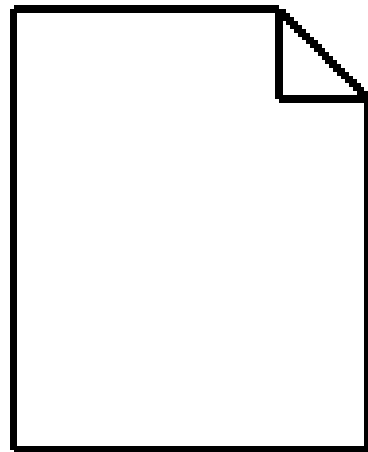
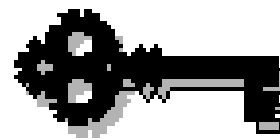


Kryptographie

Verschlüsselung (encryption) & Entschlüsselung (decryption)

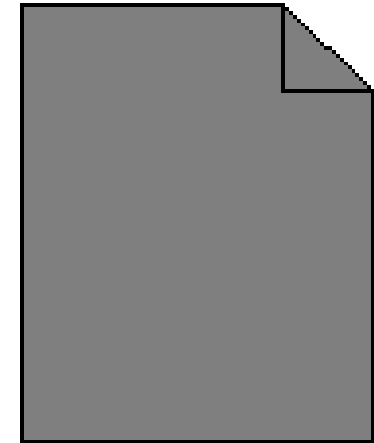
lukas.feiler@lukasfeiler.com

<http://teaching.lukasfeiler.com>



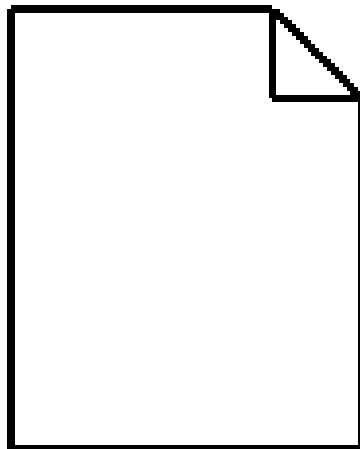
Plaintext

Verschlüsselung

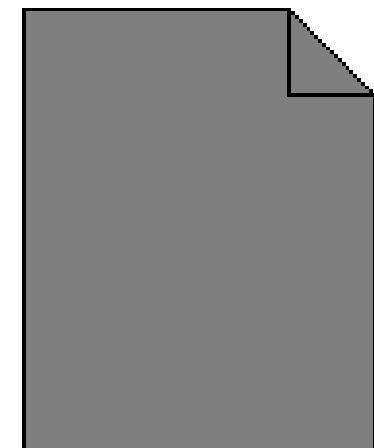


Ciphertext

Entschlüsselung



Plaintext



Ciphertext



Verschlüsselung & Entschlüsselung

Zweck der Kryptographie

„to keep a secret secret“

Geschichte der Kryptographie

- Von den Ägyptern über Caesar zu totalitären Systemen des 20. Jhdt.
- Kryptographie zur Sicherung der Privatsphäre

Substitution (Ersetzung)

z.B alle a durch b, alle b durch c usw. ersetzen (Caesar Cipher)
secret wird tfdsfu

Transposition (Vertauschung)

Reihenfolge der Buchstaben ändern

z.B. in Tabelle transformieren und in Spalten lesen

this-is-their-secret wird t-trchih-riseses-iet
als Tabelle mit 4 Zeilen:

| | | | | |
|---|---|---|---|---|
| t | - | t | r | c |
| h | i | h | - | r |
| i | s | e | s | e |
| s | - | i | e | t |

```
# dies ist ein Kommentar
# das file plaintext.txt anlegen
echo "SSL is an encrypted protocol." > plaintext.txt

# plaintext.txt verschlüsseln mit AES 256 Bit und den verschlüsselten
# Inhalt des files in encrypted.aes256 speichern
openssl enc -e -in plaintext.txt -aes256 > encrypted.aes256

# plaintext.txt löschen
rm plaintext.txt

# nun ist alles sicher, da verschlüsselt

# die Nachricht wieder entschlüsseln und in decrypted.txt speichern
openssl enc -d -in encrypted.aes256 -aes256 > decrypted.txt
```

Demonstration der Verschlüsselung einer Datei

Drei Arten von Verschlüsselungsverfahren

- symmetrische Verfahren
- asymmetrische Verfahren
- Message Digest Functions (One-way encryption)

Symmetrische Verfahren

- selber Key für Ver -u. Entschlüsselung
- z.B. DES, Triple-DES, Blowfish, AES

Key ist idR eine Passwort (beide Partner müssen dieses kennen)
40 - 1024 „Bit-Verschlüsselung“

Brute Force/Key Search Attack

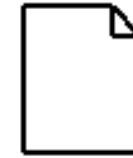
alle mögl. Keys werden durchprobiert
je mehr Bit desto schwieriger

| | | |
|---------|--------------------------------|-----------------|
| 56 Bit | Spezielle Hardware | 18 Min. |
| 128 Bit | größeres Netzwerk | 10^{22} Jahre |
| 256 Bit | Quantencomputer im Jahre 2040? | 10^{37} Jahre |

