Identifying, Mitigating Man-in-the-Middle (MitM) Attacks

Executive Summary

To complete online banking transactions, consumers key-in credentials to authentic their identities and gain website access to a host of personal data and various banking applications. But there is always a possibility that a criminal is lurking in cyberspace or on the public phone network to intercept these details using Man-in-the Middle (MitM) attack techniques. This white paper explains the MitM concept, highlights Man-in-the-Browser (MitB) and Man-in-the-Phone (MitP) attack techniques, and offers actionable advice to consumers and banks on ways to detect and mitigate the impact of such fraudulent intrusions.

Man-in-the-Middle Attack

The Man-in-the-Middle attack (often abbreviated MitM) is a form of active eavesdropping in which the attacker makes independent connections with the victims (typically end users and banks) and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.

To succeed, the attacker must intercept all messages transmitted between the two victims and substitute new ones.

A MitM attack can only succeed when the attacker can impersonate each victim to the satisfaction of the other. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MitM attacks. For example, SSL authenticates the server using a mutually trusted certification authority.

Typically during the attack, the attacker lures the end user to a fraudulent site via phishing, DNS attacks, or other methods. Once there, the attacker utilizes vulnerable authentication methods (e.g., username/password, tokens) to attack and replay the session – thus "stealing" the legitimate user's ID. One way to prevent MitM attacks is to authenticate both the client and server. The technology to implement a safe transaction utilizes x.509 certificates in a public key infrastructure deployment.

While MitM breaches have plagued online banking for some time, a new and more insidious twist involves the Man-in-the-Browser (MitB) and Man-in-the-phone (MitP) attacks. Let's have at look at these forms of attack.

Man-in-the-Browser

Man-in-the-Browser (MitB) is a Trojan (e.g., non-self-replicating malware) that infects a Web browser and has the ability to modify pages,

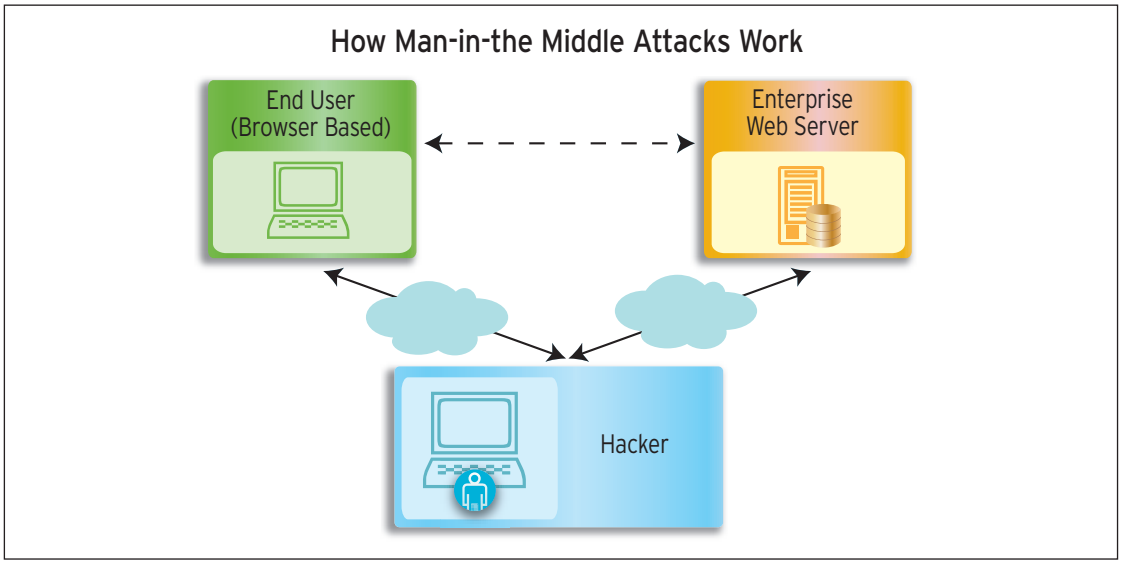

Figure 1

modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and host application. A MitB attack can succeed irrespective of whether security mechanisms such as SSL/PKI and/or two- or three-factor authentication solutions are in place. The only way to counter a MitB attack is by utilizing transaction verification[1,2].

