

AMERICAN BANKER®

THE FINANCIAL SERVICES DAILY

Friday, August 3, 2007

VIEWPOINTS

2-Way Authentication Needed for Safety



ANDREA KLEIN

Consumers who do not feel safe online are increasingly steering clear of Internet banking sites and shutting out an important channel for financial services providers to expand their customer relationships.

The industry research firm Gartner Inc. estimates that almost nine million adults in the United States have stopped banking online and that another 23.7 million decline to start out of security concerns.

The continual spread of online scams — and the reality that people are increasingly wary of online banking channels — raise the stakes for banks to protect customers and themselves from increasingly sophisticated cyberattacks.

In the past year, customers at several of the world's largest banks have fallen victim to “man-in-the-middle,” or MITM, identity theft schemes that have shaken customer confidence in online banking and battered bank reputations. As the term implies, identity thieves position themselves “in the middle” of sensitive communications between customers and banks in order to steal account and other personal information.

In one MITM scheme last summer involving a large U.S. banking company, the thieves sent seemingly authentic e-mails asking customers to verify their account information. The e-mails directed customers to a spoofed bank Web site that seemed legitimate but actually redirected the customers to a fake Web site set up by a hacker in Russia.

In redirecting customers to the spoof site (also known as “pharming”) the hacker was positioned to intercept user password/account information and potentially to use the records in fraudulent transactions or as goods for sale to other criminals. Criminals also use MITM Web sites to read, insert, and change messages between the bank and its customers.

These attacks spotlight the shortcomings of secure socket layer protocol and multifactor authentication security measures that many financial institutions have adopted. These security measures are limited because they only require that the bank and customer trust one another and do not provide the added assurances required to thwart MITM or related schemes.

Two-factor authentication also comes up short in shielding banks and their customers from MITM attacks. The two-factor authentication model uses an online password and an additional form of authentication (such as an access card) for online security. This approach authenticates users but does not enable them to confirm that they are communicating with legitimate online sites.

For example, fraudsters can create pharming sites that present their own credentials for encrypted sessions to fool users (and their PC/client-based computer security systems) into thinking they are connected to legitimate sites. The users then enter password and personal information that is intercepted on the pharming site.

Other narrow security safeguards — such as images that each user selects as a unique identifier when logging in — are ineffective against MITM. Online banks use a Web browser cookie (which serves as a small software identification tag) downloaded on a user's computer to match the user and the appropriate image. MITM schemes can steal the identifying text and images that are unique to each user's computer.

To maintain high vigilance, financial institutions must establish reciprocal trust relationships among all electronic transaction participants, authenticating the user to the site and the site to the user. A mutual authentication environment, often called a public key infrastructure, relies on a cryptographic system of two keys: a public key and a second, private key known only to the message recipient.

The bank's server creates a key encrypted with the server's private key. The server then asks for customer authentication. The customer uses his or her private key to encrypt the message. The client also

sends a second key to the bank, which the bank's server automatically decrypts.

Creating this secure encrypted tunnel between the two transaction parties lets each be certain the other is known and trustworthy.

Crucial factors for effective mutual authentication include:

- Establishing a single system to govern access control, client authentication, and user authenticity — including secure socket layer protocol, digital signing, and nonrepudiation.
- Keeping keys in separate locations. Separate the keys used to create the secure channel session and those used to authenticate the signing and relying parties.
- Issuing utility and identity certificates. Issue each certificate holder both types of certificate. The utility certificate is for encryption, data confidentiality and integrity, and secure socket layer protocol and secure key distribution. The identity certificate is used for digital signing.

In addition to verifying all parties in an online transaction, mutual authentication must be done instantaneously to

deliver the level of service that today's bank customers demand.

Banks must also consider the international dynamics of today's economy by addressing the need for solutions that work across borders and providing globally recognized dispute-resolution systems. Added levels of online banking trust, however, must be created and managed without adding to the burden on banks, financial institutions, or customers.

Protecting and maintaining trusted customer relationships is a priority for any bank or financial services firm. By establishing true, two-way authentication, banks are defending their customers — and their reputations — against increasingly sophisticated online hacks and attacks.

A trusted online banking solution is a crucial gateway to adding customers and enhancing relationships.

Ms. Klein is the chief marketing officer of IdenTrust Inc., a San Francisco digital identity authentication system provider formed in 1999 by a consortium of banking companies including Citigroup Inc., ABN Amro Holding NV, and Deutsche Bank AG.

IdenTrust™
WE PUT THE TRUST IN IDENTITY