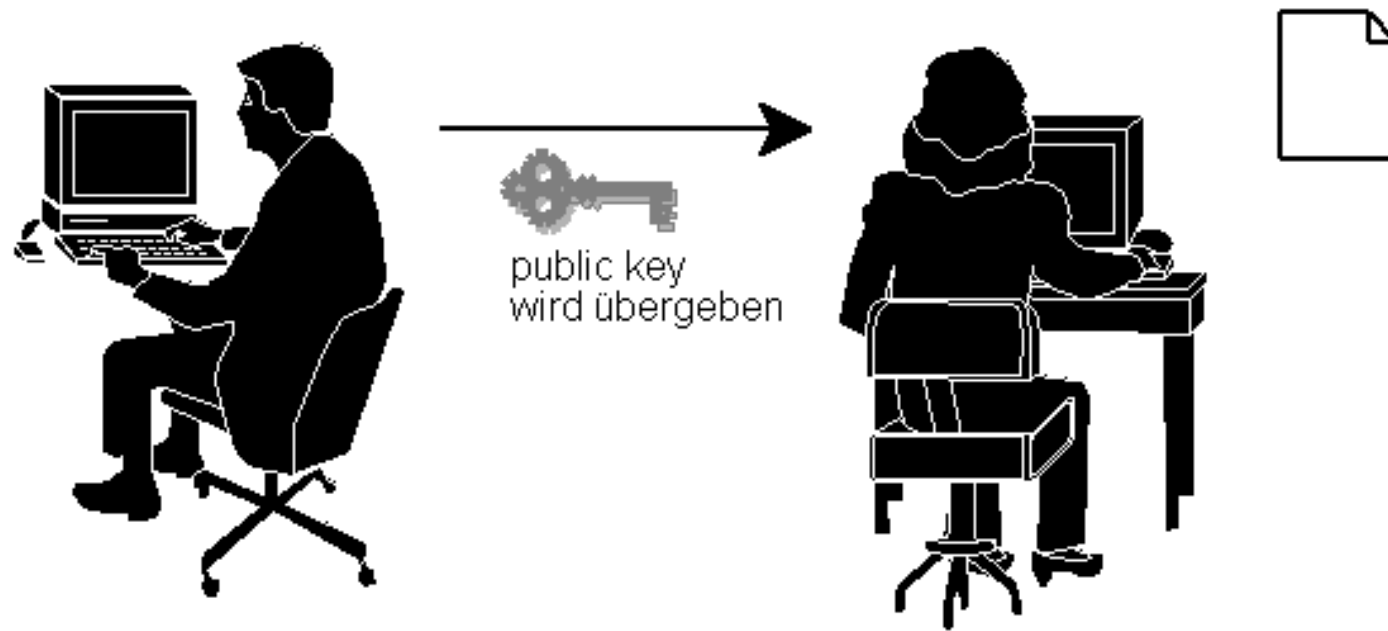
kryptographische Analyse
den Algorithmus „knacken“

Asymmetrische Verfahren (public key encryption)

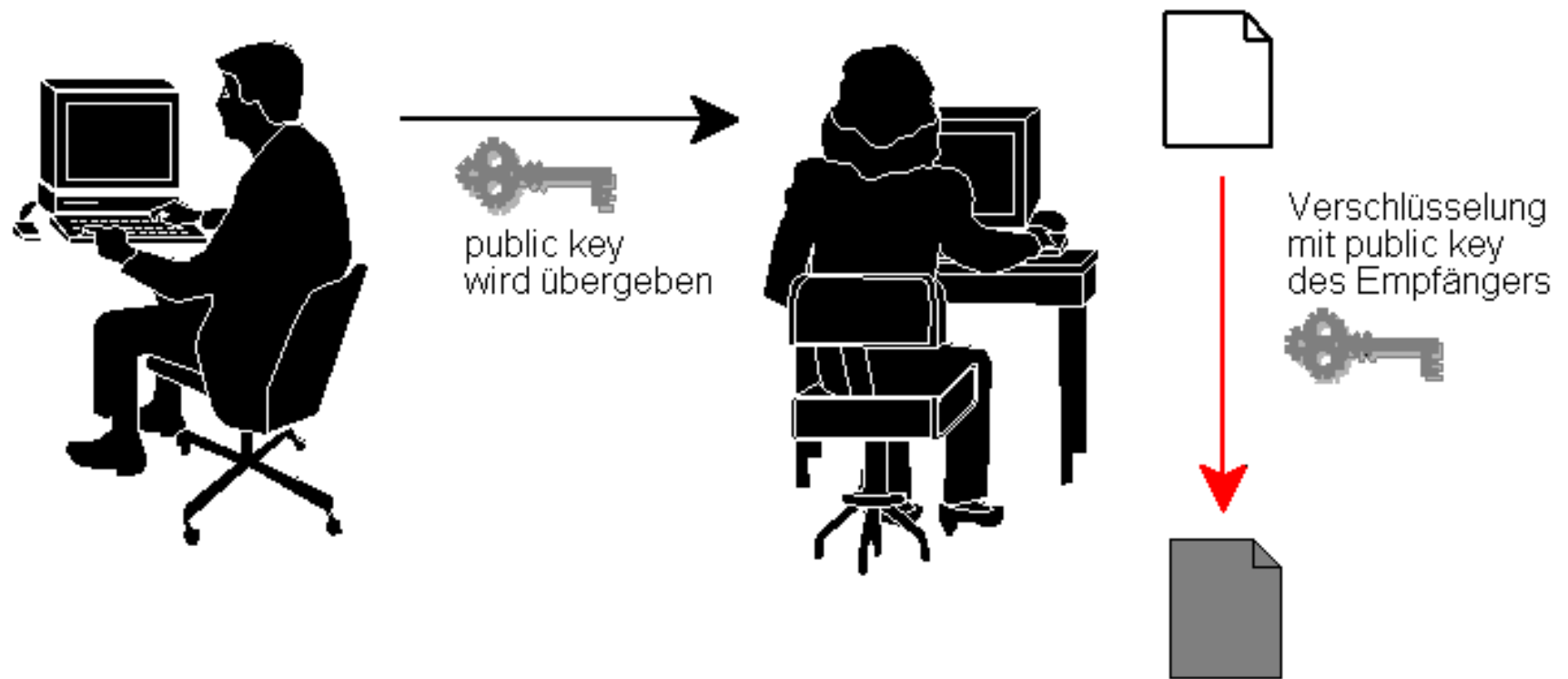
- ein Key zum Verschlüsseln (public key), ein anderer zum Entschlüsseln (private key)
- z.B. DSA, RSA