The MitB Trojan works by utilizing common facilities provided to enhance browser capabilities such as browser helper objects etc., and is therefore virtually undetectable to virus scanning software. For example, in an Internet banking transaction such as a funds transfer, the customer will always be shown, via confirmation screens, the exact payment information as keyed into the browser. When a MitB Trojan is applied to the transaction, the bank receives materially altered instructions (i.e., a different destination account number and possibly amount). The use of strong authentication tools primarily authenticates the validity of identity credentials and creates an increased level of false confidence on the part of both customer and bank that the transaction is secure.

An example of a MitB threat is Silentbanker. Silentbanker is a Trojan horse that records keystrokes, captures screen images, and steals confidential financial information to send to the remote attacker.

One of the most effective methods in combating a MitB attack is through an Out-of-Band (OOB) transaction verification process. This overcomes the MitB Trojan by verifying the transaction details, as received by the host (bank), to the user (customer) over a channel other than the browser; typically an automated telephone call. OOB transaction verification is ideal for mass market use since it leverages devices already in the public domain (e.g., landline, cell phone, etc.) and requires no additional hardware devices, yet it enables "three-factor" authentication (utilizing voice biometrics), transaction signing and transaction verification.

Here's how a typical MitB attack works:

- Victim accesses the bank's website to perform an online banking transaction.
- Enters Username for Identity authentication.
- Enters PIN details and submit request.
- Typically as the page is rendered, software now resident in the victim's browser wakes up (This malicious bit of code was installed unknowingly on his machine (during the download of a screen saver or video clip).
- This software inserts few additional lines into the code – maybe five lines of JavaScript – an alert box, a timer function, and maybe some in-page content -and sends a message to the hacker, far away.

- What happens next looks perfectly normal. Upon loading, the alert box pops up – something like the dialog box pictured below – and says "Server synchronization in process... please be patient", accompanied by an animated GIF in the bank's colors.
- Except at that moment, as the victim watches the seconds pass, a hacker somewhere is receiving a timely message that the victim has started an authenticated session and is ready to transact, using the credentials contained in the message.
- The hacker gets all the essential details and can login as the victim and move funds.
- And sometimes, the crimeware is configured in such a way that it allows the hacker session to kick in when the victim "logs out".

