

# Digitale Verhütung: **Verschlüsselte Datengräber** Umgebungsmöglichkeiten

towo

Chaos Computer Club Cologne e.V.  
<http://koeln.ccc.de/>

2007-11-29



# Gliederung

- 1 Grundlagen
- 2 Layer-Eight-Probleme
  - Algorithmus
  - Passwort
  - Backups
  - Nutzer
- 3 Technische Umgehung
  - Direkte Angriffe
  - Seitenkanalangriffe
- 4 Abschlußbemerkungen



*„Eine Kette ist nur so stark wie ihr schwächstes Glied“  
(alte Volksweisheit)*



*„Eine Kette ist nur so stark wie ihr schwächstes Glied“  
(alte Volksweisheit)*



## Elementares (1/2)

- Das Erstellen einer sicheren Datenverschlüsselung ist viel Arbeit.
- Im Heimbereich ist es noch überschaubar machbar.
- Auf Firmenniveau wird es schnell zu einer ernsten Herausforderung.



## Elementares (2/2)

Wie bei jeder Verschlüsselung gilt:

- Sie funktioniert nur, wenn konsequent genutzt.
- Sobald sie kompromittiert ist, bleibt sie kompromittiert.



# Einführung

„Layer Eight“: Vergleiche OSI-Schichtenmodell.

- Lücken in sicheren Systemen sind meist reine Nachlässigkeit.
- Selbst behobene Probleme beeinträchtigen die Sicherheit.
- Planungsprobleme fallen erst auf, wenn es zu spät ist.



Im Folgenden werden die trivialen Ansatzpunkte für das Aushebeln der Sicherheit einer Verschlüsselung behandelt.



# Der Algorithmus

- Der Algorithmus ist die technische Methode der Verschlüsselung.
- In allen aktuellen Algorithmen ist zu viel Mathematik für diesen Vortrag.
- A.J. Menezes, P.C. Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, 1996, CBC Press



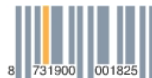
# Fakten

- Die Stärken verschiedener Algorithmen sind nicht gleich.
- Eine gute Wahl des Algorithmus ist wesentlich.
- Häufig werden Kompromisse geschlossen zu Gunsten der Leistung.



# Das Passwort

- Das Passwort ist genauso wichtig wie der Algorithmus.
- Schwache Passwörter machen jedes System nutzlos.
- Der Sinn von schweren Passwörter wird oft nicht verstanden.



# Passwort-Praxis

- Passwort zu einfach, z.B. „12345“, „abcd“ oder der eigene Vorname.
- Passwort wird mit Postit an der Monitor geklebt.
- Gleiches Passwort an verschiedenen Stellen nutzen.
- Probleme bei Passwörtern mit Umlauten und Sonderzeichen.



# Backups

- Sicherung des Inhalts einer Festplatte.
- Oft: Sicherung des **logischen** Inhaltes.
- **Physisches** Backup eher selten.



# Problematik eines Backup

- Natürlich eine wichtige Angelegenheit.
- Das Problem: Backups werden selten verschlüsselt.
- Bei Firmen weniger das Problem, da die Backups im Tapet-Safe landen.
- Heimanwender haben selten Tape-Safes.



# Gefahrenabwehr für Backups

- Große Verbreitungsgefahr insbesondere bei externen Medien.
- Backuplösungen bieten schlechte oder gar keine Verschlüsselung.
- Also muss man manuell nachhelfen.



# Der Nutzer

- Durch zunehmende Stärke wird Verschlüsselung immer sicherer.
- Ein anderes Glied der Kette wird das Schwächste: Der Mensch.
- Je nach „Interessenten“ ist der Weg über den Nutzer einfacher und praktischer.



# Schwachstelle Mensch

Es gibt verschiedene Methoden, über den Nutzer die Verschlüsselung zu brechen:

**Gesetze** Z.B. in UK muss man den Schlüssel hergeben, sonst Haft.

**Betrug** Den Nutzer hinter's Licht führen und von ihm den Schlüssel bekommen.

**Gewalt** "rubber hose cryptanalysis"



# Situation in Deutschland

- Es gibt (noch) keine (explizite) rechtliche Grundlage.
- Vor Gericht eventuell durch Zeugenaussage erzwingbar.  
⇒ Aussage verweigern (§55 StPO)
- Inoffiziell: Schikanierung durch Beamte oder Bürokratie.  
Nachher kann man immer noch „Tschuldigung, war ein Fehler“ sagen.

