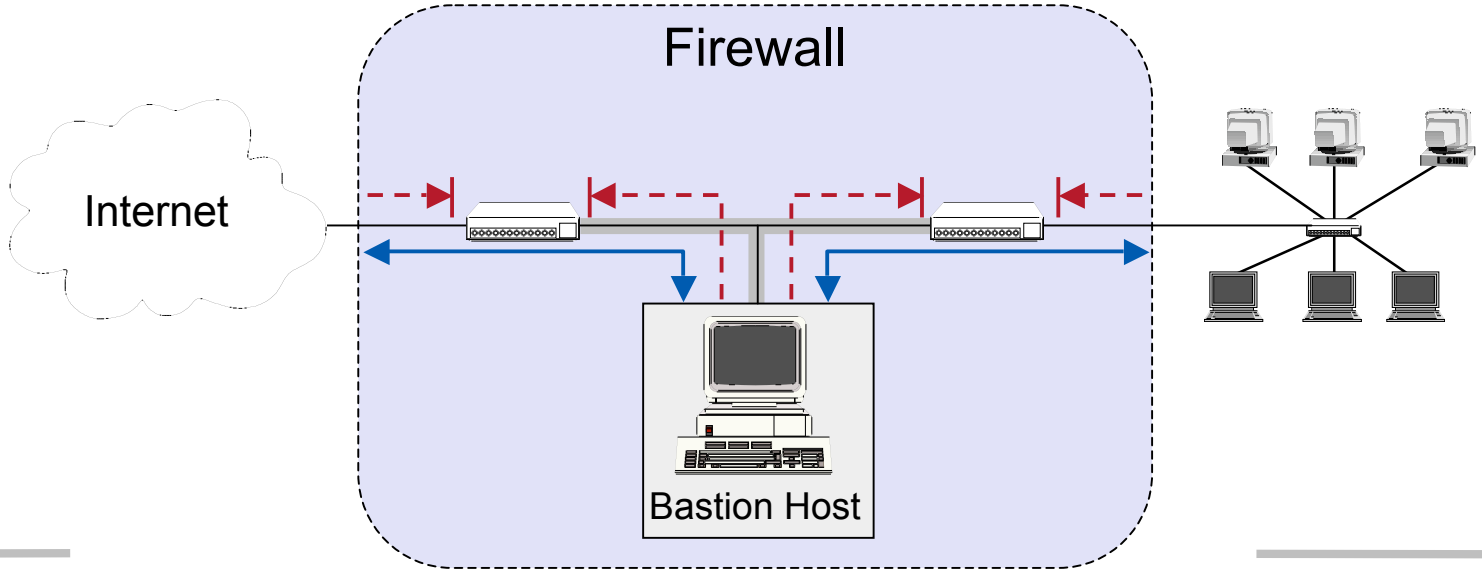
- **Screened Host**
- **Der Paketfilter**
  - erlaubt nur Verkehr zwischen Internet und dem Bastion Host und
  - Bastion Host und geschützten Netzwerk
- **Der Screened Host bietet sich als Proxy an**
  - Der Proxy Host hat die Fähigkeiten selbst Angriffe abzuwehren



# Firewall-Architektur Screened Subnet

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **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

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **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

# *Ende der 21. Vorlesung*


**Albert-Ludwigs-Universität Freiburg**
**Rechnernetze und Telematik**
**Prof. Dr. Christian Schindelhauer**

**Systeme II**

**Christian Schindelhauer**

**schindel@informatik.uni-freiburg.de**