



Open Source Security

Ist Open Source sicherer als Closed Source?

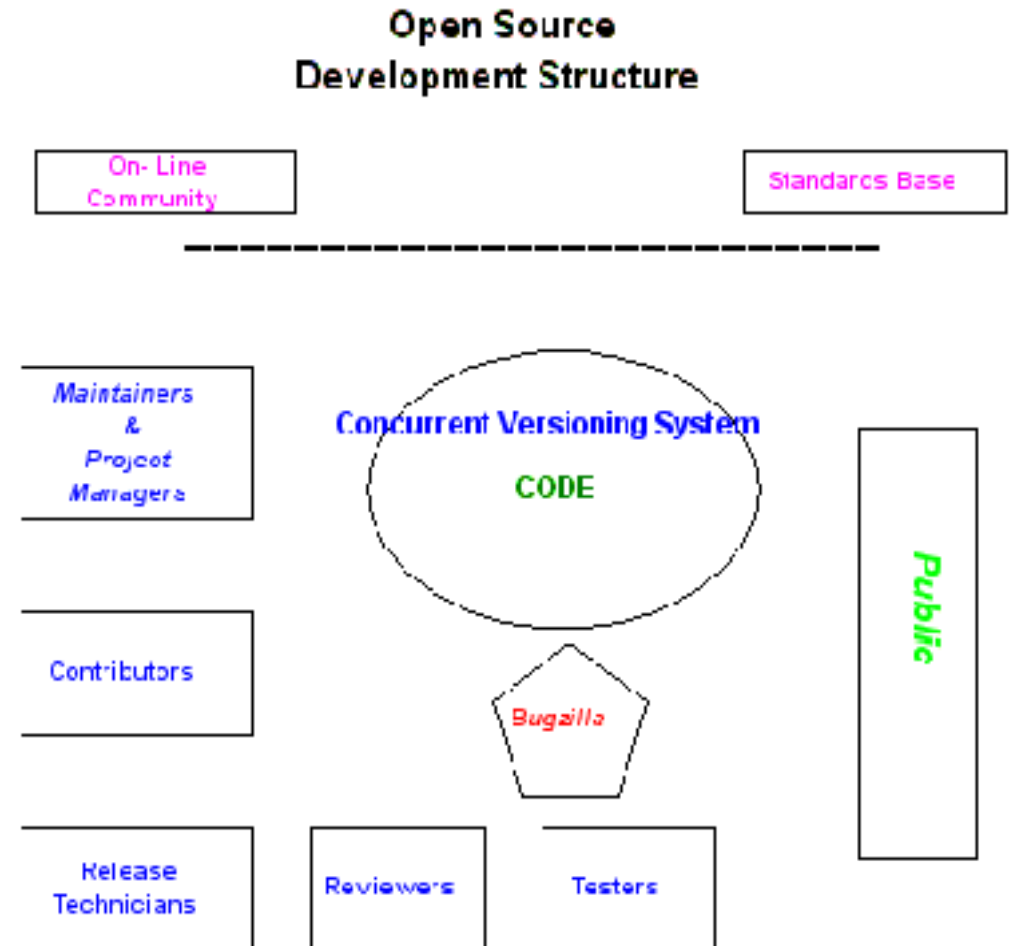
- Dinçel Ataç
- Birol Kayapinar
- Wolfram Riedel

