

06.07.2006

PRESSEMELDUNG

Auch mit gängigen Betriebssystemen muss Datenkommunikation nicht gefährlich sein:

“Airbag für Betriebssysteme” jetzt zum Download im Internet

Gelsenkirchen, 21. Juni 2006.- Das Forschungs- und Entwicklungsprojekt EMSCB (European Multilaterally Secure Computing Base) stellt seine ersten Ergebnisse zur freien Verfügung. Die vertrauenswürdige, faire und offene Sicherheitsplattform Turaya ist die erste Technologie, die hohe Sicherheit auf Basis von Trusted Computing-Funktionalitäten umsetzt und somit einen wesentlich höheren Sicherheitsstandard schafft. Die Quellcodes der Pilotanwendungen für Festplattenverschlüsselung und VPN (Virtual Private Network), die jetzt auf der Webseite zum Download bereit stehen, sollen ein Innovationsimpuls für die deutsche Wirtschaft sein. Weitere Prototypen folgen im Bereich ERM (Enterprise Rights Management) in Kooperation mit SAP und im Automotive-Bereich mit Bosch/Blaupunkt.

Der Quellcode der allerersten Sicherheitsplattform mit Trusted Computing Support ist unter Open Source Lizenzen veröffentlicht. Das Konsortium European Multilaterally Secure Computing Base “EMSCB“ stellt die Quellcodes der ersten Ergebnisse unter www.emscb.de zur Verfügung. „Auf dieser Grundlage ist es jedem Unternehmen erstmals möglich, hochsichere, vertrauenswürdige Anwendungen zu entwickeln, die Trusted Computing-Funktionalitäten nutzen“, betont Professor Pohlmann, Leiter des Instituts für Internet-Sicherheit in Gelsenkirchen. Zusätzlich bietet das EMSCB-Konsortium Interessenten den direkten Anschluss an das Kompetenz-Zentrum an, so dass das notwendige Know-how jederzeit abrufbar sei.

Die Technologie wird unter dem Namen „Turaya“ bekannt gemacht. Eine Demo-CD (CD-Image) mit den ersten Meilensteinen „Turaya.Crypt“ (Festplattenverschlüsselung) und „Turaya.VPN“ (Virtual Private Network) steht zum Download bereit.

Die Sicherheitsplattform setzt mit Hilfe von Trusted-Computing-Technologien hochsichere Funktionen und Anwendungen vertrauenswürdig um. Über eine Virtualisierungsschicht können Prozesse voneinander getrennt werden. So kann beispielsweise ein herkömmliches, un-

06.07.2006

PRESSEMELDUNG

sicheres Betriebssystem neben sicheren Applikationen oder abgesicherten Betriebssystemen ausgeführt werden. Die Sicherheitsplattform setzt auf einem L4-Mikrokern auf.

Durch Trusted-Computing-Funktionalitäten ist es möglich, über die bereits bekannte Authentifizierung von Nutzern hinaus auch Plattformen zu authentifizieren. Wichtige Daten und Schlüssel werden außerhalb des unsicheren Betriebssystems gelagert und eingesetzt. Herkömmliche Gefahren, die von Würmern, Trojanischen 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, beispielsweise 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, eingebettete Systeme und mobile Endgeräte. Dies macht die deutsche IT-Industrie unabhängig von Monopolisten und verbessert ihre internationale Position. www.emscb.de

453 Worte, 3485 Zeichen

Ansprechpartner:

Prof. Dr.-Ing. Ahmad-Reza **Sadeghi**
sadeghi@crypto.rub.de

Für die Demonstratoren Turaya.Crypt und Turaya.VPN:

Prof. Dr. Norbert **Pohlmann**
norbert.pohlmann@informatik.fh-ge.de

Ammar **Alkassar**
a.alkassar@sirrix.com

faltmann PR
fon +49.241.89 46 8-22

Sabine Faltmann
emscb@faltmann-pr.de

06.07.2006

PRESSEMELDUNG
