Catching the fraudulent 'Man-in-the-Middle' and 'Man-in-the-Browser'

There is mounting pressure on companies to detect fraud perpetrated by the new generation of cyber-fraudsters who are becoming adept at impersonating genuine customers – by being the Man-in-the-Middle or the Man-in-the-Browser. Ori Eisen, founder and Chief Innovation Officer of 41st Parameter, explains this new threat to data security and describes how DeviceInsight technology can help to detect where fraudsters are operating in this way.

Fraud rings have always been relatively sophisticated criminal outfits – they systematically break down the defences of organizations such as banks and retailers to get the information they need. As e-business grows, these fraud rings are becoming increasingly innovative in the way they perpetrate crimes. Cyber-criminals are becoming adept at defrauding customers – by being the Man-in-the-Middle (MITM) or the Man-in-the-Browser (MITB).

Virtual technologies, more successful phishing techniques and increasingly realistic imitations of genuine customers mean that prevention and detection measures need to be more effective. The first step is for businesses to understand what they are facing.

Fighting the “Man-in-the-Middle”
MITM defrauds consumers by hijacking genuine interactions. Using a proxy computer / web page, the fraudster will control the session, with the end-user having no knowledge of any wrong-doing. A website, for example, that has the look and feel of a genuine bank or a retail store page enables the fraudster to act as a middleman – taking whatever ‘commission’ he likes. Account information is disclosed during this process, which, of course, can be phished for further fraud.

There are two powerful mechanisms acting to stop MITM attacks. The first is device identification software, coupled with risk engines that assess the validity
of interactions. If these risk engines detect two devices within the same session ID, then they can escalate the situation. The MITM can be cut out by companies that capture the unique ID of every device (PC, tablet, mobile phone, etc) visiting their site and then use unique algorithms to analyse and link multiple-user sessions.

The second mechanism is campaigning, on the part of visible banking / retail brands as well as government agencies, to raise awareness of such schemes as MITM attacks. Because of these initiatives, customers are now more able to identify clearly suspicious websites and are less likely to fall into traditional traps, such as following links in spam emails.

As MITM has become more easily recognised, fraudsters have had to innovate their approach. Using similar basic principles, many have happened upon a technique that is far harder to detect – Man-in-the-Browser (MITB).

**Meet the new man on the block: Man-in-the-Browser**

MITB is harder to detect because he allows the end-user to link to the genuine website. Achieving the same end result as MITM, the MITB is able to hijack the genuine user’s session. As such, MITB is able to operate with a large amount of freedom.

MITB lets a customer initiate a transaction with the genuine website, then the fraudster controls what is submitted, alters key details and defrauds the account. That means that deliveries can be re-directed to new addresses and additional items can also be put onto a shopping list. With control over the user’s device, entirely new transactions can be initiated – particularly where fraudsters interrupt the sign-off process and, by doing so secure themselves unlimited use of the client’s account.

The fraudster hijacks the user’s machine, not simply their web session. This means that many device identification technologies are rendered useless. Sophisticated risk engines must be in operation to assess any out-of-the-ordinary and high risk activity. Any transaction deemed to be an improbable course of action for the genuine user will get passed to the investigator, who can escalate the situation accordingly.

Some items the risk engines will look out for include velocity checks – how often does the user log into the account, and are the times of log-in consistent with the user’s natural behaviour? A change in order validation details or new ACH transfers / new payees can all be signs that something fraudulent is occurring.
MITB uses malware, such as Trojans, to seize control of users’ machines. Trojans will secretly install themselves and then appear to perform a certain action but in fact perform something completely different. They can get into the system either by bundling in with a genuine download, or alternatively by crawling through the computer’s back door – without the user knowing they’ve downloaded anything.

One of the more effective methods for stopping MITB is by educating online consumers on the extent of the threat. The malware has to enter the user’s computer somehow, so if users are made aware of how this can happen, it is less likely MITB will be effective. Properly maintained firewalls and scanning of all downloads will significantly reduce a user’s risk of being a victim.

**Hijacking a Wide Area Network**

There is also another emerging fraud scheme, sometimes known as the Man-at-the-End-of-the-Line – which entails a fraudster hijacking a Wide Area Network that many customers use for online shopping. By doing this, the fraudsters are able to channel many transactions through their systems to capture information. With VPN Tunnelling there are essentially rooms full of hired fraudsters, paid to channel illegal transactions through other devices. They will capture identities and then use their own machines as proxies, just like with MITB.

The solution to stopping these attacks is a combination of the two previous approaches. Risk assessment software should always be active and may pick up inconsistencies, but multiple devices could also be picked up – depending on the precise techniques being used.

The challenge the industry faces is making fraud detection systems quicker and more sophisticated than the fraudsters. These new systems must pick up characteristics that are individual to each user. Technology systems must enable businesses and banks to enhance qualification processes and detect with even greater accuracy whether the instigator of a transaction is who they say they are. If companies can monitor suspicious transactions throughout their time in the system and gather more evidence of whether they are fraudulent or valid, then detection rates will be higher and customers will not be hindered by overly aggressive policing. All this re-enforces the need for multiple layers of fraud detection and prevention within the system.

**A layered approach to fraud prevention**

Criminals have many different techniques that enable them to infiltrate poorly protected corporate networks. These numerous threats mean that businesses must employ a layered fraud prevention approach in order to cut out the multiple entry points that fraudsters can attack.
A perimeter approach may be effective for stopping the majority of fraudsters, but without anything patrolling inside those boundaries, anyone who can break the fence will be left unabated to terrorise the system from the inside. Multiple layers of prevention and detection mean that even if one line of defence is beaten, the information within the system is not compromised.

It is vital to remember that MITM and MITB are only two of the techniques that cyber-fraudsters use. An organisation’s defences need to be made strong through a multi-layered approach. And just to make things more difficult – the measures deployed must not restrict or deter genuine users from navigating and using the system.

###

**About the author**

Ori Eisen has spent the last fifteen years in the information technology industry, and is respected for his business knowledge and leadership. His background includes an in-depth application of innovative solutions for preventing business to consumer e-commerce fraud.

Prior to launching 41st Parameter, Mr. Eisen served as the Worldwide Fraud Director for American Express focusing on Internet, MOTO and counterfeit fraud. During his tenure with American Express, Mr. Eisen championed the project to enhance the American Express authorization request to include Internet specific parameters.

Prior to American Express, Mr. Eisen was the Director of Fraud Prevention for VeriSign/Network Solutions. By developing new and innovative technologies, he skillfully reduced fraud losses by over 85 percent in just three months.

Mr. Eisen has an extensive background in developing system infrastructure and implemented solutions, and he is highly regarded in the information and payment technologies industry as a noted leader and technology innovator. Based on this reputation Mr. Eisen is often quoted by industry insiders, and receives numerous invitations to appear as a keynote speaker for industry events and conferences. Mr. Eisen is a founding member of the Merchant Risk Council and is currently serving on the Americas Advisory Board.