# Sicherheit und Opensource

Chaos Computer Club

J. Ohlig — jo@devcon.net
D. R. Tzeck — drt@ailis.de

1999.06.13

**Zusammenfassung**

Es soll gezeigt werden, weshalb ohne Quellenoffenheit nur in den seltensten Fällen ein zufriedenstellendes Maß an Sicherheit erreicht werden kann. Dies ist mit der momentanen Arbeitsweise der meisten Softwarehersteller nicht vereinbar.

Chaos Computer Club Ⓚ all rights reversed

# Was ist der CCC?

Der CCC über sich selbst:

> Der Chaos Computer Club ist eine globale Gemeinschaft, die sich grenzüberschreitend für Informations- sowie Kommunikationsfreiheit ohne Zensur von Staat und Industrie einsetzt, sich mit den Auswirkungen von Technologien auf die Gesellschaft sowie das einzelne Lebewesen beschäftigt.

Weiterführendes unter `http://www.ccc.de`

# Hackerethik

- Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- Alle Informationen müssen frei sein.
- Mißtraue Autoritäten - fördere Dezentralisierung.
- Beurteile einen Hacker nach dem, was er tut und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.
- Man kann mit einem Computer Kunst und Schönheit schaffen.
- Computer können dein Leben zum Besseren verändern.
- Mülle nicht in den Daten anderer Leute.
- Öffentliche Daten nützen, private Daten schützen.

# Überblick

- Der Begriff der Sicherheit, Bedrohungsszenarien.
- Das Zusammenspiel von Sicherheit und Vertrauen.
- Offene und geschlossene Sicherheitsmodelle.
- Anwendungsbereiche beider Modelle.
- Probleme geschlossener und stärken offener Sicherheitsmodelle.

# Was wird unter Sicherheit verstanden?

**Bestand** — das zu schützende Objekt wird nicht zerstört.

**Zugriffsmöglichkeit** — das zu schützende Objekt wird nicht meinen Zugriff entzogen.

**Integrität** — Das zu schützende Objekt wird nicht verändert.

**Authentizität** — Der Aussteller ist festzustellen.

**Geheimhaltung** — Das zu schützende Objekt unterliegt nur dem Zugriff berechtigter Personen.

# Wer bedroht Sicherheit?

**Konkurrenten** Um mir zu schaden, oder sich selber Vorteile zu verschaffen.

**„Die Öffentlichkeit“** Menschen, die denken, sie hätten ein Recht, privates ans Licht der Öffentlichkeit zu zerren.

**Staaten** Versuchen, sich selber oder ihrer eigenen Wirtschaft Vorteile zu verschaffen oder streben eine orwellsche Überwachung der Bürger an.

**Informationshändler** Versorgen die ersten drei Gruppen mit Informationen.

**Vandalen** Stören die Sicherheit um Schaden anzurichten. Entweder „Feinde“ oder Menschen, die aus purer Lust am Zerstören handeln. Manchmal werden politische Motive vorgeschoben.

# Wodurch wird Sicherheit Bedroht?

- Unsicherheiten beim Hersteller
  - In der Designphase
    Unsicheres Design durch
    - Naivität
    - mangelnde Überprüfung
    - absichtliche Schwächung
    - Backdoors
  - In der Produktionsphase
    Unsicheres Produkt durch
    - Herstellungsfehler
    - mangelnde Überwachung der Herstellung
- Unsicherheiten bei der Benutzung
  - mangelnde Kenntnis von Sicherheitsbezügen
  - mangelnde Kenntnis der Bedienung
  - Gedankenlosigkeit

# Sicherheit und Vertrauen

- Eine vollständige Überprüfung aller Komponenten ist unmöglich.
- Andere Vertrauenssubjekte müssen zur Überprüfung herangezogen werden, entweder nachträglich oder bei der Produkterstellung.
- Es ist notwendig auf den Schutz der eigenen Sicherheit durch andere zu Vertrauen.

# Auswahl von Vertrauenssubjekten

- Welches Interesse hat das Vertrauenssubjekt an meiner Sicherheit?
- Welches Interesse hat das Vertrauenssubjekt an der Durchbrechung meiner Sicherheit?
- Wer kann inwiefern Druck auf das Vertrauenssubjekt ausüben?

# Vertrauensmodelle

- Beschränkung des Kreises der Vertrauenssubjekte auf möglichst wenige Personen.

  $\longrightarrow$ geschlossene Vertrauensmodelle

- Ausweitung auf möglichst viele Vertrauenssubjekte.

  $\longrightarrow$ offene Vertrauensmodelle

# Geschlossene Vertrauensmodelle

- Eine möglichst kleiner Kreis kennt die Funktionsweise der Sicherheitsrelevanten Komponenten.

- Kriterien für Design und Herstellung werden geheim gehalten.

- „Entwurf durch die besten Spezialisten“

- „Security by obscurity“

  ⟶ Die Sicherheit wird *nur* durch die Geheimhaltung erzielt.

- „Geschachteltes Sicherheitsmodell“

  ⟶ Die Sicherheit wird durch Geheimhaltung und starke Komponenten des Sicherheitssystems erzielt.

# Gründe für die Verwendung geschlossener Vertrauensmodelle

- Hochsicherheitsbereiche bei ausreichenden finanziellen und personellen Ressourcen. Z.B: NSA oder Militär.
- Vertuschung eigener Design-Schwächen
- Selbstüberschätzung
- Patent–/Lizenzrechte
- Crypto–Exportbestimmungen
- Überkommene Denkweisen

# Probleme geschlossener Vertrauensmodelle

- Kein Peer-Review.
- Totale Abhängigkeit von den Vertrauenssubjekten.

  In Bezug auf

  - sicheres Design
  - sichere Herstellung
  - Vermeidung von Backdoors
  - Überwachung bezüglich neuer Gefahren
  - Behebung von Fehlern

# Versagen geschlossener Vertrauensmodelle

- GSM - Verschlüsselung
- Telefonkarten
- Gebühren-Impulse
- Verschlüsselungsalgorithmen

...

# Offene Vertrauensmodelle

- Die Sicherheit entsteht allein aus den Komponenten des Sicherheitssystems.
- „Auch wenn alle Komponenten und Faktoren bis auf den Schlüssel bekannt sind, muß die Sicherheit gewährleistet bleiben“
- Ein möglichst großer Kreis soll das Produkt nutzen, um Fehler in eigenem Interesse zu finden.

# Vorteile offener Vertrauensmodelle

- Peer–Review
- Keine Abhängigkeit von Einzelnen
- Backdoors werden in der Regel gar nicht eingebaut
- Anpassung an neue Gefahren/Behebung von Fehlern problemlos möglich
- Externe Berater können herangezogen werden

# Probleme offener Vertrauensmodelle

- Exportbeschränkungen
- Software–Patente

# Schlußfolgerung

Nur durch die Verwendung offener Vertrauensmodelle läßt sich für den kleinen bis mittleren Nutzer in einem hinreichendem Maße sicherstellen, daß genutzte Produkte eine hinreichende Sicherheit bieten. Dies ist regelmäßig bei Opensource–Software gegeben.
Auch hat sich gezeigt, daß man nur bei Opensource–Software mit einer zuverlässigen und schnellen Behebung von Sicherheitsproblemen rechnen kann.