

Sicherheit verstärken und Vertrauen der User erhalten

Zunehmende Aktivitäten von Cyberkriminellen erfordern neue Sicherheitsmassnahmen ELCARDeST ist die wirtschaftliche Lösung, um online Transaktionen elektronisch zu signieren – ohne jegliche Installationen auf dem Browser PC. *Serge Bignens, Jean-Marc Bost*

Einerseits schätzen die Konsumenten und Bürger mehr und mehr, dass sie Geschäfte und administrative Formalitäten zeitunabhängig bequem zu Hause erledigen können, andererseits können Industrie, Banken und Verwaltungen über das Internet mehr Dienstleistungen schneller und mit geringeren Kosten liefern.

Aber die aktuelle Entwicklung der Cyberkriminalität stellt ein reales Problem dar mit Folgen finanzieller und rufschädigender Art – und die Attacken werden zahlreicher und effektiver. Im 2004 haben die britischen Banken Schäden in der Höhe von 4,5 Mio. Pfund erlitten. Attacken durch «Key Logger» haben mehr als 1 bzw. 4 Mio. US-Dollar Verlust für französische und brasilianische Banken verursacht. Seither tauchen erheblich gefährlichere Attacken mit noch grösserer Tragweite auf.

Die Webattacken können gemäss ihren Angriffspunkten aufgeteilt werden: Der Benutzer, das Netz, der PC des Benutzers. Das Phishing (der Hacker ködert den Benutzer, indem er sich als ein anderer ausgibt) gehört zur ersten Kategorie und ist heute omnipräsent. Zur zweiten Kategorie gehört der «man-in-the-middle»-Angriff, bei dem sich eine böswillige Website dazwischen schaltet und die Transaktionen zwischen Browser und dem Service abfängt und manipuliert. Dieser Typ ist schon lange bekannt, aber erst seit kurzem effektiv (siehe Kasten «Attacken», Punkt a). Bezüglich der letzten Kategorie schaltet sich Malware zwischen den Benutzer und den Browser. Die Malwares werden mehr und mehr Realität (siehe Kasten

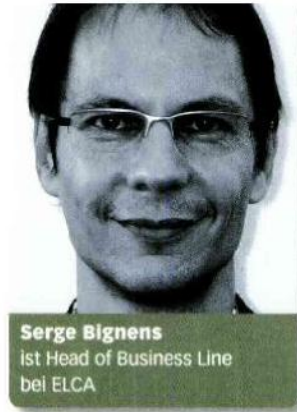
«Attacken», Punkt b).

Aktuelle PKI-Systeme sind teuer – was bringen sie?

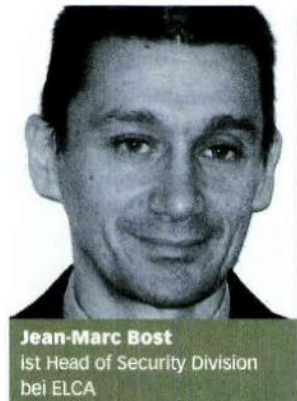
Die auf dem Markt verfügbaren PKI(Public Key Infrastructure)-Lösungen setzen die Verteilung von Schlüsseln und Zertifikaten in Form von Software, USB oder Smart Cards an die Benutzer voraus. PKI Lösungen basieren auf der systematischen Verschlüsselung des Datenaustausches und der Authentifizierung der Kommunikationsteilnehmer und verhindern damit, dass Hacker sich dazwischenschalten. Aber wie werden Malwares abgewehrt? Prominente Spezialisten warnen die Hersteller von PKI-Lösungen und deren Kunden vor blindem Vertrauen, weil man nicht sicher sein kann, wer die Schlüssel verwendet. Wenn eine Malware einen PC kontrolliert, wer kann diese an der Benutzung der Schlüssel hindern? (siehe Kasten «Attacken», Punkt c)

ELCARDeST erlaubt die Abwicklung von gesicherten und nicht abstreitbaren Transaktionen

ELCARDeST, entwickelt von ELCA mit ihrem Partner ARx, schützt die gesamte Transaktionskette, vom Internetbenutzer bis zum Serviceanbieter. Diese Lösung benötigt weder Software noch Schlüssel seitens des Internetbenutzers – dieser braucht nur einen aktuellen Web Browser, was höchste Mobilität gewährleistet. Dies ist praktisch für den Benutzer und vorteilhaft für den Serviceanbieter.



