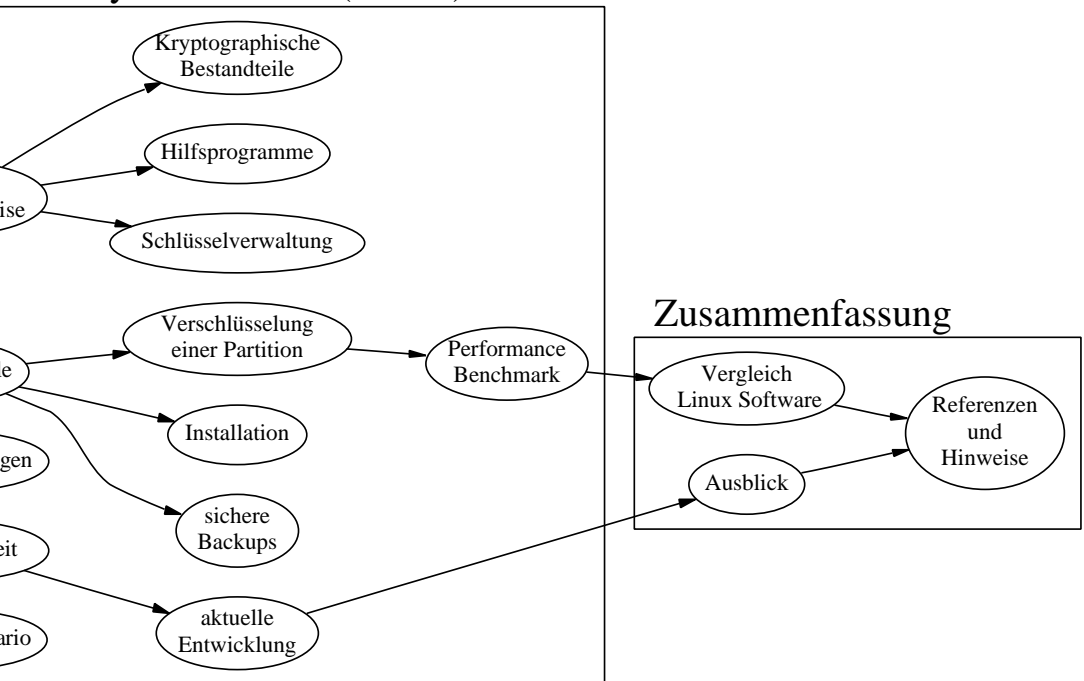


Verständnis der Verschlüsselung mit Linux

mai97ixb@informatik.uni-leipzig.de>

mai97ixb@informatik.uni-leipzig.de/~mai97ixb

Privacy Disk Driver (PPDD)



ng (für Datenträger)?

chlüsseln?

insbesondere: leicht entwendbarer) Datenträger,
(B. Laptop)

ulichen Daten (vgl. auch gesetzliche Vorschrift-
verpflichtungen)

chlüsseln?

(Einfachheit für den Benutzer)

alle Daten werden gleich behandelt; unabhängig
ätzung des Benutzers)

erschlüsselung von Datenträgern

n (Blaze, 1993)

:

x, BSD Kernel Patch)

sk Driver (Latham, 1998, ab Linux 2.0.35, [2.4.x])

tem (Ludwig, 2000, ab Linux 2.2.x, [2.4.x])

, Shender, 1998)

al., van Schaik et al., Kuhn et al., 1999)

hic File System (Cattaneo, Persiano, 1997)

Lösungen

ok zum eigenen CFSd); gute UNIX-Portabilität

off auf verschlüsselte Dateien (NFS Backend: Name/Größe/Lage nicht → Known-Plaintext-Angriff)

