Do you have something to say about this article?
Visit the Journal pages of the ISACA web site (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

The popularity of online banking has been on the rise. In 2005, Bob Sullivan of MSNBC quoted research figures from the Pew Internet and American Life Project, which showed that 53 million US citizens were banking online in 2004, and that online banking was the fastest growing Internet activity.1 Now about eight years later, the customers subscribing to online banking services have increased worldwide—accompanied by threats and vulnerabilities. Hackers, fraudsters and other individuals with malicious intentions present numerous threats to online banking. These adversaries have led banks to adopt security countermeasures. Countermeasures adopted include (but are not limited to): ensuring that customers use strong passwords, providing virtual keyboards for entering login passwords, Secure Sockets Layer (SSL) encryption, sending customers information on how to avoid falling prey to malicious attackers and implementing two-factor authentication. One method adopted by adversaries to counter banks’ security measures for online banking is man-in-the-browser (MITB) attacks, which can grant success to an attacker despite the aforementioned countermeasures, especially two-factor authentication.

TWO-FACTOR AUTHENTICATION
Many individuals have come to view two-factor authentication—the use of tokens and one-time passwords (OTPs)—as the ultimate solution in online banking security measures, a sort of holy grail for online banking security. Why is that so?

Fraud figures decreased significantly with the advent of two-factor authentication.2 A hacker, for example, might be able to crack a customer’s login password, regardless of its strength, using commonly available tools, or could obtain login credentials through spear phishing, but if a token is required to effect a transaction, hackers would be unable to proceed unless they are in possession of the token. In the case of OTPs being received as a text message (via SMS) on a customer’s mobile phone, the hacker would have to have access to the mobile phone as well. (A hacker could also hack into the mobile phone; however, the probability is low that this type of attack would be used.) Hence, two-factor authentication has resulted in a significant reduction in the possibility of fraud being successful—providing a feeling of security for both the bank and the customer.

Then, MITB attacks came along.

MAN-IN-THE-BROWSER ATTACKS
An MITB attack is essentially a man-in-the-middle (MITM) attack, but unlike typical MITM attacks, which usually occur at the protocol layer, MITB attacks are introduced between the user and browser.3 Malware, especially Trojans, is used to infect the browser. The malware is normally installed when a user clicks on an applet on a web site that he/she is duped into clicking because it claims that an update or other similar action is needed.4 MITB malware is mostly undetectable by current antivirus software, although it may be detected if protection levels are set very high, which would also inhibit many innocuous programs. MITB modifies a user’s content when an online banking site is visited by adding extra fields to the page in order to compromise second authentication mechanisms.5 In an MITB attack, the customer initiates a transaction, the attacker modifies the transaction using compromised credentials, the extra fields added by the malware alert the attacker and give the hacker control of the online banking interface, consequently manipulating the statement and account balance to reflect the customer’s intended transaction. Once the user uses a token to generate an OTP or receives it in a text message, the user enters the code and unknowingly authorizes the manipulated transaction thinking it was the correct one.

An illustration6 of this scenario is the fictional Mr. Ojo who, with a balance of US $2,500 in his account, logs into his bank’s online banking site to make a transfer of US $500 to his wife, who holds account number 12345. An MITB

©2013 ISACA. All rights reserved. www.isaca.org
attacker intercepts the transaction and transfers US $2,000 to an accomplice, who has account number 54321. Data are manipulated to show the customer that he is transferring US $500 to account 12345 and the balance left in his account is US $2,000. To complete the transaction, Ojo needs to enter the OTP sent to his mobile phone; when completed, his online banking dashboard shows that he has successfully transferred US $500 to account 12345 and his balance is US $2,000. He receives an SMS alert to that effect, and his month-end statement says the same. Unfortunately, in reality, Ojo authorized a transfer of US $2,000 to account 54321 and his available balance is US $500.

MITB attacks are expensive to carry out; therefore, they are usually performed by well-funded and organized criminals. These criminals mostly target corporate account holders with high-volume transactions.

MITB MITIGANTS
There are various methods for combating MITB attacks. The most effective weapons against MITB attacks are education and awareness. For example, MITB malware often requests logon credentials and a second-factor authentication mechanism to “train a new security feature” in order to compromise an account. Banks should inform their customers not to pay heed to such requests or seek further clarification from the bank before clicking on such a pop-up request. Customers should also generally avoid clicking update requests for any software without confirming the genuineness of such prompts. Some telltale signs of an MITB attack in progress include transactions taking longer than usual, a system slowing down and logon credentials being requested where they were not before.

Another preventive measure for online banking interfaces is the bank sending a confirmation message (e.g., an SMS, email, call) to the customer describing the transaction to be consummated and requiring a confirmation within the next few minutes to accept it. It may be that the confirmation message comes with the OTP and entering the OTP is the way to confirm that the transaction is good. In the case of customer Ojo, he would receive an SMS with the OTP stating that he is about to transfer the sum of US $2,000 to (the hacker’s accomplice’s) account 54321. This would alert Ojo of the fact that something is wrong, and he can then stop the transaction and report it to his bank. However, this measure would be at risk if the attacker also compromises the customer’s mobile phone and modifies the confirmation message that would enable the customer to complete the transaction. Additionally, the attacker may also modify the confirmation message by means of the malware, as he did the statement and balance on the account.

Behavioral pattern monitoring can also provide an adequate deterrent to the success of MITB attacks. This involves server-side monitoring of customers’ transactions. Changes in the normal pattern of transacting, location within a session (e.g., change in IP address) or having multiple sessions within a very short time frame are possible indications of a criminal action, at which time the bank would hold the transaction and alert the customer of the possible compromise. Criminals and other malicious individuals are always developing means to ensure that they are at least one step ahead of their targets; therefore, there is a need for constant monitoring and testing to avoid having that gap in any transaction.

CONCLUSION
A combination of customer education and awareness, use of confirmation alerts, and behavioral monitoring can provide an effective protection from MITB attacks and provide some margin of safety for online banking. These suggested measures of facing MITB are, by no means, exhaustive or infallible; other viable solutions are available.

Further research can be performed by banks and information security experts to solve the problem and ensure better protection against MITB attacks. The first line of defense remains awareness: banks educating their customers to avoid clicking on unusual requests claiming to be required for some form of update or the other. Customers should always seek clarification from their banks when they observe something different from what they are used to in their online transactions.
banking interface. They should also raise alarms if their online banking transactions appear to be taking longer than usual to consummate, as this could be an indication that an MITB attack is in progress.

For their part, banks should also be more observant of customer transactions by closely monitoring behavioral patterns of customer transactions. This would enable them to track down any anomalies. Summarily, extra vigilance by both customers and banks can go a long way in mitigating against MITB attacks on online banking transactions.

REFERENCES


ENDNOTES
1 Sullivan, Robert; “Click! Online Banking Usage Soars,” MSNBC.com, 2005, www.msnbc.msn.com/id/6936297/ns/business-online_banking/t@click-online-banking-usage-soars/#.T_f1KbXZCV8


6 The illustration is entirely fictitious; names and figures used do not refer to any existing people.


10 Op cit, Kelly

11 Op cit, Entrust Inc.