Serge Bignens
 ist Head of Business Line
 bei ELCA



Jean-Marc Bost
 ist Head of Security Division
 bei ELCA



Das Prinzip ist einfach: Der Benutzer sendet die gewünschte Transaktion über seinen Browser an den Service; dieser speichert die Transaktion und sendet eine signierte Bestätigung mit einem integrierten Challenge (Frage); der Benutzer antwortet auf den Challenge mit seiner persönlichen ELCARD (siehe Kasten ELCARD).

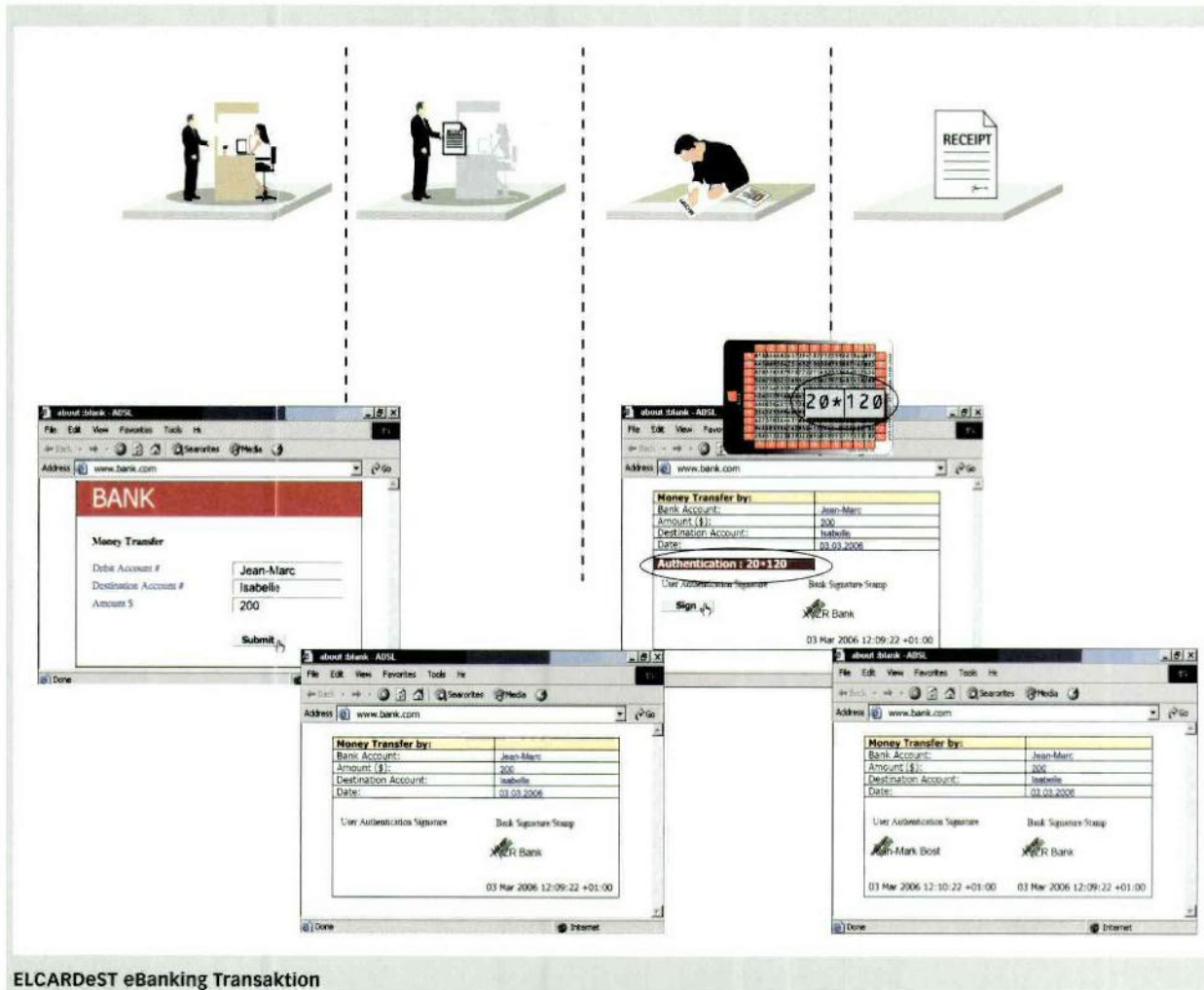
Damit bestätigt und gegenzeichnet er die Transaktion. Der Benutzer und der online Service erhalten je eine gesicherte, durch beide Partner elektronisch signierte, fälschungssichere Quittung, welche die Transaktionsdaten enthält und damit nicht abstreitbar geworden ist.

