Man-in-the-Browser
Understanding Man-in-the-Browser Attacks and Addressing the Problem
Table of Contents

Introduction.......................................................................................................................... 3
The Risk Inherent in MITB Attacks ................................................................................... 3
Keeping One Step Ahead of Cybercriminals................................................................. 4
SafeNet Solutions for Combating Man-in-the-Browser Attacks................................. 5
MobilePASS SMS Authentication Solutions: .............................................................. 5
eToken NG-FLASH with Onboard Portable Browser................................................... 6
About SafeNet..................................................................................................................... 6
Introduction

The losses attributed to financial fraud are alarming. The financial services industry has become a primary target of cyber attacks on a global scale and, in 2009 alone, suffered losses totaling $54 billion - an increase from $48 billion in 2008. Of equally grave concern to financial services institutions is the damage cybercrime can cause to reputation, along with customer churn, both of which can have a significant impact, and possibly devastating, effect to revenue.

While all types of cybercrime have been on the rise, there has been a sharp increase in financial fraud resulting from computers infected with malware. Malware typically targets desktop computers and relies on social engineering to induce unsuspecting home users to download and install malicious code on their computers.

One of the most dangerous types of malware for online banking and financial services are Man-in-the-Browser attacks. A Man-in-the-Browser attack occurs when malicious code infects an Internet browser. The code modifies actions performed by the computer user and, in some cases, is able to initiate actions independently of the user. When a user logs onto their bank account, using an infected Internet browser is enough to trigger illicit transactions that result in online theft.

The Risk Inherent in MITB Attacks

Man-in-the-Browser attacks are especially hard to detect and, in many cases, succeed in causing damage completely surreptitiously. Following are some of the ways in which MITB attacks occur and why they pose such a high risk.

• **Computers are Easily Infected:** The most common way for Internet browsers to become infected with malware is through social engineering. Often, when browsing or downloading media and other files, users are prompted to install updated versions of software. These requests are so ubiquitous that many users automatically accept. It is exactly this instinctive behavior that cybercriminals utilize. They create download prompts that closely resemble those of legitimate software vendors. Most users don’t notice the fine differences and approve the download, unwittingly infecting their browsers with malware.

The huge surge in the use of social networking platforms has also been a boon for cybercriminals spreading malware. Indeed, more than one-third of malware attacks in the second half of 2009 were carried out through social networking sites.

• **Hard to Detect:** Malware is hard to detect because malware developers use toolkits to morph and customize it for a given target. This high level of customization – sometimes for a specific country or bank – means that virus filters, which are developed for more generic virus types, do not recognize the malicious code.

• **Traditional Strong Authentication Doesn’t Help:** Strong authentication validates that a person logging on to an online resource is indeed who he or she claims to be. With Man-in-the-Browser attacks, a user can be successfully authenticated regardless of the fact that malicious code is active in the browser. When the user carries out an online transaction, the infected browser carries out illicit transactions covertly - neither the customer, nor the bank, are aware that anything irregular is happening.

• **Traditional Anti-Fraud Mechanisms and Risk-based Tools are Not Effective:** Risk-based anti-fraud tools focus on user authentication and transaction validation by requiring customers to answer a set of pre-determined security questions, and by analyzing user behavior and banking patterns. They have no way of detecting whether a transaction was initiated by malware or not.
Keeping One Step Ahead of Cybercriminals

Ensuring customer trust and the integrity of their online banking services, as well as reducing monetary loss caused by online fraud, are of utmost importance to financial institutions. Although malware is on the rise, the good news is there are concrete steps financial institutions can take to mitigate the risk of Man-in-the-Browser attacks. Following are some security measures that banks can implement today to protect their customers, uphold their reputations, and reduce monetary loss.

- **Out-of-Band (OOB) Authentication and Transaction Verification**
  OOB authentication and transaction verification requires that an information channel other than the customer’s PC computer and browser be used to deliver the transaction confirmation data and the passcode required to validate a transaction. A common form of OOB authentication is delivering a SMS passcode together with the details of the transaction to a user’s mobile phone so the user can confirm that the transaction details are correct.

  When an online transaction is initiated via the customer’s account, the bank sends an SMS containing a passcode and the details of the transaction to the customer’s mobile phone. Only after the customer acknowledges the transaction by entering the one-time password onto the online banking portal can the transaction go through.

  Although SMS authentication does not prevent malware from infecting browsers, it does utilize a secure channel of communication in order to alert bank customers to activity taking place in their bank account. If customers receive an SMS alert that an online transaction is taking place, they will either approve the transaction or notify the bank that the activity was not initiated by them.

