

Überblick

- Einführung
- Umfrage Ergebnisse aus den USA
- Gefahr Quellen
- Definition von Sicherheit
- Kurze Historie
- Arten der Sicherheit
- Angriffsbeispiele auf die Hostsicherheit

Umfrage Ergebnisse

503 Institutionen wurden abgefragt:

90 % haben Computer Einbrüche festgestellt

80 % haben zugegeben finanziell
beschädigt worden zu sein

44 % konnten die Schäden quantifizieren
und diese beliefen sich auf
\$ 455 848 000

40 % Feststellen eines Eindringens von Außen

40 % Feststellen von DoS Attacken

78 % Missbrauch von Arbeitssystemen

85 % Computer Viren

(Quelle: Computer Security Institute. Jahr 2002)

Gefahr Quellen

Umweltbedingte Gefahren

- Feuer
- Wasser
- Blitz

Technischbedingte Gefahren

- Komplexe Hardware Struktur
- Inkompatibilität

Menschenbedingte Gefahren

- Mangelhafte Konfiguration
- Unkundige Anwender
- Verbrecher, Eindringlinge
→ Angreifer.

Die Diversität des Angreifers:

- von dem unzufriedenen Mitarbeiter
- bis zu Geheimdiensten

Angreifer nutzen die Schwächen von:

- Betriebssystemen
- Anwendungen
- Netzwerkprotokollen
- Systemhardware aus

Angriffe sind durch folgende Schritte gekennzeichnet:

1. Erlangung des Zugangs zum System
2. Etablieren eines Superuser Status
3. Einrichtung einer Hintertür
4. Löschen aller Spuren

Dabei können folgende Schäden entstehen:

- . Geldverlust
- . Imageverlust
- . Verletzung gesetzlicher Vorschriften
- . Steigende Betriebskosten
- . Verlorene Geschäftsmöglichkeiten
- . Nachteile gegenüber der Konkurrenz
- . Irreführende Bilanzen

Definition von Sicherheit

- Verhindern unbefugter Aktivitäten* an, mit oder durch das eigene System.
- Gewährleisten gewollter Aktivitäten* an, mit oder durch das System

(Quelle: Seminar Bericht „Sicherheit im vernetzten Systemen“)

- Sicherheit bedeutet, gewisse Ziele trotz gewisser Bedrohungen zu erreichen. Mit Bedrohungen meint man hier meist absichtlich von Menschen ausgehende Bedrohungen.

(Quelle: <http://www-krypt.cs.uni-sb.de/>)

*Erlaubte und verbotene Aktivitäten sind in einer Sicherheitspolitik festgelegt. (Siehe Vortrag am 14.11.2002)

Wichtige Eigenschaften von Sicherheit, die bei der Umsetzung eines Sicherheitskonzeptes durchgesetzt werden müssen:

- **Verfügbarkeit**

Alle Arbeitsplätze im Netz müssen ständig Zugang zu ihren Daten haben.

- **Integrität**

Datenintegrität bezeichnet den Umstand, dass die gespeicherten Daten die Realität exakt widerspiegeln sollen.

- **Vertraulichkeit**

Die Daten des Systems können nur von den Personen gelesen und benutzt werden, die dazu berechtigt sind.

- **Authentizität**

Identität des Verfassers entspricht die Realität.

- **Non deniability**

- **Non repudiation**

Historische Entwicklung von Sicherheitsproblemen

Bis vor einigen Jahren stand der Sicherheitsaspekt von Computern und Netzwerken im Hintergrund. Die Gründe dafür liegen in deren Entwicklung.

- die Zielsetzung bei der anfänglichen Zeit war die einfache Funktionalität.

Folge:

Heutige Systeme bauen auf Paradigmen von gestern auf, bei deren Entwicklung die Sicherheit keine große Rolle gespielt hat, daraus resultiert, dass die Integration von Sicherheit sich als problematisch erweist.

Arten der Sicherheit

• Hostsicherheit

Physikalische Sicherheit

Zu verhindernde Angriffe:

- Hardware Ausbau
- Reboot von System
- Anschluss eines Rechners an das Netz
- Umkonfiguration (hardware)

Software Sicherheit

Zu verhindernde Angriffe:

- Angriff auf Betriebssystem Lücken (z.B Buffer Overflow)
- trap door
- denial-of-service
- Hijacking
- Trojanische Pferde
- Würmer
- Viren
- Logische Bomben
- Spoofing
- Sniffing
- Activ contend (HTML, JavaScript, Java, VBA, VBS, AktivX, PHP, Pearl, usw)

• Netzwerksicherheit

Angriffsbeispiele auf die Hostsicherheit

Angriffe auf Passwort

Passwort-Cracker sind nichts anderes als Programme, die mittels der Kombination von Wörterbuch-Attaken und der Brute-Force-Methode versuchen, Passwörter zu erhalten.

