Open Source Software - Sicherheit im Spannungsfeld von Ökonomie und Politik

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

Workshop "Sicherheit mit Open Source?"

CAST Forum
Darmstadt, 20. März 2003

Computers & Society

Agenda

- ***Empirie***: Beispiele für OS-Sicherheit
- ***Theorie***: Warum Software unsicher ist und was OS daran ändern kann.
- ***Prophetie***: Warum OS und TCPA vielleicht nicht zusammenpassen.

Computers & Society

Empirie: Die Probleme (I)

- **Unklare Terminologie**: Was ist mit dem Begriff ‘Sicherheit’ bei Software/IT-Systemen überhaupt gemeint?

«Security means different things to different people. It may even mean different things to the same person, depending on the context.»

-- Viega und McGraw 2001, S.14

Empirie: Die Probleme (II)

- **Fehlende Metrik**: Wie mißt man die Sicherheit von Software?

«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, S.1

Beispiel 1: SSLeay/OpenSSL

- SSLeay ist eine freie Implementierung von Netscapes Secure Socket Layer Protokoll. (Hudson und Young 1998)
- SSLeay entstand in Reaktion auf (1) den wachsenden Bedarf an sicherer Kommunikation im Web und (2) die restriktive US-Kryptopolitik im 20. Jahrhundert.
- Entwicklung begann in Australien und wurde im OS-Modell fortgeführt.
- Im Ergebnis steht starke Verschlüsselungstechnologie weltweit zur Verfügung.

«The most likely possibility is a world where strong encryption is freely available, inexpensive, and exportable. The technology would converge towards a world-wide standard. Some users, probably large commercial enterprises, would have some kind of key-recovery system in place for stored data. Few individual users would.»

-- Singleton 1998, S.37 f.

Computers & Society

Beispiel 2: Apache-Sicherheit

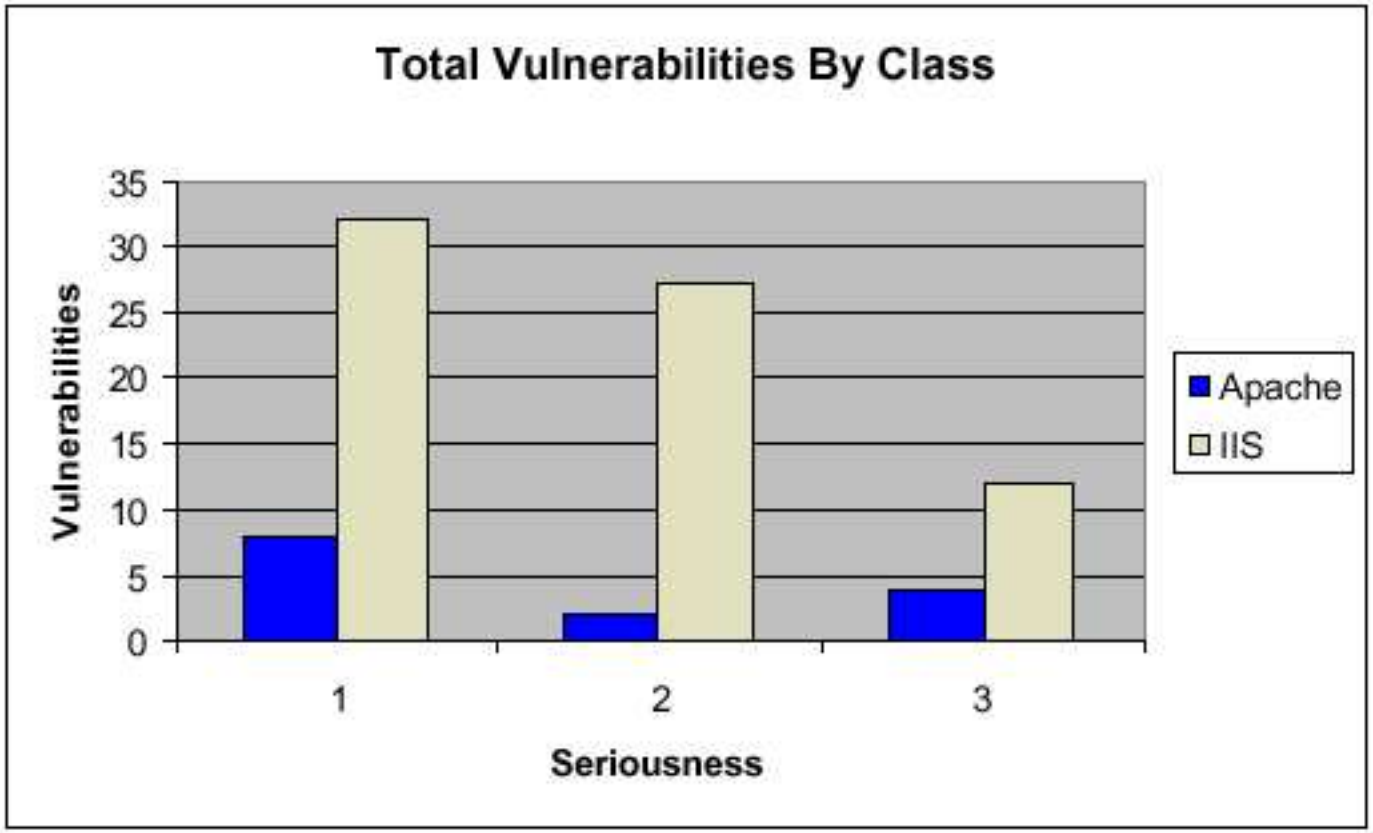
- Ronald W. Ritchey (Booz Allen Hamilton) hat 2001 die Sicherheit von Apache Webserver und MS Internet Information Server untersucht.
- Untersuchung wertet 'reported security vulnerabilities' (S. 2) von SecurityFocus aus.
- Ergebnis: OS Apache Webserver (59% Marktanteil) deutlich sicherer als IIS (28% Marktanteil).

