Software-Entwicklung, Geistiges Eigentum und IT-Sicherheit

Robert Gehring
TU Berlin
(rag@cs.tu-berlin.de)

FIfF-Jahrestagung 2002

Universität Freiburg

Die Attitüde

«The legislation would immunize groups such as the Motion Picture Association of America and the Recording Industry Association of America from all state and federal laws if they disable, block or otherwise impair a "publicly accessible peer-to-peer network."

Anyone whose computer was damaged in the process must receive the permission of the U.S. attorney general before filing a lawsuit, and a suit could be filed only if the actual monetary loss was more than $250.»

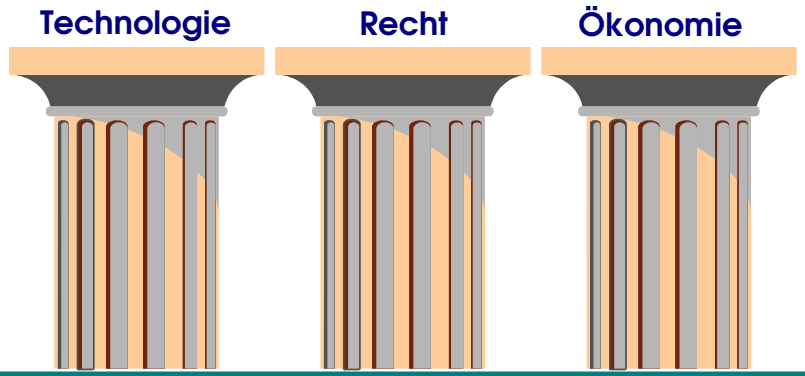
-- Declan McCullagh: Could Hollywood hack your PC? CNET News.com, July 23, 2002

Highlights

- 1999 - "I love you"-Virus verursacht Schaden von ca. **US$ 12 Milliarden** (McAfee 2001)
- 2001 - Unzuverlässige Software kostet U.S.-Industry ca. **US$ 78 Milliarden/Jahr** (CIO Magazine)
- 2002 - Laut NIST-Studie - beträgt der Verlust durch fehlerhafte Software ca. **US$ 60 Milliarden/Jahr** (in den USA)

These: Sicherheitsmängel bei Software

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



Computers & Society

Technische Ursachen (I)

- Problem der **unvollständigen Spezifikation**

«(T)he formal specifications required for verification are at least as difficult to create, and as error-prone, as programs.»

-- Hamlet 1995: 194

«(M)odern Systems have so many components and connections - some of them not even known by the systems' designers, implementers, or users - that insecurities always remain.»

-- Schneier 2000: xii

Technische Ursachen (II)

- Problem der **unvollständigen Tests**

«The developers are so in tune with what (the system) should do, they cannot see what it might be able to do.»

-- Pipkin 2000: 75

«In general, it is impractical, often impossible, to find all the errors in a program. This fundamental problem will ... have implications on the economics of testing ...»

-- Myers 1979: 8

Ökonomische Rationalität (I) - Die Anbieter

- Arbeiten **profitorientiert** (`time to market' ist kritischer Faktor)
- **Begrenzte Produktunterstützung**
- Service ist ein **Geschäftsmodell**

«The revenue of software vendors is predicated on acquiring new customers. That initial sale provides software vendors with their biggest profit. So there is a built-in incentive for vendors to rush a new release of software out the door before it is completely tested and debugged.»

-- Levinson 2001

Ökonomische Rationalität (II) - Die Kunden

- **Asymmetrische Informationen** über Produktqualität
- **'Adverse selection'**-Problem

«Even if consumers are willing to pay for more secure systems, choosing a system based on its security properties is difficult. This is not a failing of the consumer, as even industry experts rarely have little more than crude heuristics available to them to compare the security of competing products.»

-- Schechter 2002: 1

Ökonomische Rationalität (III) - Netzwerkeffekte

- Dominierende Anbieter setzen auf **proprietäre Technologien**
- **Notwendige Kompatibilität** zwingt Kunden zum Einsatz der dominierenden Produkte

«By keeping its interface proprietary and by providing an exclusive set of applications, a platform owner has some hope of exploiting "network effects" to become a de facto standard in the market.»

-- Samuelson and Scotchmer 2002: 1617

Rechtliche Ursachen

- Effektiv **keine Haftung** für COTS-Software
- **Geschäftsgeheimnis**-Schutz
- Gesetzlicher Schutz für "**Geistiges Eigentum**" (UrhR, PatR)

«Given that risk-taking is being subsidized, it should not be surprising to see the risk level increase.»

-- Lunney 2001: 877

Ursachen im UrhR

- Einschränkungen für **'Reverse Engineering'**
  - **Reparatur** von Software weitgehend **unzulässig**.
  - **Sicherheitserweiterungen** generell **unzulässig**.
- UrhR kennt keine Haftung für **'*written speech*'**.

«Encryption and computer security may be crippled if researchers are at risk of liability under the DMCA in the ordinary course of their research.»

-- Samuelson and Scotchmer 2002: 1649

Ursachen im PatR

- **Binärcode-Distribution bevorzugt**, um Patentverletzungsklagen zu vermeiden.
- **Patentierte Technologie** blockiert Substitutionsprodukte.
- **Ausbreitung** von sicherer Technologie wird **behindert**.
- **Absicherung** von Systemen ist als *business model* **patentierbar**.

Wege zur Sicherheitsverbesserung?

- **Risiken sind unvermeidbar**. Wir brauchen ein adäquates Risikomanagement.

  Das **Open Source (OS)-Modell** könnte ein guter Ansatzpunkt sein.

«Security information about proprietary software often takes longer to develop because only the proprietor has unrestricted access to the code and so the decision of whether to apply resources to security analysis of it is constrained. Opening source permits anyone who cares to apply resources to this task to do so.»

-- Landwehr 2002: 2

Warum das OSS-Modell?

- Ermöglicht **unabhängiges** `peer review'.
- Paßt UrhR (qua Lizenz) an **Spezifika von Software** an (z.B. Recht zur Modifikation).
- Weist i.d. Praxis **kurze Reaktionszeiten** bei Sicherheitsproblemen auf.
- Fördert **Qualitätstransparenz** (Quellcode-Distribution).

Die Bedrohung durch Patente

- OSS ist (bzgl. Patentverletzung) **inspizierbar** - Binärcode nicht.
- Umfassende **Patentrecherche** (bzgl. Software) ist nur von Patentanwälten durchführbar.
- OSS-Entwickler sind in schächerer Position bei **Patentverletzungsklage** (kein Geld, kein eigenes Patentportfolio).

Empfehlungen

- "**Gesetzesfolgenabschätzung**" mit Fokus IT-Sicherheit.
- "**Fair use**"**-Verteidigung** sollte in Patentrecht eingeführt werden.

«Der Umgang mit dem Quelltext von Computerprogrammen muss patentrechtlich privilegiert werden. Das Herstellen, Anbieten, in Verkehr bringen, Besitzen oder Einführen des Quelltextes eines Computerprogrammes in seiner jeweiligen Ausdrucksform muss vom Patentschutz ausgenommen werden. (Quelltextprivileg)»

-- Lutterbeck/Horns/Gehring 2000

Referenz

http://ig.cs.tu-berlin.de/ap/rg/index.html