1 Angriffspunkte

- Programme, die mit erweiterten Rechten ausgeführt werden müssen (**passwd**, **su**, ...) verwenden den S-Bit Mechanismus
- Programmierfehler in diesen Programmen
  - unkontrollierte Dateizugriffe
    z.B. Öffnen einer Datei **/tmp/<PID>** um zu schreiben
  - buffer overflow

```
...
char username[9];
char buffer[256];
...
strcpy(username, argv[1]);
...
gets(buffer);
...
sprintf(buffer, "%s", argv[1]);
```


Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.

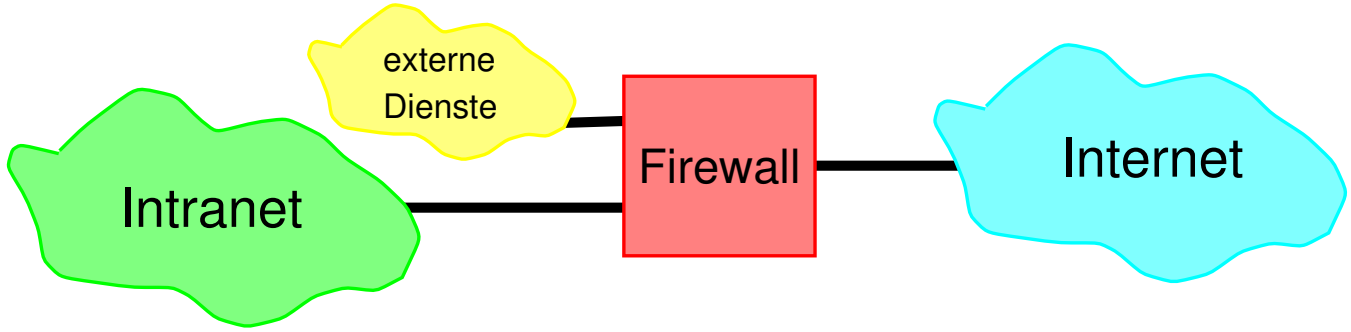
H.4 Netzdienste unter UNIX

- Datentransfer- / Kontrolltransferdienste rlogin, rsh, telnet, ftp
  - ◆ Authentisierung mit Klartextpaßwort
  - ◆ Angriffsmöglichkeiten:
    - Paßwörter sammeln durch Abhören des Netzverkehrs
    - Übernahme von Verbindungen
- Datentransfer- / Mitteildienste E-Mail, WWW
  - ◆ Keine Authentisierung
  - ◆ Absender kann beliebig angegeben werden, Mails können modifiziert werden.

Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.

H.6 Firewalls

- Mit einer Firewall werden vertrauenswürdige und nicht vertrauenswürdige Netzwerksegmente getrennt.

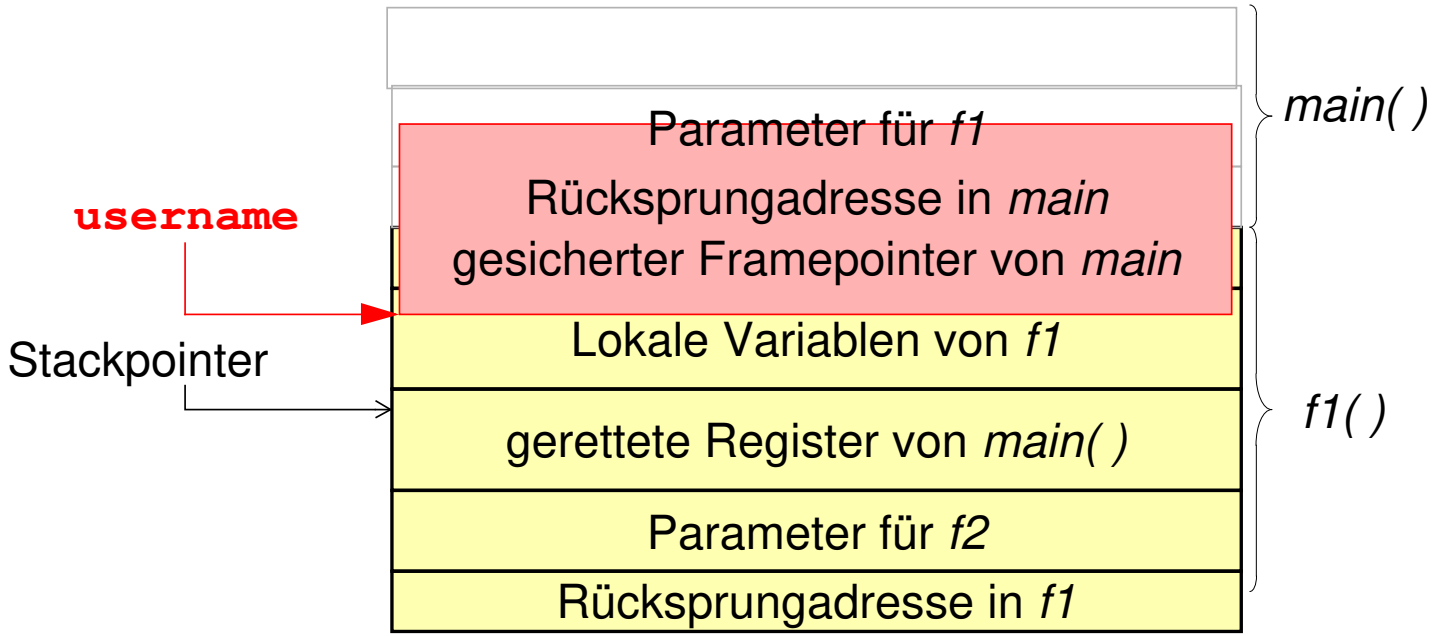


- Firewall-Funktionalität:
  - ◆ Intelligenter Router (erlaubt nur gewisse Dienste)
  - ◆ Paket-Filter: filtert "defekte" Pakete / SYN-Attacken
  - ◆ Gateway:
    - WWW-Inhalt filtern
    - Adressen umsetzen
  - ◆ Sicheres Tunneln: z.B. mit "virtual private network"

Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.

2 Vorgehensweise

- Zugriff auf das System über beliebigen Account
  (z.B. Paßwort mit crack geraten)
- Auslösen eines buffer overflow



- Erlangung von Systemverwalterprivilegien

Reproduktion jeder Art oder Verwendung dieser Unterlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, bedarf der Zustimmung des Autors.