

Open Source Code von "Turaya" veröffentlicht:  
**Erste Piloten der Sicherheitsplattform mit Trusted-Computing-Funktionalitäten**

**Gelsenkirchen, 19. Juni 2006.-** Die Meilensteine „Turaya Crypt“ und „Turaya VPN“, die auf der ersten vertrauenswürdigen Open Source Sicherheitsplattform mit Trusted Computing Support basieren, stehen auf [www.emscb.de](http://www.emscb.de) zum Download bereit. Durch die Plattform können Prozesse über eine Virtualisierungsschicht voneinander getrennt werden, damit wird die Ausführung sicherer Applikationen neben einem unsicheren Betriebssystem möglich. Die Turaya-Piloten nutzen zurzeit Linux als auf dem Sicherheitskern eingesetztes Betriebssystem.

Der Source Code der ersten Sicherheitsplattform mit Trusted Computing Support ist am 19 Juni unter Open Source Lizenzen veröffentlicht worden. Das Konsortium European Multilaterally Secure Computing Base "EMSCB" stellt die Quellcodes der ersten Piloten unter [www.emscb.de](http://www.emscb.de) zur Verfügung. Die Technologie wird unter dem Namen „Turaya“ bekannt gemacht. Ein CD Image mit den ersten Meilensteinen „Turaya Crypt“ (Festplattenverschlüsselung) und „Turaya VPN“ (sicheres VPN-Modul) steht zum Download bereit.

Die Sicherheitsplattform unterstützt Trusted-Computing-Technologie und setzt darauf aufbauend hochsichere Funktionen vertrauenswürdig um. Über eine Virtualisierungsschicht können Prozesse voneinander getrennt werden. So kann beispielsweise ein unsicheres Betriebssystem neben sicheren Applikationen oder abgesicherten Betriebssystemen ausgeführt werden. Die Sicherheitsplattform basiert auf einem L4-Microkern. Die ersten Turaya-Umsetzungen nutzen zurzeit Linux als auf dem Sicherheitskern eingesetztes Betriebssystem.

Die Sicherheitsplattform ermöglicht hochsichere Anwendungen. Trusted-Computing-Funktionalitäten machen es möglich, über die bereits bekannte Authentifizierung von Nutzern hinaus auch Plattformen zu authentifizieren. Wichtige Daten und Schlüssel können außerhalb des unsicheren Betriebssystems gelagert und eingesetzt werden. Herkömmliche Gefahren, die von Würmern, Trojanischen

06.07.2006

---

## PRESSEMELDUNG

Pferden und Viren ausgehen, werden auf diese Weise eingeschränkt und teilweise verhindert.

Beispiele für Anwendungen sind sichere Web-Applikationen wie Online Banking, sichere Web-Services und Anwendungen, die ein sicheres Policy Enforcement (Enterprise Rights Management)voraussetzen, wie z.B. ein sicheres Dokumentenmanagement (4. Meilenstein 2007) Die nächsten Prototypen im Bereich Enterprise Rights Management werden in Kooperation mit SAP und Bosch/Blaupunkt entwickelt.

### HINTERGRUND:

Im Rahmen des vom Bundesministerium für Wirtschaft und Technologie BMWi geförderten Projektes EMSCB entwickelt ein Konsortium aus Wirtschaft und Wissenschaft eine vertrauenswürdige, faire und offene Sicherheitsplattform. Ziel ist eine offene Sicherheitsarchitektur, die auf Trusted-Computing-Technologie aufsetzt und zu existierenden Betriebssystemen kompatibel ist, aber gleichzeitig deren Gefahren beseitigt. Die Architektur dient als Basis für die Realisierung sicherheitskritischer Anwendungen und liefert der deutschen Industrie eine standardisierte Technologie für die Entwicklung neuer innovativer Produkte für PC- und Server-basierte Plattformen, Embedded Systems und mobile Endgeräte. Dies macht die deutsche IT-Industrie unabhängig von Monopolisten und verbessert ihre internationale Position. [www.emscb.de](http://www.emscb.de)

389 Worte, 2993 Zeichen