2011 FFIEC Authentication Guidance: A New Standard For Online Banking Security

PhoneFactor, Inc.
7301 West 129th Street
Overland Park, KS 66213
1-877-No-Token / 1-877-668-6536
www.phonefactor.com

2011 FFIEC Authentication Guidance: A New Standard For Online Banking Security

The long overdue update to the FFIEC Guidance on Authentication in an Internet Banking Environment, released in June 2011, sets a new standard for online banking security. Since the last update in 2005, the online banking threat landscape has changed dramatically, creating a significant gap between the FFIEC recommendations and those security measures that are actually effective in mitigating online banking fraud. As a result, financial institutions and their customers are at risk and fraud rates have spiked.

The latest FFIEC Authentication Guidance requires a fundamental change in the way financial institutions approach online banking security. The Guidance calls for a layered security approach which extends security controls beyond logins to transactions and administrative changes. It also calls for stronger authentication, and recommends out-of-band methods as a means to protect against today's online banking threats. Examiners will begin using the updated Guidance in January 2012, giving financial institutions less than six months to implement enhanced security controls.

This whitepaper provides an overview of the updated Guidance as well as the threat landscape which helped define it. This whitepaper also examines why the security measures specified in the 2005 Guidance are no longer effective, and why methods like out-of-band authentication with transaction verification are key to protecting online banking today.

Contents

Overview Of 2011 FFIEC Authentication Guidance

The Federal Financial Institutions Examination Council (FFIEC) is an interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. It is comprised of members from the Federal Reserve Bank (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), Mergers & Acquisitions International Clearing (MAIC), and the Consumer Financial Protection Bureau (CFPB). Its purpose is to make recommendations to promote uniformity in the supervision of financial institutions. In 2001, the FFIEC issued a guidance entitled Authentication in an Electronic Banking Environment, which was subsequently updated in 2005 as Authentication in an Internet Banking Environment. The guidance provided a recommended framework for evaluating risk and the application of authentication systems and practices.

The 2005 Guidance called for the use of strong and multi-factor authentication methods to defeat attacks such as password phishing, which were widely employed by attackers to steal online banking credentials and hack into accounts. The 2005 Guidance had a significant impact on online banking and resulted in widespread use of technologies such as device identification, challenge questions and one-time password tokens, particularly for commercial accounts.

The threat landscape has changed dramatically since 2005, and in June 2011 a supplement to the Guidance was issued that provides an updated view of today's more sophisticated threats and the security controls which are effective in protecting against them. Whereas the 2005 Guidance focused on stronger authentication of online banking logins, the 2011 Guidance instead calls for a layered approach. The Guidance recommends layering multiple security controls for enhanced protection, and requires financial institutions to extend security controls beyond account logins to funds transfers and administrative functions. The use of out-of-band verification for transactions was recommended as an effective control against these attacks.

In addition, the update calls for an overall strengthening of authentication technologies. According to the 2011 Guidance, out-of-band authentication has taken on a new level of importance given the preponderance of malware on customer PCs, which can defeat OTP tokens, device identification, challenge questions, and many other forms of strong authentication. In particular, closed loop methods that complete the authentication in the out-of-band channel are seen as offering a greater level of security.

Bank examiners will begin using the updated Guidance in January 2012, providing less than six months for financial institutions to become compliant.

The Current Threat Landscape

In 2005 password phishing was the principal online banking threat. Today malware dominates the threat landscape. Security researchers found malware targeting online banking on computers at 90 percent of the Fortune 500. Reports indicate that as much as 50 percent of malware goes undetected by anti-virus and anti-malware software.

Malware has evolved beyond simple keylogging functions to perform sophisticated real-time attacks. Unlike passive attacks, such as phishing or keylogging schemes that are used to obtain account credentials for use by the attacker at a later time, Man-in-the-Middle (MITM) and Man-in-the-Broswer (MITB) attacks target live online banking sessions. Attackers use malware running on the user's computer to infiltrate active online banking sessions and transfer funds to "mule" accounts through ACH, wire transfers, payroll and bill payments. MITM/MITB attacks defeat security questions, device IDs, certificates, one-time passcodes from hardware and software tokens, and most other security measures.

In addition to being seen as the greatest threat to online banking today, real-time threats from malware were ranked as the most prevalent attack for banks who participated in the recent Online Banking Security Survey conducted by PhoneFactor. Today, malware targeting online banking is responsible for millions of dollars in fraudulent financial transactions each month. Cybercriminal groups are making national headlines for leveraging malware like ZeuS, SpyEye, and their countless variants, to perpetrate fraud. For every crime ring that is busted, countless other groups are actively launching new attacks.

Existing Security Measures Fall Short

As the number of malware-infected computers grows exponentially, measures that rely on end point security have increasingly become ineffective. Because malware like ZeuS runs on the same computer the end user is logging in from, the attacker can hijack a user's banking session without being detected by the online banking application or the end user. The user logs in as he normally would with a username and password. Once the user is authenticated, so is the attacker. The attacker can initiate new transactions, such as ACH and wire transfers, and reroute the user's valid transactions to "mule" accounts. In some cases, the attacker just takes over the user's session and displays a message to the user that the banking website is currently unavailable.