## § 55 Abs. 1 StPO

Jeder Zeuge kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihm selbst oder einem der in § 52 Abs. 1 bezeichneten Angehörigen die Gefahr zuziehen würde, wegen einer Straftat oder einer Ordnungswidrigkeit verfolgt zu werden.



# Situation in Deutschland

- Es gibt (noch) keine (explizite) rechtliche Grundlage.
- Vor Gericht eventuell durch Zeugenaussage erzwingbar.  
⇒ Aussage verweigern (§55 StPO)
- Inoffiziell: Schikanierung durch Beamte oder Bürokratie.  
Nachher kann man immer noch „Tschuldigung, war ein Fehler“ sagen.

## §55 Abs. 1 StPO

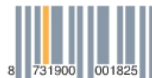
Jeder Zeuge kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihm selbst oder einem der in § 52 Abs. 1 bezeichneten Angehörigen die Gefahr zuziehen würde, wegen einer Straftat oder einer Ordnungswidrigkeit verfolgt zu werden.



Bei den meisten der vorhergehenden Punkte war die Hauptschwachstelle ein konkrete Folge aus dem Versagen des Nutzers.

Vergleiche auch:

<http://ars.userfriendly.org/cartoons/?id=19980506>



# Technische Umgehungsmethoden

Die folgenden Methoden, eine Verschlüsselung zu überwinden, beruhen rein auf den **technischen** Aspekten der Verschlüsselung - **und ihrer Einbettung**.



# Direkte Angriffe

- Bruteforce** Einfach Passwörter durchprobieren, bis es passt.
- Wörterbuch** Mit Begriffen aus einem Wörterbuch den Schlüssel raten.
  - MITM** Dazwischenschleusen eines Agenten (Software, Hardware, Mensch), der sich in die Kommunikation einklinkt.
- Mathematik** Diverse mathematische Methoden der Annäherung an einen Schlüssel (lineare, differentielle Kryptoanalyse).

Alles sehr zeitaufwändig.



# Direkte Angriffe

- Bruteforce** Einfach Passwörter durchprobieren, bis es passt.
- Wörterbuch** Mit Begriffen aus einem Wörterbuch den Schlüssel raten.
  - MITM** Dazwischenschleusen eines Agenten (Software, Hardware, Mensch), der sich in die Kommunikation einklinkt.
- Mathematik** Diverse mathematische Methoden der Annäherung an einen Schlüssel (lineare, differentielle Kryptoanalyse).

Alles sehr zeitaufwändig.



# Seitenkanalangriffe

Seitenkanalangriffe sind Methoden, um über die Einbettung der Verschlüsselung diese zu brechen.

- Trojaner
- Keylogger
- EMSEC/TEMPEST
- Spannungsanalyse
- Datenpersistenz
- ...



# Trojaner

- Inzwischen leidlich bekannt.
- Ermöglichen es, bei laufenden Betrieb Daten auszulesen und zu manipulieren.
- Umgeht daher automatisch Festplattenverschlüsselung.
- Deshalb sehr beliebt beim Innenministerium.



# Trojaner: Evaluation

## Vorteile

- Man kann gezielt Daten auslesen.
- Kann auch autark von Netzverbindungen genutzt werden.
- Falls vorsichtig implementiert schwer zu entdecken.

## Nachteile

- Er muss erstmal eingeschleust werden.
- Je nach Konfiguration und Aufgabenprofil muss er individuell angepasst werden.
- Braucht oft regelmäßige Updates  
⇒ erhöhte Laufkosten.



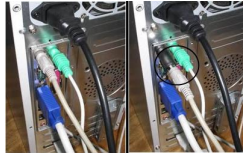
# Keylogger



- Kleine Geräte, die zwischen Tastatur und Rechner gesteckt werden.
- Fallen im Gebrauch absolut nicht auf.
- Sehr leicht zu übersehen.