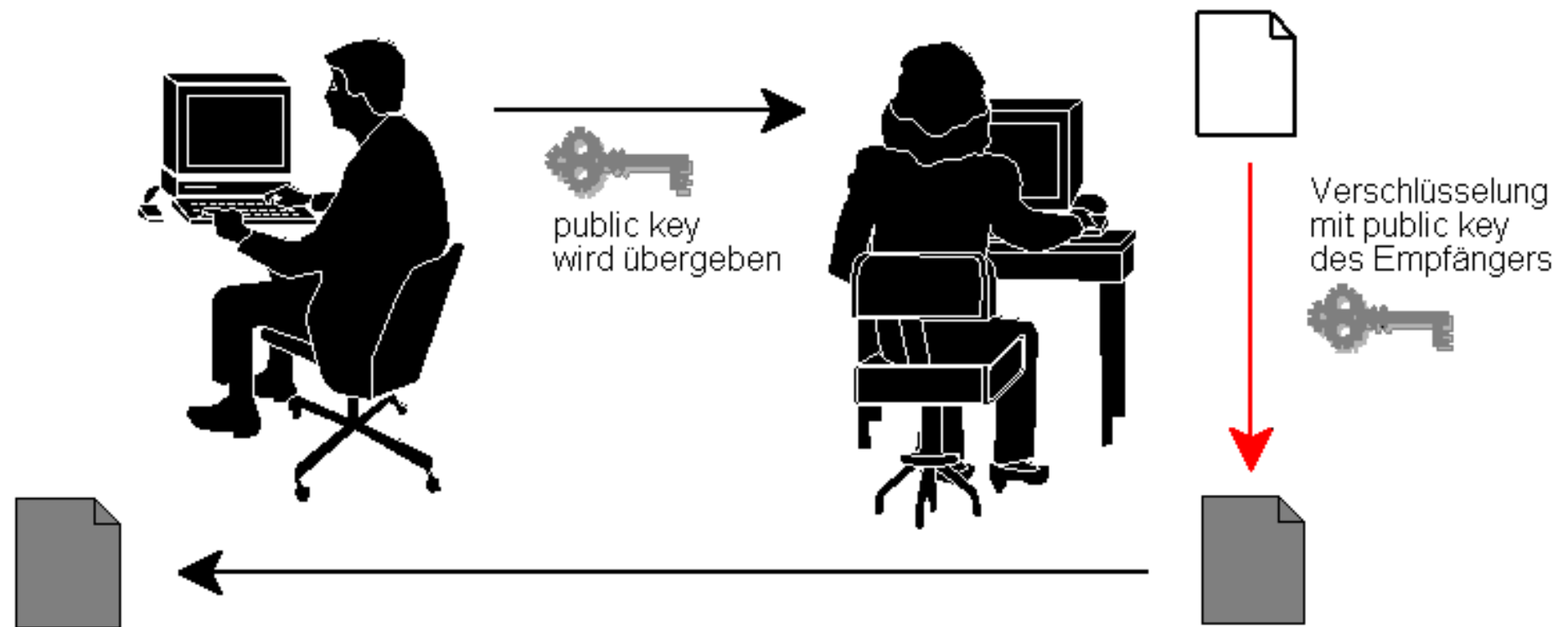
Public Key Encryption



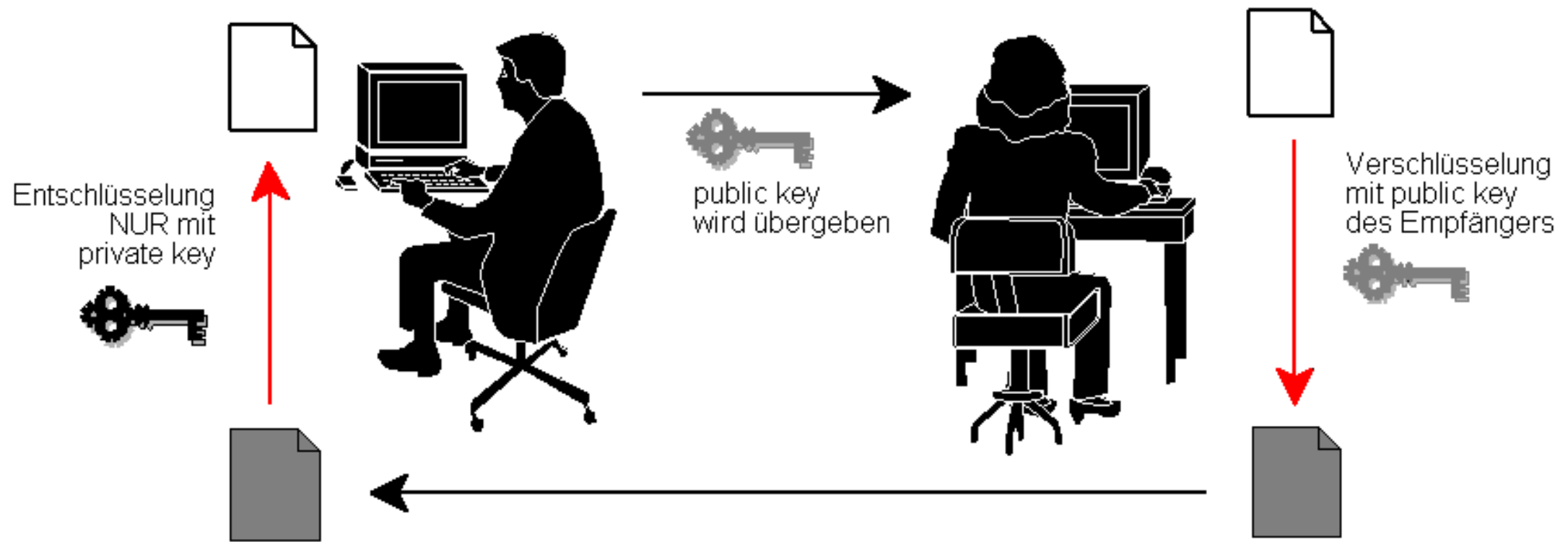
Public Key Encryption



Public Key Encryption



Public Key Encryption



Public Key Encryption

Brute Force/Key Search Attack
vom Public Key den Private Key errechnen

kryptographische Analyse
den Algorithmus „knacken“

Angriffsmethoden gegen asymmetrische Verfahren

Message Digest Functions (One-Way-Encryption)

Anhand des Inhalts einer Datei eine eindeutige 128 od. 256 Bit Zahl errechnen.