Netzwerkbetrieb (NFS) → Klartext versendet, da Ver-
füg

da viele Kernel/User Space Transfers

(Geschwindigkeit): DES (-/+), 3DES(+/-), SAFER-
in (-/+), aber Blowfish-Patch (+/+)

sroutinen im Kernel (als VFS), aber TCFS IO-
ultat: bessere Performance)

seitig, kein Klartext mehr im Netzwerkbetrieb

) Schlüsselverwaltung (Login-Passwort)

ische Dateisysteme

Sicherheitsl cher

rtet (nur 2.0.x, 2.2.10)

hrfach) in freien Datentr gerbl cken versteckt
(system)

bestreitbar; zus tzlich Verschl sselung m glich

LOOP-Ger t basierte L sungen

Schl sselteilung, Authentifizierungsmodule); **aber:**
kritischen Anwendungen eingesetzt zu werden

n basierend auf dem LOOP-Ger t → sogenann-
linux-Kern als Patch verf gbar

ck

schlüsselte Dateisysteme erzeugen

dem Gerätetreiber (in Form eines Kernelpatches)

`sys-group.com`>

0.3) konsequent verbessert und weiterentwickelt

chlüsselungstechnologie (Blowfish, Whitening-Verfahren)

bedienen

“ (GPL)

unberechtigtem Zugriff auf die Daten eines Speichermediums bei ausgeschaltetem Rechner.

Backups.

Backups.

Computer mit einer Floppy zu booten und den Speicher zu kopieren.

gegen folgenden Angriffen:

in einem Mehr-Benutzer-System bei eingemounteten Speichermedien (z.B. Unix-Zugriffsschutz)

falls verschlüsselte Medien eingemountet wurden.

oder im Netzwerk.

„Das weiße Pferd“.

ert; Blowfish in i386 Assembler implementiert

≥ 2.0.35 oder 2.2.x [z.Z. Adaption für 2.4.x]

für Kernquellen verfügbar

. gcc ab Version 2.7) zum Kompilieren des Li-
sprogramme

ext3, reiserfs) mit folgenden Eigenschaften:

n vom Dateisystem nicht verwendet werden

und/oder entsprechend schutzwürdige Daten

`/linux01.gwdg.de/~alatham`

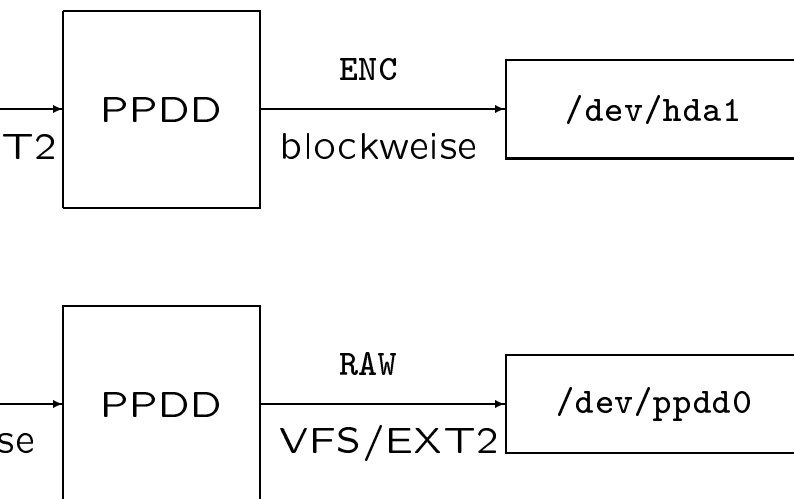
`gwdg.de/pub/linux/misc/ppdd`

r mit dem öffentlichen Schlüssel des Autors!

Funktionsweise des „Gerätetreibers“

Geräteidentifikationsnummer block-major-92

Geräteart: PDD- oder PDDOP-Gerät, benutzt aber keine kryptographische Verschlüsselung; **Funktionsweise (grob):**



Bestandteile

Blowfish

einsetzbar

analytisch untersucht

Architektur

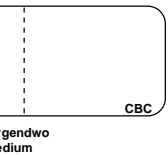
Angabe

der Rohdatenstruktur. Bsp: (Permutation)

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 0 & 0 & 0 & 3 & 3 & 0 \\ 0 & 0 & 7 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

te Merkbarkeit) zur Authentifizierung

-Konzept:



- Master-Phrase nicht ständig verwendet
- Änderung der Working-Phrase leicht möglich (nur der Master-Phrase muß neu verschlüsselt werden)
- Backups enthalten keine verschlüsselte Master-Phrase → komprimierte Working-Phrases haben keinen Zugriff

schlüsselt. 2: CBC-Modus garantiert Änderung
nmodifikation. 3: Datenblock gleichen Inhalts an
Mediums wird jeweils anders verschlüsselt.

ck, überschreibt ggf. freien Speicherplatz mit zufälligen
Blöcke. (zur **Einrichtung**)

ase“ von Tastatur ein), trennt oder zeigt Statusinforma-
benutzung)

schen der Working-Phrase und Ändern der Master-Phrase.

ltreiber und Erstellen verschlüsselter Backups.

ltreiber und Wiedereinspielen verschlüsselter Backups.

ben eines verschlüsselten `root`-Filesystems.

s zwischen verschiedenen Versionen von PPDD.

als Schutz vor böswilliger Veränderung der verschlüsselten
Aufruf von `ppddsetup` überprüft.

ation der Software [nur PPDD 1.x]

prüfen

g anpassen

```
fig  
sk driver support  
ke clean; make bzImage)
```

Wartung einer Partition [nur PPDD 1.x]

Wartung der Master-Phrase

```
dd if=/dev/urandom of=/dev/hda3  
bs=1M count=1 (1 Partition mit Zufallsdaten)
```

(Voraussetzungen beachten!):

```
dd if=/dev/urandom of=/dev/hda3  
bs=1M count=1
```

(a)

t

Kann auch bei normaler Nutzung der Partition ausgeführt.

en sicherer Backups [nur PPDD 1.x]

`w/ppdd0`

angreifen, die durch Spying-Techniken (z.B. versteckte
e Working-Phrase erlangt haben, keinen Zugriff auf die

`s=1k`

`mount /dev/ppdd0 /crypt`

mark mit bonni++ [von PPDD 1.x]

Durchsatz verringert sich auf die Hälfte!

320: Cyrix MII 250 MHz, 320 MB RAM, IDE/UDMA33
Testpartition 2GB/ext2

```
-- --Sequential Input- --Random-
e- -Per Chr- --Block-- --Seeks--
CP K/sec %CP K/sec %CP /sec %CP
29 2133 94 10479 25 7.5 0 (ohne PPDD)
40 1038 84 1943 74 2.7 0 (mit PPDD)
-- -----Random Create-----
-- -Create-- --Read--- -Delete--
CP /sec %CP /sec %CP /sec %CP
99 91 99 399 99 97 35 (ohne PPDD)
97 88 99 394 99 239 89 (mit PPDD)
```

ktion auf die Hälfte (Char), Fünftel (Block)

er: keine Messung im Kernel Space

: 97 sec vs. 239 sec

g

- schwerwiegende Implementierungsänderung

Vielfaches von 4096 (Linux-Bug)

sondern C → architekturunabhängig

en (LOOP-Gerät, Crypto API), sondern

to API]

LOOP-Gerät [loop-jari-2.4.xx.y.patch]

setup(8), mount(8), umount(8)]

2fsprogs

basierend auf [Ludwig00]

	CryptFS	StegFS	FSFS	PPDD
el	kernel	kernel	kernel	kernel
	Datei	Datei	Block	Block
	Verzeichnis	Datei	Partition	Partition
	+	-	++	++
	(ja)	ja	ja	nein
	++	-	-	-
	+	-	+	+
	+	+++	++	+++
	nein	nein	ja	ja

ise

Dateisystemen unter Linux, Diplomarbeit, 2000

isks with Linux, <http://drt.ailis.de/crypto/linux-disk.html>
<http://EncryptionHOWTO.sourceforge.net/>

Latham, November 1999

April 1999

g.de>
/ der eMail

/~alatham/ppdd.html

/~ezk/research/cryptfs/

StegFS/

/