«Apache is the clear winner with a significantly smaller number of and average exposure to vulnerabilities. For the most severe vulnerabilities, Apache had roughly 4 times less security exposure than IIS. (...) For all classes of vulnerabilities, Apache's vulnerability exposures lasted 1/2 the time of IIS's.»

-- Ritchey 2001, S.5

Computers & Society

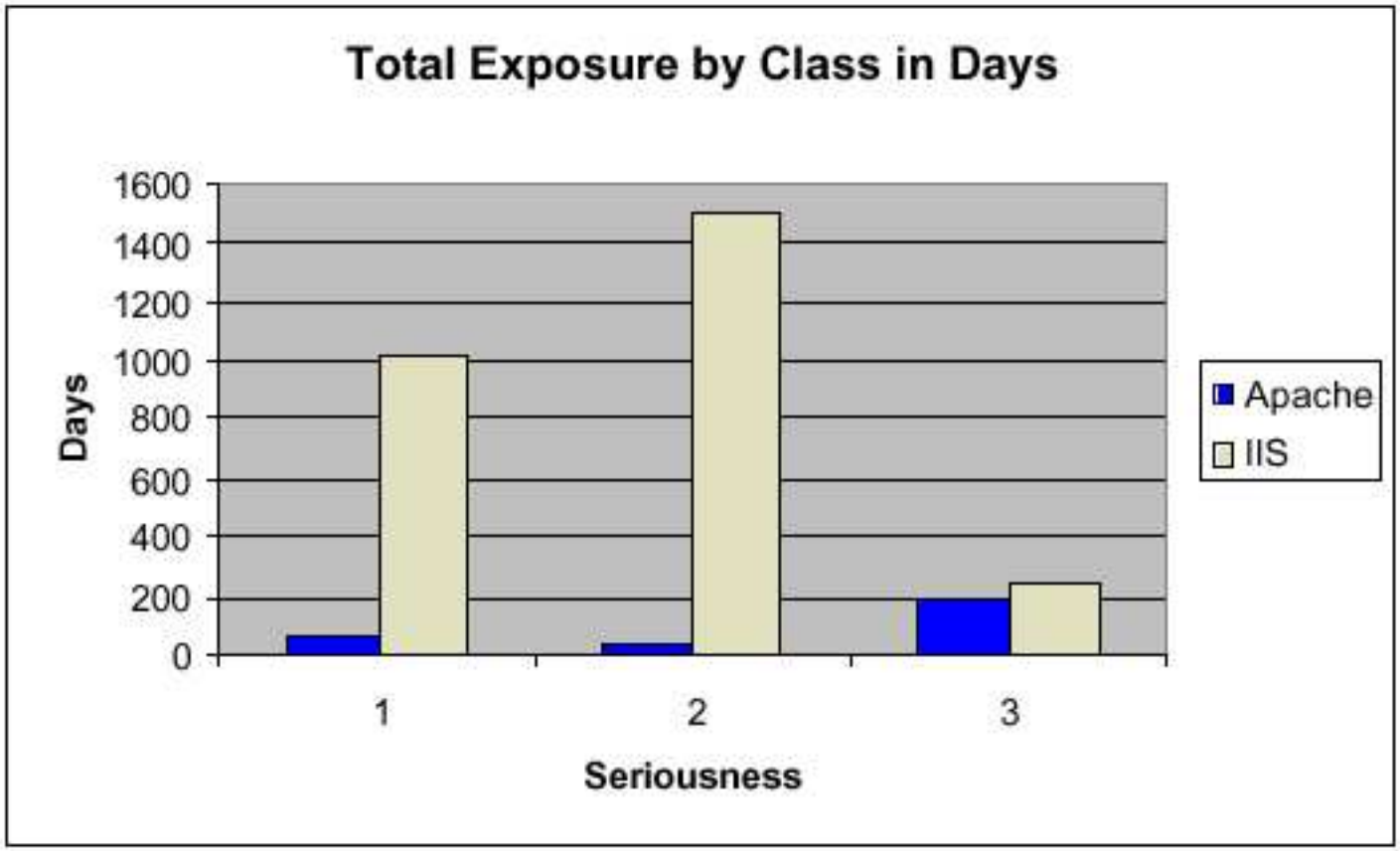
Apache-Sicherheit (Forts.)



-- Ritchey 2001, S. 6

Computers & Society

Apache-Sicherheit (Forts.)



-- Ritchey 2001, S. 6

Computers & Society

Beispiel 3: Linux TCP/IP-Stack