Grundgedanke: keine zwei Dateien mit der selben Message Digest.
z.B. MD5, SHA-1

```
# dies ist ein Kommentar
```

```
# das file test1.txt anlegen  
echo "This is a test." > test1.txt
```

```
# das file test2.txt anlegen  
echo "this is a test." > test2.txt
```

```
# komplett unterschiedliche MD5-Summen auf Grund eines Zeichens!  
md5sum test1.txt test2.txt
```

```
# test2.txt dem file test1.txt gleichsetzen  
echo "This is a test." > test2.txt
```

```
# selber Inhalt, selbe MD5-Summen!  
md5sum test1.txt test2.txt
```

Demonstration von Message Digest Functions

Symmetrische Verfahren

- sehr schnell
- nicht geeignet bei unbekannten Kommunikationspartner

Asymmetrische Verfahren (public key encryption)

- langsam
- gut geeignet bei unbekannten Kommunikationspartnern

Message Digest Functions

- nur One-Way

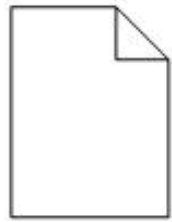
Vergleich der verschiedenen Verfahren

Digitale Signatur mit public key encryption

- Unterschrift wird mit Private Key erzeugt
- Mit Public Key verifizierbar

→ Message Digest der Nachricht wird mit Private Key verschlüsselt.

Anwendungsgebiet: E-Mail z.B. mit GnuPG (www.gnupg.org)



Message Digest Function



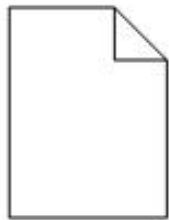
b99e98584b39...



Verschlüsselung mit
Private Key des Signator

Elektronische Signatur

ghdr



Message Digest Function

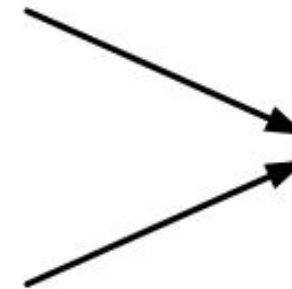


b99e98584b39...

Entschlüsselung mit
Public Key des Signator



b99e98584b39...



= ??

ghdr



- 1) über asymmetrische Verfahren (z.B. DSA) wird eine sichere Verbindung hergestellt
- 2) über diese wird ein gemeinsamer Key vereinbart
- 3) dieser Key wird für schnellere symmetrische Verfahren (z.B. 3DES, AES) verwendet
- 4) mit Message Digest Functions (z.B. MD5) wird Integrität der Daten sicher gestellt

Gemeinsamer Einsatz der Verfahren am Beispiel SSH od. SSL

IDS – Intrusion Detection System

Zwei Arten von Einbruchserkennungssystemen:

- Host Based IDS (HIDS)
- Network IDS (NIDS)

Die Anatomie eines Angriffs: „the 5 Ps“

- 1) Probe
- 2) Penetrate
- 3) Persist
- 4) Propagate
- 5) Paralyze

1) Probe



Der Angreifer versucht Informationen über das System zu erlangen:

- www, google, DNS, whois
- Port Scans, Vulnerability Scans

Probe, Penetrate, Persist, Propagate, Paralyze



2) Penetrate



Der Einbruch selbst:

- durch das Ausbeuten einer Vulnerability (meist mittels eines Exploits)
- idR schwer bemerkbar

Der Angreifer „owned“ jetzt das System

Probe, Penetrate, Persist, Propagate, Paralyze



3) Persist



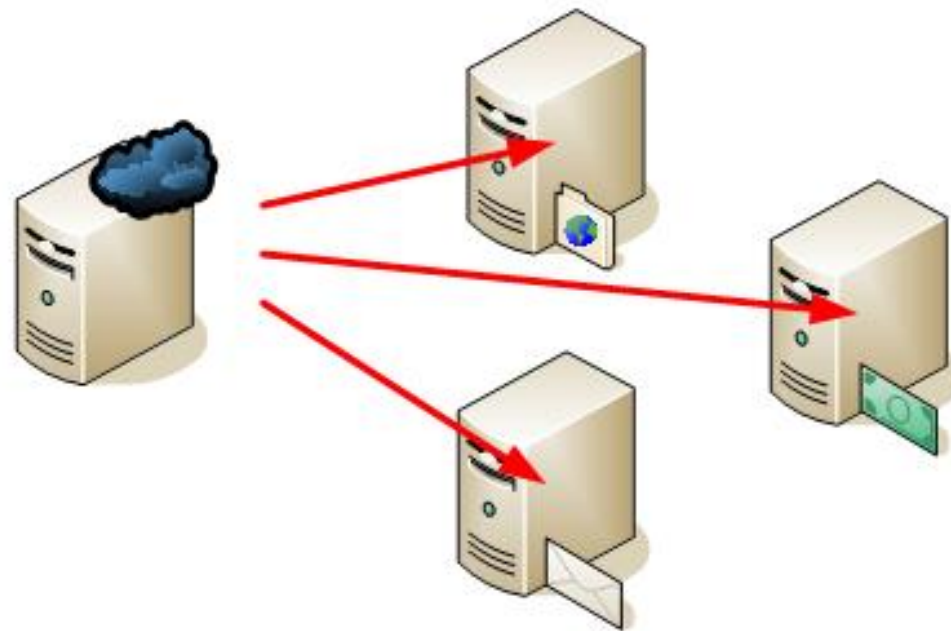
Der Angreifer stellt sicher auch später noch Zugriff zu haben: Backdoors