# Keylogger: Evaluation



## Vorteile

- Leicht zu installieren (physischen Zugriff vorausgesetzt).
- Wird praktisch nie vom Benutzer bemerkt.

## Nachteile

- Braucht physischen Zugriff auf den Rechner.
- Funktioniert nur schlecht bei Notebooks.
- Muss manuell entfernt und ausgelesen werden.



# EMSEC/TEMPEST

## „Emission Security“ - Emissionssicherheit

- Grob vereinfacht: Rechner geben - wie jede andere Elektronik - elektromagnetische Wellen ab.
- Man kann aus der Ferne mitlauschen, was der Rechner gerade macht. („Van-Eck-Phreaking“)
- Ermöglicht zum Beispiel Rekonstruktion des Bildschirminhaltes.
- Hardware lässt sich abschirmen, bzw. abgeschirmt herstellen.



# TEMPEST: Evaluation

## Vorteile

- Man braucht keinen physischen Zugriff auf den Rechner.
- Hardware ist fast nie gesichert (im Privatbereich).  
BSI unterhält eine Liste von sicherer Hardware<sup>1</sup>.
- Es ist nicht direkt nachverfolgbar.

## Nachteile

- Es braucht trotzdem physische Nähe zum Ziel.
- Indirekte Erkennungsgefahr (Kleintransporter vor der Haustür).
- Die Daten müssen aktiv benutzt/dargestellt werden.

---

<sup>1</sup> [http://www.bsi.de/literat/doc/vshardw/TL\\_03305.pdf](http://www.bsi.de/literat/doc/vshardw/TL_03305.pdf)



# Spannungsanalyse

Beispiel für eine stark hardwarebezogene Methode.

- Von der Spannungsaufnahme des Prozessor Rückschlüsse auf durchgeführte Operationen machen.
- Weniger praktisch bei Verschlüsselungen.
- Sehr nützlich beim Analysieren von verdeckten/gesicherten Schaltkreisen.



# Datenpersistenz

- Daten in Speicher gehen nicht direkt verloren, wenn man den Rechner ausschaltet.
- Insbesondere der Auslagerungsspeicher (swap) ist sehr anfällig, denn:
  - 1 Er wird nicht automatisch gelöscht.
  - 2 Er ist nicht flüchtig.
- Es ist also leicht, nach dem Herunterfahren des Rechners noch die Daten auszulesen.

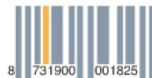


# Restauration von Daten

- Auch nach dem Löschen kann man noch Daten wiederherstellen (für viel Geld).
- Selbst Hauptspeicher (RAM) ist nicht davor sicher, ausgelesen zu werden.<sup>2</sup>
- Angreifer brauchen nur physischen Zugriff und können sich dann am Swap bedienen.
- Da bei einer Hausdurchsuchung auf jeden Fall auch der Rechner mitwandert...

---

<sup>2</sup>[http://www.cs.auckland.ac.nz/~pgut001/pubs/secure\\_del.html](http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html)



# Gefährdung durch persistente Daten

- Im Haupt- sowie Auslagerungsspeicher sind alle Daten unverschlüsselt.
- Es ist möglich, den swap ähnlich Festplatten zu verschlüsseln.
- Hauptspeicher kann aber (mit Ausnahme von Hardwaremitteln) nicht verschlüsselt werden.
- Umgeht also indirekt und unfreiwillig Verschlüsselung.



...

Es existieren noch weite hardwarebasierte Attacken, wie z.B.:

- Timing,
- Berechnungsfehler,
- Thermoanalyse,
- Speicherbedarf,
- Fehleingaben.



# Zusammenfassung der Probleme

- Verschlüsselung ist unbequem.
- Verschlüsselung ist aufwändig.
- Verschlüsselung ist nicht alles, was man beachten muss.



# Konsequenzen

- 1 Sicherheit ist teuer.
- 2 Wer sicher sein will muss **alles** absichern.
- 3 Man kann sich nicht perfekt absichern.



# Fragen?

