How to secure online banking from man-in-the-middle attacks
How to secure online banking from man-in-the-middle attacks

Online banking has been steadily growing over the past decade. Almost every bank worldwide is offering online banking services to its retail customers. According to Forrester online banking adoption in the US will by 2011 grow with 55% to roughly 72 million households. By then 76% of the online households will bank online. The growth in online banking adoption in the US also comes from the younger Generation Y who grew up with the internet and they are already confidently shopping online. But how secure is online banking? Are our financial transactions at risk due to man-in-the-middle attacks? What is man-in-the-middle attack and how can banks protect themselves and their clients?

MAN-IN-THE MIDDLE ATTACKS

Man-in-the-middle attacks are on the rise. In recent reports Gartner already advises to protect against more-sophisticated attacks. Moreover, recent cases in Europe and the US demonstrate that fraudsters are developing more complex mechanisms to intercept and alter financial transactions. Man-in-the-middle attacks typically are attacks on online banking systems. The fraudster is nestling himself in the communication flow between the customer and the bank with the aim of manipulating the transaction data to his own advantage leaving the bank and the customer unaware. Technically speaking, man-in-the-middle attacks can take two forms: remote and local man-in-the-middle attacks.

With remote man-in-the-middle attacks, the fraudster will use a myriad of techniques, such as phishing and pharming, to lure the banking customer to a rogue website. When the banking customer logs onto his account to make a transaction, the rogue website is obtaining the password and transaction details, such as the beneficiary’s bank account number and the monetary amount of the transaction. The transaction details often will be altered and used by the fraudsters on the real banking website to their financial benefit.

A local man-in-the-middle attack is carried out by malicious software that is installed on the end-user’s computer. This software, also called spyware or crimeware, typically infects the computer through downloads or e-mail attachments. Once the software is installed, it tracks which websites the end-user visits. When the crimeware detects that the end-user is visiting an online banking website, it waits for the user to be logged on and then initiates or alters financial transactions without the user knowing.
HOW CAN BANKS AND CUSTOMERS PROTECT THEMSELVES?

The customer should learn to behave securely when banking over the Internet, just as he should do with other applications such as buying goods online. It is therefore very important that the customer becomes familiar with the “Internet street smarts” and be able to assess the risks involved in visiting strange websites and downloading (il)legal software. He should also be decently equipped before setting foot on the Internet, and have anti-virus, anti-spam and anti-spyware software installed on his computer.

Banks should take precautions as well, and strengthen access control to their online banking applications by means of authentication technology. Strong authentication mechanisms come in two important flavors: one-time passwords and electronic signatures.

One-time passwords are used for the authentication of the end-user when he logs onto the application. One-time passwords are generated based on a variable parameter, such as the time or a random number. They are valid for only a limited amount of time (typically in the range of minutes) and can only be used once. The strength of one-time passwords lies in the fact that they narrow down the window of opportunity for a fraudster to perform an attack. Hence, it becomes more difficult to perform fraudulent activities, especially when compared to the possibilities to perform fraudulent action when using static passwords. One-time passwords, however, do not provide protection against the injection of or alteration to financial transactions. In order to resolve this problem electronic signatures should be used.

Electronic signatures, the second type of authentication mechanism, authenticate the financial transactions. E-signatures allow the bank to verify whether a transaction was initiated by the genuine end-user and was not altered in transit. It prevents the fraudster from submitting transactions or modifying existing transactions. As a result e-signatures offer the ideal security control against both local and remote man-in-the-middle attacks.

HOW DOES IT WORK?

When the end-user wants to make a financial transaction using e-signature, a Message Authentication Code (MAC) will be calculated over the transaction. The calculation uses the original transaction and a secret key as input. The secret key is something the end user shares with the bank and which is only known by them. The result of the calculation is the so-called MAC, or e-signature. The end-user electronically submits the transaction and the corresponding MAC to the bank. Upon receipt, the bank computes the MAC over the transaction with the secret key. It then compares the calculated MAC with the MAC it received from the end-user. If both are the same, the bank is sure that the genuine end-user submitted the transaction, and that the transaction was not modified in transit. As a result, the financial transaction can then be processed. If there is no match, the bank knows that either a crook submitted the transaction, or the transaction data was altered in transit. In that case, the bank rejects the transaction.
We can conclude that the calculation mechanisms, the use of a secret key more specifically, used to generate e-signature, effectively protect banks and end-users against men-in-the-middle attacks and therefore ensure secure online financial transactions.

VASCO Data Security is specialized in strong two factor authentication. VASCO’s solutions for online banking are used by more than 1000 banks worldwide. The solution is typically based on VACMAN Controller technology and Digipass authentication. VASCO has embedded its software client authentication product Digipass into its VACMAN Controller server side authentication products. This means that banks which installed VACMAN Controller, can immediately protect their customers’ assets against phishing, pharming, man-in-the-middle attacks and Trojan Horses with best-of-breed Digipass strong authentication and e-signature technology. If the customer wants, he can diversify its authentication offerings to its different user segments. To do so, he can choose from a range of more than fifty Digipass authentication products, ranging from one button token, web and mobile phone authentication mechanisms and card readers.

Frederik Mennes,
Security Architect at VASCO Data Security

Learn how to protect your online banking users from Man-in-the-Middle attacks.

Attend one of our upcomming Banking Summits.

Get an overview at: www.vasco.com/events

About VASCO

VASCO designs, develops, markets and supports patented DIGIPASS®, DIGIPASS PLUS®, VACMAN®, IDENTIKEY® and aXSGUARD™® authentication products for the financial world, remote access, e-business and e-commerce. With tens of millions of products sold, VASCO has established itself as the world leader in Strong User Authentication for e-Banking and Enterprise Security for blue-chip corporations and governments worldwide.

www.vasco.com

BRUSSELS (Europe)
phone: +32.2.609.97.00
email: info-europe@vasco.com

BOSTON (North America)
phone: +1.508.366.3400
email: info-usa@vasco.com

SYDNEY (Pacific)
phone: +61.2.8061.3700
email: info-australia@vasco.com

SINGAPORE (Asia)
phone: +65.6323.0906
email: info-asia@vasco.com

Copyright © 2009 VASCO Data Security, Inc. VASCO Data Security International GmbH. All rights reserved. VASCO®, Vacman®, IDENTIKEY®, aXSGUARD™™, DIGIPASS® and Digipass® logo are registered or unregistered trademarks of VASCO Data Security, Inc. or VASCO Data Security International GmbH in the U.S. and other countries. VASCO Data Security, Inc. and/or VASCO Data Security International GmbH own or are licensed under all title, rights and interest in VASCO Products, updates and upgrades thereof, including copyrights, patent rights, trade secret rights, mask work rights, database rights and all other intellectual and industrial property rights in the U.S. and other countries. Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation. Other names may be trademarks of their respective owners.