- z.B. remote control software
- z.B. ein neuer Account

Probe, Penetrate, **Persist**, Propagate, Paralyze



4) Propagate



Angriff weiterer Rechner im selben Netzwerk

- idR keine schützende Firewall
- oft durch ausnützen von Trust Relationships

Probe, Penetrate, Persist, **Propagate**, Paralyze

5) Paralyze



Going for the „soft, chewy center“

→ Erreichen des Primärziels des Angriffs

z.B: - DoS

- Angriff auf Dritte (z.B. via WAN od. VPN)
- DB-Server mit Kreditkartendaten
- File-Server mit Unternehmensgeheimnissen

Probe, Penetrate, Persist, Propagate, **Paralyze**

Host Based Intrusion Detection Systems (HIDS)

z.B. Tripwire, AIDE

- Vorteile eines HIDS
 - Hacker lassen idR eine (auffindbare) Backdoor zurück
- Funktionsweise
 - Message Digest für jedes File
 - Überwachung der Log-Files
- Nachteile
 - meist sind nur bereits erfolgreiche Angriffe erkennbar

Network Intrusion Detection Systems (NIDS)

z.B. Snort

- Vorteile eines NIDS
 - zentralisierte Infrastruktur
 - auch nicht erfolgreiche Angriffe werden erkannt

- Funktionsweise
 - es wird nach bestimmten Patterns gesucht

z.B: IIS Unicode exploit (CVE-2000-0884 bzw. MS00-078)
ermöglicht das ausführen von Commands auf
einem Windows Server mit IIS 4.0 & 5.0:

`http://www.example.com/scripts/..%c0%af../winnt/
system32/cmd.exe?/c+dir`

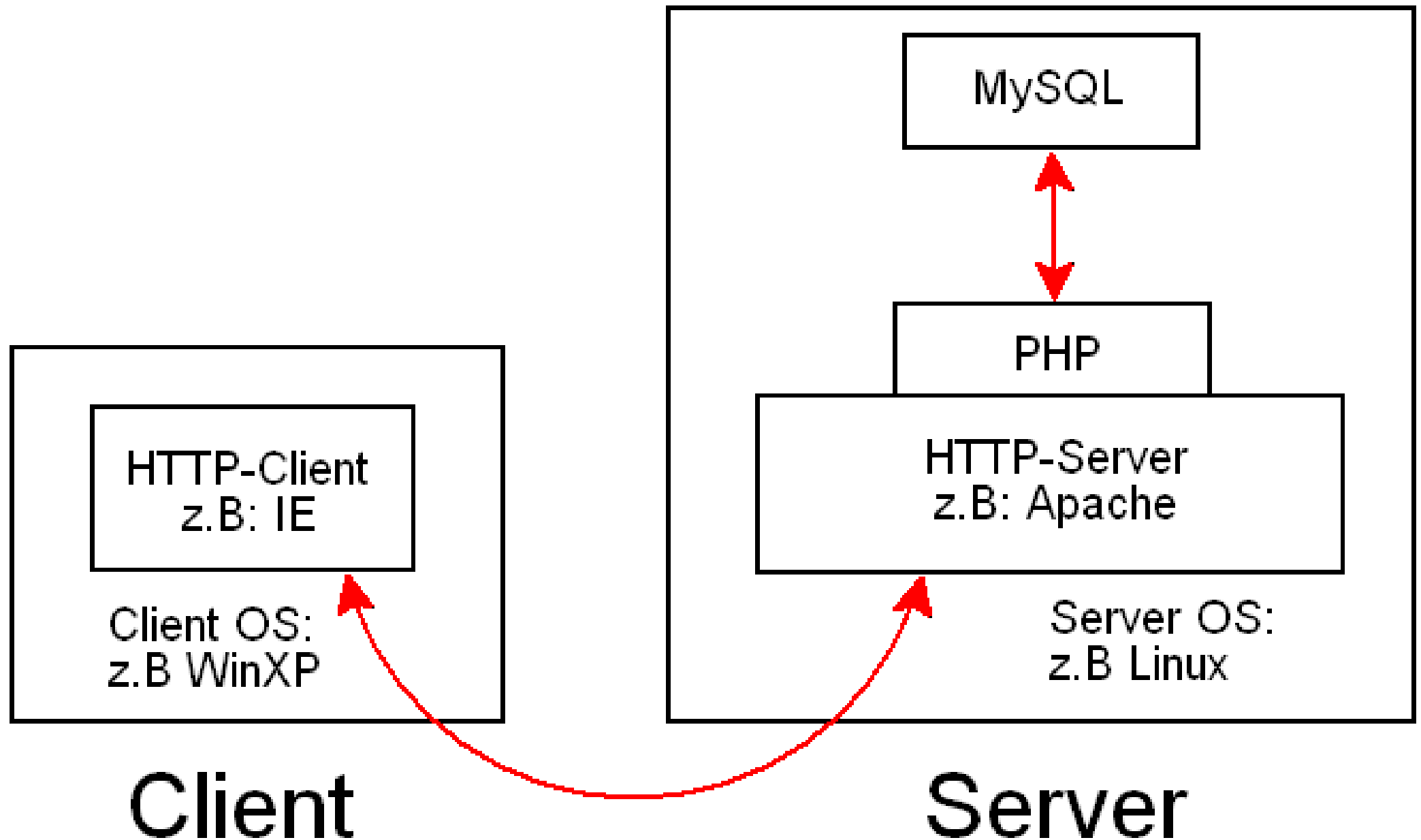
IPS – Intrusion Prevention System

Durch Reaktion auf Angriffe

Gefahr: False Positives

sehr junge Technologie

Serverarchitekturen

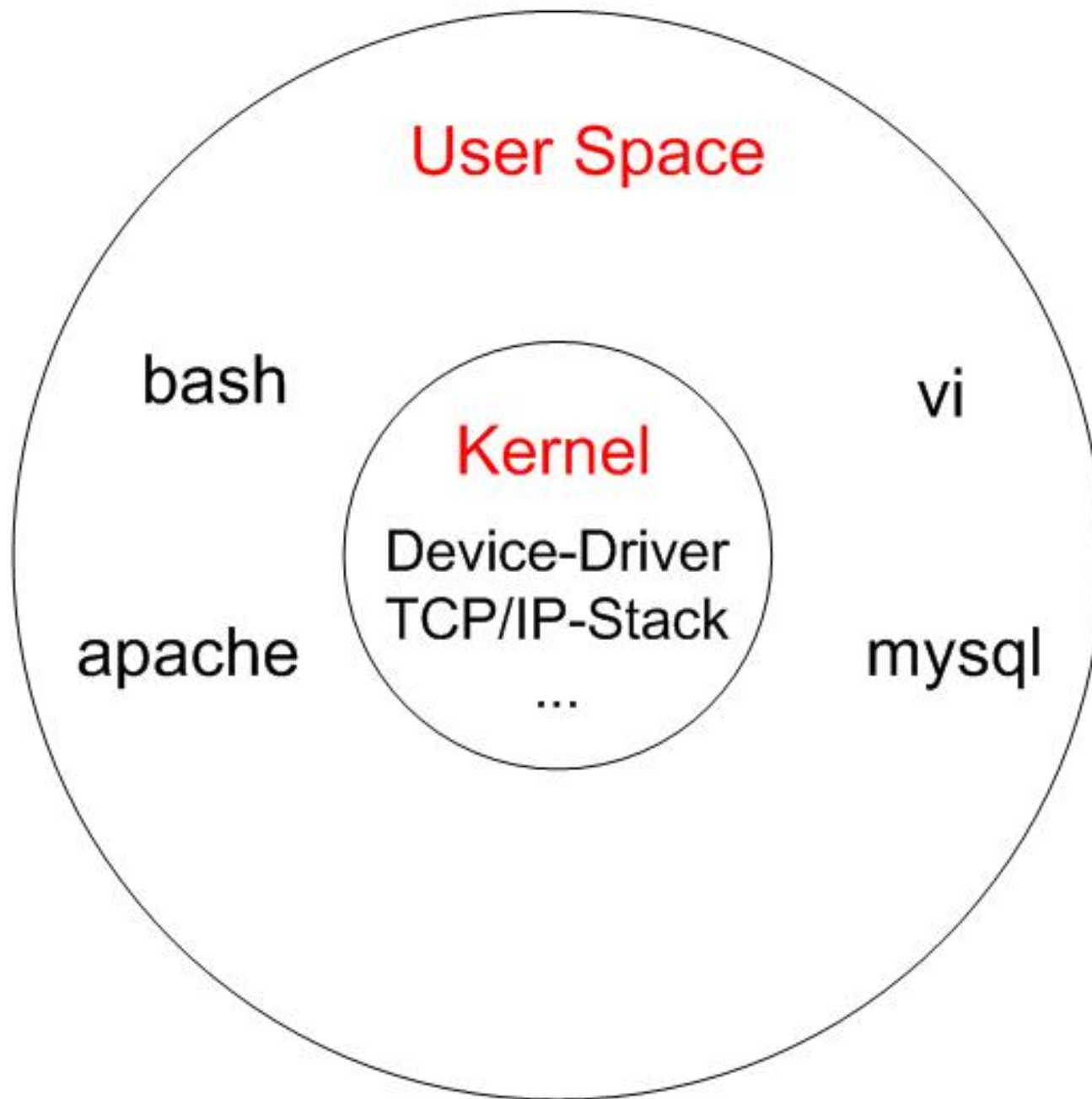


Client/Server Model mit typischem Web-Server

Eine kleine Einführung in Unix

Unix-Derivate: Linux, AIX, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X, SCO Unix, ...

kein Unix: z.B. Windows, DOS, Mac OS 9



Die Shell als Interface zwischen Mensch und Unix

Grundbefehle: ls, pwd, cd, more, man, ...

Wichtigsten Eigenschaften von Unix

- File-based
- Multi-User
- Multi-Tasking

- jede Information in Form einer Daten
- jeder Befehl ist eine eigene Datei
die Shell sucht nach Befehlen nur in \$PATH

- Verschiedene Arten von Usern: root & der Rest
- Benutzergruppen
- File Permissions
 - r ... lesen (read)
 - w ... schreiben (write)
 - x ... ausführen (execute)