- **Certificate-based Authentication Combined with a Secure Browsing Environment**
  Another way of protecting against Man-in-the-Browser attacks is to use certificate-based strong authentication together with a secured browsing environment that has additional measures to secure the browser from getting infected with malware. For example, by using a portable browser stored on a USB authentication token, the likelihood of a browser getting infected with malware is reduced. In this case, when going online, the user first authenticates himself and then loads the “clean” browser directly from the token. The trusted browser can be pre-configured to open a specific Internet site and can block any attempt to browse to other undesigned sites.

  Trusted browsers constitute a pre-emptive security measure against malware. Since the browser is stored on an external flash memory device and protected by a security shell, it is insulated from regular online interaction and, therefore, not exposed to malware.

**Most Targeted Sectors for Cybercrime, Q3 2009**

![Pie chart showing the most targeted sectors for cybercrime in Q3 2009. Payment Services 33%, Other 13%, Financial 39%, Retail 2%, Auction 13%. Source: Anti Phishing Working Group.](image)
SafeNet Solutions for Combating Man-in-the-Browser Attacks

SafeNet's broad range of strong authentication solutions include both SMS OOB authentication and Secure Browsing solutions necessary for preventing financial fraud that can result from Man-in-the-Browser attacks.

MobilePASS SMS Authentication Solutions

SafeNet’s MobilePASS family of One-Time-Password (OTP) and SMS software authentication solutions combines the security of two-factor authentication with the convenience and simplicity of mobile devices and SMS messages. MobilePASS’s innovative technology delivers one-time passcodes via short message service (SMS) to mobile phones, enabling transaction verification and allowing online banking customers to validate online transactions.

1. User carries out online transaction on their online bank portal

2. Bank sends transaction details and a one-time passcode to the user via SMS

3. User approves the transaction by entering the passcode on the bank portal

4. Bank confirms the transaction

MobilePASS Benefits

• Zero footprint (no software installation)
• Reduced TCO and deployment costs – no hardware to buy or distribute - the mobile phone that users carry with them all the time turns into a “hardware” token
• Easy deployment and setup for financial organizations
• Supports any device
• Easy and convenient for end users
• Flexibility of moving between devices (for people who change phone models)
• Perfect as backup and in case of emergency
• Ideal as a temporary alternative for lost tokens
eToken NG-FLASH with Onboard Portable Browser

eToken NG-FLASH with a portable browser is a secure, zero-footprint certificate-based USB strong authentication token with onboard Flash memory. It features a portable Web browser that runs from the encrypted flash memory of the eToken NG-FLASH device for secure access to Web applications.

eToken NG-FLASH with portable browser offers an all-in-one Web access security solution that reduces the risk of malware exposure:

**Browser Integrity** - Running a portable browser application from the eToken NG-FLASH ensures that a clean and non-infected browser image is used to access sensitive Web applications. Storing the browser on a read-only memory partition of the eToken NG-FLASH device protects the browser from tampering.

**Browser Process Protection** - When integrated with a hardened third-party browser, employing memory and process protection measures prevents malware that is already residing on the PC from infecting the browser at execution time, and from manipulating sensitive data when the browser is running.

**Multi-Factor Authentication** - eToken NG-FLASH positively verifies the identity of the user and secures the communication channel between the browser and the Web application using SafeNet’s SSL client-certificate authentication.

---

**eToken NG-FLASH Portable Browser Benefits**

- Comprehensive access security solution that authenticates users and prevents all forms of cyber attacks including:
  - phishing
  - pharming
  - Man-in-the-Middle
  - Man-in-the-Browser
- Plug-and-play convenience for end users: no administrator rights or installation required, the portable browser launches automatically once plugged into the user’s USB port
- Flexibility and portability – eToken NG-FLASH can be used on any computer with an Internet connection and USB port
To learn more about SafeNet Authentication Solutions for Financial Services, visit www.SafeNet-Inc.com/authentication

About SafeNet
SafeNet is a global leader in information security, founded more than 25 years ago. The Company protects identities, transactions, communications, data, and software licensing through a full spectrum of encryption technologies, including hardware, software, and chips. More than 25,000 corporate and government customers in 100 countries, including UBS, Nokia, Fujitsu, Hitachi, Bank of America, Adobe, Cisco, Microsoft, Samsung, Texas Instruments, the U.S. Departments of Defense and Homeland Security, and the U.S. Internal Revenue Service, trust their security needs to SafeNet. In 2007, SafeNet was acquired by Vector Capital, a $2 billion private equity firm specializing in the technology sector. For more information, visit www.safenet-inc.com.