Unix für Insider

Security Tools für Unix

Mirko Dziadzka
dziadzka@ai-lab.fh-furtwangen.de

Inhalt

- Motivation
- Kryptographische Grundlagen
- Welche Tools gibt es unter Unix ?
  - CFS
  - ssh
  - PGP
- Ausblick

Was wollen wir schützen ?

- Daten auf der Festplatte
- Daten während des Transports
  - E-Mail
  - Passwörter beim Login
  - Kreditkarteninformationen beim Einkaufen im Internet
- stattfinden der Kommunikation

Kryptographische Grundlagen

- symmetrische Verschlüsselung / private Key Verfahren
- unsymmetrische Verschlüsselung / public Key Verfahren
- kryptographische Hashfunktion

Symmetrische Verschlüsselung

- Zum Verschlüsseln und Entschlüsseln wird ein und derselbe Key benutzt
- Relativ schnelle Verfahren (10 Mbit/s)
- Beispiele:
  - DES, 3DES
  - IDEA
  - RC5

Unsymmetrische Verfahren

- zwei Keys, einen zum Verschlüsseln, einen zum Entschlüsseln
- Relativ langsam, nicht für große Datenmengen geeignet
- Beispiele:
  - RSA
  - DSS

Kryptographische Hashfunktion

- Hashfunktion: bildet einen Text auf wenige Zeichen ab
- kryptographisch: nicht invertierbar, keine Kollisionen erzeugbar
- Beispiele:
  - MD2
  - MD4
  - SHA

Einmal-Passwörter

- Bei einem normalen telnet oder rlogin gehen Passwörter im Klartext über das Netz. Wenn man das nicht verhindern kann, darf jedes Passwort nur einmal gültig sein.
- Beispiele:
  - S/Key unter Unix und im Firewall-Bereich
  - PIN + TAN beim Homebanking

Sichere Verbindungen

- Verschlüsselung der gesamten Verbindung
- Authentifizierung des Servers
- Authentifizierung des Clients
- Beispiel:
  - ssh + slogin + scp
  - SSL (Netscape)

E-Mail

- Schutz vor unberechtigtem mitlesen
- Authentifizierung des Absenders
- Beispiel:
  - PGP: Pretty Good Privacy
  - PEM: Privacy Enhanced Mail

Pretty Good Privacy

- Ursprünglich von Phil Zimmermann geschrieben
- Jetzt vom PGP Inc. weiterentwickelt (http://www.pgp.com)
- Aktuelle Versionen
  - PGP 2.6.3i
  - PGP 5 / PGP 5.5

Verschlüsselte Filesysteme (1)

- CFS (Cyptographic File System)
  - Verschlüsselt einzelne Verzeichnisbaüme transparent
  - jedes Unix
  - 3DES

Verschlüsselte Filesysteme (2)

- LOOPCRYPT
  - Verschlüsselt eine ganze Platte
  - verschiedene Versionen für Linux-Kernel
  - triviale Implementation für DOS
  - diverse Shareware für WIN

Anonymität

- Anonyme E-Mail senden
  - Mixmaster
  - Anon-Server
- E-Mail anonym empfangen
- Anonymes WWW/UseNet surfen

Zukünftige Entwicklung

- IPv6 / IPSec
- Mixmaster für HTTP und NNTP
- Onion-Routers

Weitere Informationen

- news:fhf.ufi
- PGP Dokumentation
- Cryptography-FAQ