setzbar für

user, dem das File gehört

group, der das File gehört

others, dem Rest

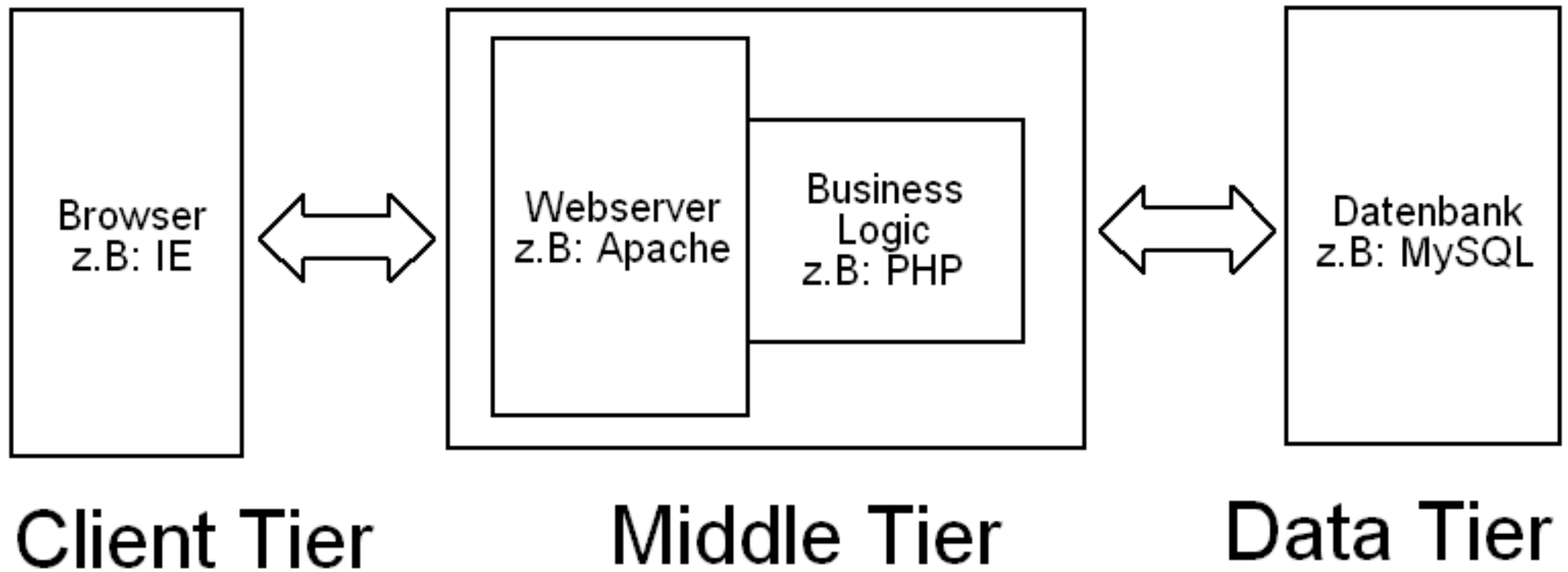
Ownership ändern mit chown/chgrp

Permissions ändern mit chmod

- mehrere Prozesse werden gleichzeitig ausgeführt
- nützliche Befehle
 - ps ... Liste an laufenden Prozessen anzeigen
 - kill ... einen Prozessen beenden
 - Ctrl-C ... einen Prozess abbrechen
 - Ctrl-Z ... einen Prozess in den Hintergrund schicken
 - bg ... Hintergrund-Prozesse anzeigen
 - fg ... einen Prozess in den Vordergrund holen

