8 Verschlüsselnde Dateisysteme — eCryptfs

- In Linux ab Version 2.6.19
- Ähnliche Struktur wie EFS
  - ➤ mehrbenutzerfähig
  - ➤ zufälliger FEK wird mit Public Key verschlüsselt und in Metadaten der Datei abgelegt
- Schlüsselverwaltung über *user session key ring* im Kern oder über user-level Prozess *ecryptfsd*

9 Generelles Problem partieller Verschlüsselung

- Partielle Verschlüsselung schützt bei Verlust des Mediums oder des Rechners
- sie schützt nur teilweise bei Angriffen auf das laufende System
  - ➤ während der Datenbearbeitung existieren - zumindest temporär - immer undichte Stellen

➥ nur in Kombination mit absolut dichtem Zugriffsrechtekonzept wirkungsvoll

▲ ABER: zwei große Schwachstellen:

- ◆ Administrator (Super-User)
  - ➤ hat Zugriff auf Speicher und unverschlüsselte Partitionen
- ◆ das Betriebssystem selbst
  - ➤ was tut eigentlich das Betriebssystem?
  - ➤ so lange das Betriebssystem selbst nicht verschlüsselt (oder signiert) wird, ist es immer angreifbar

9 Generelles Problem partieller Verschlüsselung (2)

? wie sicher sind Daten und Programme auf einem Notebook
- ➤ in einem Hotel-Zimmer
- ➤ im Büro
- ➤ in aufgegebenem Gepäck
- ➤ in einem Schließfach am Bahnhof
- ➤ in einem geparkten Auto

? welches Betriebssystem läuft eigentlich auf dem Rechner (danach!)?

? welchen Wert hat jetzt die Verschlüsselung von Dateien oder Partitionen?

➥ so lange man das Gerät nicht immer im Blick hat, kann man nicht sicher sein, was mit ihm passiert ist!

9 Generelles Problem partieller Verschlüsselung (3)

➥ Lösung

■ Verschlüsselung aller Partitionen
inklusive der Root-Partition und der Swap-Bereiche
- ➤ normales Booten nicht mehr möglich

■ Booten von sicherem Medium
- ➤ USB-Stick
- ➤ CD

◆ Eingabe des Root-Dateisystemschlüssels in der frühen Boot-Phase

▲ ABER: auch solch ein System ist angreifbar, wenn es läuft!
- ➤ Netzwerkzugriffe
- ➤ unverschlüsselte NFS-Dateisysteme
- ➤ Schwachstellen in Programmen