Daten sicher löschen

— Zuverlässige und unumkehrbare Datenvernichtung —

Stefan Schumacher

www.net-tex.de
stefan@net-tex.de
PGP:0xB3FBAE33

Chemnitzer Linux-Tage 2007

Id: daten-sicher-loeschen-folien.tex,v 1.16 2007/02/24 11:43:32 stefan Exp



Inhaltsverzeichnis

1. Motivation
2. Speicherverfahren
3. Löschen durch Überschreiben
4. Programme
5. Zerstörende Verfahren
6. Vorbeugung und Organisatorisches

Literatur

- `www.net-tex.de/netbsd/daten-sicher-loeschen.html` Aufsatz zum Vortrag, inkl. kompletter Bibliographie
- Konferenz der Datenschutzbeauftragten des Bundes und der Länder: *Sicheres Löschen magnetischer Datenträger*
- Gutmann, Peter: *Secure Deletion of Data from Magnetic and Solid-State Memory*
- Messmer, Hans P.: *Das PC-Hardware-Buch*
- Schumacher, Stefan: *Einführung in kryptographische Methoden*
- Schumacher, Stefan: *Methoden zur Datensicherung*
- Schumacher, Stefan: *Verschlüsselte Dateisysteme für NetBSD*



Motivation

- Normale Löschvorgänge (rm(1)) löschen Daten nicht wirklich sondern dereferenzieren nur Einträge im Dateisystem
- Daten sind noch da
- können rekonstruiert werden (Software oder spezielle Geräte)
- müssen sicher gelöscht werden
- erfordert spezielle Verfahren

Dateisystem

- verwenden Blöcke in die Dateien verteilt werden
- haben Index um Blöcke den Dateien zuzuordnen (Inode == Index Node)
- Löschen der Datei löscht Indexeinträge
- Block wird eventuell irgendwann überschrieben
- Block muss nicht voll belegt sein $\rightsquigarrow$ *File Slacks*

Speicherverfahren magnetischer Datenträger

- magnetische Partikel werden ausgerichtet
- repräsentieren physikalisch die logische Bitfolge über Flußwechsel
- verschiedene Codierungsverfahren (RLL, FM, MFM, neue proprietäre)

Speicherverfahren magnetischer Datenträger

- Remanenz: zurückbleibende Aurichtung der Elemtarmagnete nach Abschalten des äußeren Magnetfeldes
- Koerzitiv-Feldstärke: Feldstärke des äußeren Magnetfeldes um Remanenz zu überwinden
- Hystereseschleife: Diagram, an dem Remanenz und Koerzitivfeldstärke abgelesen werden können
- Curie-Temperatur: Temperatur bei der ferromagnetische Stoffe ihre magnetischen Eigenschaften verlieren.

Speicherverfahren optischer Datenträger

- Laser tastet Trägerschicht ab
- speichern Daten optisch als Vertiefung
- Übergänge repräsentieren Bitfolge
- empfindliche Trägerschicht
- untere und obere Schutzschicht

Speicherverfahren von Flash-EEPROMs

- verwenden Feldeffekt-Transistoren (FETs)
- Floating Gate zwischen Source und Drain wird gesperrt oder geöffnet $\rightsquigarrow$ Bitfolge
- haben keinerlei Remanenz oder ähnliches
- aber begrenzte Anzahl an Löschzyklen (100.000 – 1.000.000)

Löschen durch Überschreiben

- Daten in Blöcken werden nicht gelöscht
- Idee: Daten mit Müll überschreiben

Probleme:

- Remanenz, Nebenspuren
- defekte Sektoren
- Dateisysteme (File Slack, dynamische Blockanpassung, Caches)
- Caches (Schreibcache deaktivieren, sonst wird der Cache überschrieben)
- Betriebssysteme (Swap, Temp)
- unbekannte Kopien (z.B. /var/tmp/vi.recover/)

Standards für Überschreibe-Verfahren

einfaches Überschreiben mit Nullen oder Einsen

- schützt nur vor Software
- Muster der alten Daten werden nicht verwischt (Remanenz)
- unsicher

Richtlinie zum Geheimschutz von Verschlussachen beim Einsatz von Informationstechnik

- Sieben Durchläufe: $0xFF, 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xAA$
- Muster der alten Daten werden etwas verwischt
- unsicher



Standards für Überschreibe-Verfahren

US Department of Defense

US DoD 5220.22-M (E)

- Drei Durchläufe: $0xFF, 0x00, Zufallsdaten$
- unsicher

US DoD 5220.22-M (ECE)

- Sieben Durchläufe:
  $0xFF, 0x00, Zufallsdaten, Zufallsdaten, 0xFF, 0x00, Zufallsdaten,$
- mittelmäßig sicher, erfordert hohen Laboraufwand

Standards für Überschreibe-Verfahren

Peter Gutmann, 1996

- gute Idee, die spezifische Bitmuster verwendet
- Analyse der Speicherverfahren ((1,7)RLL, (2,7)RLL und MFM)
- 27 Läufe mit speziellen Bitmustern für (1,7)RLL, (2,7)RLL und MFM
- 4x Zufallsdaten am Anfang und Ende $\rightsquigarrow$ 35 Durchläufe
- sehr sicher auf (1,7)RLL, (2,7)RLL und MFM-Medien
- aber heute kaum mehr praktikabel, da Speicherverfahren unbekannt

Standards für Überschreibe-Verfahren

R. Pfitzner

R. Pfitzner, Brandenburgischer Datenschützer

- andere Idee als Gutmann:
  statt Bitmustern Wahrscheinlichkeitstheorie
- Wie oft muß ich Zufallsdaten schreiben, damit jedes Bit mit 99%-iger Wahrscheinlichkeit zweimal fällt?
- 33-mal damit jedes Bit zweimal fällt
- 7-mal damit jedes Bit einmal fällt
- sehr sicheres Verfahren, erfordert sehr hohen Laboraufwand

Wann einsetzen?