- Reasoning, Dienstleister für Qualitätssicherung bei Software, untersucht automatisiert die TCP/IP-Implementierungen von proprietären und Open Source-Betriebssystemen.
- Untersucht wurden u.a. 'memory leaks' und 'buffer overruns'.
- Ergebnis: Qualität der Linux- (Open Source-) Implementation kann mit den besten proprietären Systemen mithalten.

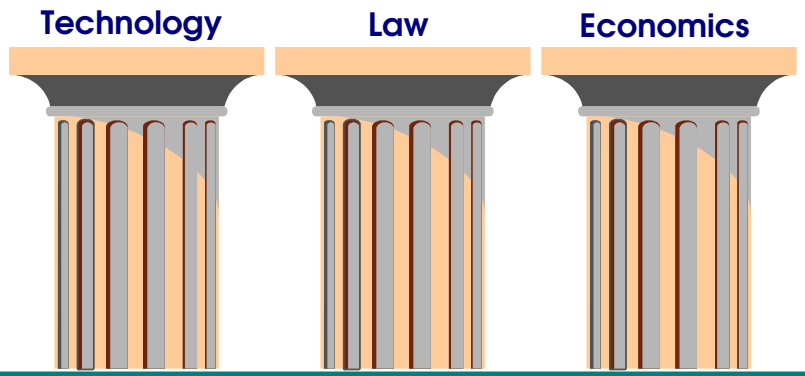
«The Linux defect rate was 0.1 defects per 1,000 lines of code, Reasoning found. The rate for the general-purpose operating systems -two of them versions of Unix- was between 0.6 and 0.7 per 1,000 lines of code. The rates for the two embedded operating systems were 0.1 and 0.3 per 1,000 lines of code.»