Malware is impervious to one-time passcode technologies and most other strong authentication methods available today. Security tokens and SMS text methods that require a user to enter a one-time passcode into the banking website are easily defeated by MITM/MITB attacks. The attacker simply intercepts the passcode or injects itself into the banking session after the passcode has been entered.

In addition, malware is increasingly designed to target a computer's operating system, making it extremely powerful and difficult for antivirus software to detect and remove. This class of malware also defeats browser plug-ins and other software-based methods that try to lock down the online banking session. The malware simply subverts the software that is intended to protect against it.

A Layered Security Approach Is Required

Given the sheer number of attack vectors, the FFIEC is requiring that financial institutions adopt a layered approach to security. Layered security is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control. Effective controls include:

- Fraud Detection and Monitoring
- Dual Authorization
- Out-Of-Band Transaction Verification
- Transaction Limits, Such as Transaction Value Thresholds, Allowable Payment Windows, Etc.
- IP Black List
- Policies For Addressing Devices And Customers Who May Be Facilitating Fraud
- Enhanced Control of Administrative Activities
- Customer Education

As part of a layered security program, the application of these security controls must extend beyond the account login to the initiation of funds transfers, such as ACH and wire transfers. Because malware is capable of infiltrating authenticated sessions as described, it is no longer sufficient to simply authenticate the user's online banking login. Authentication is a fundamentally important part of a secure online banking system. It establishes the first level of trust between the bank and the end user upon which all other layers of security are built. And while this remains a critical security measure, it must be coupled with transaction-level verification.

The application of simple business rules, such as transaction type or amount, or more sophisticated methods, such as behavioral patterns and other non-device based criteria which are harder for attackers to mimic, can be used to identify anomalous transactions. By requiring the user to approve anomalous transactions, a fraudulent ACH or wire transfer can be stopped before it is processed. This

provides a last line of defense. Even if the user's authenticated session is compromised, the attacker will be unable to complete a transaction without the approval of the account holder.

In addition, the 2011 Guidance requires enhanced security for administrators of business accounts. Administrative functions, such as access levels and transaction limits, should be subjected to greater scrutiny and additional authentication. In particular, the Guidance recommends out-of-band authentication and transaction verification to confirm administrative changes.

Out-Of-Band Takes On A New Level Of Importance

The 2011 Guidance points out that out-of-band authentication has taken on a new level of importance given the preponderance of malware. With existing measures failing to protect against malware, focus has shifted to out-of-band methods that use a separate channel for authentication. Out-of-band authentication methods, such as a phone call or closed loop text message, circumvent malware running on the user's computer. Out-of-band authentication, particularly when coupled with transaction verification, is recognized by the FFIEC Guidance as effective in mitigating online banking fraud.

For example, PhoneFactor places an automated phone call or sends a text message to the user's registered phone number to verify online transactions. The transaction details are provided as part of an automated phone call, such as, "This is Your Bank calling to verify the transfer of $50,000 to account 10015 at Bank of Nigeria," or are alternately provided in the text message. If the transaction is valid, the user simply presses # (or a PIN) or replies to the text message to approve the transaction. If the user does not answer the call or respond to the text message, the transaction is denied or flagged for further review. Because the transaction is verified across the telephone network (there are no passcodes to enter into the banking website), it is completely out-of-band and not vulnerable to MITM attacks.

Summary

As the sophistication of attacks evolve, so do the countermeasures necessary to mitigate them. Financial institutions that have failed to conduct regular security reviews and update their security controls accordingly, as recommended by the FFIEC, will need to act swiftly to enhance their security policies and systems to meet the updated Guidance by January 2012. Institutions whose primary focus to date has been on session authentication will need to expand the scope of their security measures to also include funds transfers and administrative functions. For

many, this will involve migrating away from OTP tokens, which have proven to be vulnerable to attack, and even some forms of seemingly out-of-band authentication that deliver an OTP via an out-of-band channel. Instead, financial institutions will need to look to other methods, such as fully out-of-band technologies that can be used to verify logins, transactions, and administrative functions and offer protection from keyloggers and MITM/MITB attacks.

About PhoneFactor

PhoneFactor is the leading global provider of phone-based authentication. The company's award-winning platform is trusted by leading organizations to secure millions of logins and transactions each year. PhoneFactor provides strong, closed-loop out-of-band security and is extremely user-friendly. It works with the customer's existing phone and can be used to secure online banking transactions, such as ACH, wire transfers, and payroll payments, as well as account logins. There are no devices to mail or certificates to install, so set up and deployment are quick and easy. No user training is required, and there is very little ongoing user support. PhoneFactor was recently named to the Bank Technology News FutureNow list of the top 10 technology innovators securing the banking industry today and a finalist in the SC Magazine Reader Trust Awards.

For more information, contact PhoneFactor at ***877.No.Token (877.668.6536)*** *or visit our website at* ***www.phonefactor.com.***