- prinzipielle Probleme (File Slacks, Remanenz, Nebenspuren ...)
- Swap, /tmp, Sicherungskopien beachten (verschlüsseln)
- Nur verwenden, wenn Datenträger unter Kontrolle bleibt
- Nicht ausreichend bei Herausgabe des Mediums
- Dann: Pfitzner-Verfahren auf Raw-Gerät

rm(1)

- `rm -P` Überschreibt Dateien vor dem Löschen
- Drei Durchläufe: $0xFF, 0x00, \textit{Zufallsdaten}$
- unsicher

wipe(1)

- von Tom Vier, `http://wipe.sf.net/`
- Unmengen verschiedener Optionen
- überschreibt mit Zufallsdaten oder definierten Bytes
- sehr schneller Pseudozufallsgenerator, kann Daten an STDOUT schicken

```
wipe -x 2 -p 4 -v /foo/
```

2x Zufallsdaten, 4 Durchläufe, Fortschrittsanzeige

dd(1)

arbeitet auch auf Raw-Geräten, unterhalb des Dateisystems

```
dd if=/dev/urandom of=/dev/wd1d bs=2m
```

schreibt Zufallsdaten in die 2. IDE-Platte, langsam

```
wipe -T -x 1 -o 2097152 -a | dd of=/dev/wd1d bs=2m
```

benutzt wipe als PRNG, wesentlich schneller

```
wipe -T -x 1 -o 2097152 > /tmp/wipe.datei ;
buffer -i /tmp/wipe.datei -o /dev/nrst0
```

Buffer schreibt zwischengepuffert auf Magnetbänder



cdrecord(1)

löscht und brennt CDs/DVDs

```
cdrecord -dev=15,1,5 -blank=all
```

CD komplett löschen (dauert)

NetBSD/Schrubber

www.net-tex.de/netbsd/daten-sicher-loeschen.html

- abgespecktes NetBSD/i386 3.1 auf Live-CD (97MB)
- mit Wipe und Buffer
- wipe-33.sh überschreibt Partitionen 33-mal mit wipe(1) und dd(1)

```
export DURCHLAEUFE=50
./wipe-33.sh sd0d sd1d wd0d wd1d
```

überschreibt SCSI- und IDE-Platten 50-mal mit Wipe



Zerstörende Verfahren für magnetische Datenträger

Curie-Temperatur

- spezifische Temperatur, bei der ferro-magnetische Stoffe ihre magnetischen Eigenschaften verlieren
- $> 900C \rightsquigarrow$ Hochofen o.ä.
- T_C muß *überall* einwirken
- definitiv sicher

Zerstörende Verfahren für magnetische Datenträger

Degaußer

- starkes Magnetfeld das Hystereseschleife mehrfach durchläuft
- benötigt ca. 1 Tesla
  (Erdmagnetfeld: $50\mu T$, stärkster europäischer Kernspintomograph in Magdeburg hat 7T)
- Magnetfeld muß überall einwirken
- definitiv sicher
- kann man Mieten, vorher Überschreiben sinnvoll

Zerstörende Verfahren für magnetische Datenträger



Abbildung: Degaußer 2 von Ibas (Quelle: www.ibas.de)

Zerspanen

- Späne von Häckslern können rekonstruiert werden (Puzzlespiel, auch automatisierbar)
- sehr kleine Späne erforderlich, ca $1mm * 1mm$
- abschleifen mit Winkelschleifer oder auf Drehbank
- vorher Degaußer und Überschreiben sinnvoll
- Schutzkleidung! (Schutzbrille, Handschuhe)

CDs/DVDs

- Trägerschicht muß vernichtet werden
- abschleifen oder verätzen der oberen Schutzschicht
- untere Schutzschicht zu zerkratzen ist sinnlos
- Mikrowelle erzeugt giftige Dämpfe und Brandgefahr

Organisatorisches

Schutzstufen und Löschverfahren festlegen

- **SS0:** keine Schutzwürdigkeit (öffentliche Daten)
  1-mal Zufallsdaten
- **SS1:** sensible Daten geringer Schutzwürdigkeit
  7-mal Zufallsdaten
- **SS2:** Personendaten, geheime Geschäftsdaten (internes ReWe)
  33-mal Zufallsdaten
- **SS3:** Betriebsgeheimnisse, Patientendaten, Forschungsdaten
  33-mal Zufallsdaten und definitive physikalische Vernichtung



Vorbeugung

- Datensparsamkeit – Was ich nie gespeichert habe, muß ich nicht löschen
- verschlüsselnde Dateisysteme (auch für Swap und Temp)
- Medienwahl berücksichtigen (Sicherung auf DVD statt Band)
- verschiedene Sicherungskreise (Buchhaltung ./. Personalakten)
- auch Sicherungen verschlüsseln
  `dump -0a -f - /home | mcrypt > Sicherung.nc`
- markieren Sie Medien mit sensiblen Daten eindeutig
- Geben Sie Datenträger nicht aus der Hand (Giftschrank)
- Medienbrüche beachten (Ausdrucke etc.)

Ende

Fragen?

Kontakt: www.net-TEX.de

stefan@net-TEX.de

NetBSD-Stand im Foyer



Weiteres

Wilhelm Dolle: Computer-Forensik in der Praxis

Sonntag, Raum V3, 14:00 Uhr
Unter anderem: Datenrekonstruktion

Stefan Schumacher: Systrace

Sonntag, Raum V3, 12 Uhr
Systrace setzt Richtlinien auf Systemcall-Ebene durch, ermöglicht Sicherheitsrichtlinie auf Kernel-Ebene