PrivaSphere™
Secure Messaging Service

Medienmitteilung

Schutz vor Man-in-the-Middle-Angriffen

Zürich, 17. November 2005 – PrivaSphere AG hat eine Technologie entwickelt, die SSL/TLS-basierte eCommerce-Anwendungen wirksam vor "Man-in-the-middle" (MITM) Angriffen schützen kann. Früher diesen Monat wurde durch Mitglieder der Arbeitsgruppe Identitätsschutz im Internet e.V. nachgewiesen, dass die aktuell eingesetzten Benutzerauthentisierungsverfahren, wie z.B. iTAN, nicht wirksam vor MITM-Angriffen schützen.

Der neuartige Lösungsansatz besteht darin, dass eine Benutzerauthentisierung logisch an eine bestimmte SSL/TLS-Verbindung gebunden wird. Sowohl der Client als auch der Server „sehen“ eine SSL/TLS-Verbindung. Die Benutzerauthentisierung ist nur dann gültig, wenn sie aus Sicht des Client und aus Sicht des Servers über die gleiche SSL/TLS-Verbindung läuft. Das Verlockende an der neuen Technologie ist, dass sich fast alle Benutzerauthentisierungsverfahren in diesem Sinne "SSL/TLS-bewusst" machen lassen, ohne dass der Client - d.h. der Web Browser - geändert werden muss.

Der Sicherheitsspezialist PD Dr. Rolf Oppliger, eSECURITY Technologies, bringt es auf den Punkt: „Wenn es einem MITM gelingt, eine SSL/TLS-Verbindung zum Client und eine andere SSL/TLS-Verbindung zum Server aufzubauen und die Benutzerauthentisierung der ersten Verbindung über die zweite Verbindung weiterzureichen, dann kann der Server erkennen, dass die Verbindung nicht zur Benutzerauthentisierung passt, und kann damit neu nun einen Angriff unterbinden.“

Eine besonders interessante Möglichkeit ergibt sich aus dem Einsatz von unpersönlichen PKCS #11-Tokens (z.B. Smartcards oder USB-Tokens). Das Verfahren ist mit kleineren Anpassungen auch für Einweg-Passwort- und Challenge-Response-Verfahren einsetzbar. PrivaSphere arbeitet mit Herstellern von Authentisierungssystemen an einer diesbezüglichen Implementation. Das Verfahren wurde zur Patentierung angemeldet.

Über PrivaSphere

PrivaSphere AG ist der innovative Schweizer Anbieter von sicherer und authentisierter eMail Übertragung. Die Schweizer Aktiengesellschaft wurde im Oktober 2002 gegründet. Mit PrivaSphere können Firmen- und Individualkunden spontan sicher via Internet kommunizieren ohne Installation von Software oder Hardware. PrivaSphere wurde im November 2004 mit dem CTI Start-Up Label der schweizerischen Förderagentur für Innovation ausgezeichnet und ist Preisträger des Swiss Technology Awards 2005.

Weitere Informationen:

PrivaSphere AG
Paul Frey
Fichtenstrasse 61
8032 Zürich
Fon: +41 43 299 55 88
frey@privasphere.com
www.privasphere.com
Secure contact: https://www.privasphere.com/frey@privasphere.com