Zu den systematischen ausprobieren wird auch folgende Punkte integriert:

- jedes Wort auch rückwärts testen
- Groß- und Kleinschreibung kombinieren
- Wörter zusammenhängen (z. B. Wort vorwärts + Wort rückwärts)
- Einfügen von Zahlen am Anfang, Ende oder im Wort

UNIX-Passwort-Cracker:

- Crack
- John the Ripper
- Hades
- CrackerJack

Windows NT- Passwort-Cracker:

- 10phtCrack 2.0,
- ScanNT
- NTCrack

Beispiel:

Unter Unix liegen die Passwort Datei unter:

/etc/passwd

➤ für jeden Benutzer lesbar

ein Eintrag in diese Datei sieht wie folgt:

*ahmet:1/ghdtezEGRg:10000:10000:Ahmet
Yilmaz:home/ahmet:/bin/bash*

mit dem Aufruf „crypt“ kann beliebige Wörter
verschlüsselt werden

bis der korrespondierende Wort zu „ghdtezEGRg“
gefunden wird.

Angriffe auf Betriebssystem Lücken:

Beispiel:

➤ Buffer Overflow

Beliebte Angriffstechnik um eine Administrator-Berechtigung zu erlangen. Dabei passiert folgender Vorgang:

- Ein Server-Programm legt seine Daten vor der Verarbeitung in einem Puffer-Speicher ab.
- Ein Überlaufen des Speichers wird aber nicht geprüft und verhindert.
- Das Programm des Angreifers überflutet gezielt den Puffer und überschreibt damit die angrenzenden Speicherdaten.
- Das Server-Programm stürzt ab und hinterlässt das aufrufende Programm, das meist mit Administrator-Berechtigung läuft.
- Am Ende der gesendeten Daten wird der Aufruf einer Shell übertragen (z.B.: /bin/sh). Beispiel aus dem Programm qpop (Hack für POP3-Server):
- `char shellcode[] =`

```
"\xeb\x22\x5e\x89\xf3\x89\xf7\x83\xc7\x07\x31\xc0\xaa"
```

```
"\x89\xf9\x89\xf0xab\x89\xfa\x31\xc0xab\xb0\x08\x04"
```

```
"\x03xcd\x80\x31\xdb\x89\xd8\x40xcd\x80\xe8\xd9\xff"
```

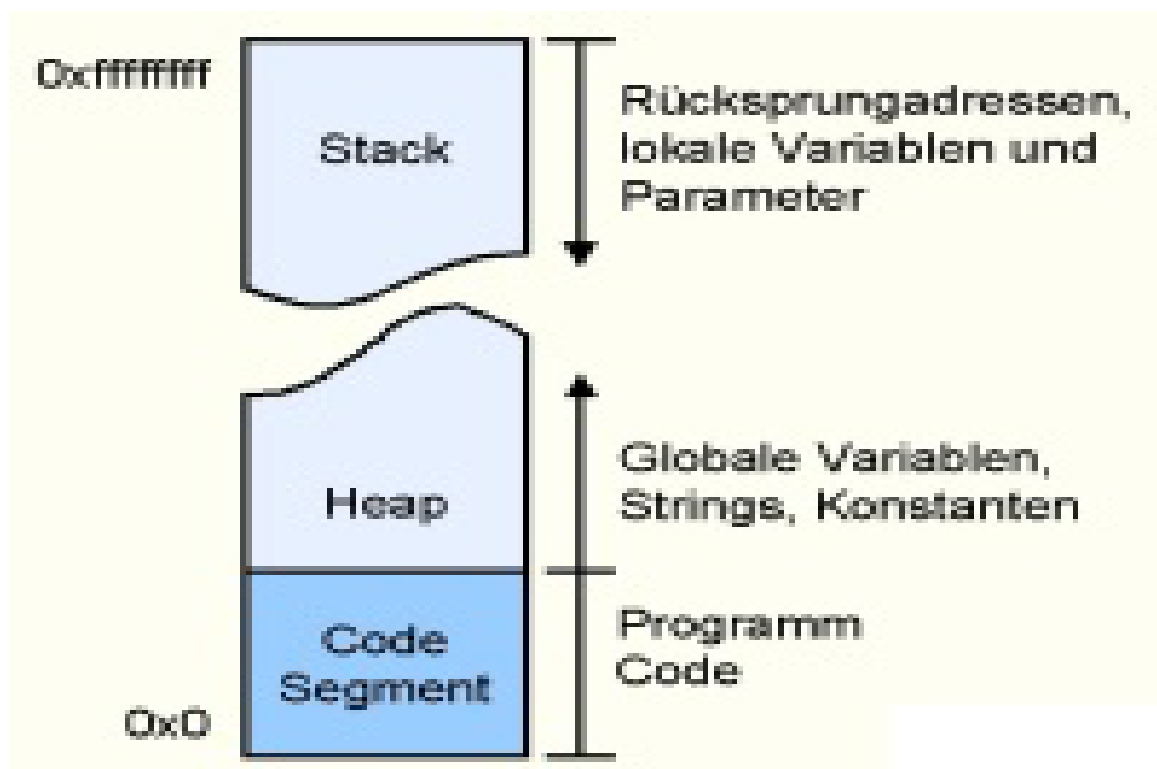
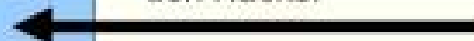
```
"\xff\xff/bin/bash.....";
```