-- Shankland 2002

These: Unsicherheit von Software

«Insecurity of software is due to interaction of technological and legal shortcomings, fostered by economic rationality.»

-- Gehring 2001



Computers & Society

Ökonomische Rationalität (I) - Softwareanbieter

- Profitgenerierung and ineffiziente Haftungsregelungen.
- Begrenztes Angebot an Serviceleistungen.
- Service als 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

- Informationsasymmetrie
- 'Adverse selection'

«The customers learn about the quality of the software only after purchase and having tried it out. Certification, as it is often proposed to close the information gap, won't be successful under the existing regulative framework, as Anderson (2001b) explained.»

-- Gehring 2003

Computers & Society

Ökonomische Rationalität (III) - Netzwerkeffekte

- Anbieter bevorzugen proprietäre Technologie, um Marktanteil abzusichern.
- Kunden müssen dominierende Technologie wählen, um kommunizieren zu können.

«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

Computers & Society

Angedeutet: Rechtliche Ursachen

- Haftungsregelungen
- Geschäftsgeheimnisse
- Geistiges Eigentum

«Legal liability for sotware developers is unclear and nonuniform, and faulty software persists.»

-- Kotyk Vossler und Voas 2000: 451

«The reality is that the amount of software quality offered is market driven. The top suppliers of reusable commercial software have determind how to maximize profit with minimal acceptable quality.»

-- Kotyk Vossler und Voas 2000: 483

Computers & Society

Abhilfe?

- Eine integrierte Risikomanagementstrategie wird benötigt.

  Das Open Source-Modell könnte ein geeigneter 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

Computers & Society

Die Stärken des OSS Modells

- Ermöglicht unabhängigen ‘peer review’-Prozeß.
- Paßt das Urheberrecht den Erfordernissen von Software an (Modifikation, Weitergabe).
- Hat kurze Antwortzeiten bei Sicherheitsvorfällen.
- Macht Code-Qualität transparent.
- Ermöglicht und fördert Wettbewerb.

Computers & Society

Der TCPA-Ansatz

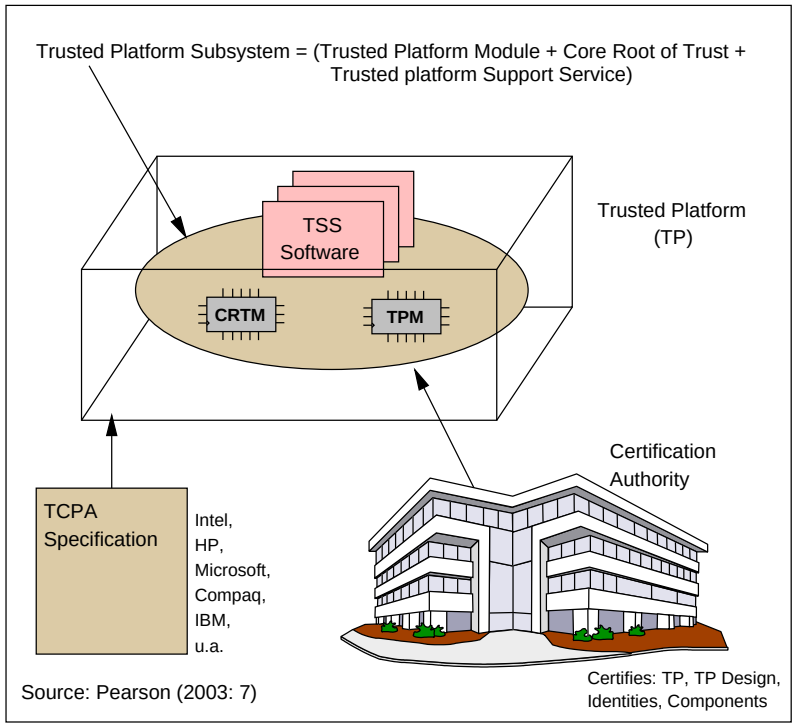
- ‘Trusted systems’ statt ‘secure systems’ (Pearson u.a. 2003, S.17 f.).
  - Hardware-/Software-Kombination (TPM).
  - TCPA-konformes Betriebssystem.
  - Kryptographische Schlüssel.
  - Zertifizierung(en) durch ‘Trusted Third Party’.
- Wirksame Zugriffskontrolle.
- Standardisierung statt Wettbewerb.
- Bildet Grundlage für DRM.

