I Sicherheit in heutigen Betriebssystemen

I.1 Überblick

- UNIX-Sicherheitsmechanismen
- Angriffsmöglichkeiten
- Netzdienste unter UNIX
- Verschlüsselungsverfahren
- Firewalls

I.2 UNIX-Sicherheitsmechanismen

- Authentisierung durch private Paßwörter
- Paßwörter werden verschlüsselt gespeichert:
  /etc/passwd, NIS (Network Information Service)
- Verschlüsselungsalgorithmus DES:
  - Digital Encryption Standard von IBM,
    1977 standardisiert, 56 Bit Schlüssellänge
  - gilt als dekodierbar
- Problem:
  - Verschlüsselte Paßwörter sind öffentlich zugänglich
  - Wörterbuchattacken möglich (crack)

I.2 UNIX-Sicherheitsmechanismen (2)

- Lösungsansatz:
  - Verschlüsselte Paßwörter werden in Shadow-Dateien gespeichert (**/etc/shadow**), die nur mit Systemverwalterprivilegien lesbar sind
  - Problem: alle Programme, die Paßwörter überprüfen (z.B. **xlock**), müssen Systemverwalterprivilegien erhalten
- Weitergehende Lösungen:
  - Verwendung verbesserter Authentisierungsverfahren:
    - Kerberos (am MIT entwickeltes Sicherheitssystem)
    - DCE (Distributed Computing Environment)
  - Integration dieser Authentisierungsverfahren in bestehende Betriebssystemdienste z.B. durch PAM (Pluggable Authentication Modules)

I.3 Angriffe auf UNIX-Systeme

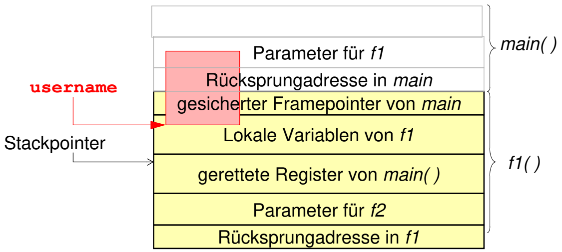
1 Angriffspunkte

- 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]);
```

2 Vorgehensweise

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



- Erlangung von Systemverwalterprivilegien

3 Gegenmaßnahmen

- Kapselung der sicherheitskritischen Abschnitte
  (TCB: Trusted Computing Base)
- Verwendung der zusätzlichen Privilegien nur in den TCBs
  (hilft nicht gegen buffer overflow Probleme)

```
...
seteuid(0);
fd = open("/etc/passwd", O_RDWR);
seteuid(getuid());
...
```

- Sorgfältige Programmierung

```
...
strncpy(username, argv[1], 8); username[8] = 0;
...
fgets(buf1, sizeof(buf1), stdin);
...
snprintf(buf2, sizeof(buf2), "%s", argv[1]);
...
```


4 Risikoabschätzung

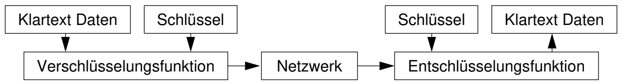
- Bekannte Sicherheitslücken verbreiten sich sehr schnell!!!
  - bugtraq-Mailingliste
  - `http://www.rootshell.com/`
  - `http://www.dhp.com/~fyodor/`
  - IRC (Internet Relay Chat)
- Alle schlecht gewarteten Systeme im Internet sind angreifbar
  (Auch Heimrechner, die über PPP angebunden sind!!!)
  - Beispiel Linux:
    - In Standard-Distributionen sind oft 20-30 Dienste eingeschaltet.
    - Bereits wenige Wochen nach Erscheinen werden Sicherheitslücken bekannt.

I.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.

I.5 Verschlüsselungsverfahren

- Verschlüsselung über Netzwerk allgemein:



- Symmetrische Verfahren (DES, IDEA, ...):
  - ◆ Verschlüsselung und Entschlüsselung mit dem gleichen Schlüssel
- Asymmetrische Verfahren (RSA, El Gamal, Diffie/Hellman):
  - ◆ Verschlüsselung und Entschlüsselung mit unterschiedlichem Schlüssel
  - ◆ ein Schlüssel läßt sich nicht aus dem jeweils anderen berechnen
  - ◆ Idee:
    - Verbreitung eines Schlüssels ("öffentlicher Schlüssel")
    - Geheimhaltung des anderen Schlüssels ("privater Schlüssel")
    - → Alle können Daten verschlüsseln, die man nur selbst entschlüsseln kann

1 Anwendung von Verschlüsselung

- Mail, WWW:
  - ◆ Signieren und Verschlüsseln von Mail und WWW-Seiten
  - ◆ Dazu nötig: öffentlicher Schlüssel des Kommunikationspartners
  - ◆ Beispiele: Mail: PGP, S/MIME (Netscape)
    WWW: TLS (Transport Level Security, vormals SSL)
- Datentransfer- / Kontrolltransferdienste ssh, scp, slogin
  - ◆ Verschlüsseln bei Verbindungsaufnahme und Verschlüsselung der Daten
  - ◆ Jeder Rechner besitzt einen öffentlichen Schlüssel
  - ◆ Problem: Die öffentlichen Schlüssel müssen verteilt werden
  - ◆ Bei **slogin/ssh/scp** bin ich sicher, daß keiner mithört und daß ich auch genau mit dem Rechner verbunden bin, den ich angebe

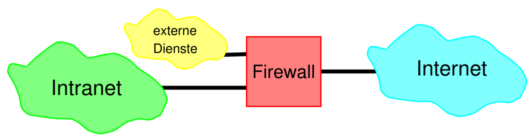
```
usa> slogin faui01a.informatik.uni-erlangen.de
Password: xxx                # nur die faui01a bekommt das
Paßwort
faui01a>                     #
```


2 IP Security

- Eigenständiges Sicherheitskonzept für IP
- sichert Integrität, Authentizität und / oder Vertraulichkeit zu
- Protokolldefinition unabhängig von den verwendeten Verschlüsselungsverfahren (z.B. MD5, 3DES)
- Kernprotokoll:
  - ◆ AH: Authentication Header
    Integrität, Authentizität, Sicherheit vor Wiederholungen (replay)
  - ◆ ESP: Encapsulating Security Payload Header
    zusätzlich zu AH: Vertraulichkeit
- Header können getrennt oder gemeinsam verwendet werden
- Zusatzprotokolle für Schlüsselaustausch (IKE),
  Definition von öffentlichen Schlüsseln und Zertifikaten (SPKI) und
  Namensauflösung (DNSsec)

I.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"