

Ökonomie und IT-Sicherheit



Ein Denkanstoß

Robert A. Gehring

Workshop
Grenzflächen der Informatik
und
Methoden von Informatik und Gesellschaft

Dagstuhl, 8.–12. Oktober 2004

Das Problem...

Software im 21. Jahrhundert: Nach Jahrzehnten Forschung gibt es noch immer keine „sichere Software“:

- Spam verstopft die Mailboxen
- Wöchentlich machen neue Viren die Runde.
- Täglich werden Einbrüche in Systeme gemeldet.
- „Spyware“ ist allgegenwärtig.
- „Datenschutz“ ist eine Chimäre... (usw. usf.)

Die Lösung...

„The answer to the machine is in the machine.“ (Charles Clark, Rechtsvertreter des „International Publishers Copyright Council“)

Also:

- Die Kryptographie wird's richten.
 - Asymmetrische Verschlüsselung;
 - Digitale Signatur;
 - PKIs;
 - DRM;
 - Trusted Systems... (usw. usf.)

Allerdings...



(da war doch noch was ...)

„Security, palpable security that you or I might find useful in our lives, involves people: things people know, relationships between people, people and how they relate to machines.“

(Bruce Schneier, Secrets & Lies, p. xi, 2000)

Also, was ist die Frage – und zu welcher Antwort?

2002: Die „ökonomische Wende“



Berkeley, 2002: 1st Workshop on Economics and Information Security. Veranstalter/Teilnehmer u.a.: Hal Varian, Bruce Schneier, Ross Anderson, Doug Tygar, Andrew Odlyzko, Pamela Samuelson u.a.m. IT-Fachleute, Ökonomen und Juristen suchen den gemeinsamen Nenner.


Der gemeinsame Nenner



„It's the economy, stupid!“

(Bruce Schneier, WEIS 1, 2002).

Z.B. COTS-Software



«Sicherheitsmängel bei Software sind das Resultat der Wechselwirkung von technischen, rechtlichen und ökonomischen Ursachen.» (Gehring 2002)

Die Mängel der Technologie



Unvollständige Spezifikationen.

Unvollständige Tests.

Wie mißt man Sicherheit?

Immer noch gilt: „No silver bullet.“ (Brooks 1987)

**Softwareentwicklung ist eher „Kunsthandwerk“,
weniger Ingenieurwissenschaft.**

Die Schwächen des Rechts

Fehlende Haftung.

„Software ist ein Gedicht.“ (Naja, fast jedenfalls – sagt das Urheberrecht.)

Und Software kann ein Geschäftsgeheimnis sein.

Der Anwender ist ggü. dem Urheber im Nachteil:

- Reverse Engineering wird zunehmend eingeschränkt.
- Reparatur ist weitgehend verboten.
- Sicherheitserweiterungen sind verboten.

Binärcodevertrieb schützt z.T. vor Patentklagen.

Die ökonomische Realität (I)

Software-Anbieter:

- Müssen Profit machen, d.h. Kosten senken und Einnahmen steigern.

Software-Anwender:

- Verfügen über *asymmetrische Informationen*, was „*adverse selection*“ fördert.
- Müssen auf einem verzerren Markt mit Monopolen einkaufen.

Die ökonomische Realität (II)



Netzwerkeffekte

- Software-Anbieter setzen auf proprietäre Technologien.
- Software-Anwender zum Einsatz der proprietären Technologien genötigt („*lock-in*“), da damit der größte „Nutzen“ verbunden ist.

Fazit



Qualitäts- /Sicherheitsüberlegungen werden im klassischen Modell der Produktion, Vermarktung und des Einsatzes von COTS-Software in der Regel zurückstehen müssen.

Schlußfolgerung



Nennenswerte – und nachhaltige – Verbesserungen (bei Sicherheit/Qualität) **bedürfen einer anderen Ökonomie.**

Die Anreize müssen innerhalb der Kette **Produktion – Distribution – Einsatz** grundlegend verändert werden.

Dafür ist ein integrierter Ansatz erforderlich (Recht, Technik, Ökonomie).

Möglicherweise ist das **die Botschaft von „Open Source“.**