«A TCPA-enabled operating system could prevent a user from running an "unapproved" application.»

-- Arbaugh 2002, S.78

Computers & Society

Der TCPA-Ansatz (Forts.)



Computers & Society

Das OS-Entwicklungsmodell

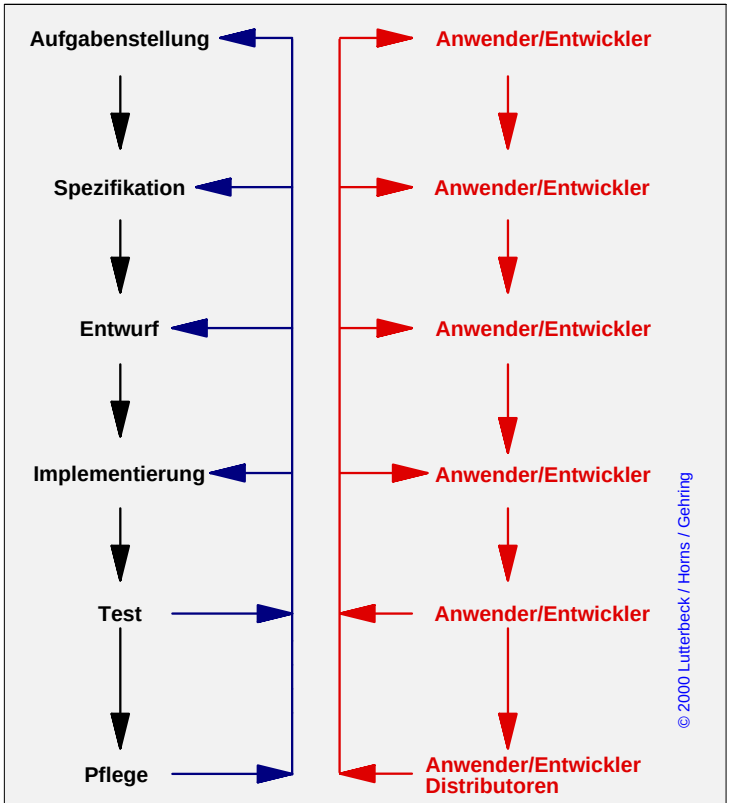
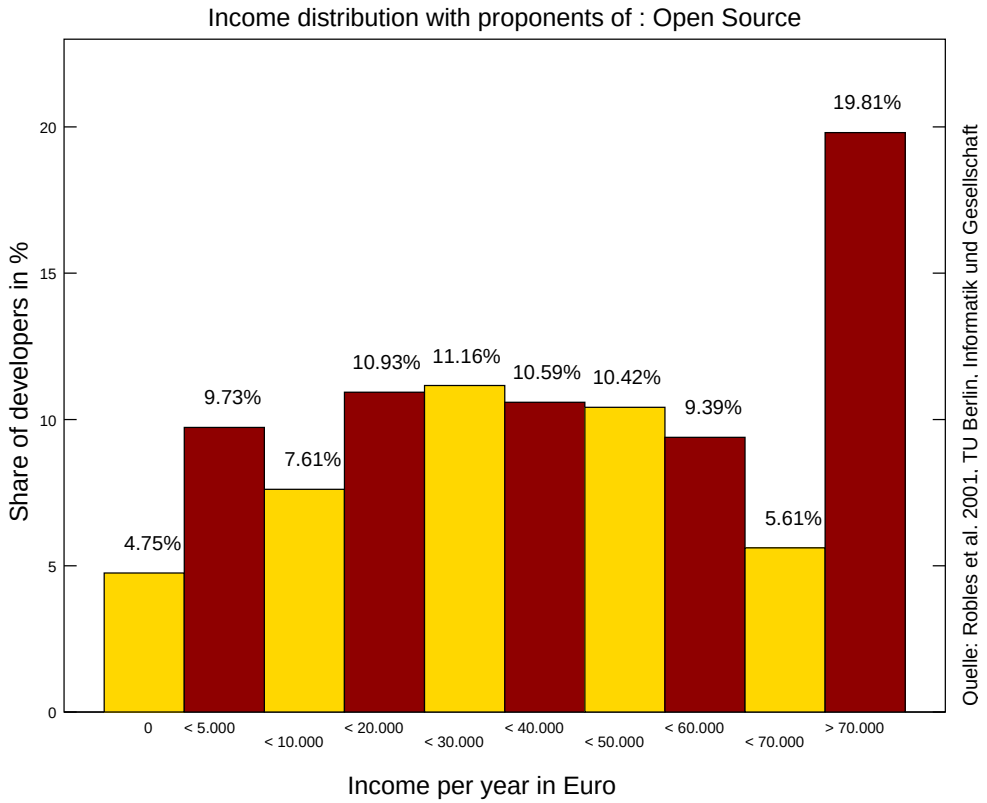