Das System der signierten Quittungen verbindet die Transaktionsdaten mit dem einmaligen Challenge-Response, die nicht mehr ein zweites Mal durch eine «man-in-the-middle» oder Malware benutzt werden kann. Mit der Lösung der integrierten elektronischen Signatur werden die technischen Anforderungen an eine sichere Verwahrung der Schlüssel und die Qualifikation der Zertifikate erfüllt, was der Lösung eine unwiderlegbare Beweiskraft verleiht. ■

«Das Internet und darüber angebotene Services sind weiter im Aufwind, aber das Vertrauen der Kunden ist gefährdet.»

Attacken

- a) Die CityBank in den USA ist das erste bekannte Opfer eines «man-in-the-middle»-Angriffs. Dieser Angriff hat das Vertrauen in die kostspieligen «Time-Tokens» (zeitgesteuerte Passwortgeneratoren) geschmälert, die als Schutz gegen das Phishing eingeführt wurden.
- b) Seit 2003 erfahren die Banken Angriffe durch arglistige Programme, Malwares, welche die im Browser eingegebenen und angezeigten Daten manipulieren. Kürzlich wurden 10000 australische PCs durch eine Malware verseucht, die alle persönlichen, mit einer Applikation ausgetauschten Daten abfängt. In einer neueren Studie hat Microsoft mit Ihrer Anti-Spyware festgestellt, dass ca. 62 Prozent der überprüften PCs infiziert waren. Das SANS Institut schätzt, dass in den USA 9,9 Mio. Computer mit Key-Logger verseucht sind.
- c) ELCA konnte die Machbarkeit einer Massenattacke auf Transaktionen über einen Browser zeigen, unabhängig davon, ob der Zielsever durch gegenseitige Authentifikation und verschlüsselte Kommunikation geschützt ist.



ELCARDest eBanking Transaktion

ELCARD

Die ELCARD ist eine einfach herzustellende und günstige Kunststoffkarte, die an die Internetbenutzer verteilt wird. Sie ermöglicht dem Benutzer eine starke Authentifizierung gegenüber einem Internetservice mittels Challenge-Response-Verfahren, um auf Informationen zuzugreifen oder Dokumente zu signieren. Der Internetservice unterbreitet dem Benutzer einen Challenge in Form einer Koordinate der Tabelle. Die Antwort wird durch den Inhalt der Zellen bestimmt, die mittels einer geheimen Abfolge durch-

laufen werden. Dieser Pfad ist das Geheimnis, das nur der Benutzer selbst kennt.

Für weitere Auskünfte:

ELCA

Steinstrasse 21, 8003 Zürich
 Tel. +41 44/456 32 11, Fax +41 44/456 32 00
 E-Mail: info.zurich@elca.ch
www.elca.ch