Dezember 2003



Open Source Softwareentwicklung

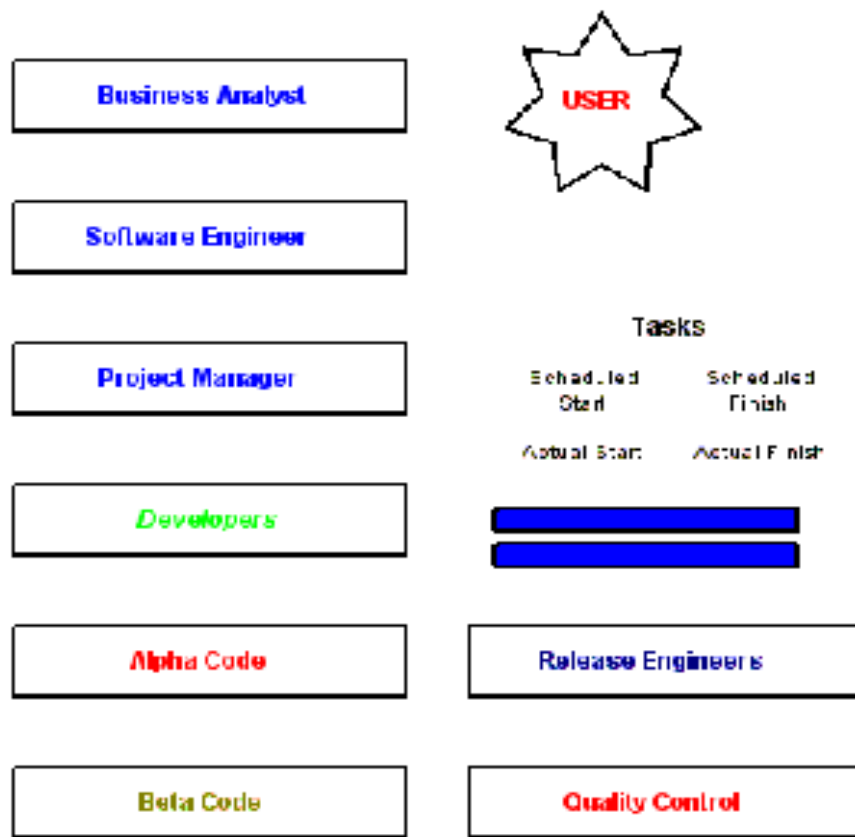
- Kontrolle beim Benutzer: Änderungen und Weitergabe möglich
- “Given enough eyeballs, all bugs are shallow” (E. S. Raymond)
- Aufbau auf vorhandenem, zuverlässigem Code, gute Code-Qualität
- kontinuierliche Releases
- schneller Support durch aktive Community





Closed Source Softwareentwicklung

Closed Structured Development Method



- Kontrolle beim Hersteller: Abhängigkeiten, Monopole
- Kinderkrankheiten und Inkompatibilitäten durch “Reinventing the Wheel”
- Security by Obscurity, Risk-Management-Strategien
- Patch- und Produktzyklen
- Kundensupport-Monopol



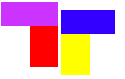
Asymmetrien beim Angriff auf Open vs. Closed Source Software

- Closed Source:
 - Angriffe sind schwierig, aber nicht unmöglich
 - Absicherungen nur vom Hersteller durchführbar
- Open Source:
 - Angriffe sind einfach
 - Absicherungen sind leicht möglich und können selber durchgeführt werden
- “In security, rapid response is everything.” (S. Schlesinger)



Beispiele für Angriffe

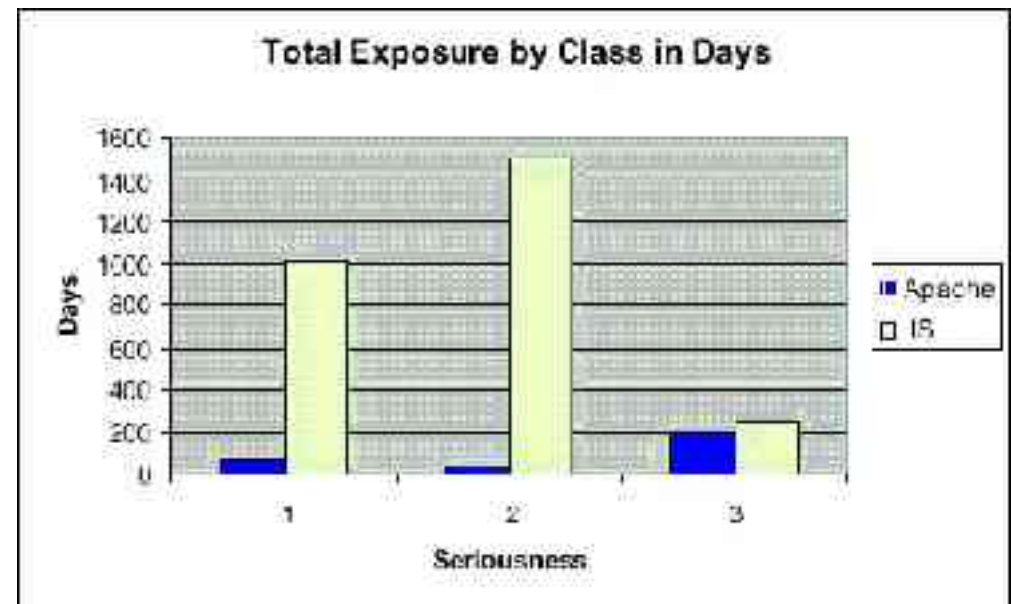
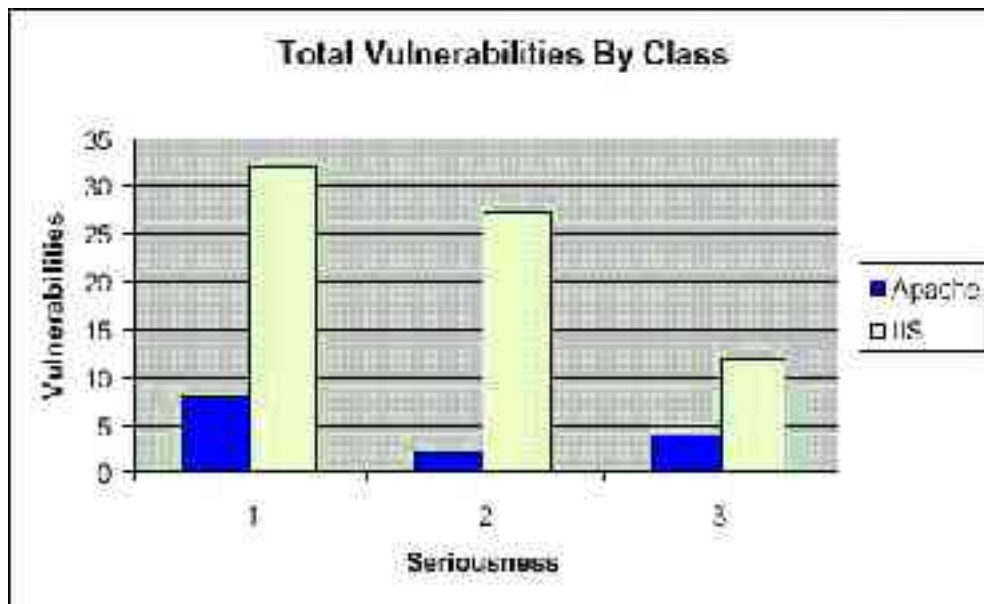
- Debian-Server:
 - Zugang mittels gesnifftem Passwort,
Root-Rechte mittels Kernel-Exploit
 - Intrusion Detection System: Snort
 - Vorbeugen durch konsequente Verschlüsselung:
z.B. mit OpenSSL
- Outlook-Würmer:
 - Verbreitung über E-Mail-Programm Outlook,
z.B. I-Love-You, Lovesan