Three Tier Application Model

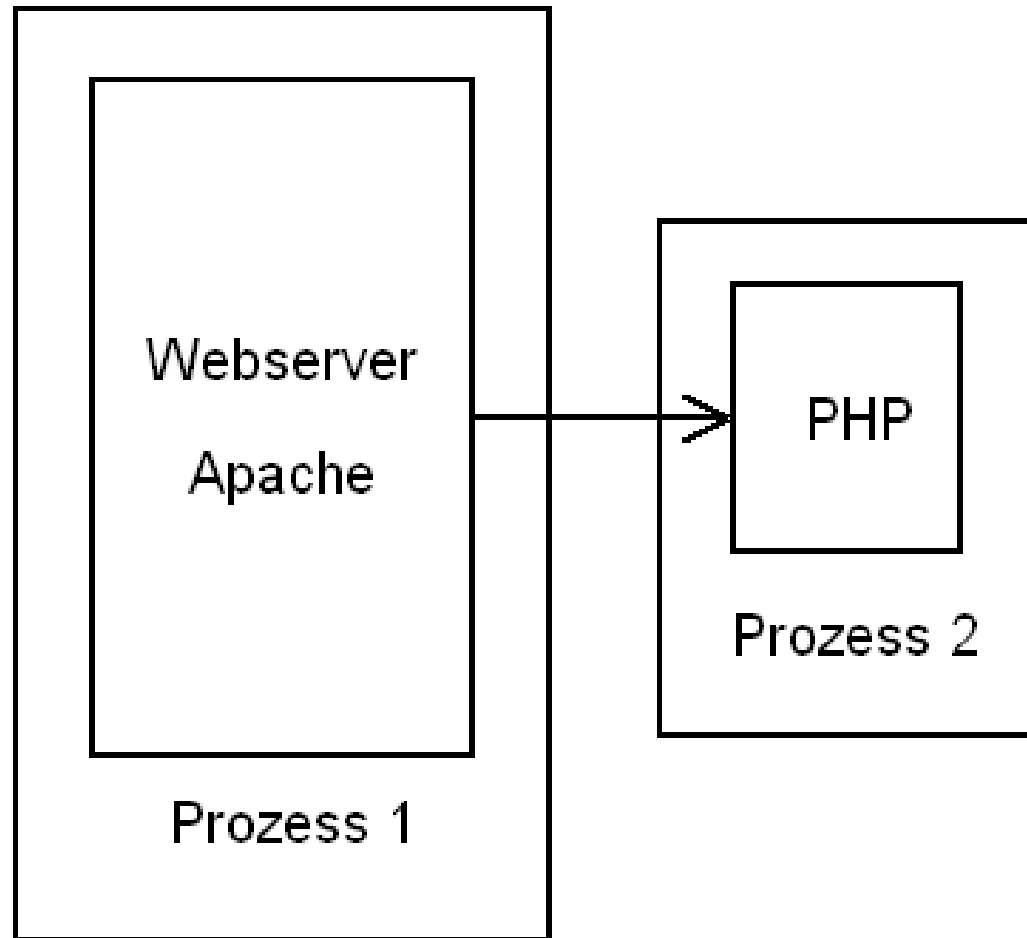
- Client Tier
- Middle Tier
- Data Tier



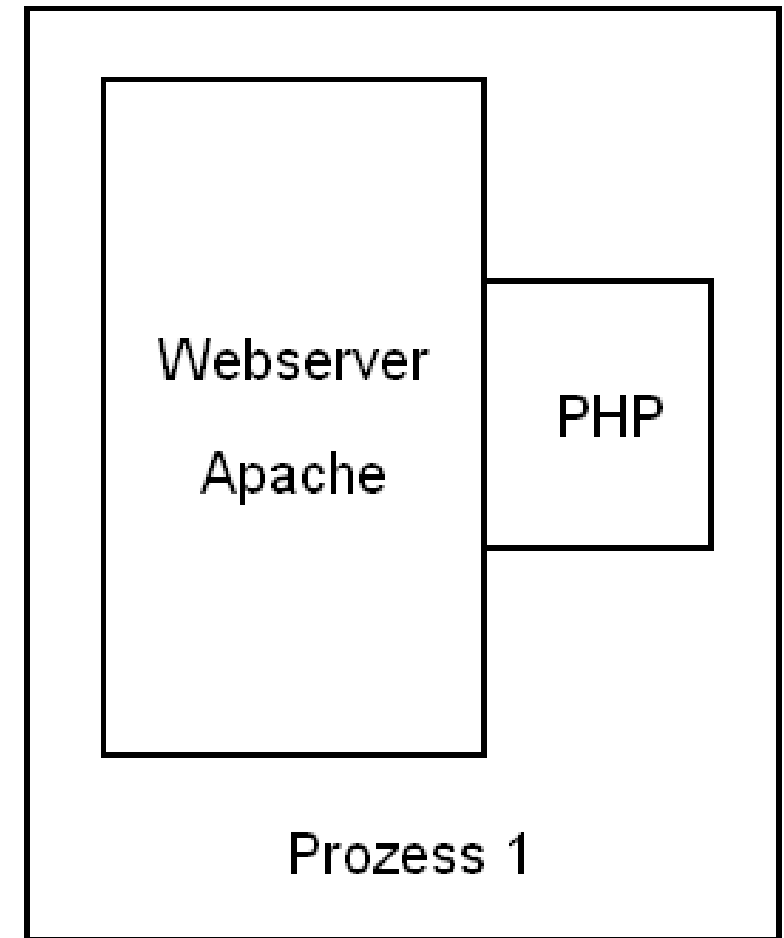
Three Tier Application Model (Tier = Stufe!)

Live Installation von Apache/PHP/MySQL auf WinXP

PHP über CGI



PHP als Apache-Modul



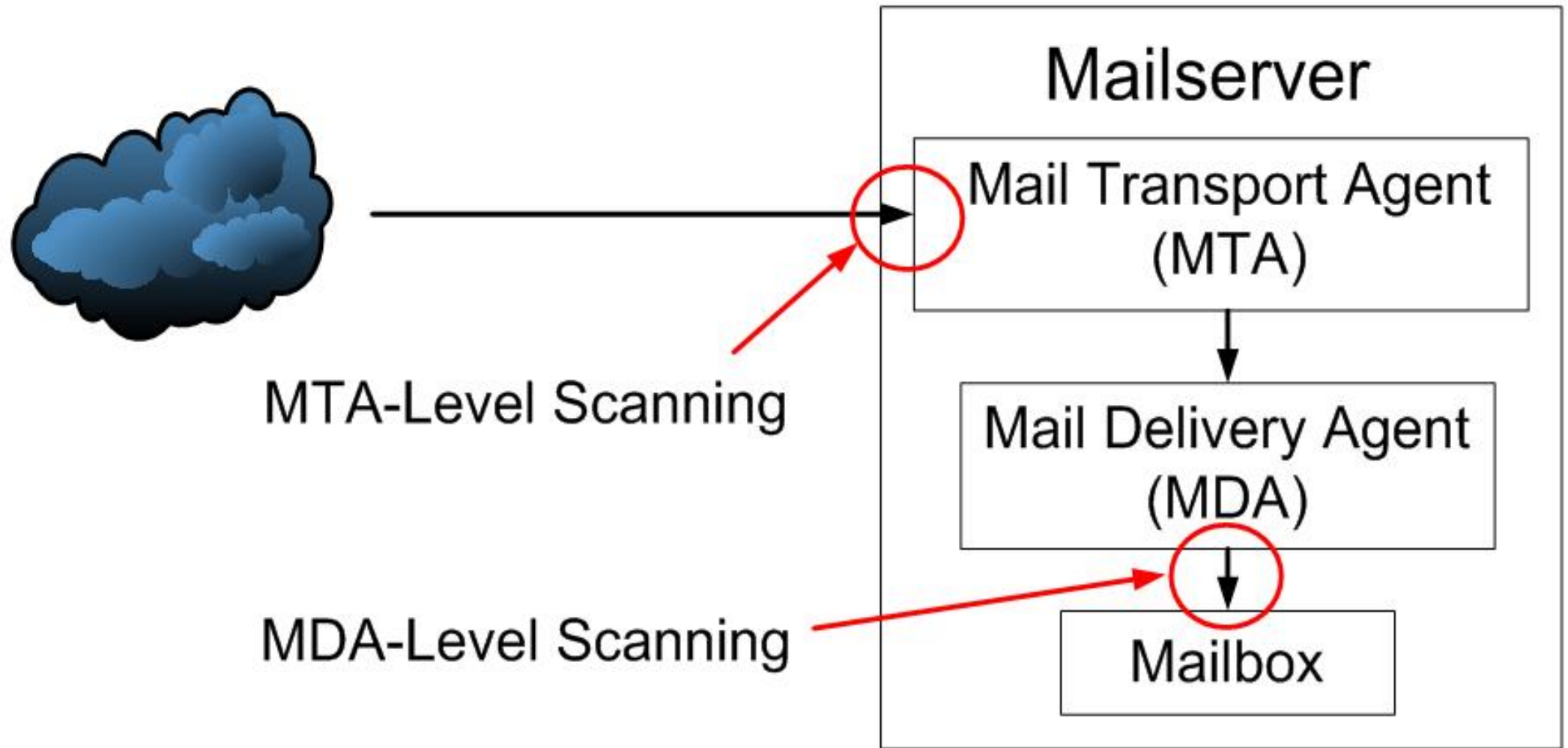
Architektur eines Mail-Server

Mail Transport Agent (MTA)/SMTP Server: qmail, sendmail, postfix, ...

Mail Delivery Agent (MDA): liefert Mails in best. Mailboxen

Anti-Virus Software: z.B. Clam AV, Symantec, ...

Anti-Spam Software: z.B. SpamAssassin



Spam –u. Virus-Scanning ist an verschiedenen Stellen möglich

Mailserver-Architektur: verschiedene Filtermöglichkeiten

Exkurs: Open Source Software (OSS)

FSF (Free Software Foundation) & GNU (GNU's Not Unix)
GNU/Linux

- GNU GPL (General Public Licence)
- GNU LGPL (Lesser General Public Licence)
- ...