Abb.: "Open Source"-Software-Entwicklung und Aufgabenverteilung

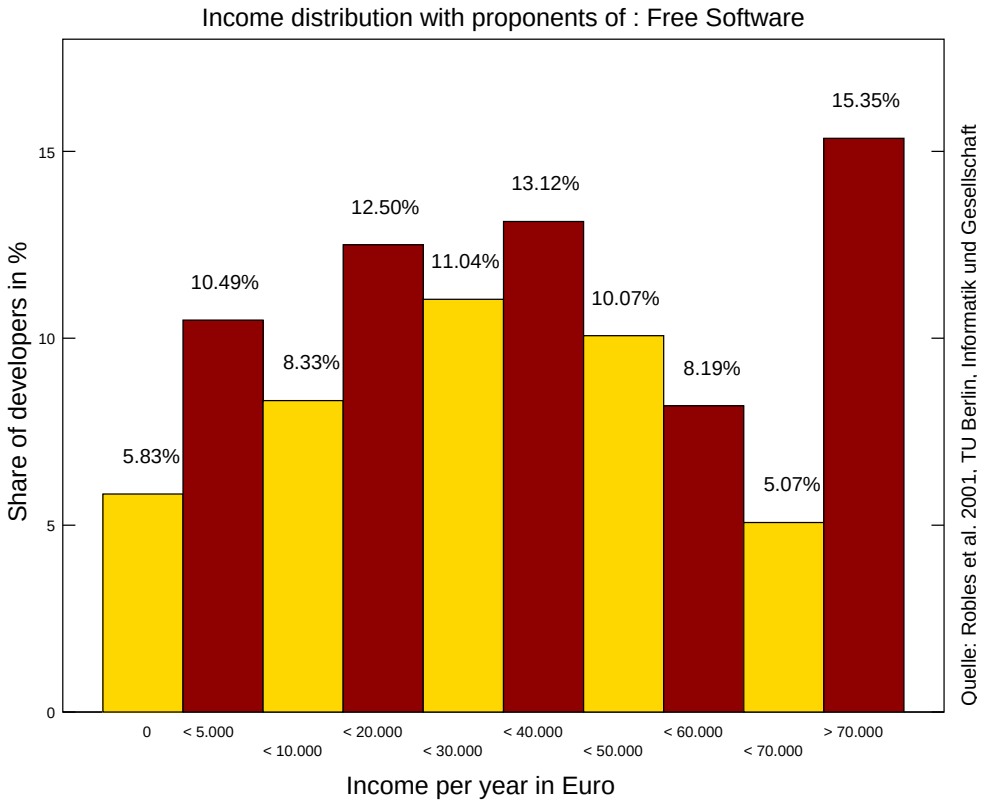
Computers & Society

Einkommensverteilung bei den Entwicklern (I)