Open Source vs. Closed Source

Empirischer Vergleich: Apache vs. IIS

- weniger sicherheitskritische Fehler
- entdeckte Fehler werden schneller beseitigt



Quelle: Ritchey 2001, zitiert bei Gehring 2003



Zertifizierungen für ein Open Source Betriebssystem

- Sicherheitszertifizierung von IT-Produkten und IT-Systemen des BSI (Bundesamt für Sicherheit in der Informationstechnik)
- Linux Enterprise Server 8 auf IBM xSeries Servern
- evaluiert nach Common Criteria (ISO 15408), Sicherheitsstandard für unternehmenskritische IT-Produkte



Open Source in der Politik

“Man sollte seine Geschäfte niemals von der Gnade oder dem Geschick anderer Firmen abhängig machen.”
(John “Maddog” Hall, Präsident von Linux International)

- Unabhängigkeit (Investitionssicherheit, Planungssicherheit)
- Softwarevielfalt, Vermeidung von Monokulturen
- weniger Verzerrung des Wettbewerbs
- Interoperabilität



e-Government mit OSS

- Webservice für e-Government mit Open Source Software
 - Projekt “Leopard” basierend auf LAMP
(Linux, Apache, MySQL, PHP/Perl/Python)
 - standardisierte Webanwendungen für Behörden



Projekt des Open Source
Software Institute (OSSSI)

- Verbesserung der Kommunikation der Behörden untereinander
- Verbesserung der Verständigung mit den Bürgern
- Haushalt wird entlastet



e-Voting mit Open Source Software

- Überprüfbarkeit durch die Öffentlichkeit schafft mehr Vertrauen bei den Wählern und trägt zu mehr Transparenz in der Demokratie bei
- Debian GNU/Linux bei Wahlen im Oktober 2001 im australischen ACT-Distrikt eingesetzt
- IT-News: "Die einzige Plattform, die Robustheit und Vertrauen der Wähler gewährleistet, war Debian GNU/Linux, mit all seinem Quellcode, der unter der General Public License (GPL) lizenziert ist."



Open Source Security – Ein Fazit

Ist Open Source sicherer als Closed Source?

Empirische Daten sprechen dafür, aber offene Quellen sind keine Garantie, sondern Grundvoraussetzung.

Kommerzielle Hybridlösung: Open Source Software gebündelt mit Hardware, Closed Source Frontend und Servicevertrag

Open Source Software sorgt in demokratischen Gesellschaften für mehr Transparenz und Sicherheit und sollte deshalb gefördert werden.