'Security-on-a-Stick' to protect consumers and banks from the most sophisticated hacker attacks

October 29 2008

The "security-on-a-stick" solution — a handy USB-sized device with a display, a smart card reader and buttons — protects a user's e-banking transactions from even the most malicious attacks. With the new device, developed by an expert team at IBM's Zurich Research Lab, a user sees exactly what transaction data the banking server receives. Moreover, he or she can approve or cancel each transaction directly with the banking server using the buttons on the device.

(PhysOrg.com) -- Resembling a memory stick with an integrated display, a prototype USB device developed at IBM's Zurich Research Lab brings a new level of security to online banking for consumers. Pilot devices are ready and available to banks for trials.

The Zone Trusted Information Channel (ZTIC) plugs into the USB port of any computer and creates a direct, secure channel to a bank's online

transaction server, bypassing the PC which could be infected by malicious software (malware) or susceptible to hacker attacks.

The consumer can use the security stick to logon and validate all transactions via a display, while the USB device is securely connected to the server, safeguarding against today's ever more fiendish forms of attacks that can manipulate data in the background, hidden from the consumer and the bank. The USB device adds an extra level of security to the existing authentication solutions provided by smart card, PIN or one-time validation code, in order to counter the newest and most highly manipulative security threats.

Hackers are becoming increasingly inventive in their attempts to attack financial transactions on the Internet. Among the increasingly prominent threats are so called "Man-In-The-Middle" attacks, where a hacker inconspicuously intercepts and modifies the messages flowing between a user and a financial institution. The modified messages appear to be official transactions from the financial institution, and the messages going to the financial institution appear to be from the consumer.

Malware is an even more fiendish form of attack, where the hacker manages to install a virus or Trojan Horse in a user's personal computer and is then free to manipulate the messages seen by and sent by the user. This allows the attacker to redirect communications and manipulate the data displayed by the internet browser in real-time during the user's e-banking session and totally unnoticeable to the user's eyes.

Nearly 90 percent of identity attacks online are targeted at the financial services sector. A 2007 international study by the Swiss Reporting and Analysis Centre for Information Assurance (MELANI), found that successful malware intrusions have increased and that currently established "two-factor authentication systems (e.g. transaction

authentication numbers, SecurID, etc.) do not afford protection against such attacks and must be viewed as insecure once the computer of the customer has been infected with malware."

ZTIC provides an extra layer of security in the presence of both of these attacks.

"In the presence of an ever more professionally operating e-crime scene, it became obvious that PC-software based authentication solutions were potentially vulnerable and that we needed to innovate to stay ahead. That was the starting point for developing the ZTIC," explained Dr. Peter Buhler, Manager Computer Science at IBM's Zurich Research Lab. "The design of the solution was governed by and is based on the analysis of pros and cons of present and announced alternative solutions."

This solution effectively moves all the cryptographic and critical user-interface processes away from a consumer's PC onto the ZTIC device, creating a trusted communication endpoint between the banking server and the user. With the new device, a user can then communicate securely with sensitive online services such as a banking server. In combination with a smart card, which can be inserted into the device, this new solution brings a new level of end-to-end security to online banking.

After initial lab prototypes had been realized by the researchers, first pilot devices have now been industrially manufactured and are ready for trials.

Even if a user's PC should be infected by malware that manipulates the information flow in the PC, the user can cancel the transaction while displayed on the ZTIC device. What the user sees on the ZTIC display is identical to what the server "sees," no matter what malicious intervention may occur on the PC or anywhere in the Internet. "Owing to the direct secure connection between ZTIC and server, the device essentially

provides a safe window to the server," states Buhler.

Moreover, the ZTIC has been designed such that no change is required in either the server software or the software running on the client's PC. It runs on all major home computing operating systems.

Technological Specifications

The researchers designed the ZTIC as an USB device of about the same size as a memory stick. It runs the commonly used TLS/SSL protocol. The ZTIC hardware consists conceptually, at a minimum, of a processing unit, volatile and persistent memory, a small display and at least two control buttons (OK and Cancel) as well as an optional smartcard reader. The software is minimally configured with a complete TLS engine including all cryptographic algorithms required by today's SSL/TLS servers, an HTTP parser for analyzing the data exchanged between client and server, plus custom system software implementing the USB mass storage device profile and a networking proxy for running on a PC. It supports TLS/SSL client authentication as well as common chip-card based challenge/response protocols.

Provided by IBM