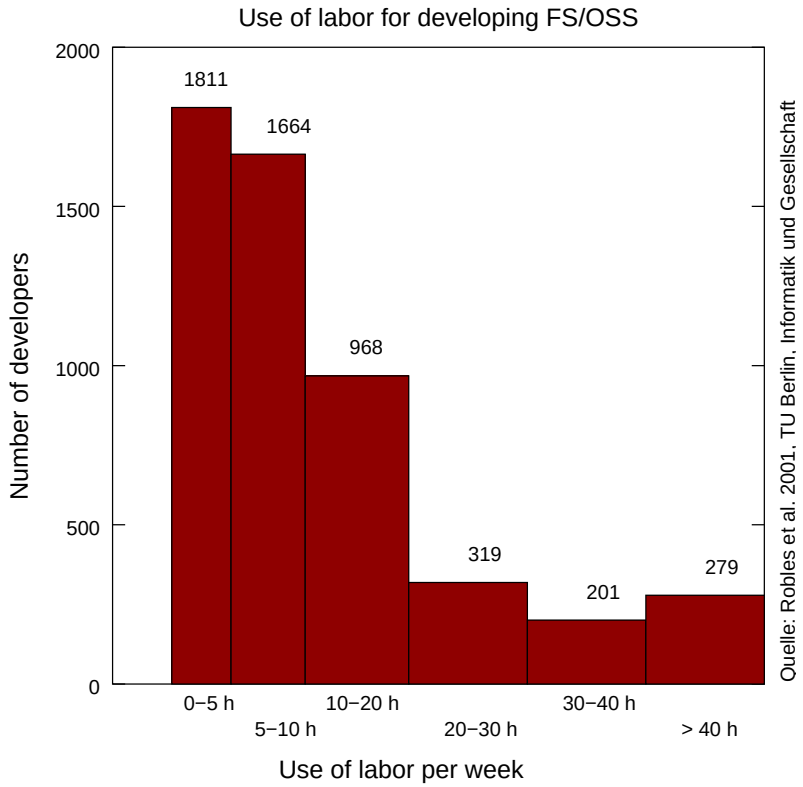
Computers & Society

Einkommensverteilung bei den Entwicklern (II)



Computers & Society

Zeitaufwand bei den Entwicklern



TCPA und Open Source?

- Es bleiben Fragen offen ...
  - Das OS-Modell lebt von der *Initiative des Einzelnen* und der Interaktion innerhalb einer inhomogenen 'Community'. TCPA stört die Initiative des Einzelnen. Wie wirkt sich das auf die 'Community' aus?
  - Zertifizierung kostet (viel) Geld. Warum sollten die einzelnen Entwickler dafür Geld ausgeben, wenn sie keines damit verdienen?
  - Zertifizierung kostet (viel) Zeit. Warum sollten die einzelnen Entwickler die Zeit in die Zertifizierung statt in das 'Codieren' stecken?
  - usw. usf.

Computers & Society

Spekulation TCPA & OSS

- Der industrieweite Umstieg auf TCPA verschafft den großen Open Source-Anbietern (IBM, HP, RedHat, SuSE, ...) einen strategischen Vorteil innerhalb der 'Community'.
- Individuelle Entwickler, unterfinanzierte Wissenschaftler und kleine Anbieter verlieren an Einfluß.

«Es muß gründlich diskutiert werden, ob diese Verschiebungen nicht das ganze Open Source-Modell in seiner Überlebensfähigkeit gefährden.»

Computers & Society

‘Bringing home message’

"Improving information security is an important and timely goal, but not at the cost of further weakening fair use doctrine, encouraging anticompetitive behavior, or eliminating privacy."

-- Arbaugh 2002, S.79

Computers & Society

Reference

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

Computers & Society