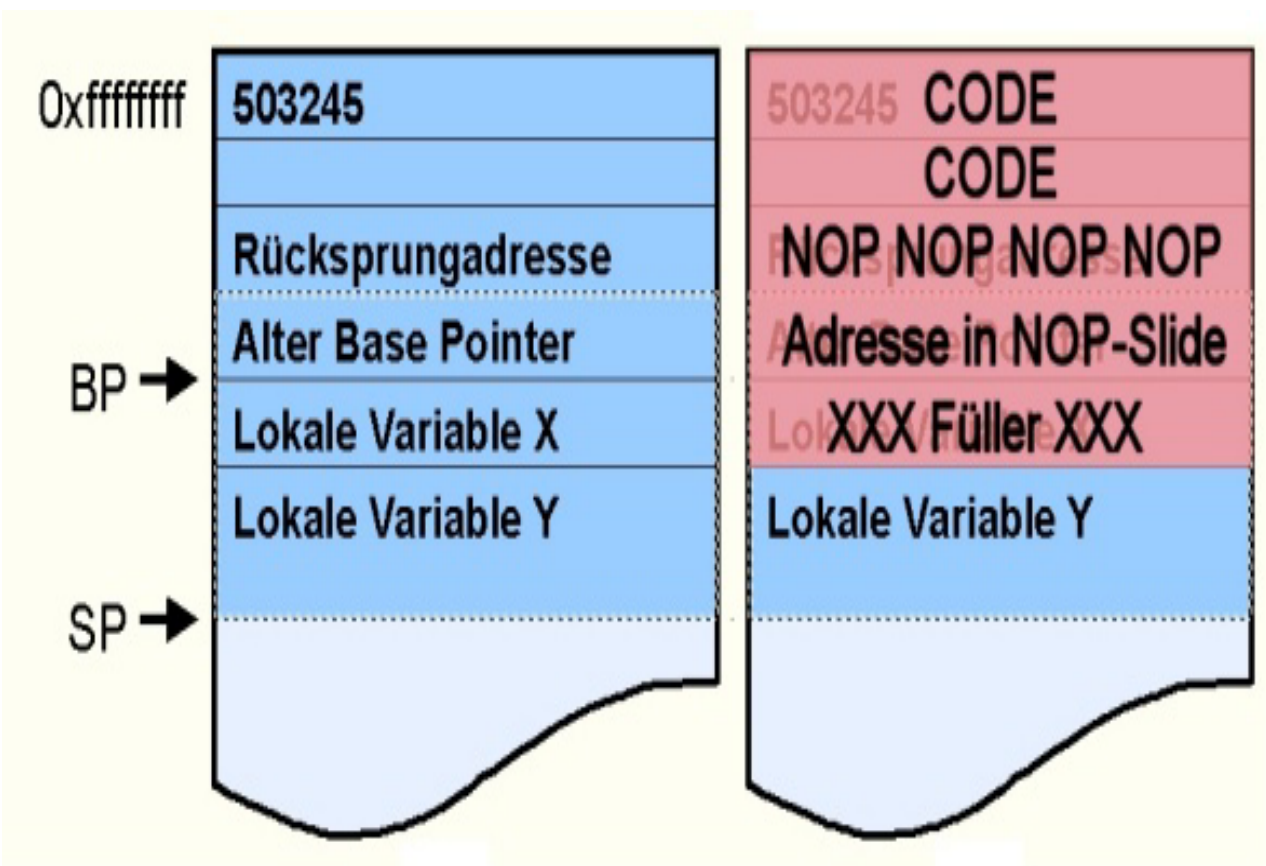
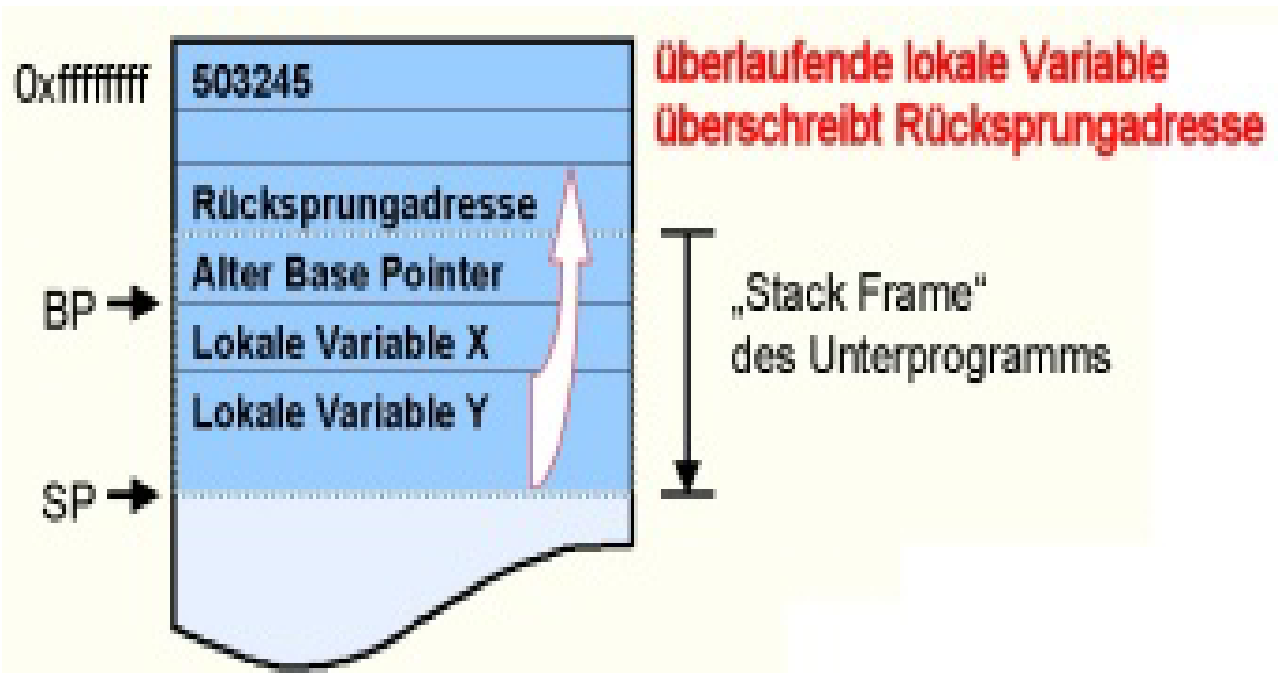
- Damit hat der Hacker Zugriff auf alle Funktionen des Betriebssystems.

```
cmd = lese_aus_netz();
do_something (cmd);

int do_something(char *string){
    char buffer[4];
    strcpy(buffer,string);
    ....
    return 0;
}
```

Dieser harmlose Befehl
ist der Einstiegspunkt für
den Hacker





(http://www.kes.info/_archiv/_onlinearch/01-05-6-overflow.htm)

Literaturverzeichnis

<http://www.netzmafia.de/skripten/sicherheit/index.html>

<http://www.heise.de/ct/01/23/216/>

<http://www.theo2.physik.uni-stuttgart.de/jtb/overflow/tutorial.html>

<http://www.gocsi.com/press/20020407.html>

<http://www-krypt.cs.uni-sb.de>

http://www.kes.info/_archiv/_onlinearch/01-05-6-overflow.htm

Secrets & Lies.(IT-Sicherheit in einer vernetzten Welt) [Bruce Schneier]

Computersicherheit [Georg Erwin Thaller]

Hacker's Guide .(Sicherheit im Internet und im lokalen Netz) [Anonymous]

Linux Hacker's Guide .(Sicherheit für Linux-Server und -Netze) [Anonymous]

Seminar Bericht 224. (Sicherheit in vernetzten Systemen. Uni-HH)
[Herausgeber: Hans-Joachim Mück, Carsten Benecke, Stefan Kelm]