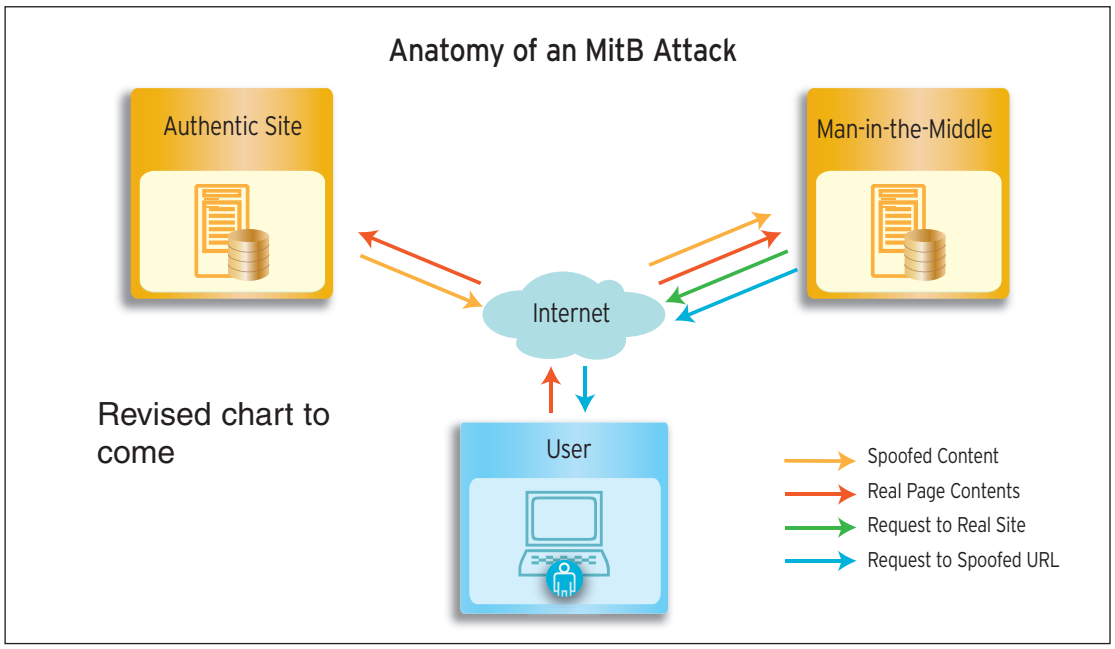

Figure 2

Man-in-the-Phone

Telephone banking customers and banks need to be aware of a new low-tech, Man-in-the-Phone (MitP), fraud technique being employed by criminals.

MitP scams have observed at several large retail banks. These scams appear to have originally targeted British banks but this fraud is now spreading to the U.S. and Canada.

MitP blends new and old fraud techniques to trick banking customers into authorizing transactions via the phone channel. MitP builds on the successes realized from MitB attacks in which criminals use Trojans to infect users' Internet browsers to modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and host application. MitP also leverages "social engineering," by using trickery or deception during a phone conversation to convince an individual to divulge information.

Here's how a typical MitP attack works:

- In a typical MitP attack, a fraudster impersonates a bank representative and calls the banking customer to inform him/her that his/her savings, checking or card account may have been breached or compromised.
- The fraudster advises the customer that to remedy the situation he/she should remain on the line and verify a few account details.
- At the same time, the fraudster initiates a call to the customer's bank and connects the customer with a real bank representative while the fraudster remains muted on the line.
- The bank requests authentication information, such as social security number, passwords and other personal information, which is then provided by the customer.

- Once the personal information is provided, the fraudster quickly ends the conference line and informs the customer that the issue has been resolved.
- Meanwhile, with the personal information gathered during the call, the fraudster can take over the customer's phone banking relationship and transfer money out of the customer's accounts.

Precautions against MitP Attacks

For consumers: It is recommended that banking customers never share account or personal information with anyone that calls and requests to "verify" banking credentials. Customers should always tell such callers that they will call the bank to provide such information using the bank's phone number listed on the back of an ATM, debit or credit card. While this sounds obvious, many consumers do not take this simple precaution.

For banks: It is recommended that banks combine cross-channel behavior profiling and anomaly detection technologies with better call center processes and training. Call center employees should be trained to listen more closely and ask who originated the call. Attacks may be thwarted or losses minimized if bank employees ask simple (but random instead of static) security questions at various points in the phone conversation when confirming personal credentials. Fraudsters are less likely to trick customers into sharing answers to several security questions.

Conclusion

As consumers shift more financial transactions to secure online arenas, fraudsters have become more creative in utilizing traditional telephones. Access through mail and telephone transactions grew from 3% of ID theft in 2006 to around 40% in recent years, and fraudsters are getting creative and leveraging new techniques, so consumers need to be as diligent as ever in protecting their personal information.

Footnotes

[1] The MitB threat was demonstrated by Augusto Paes de Barros in his presentation, "O futuro dos backdoors — o pior dos mundos", covering backdoor website intrusions in September 2005.

[2] Anointed MitB by Philipp Gühring in a white paper, "Concepts against Man-in-the-Browser Attacks", published January 27, 2007.

About the Author

Dhananjay Sakhalkar is a consultant within the Cognizant Business Consulting, Wholesale Banking group. His areas of expertise include Payments & Cash Management, Financial Messaging, and Business Lending. Dhananjay has more than 12 years of experience in the areas of business consulting, application development, requirements gathering, project management, and is a PMP certified professional. He can be reached at Dhananjay.sakhalkar@cognizant.com.

About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting, and business process outsourcing services. Cognizant's single-minded passion is to dedicate our global technology and innovation know-how, our industry expertise and worldwide resources to working together with clients to make their businesses stronger. With over 50 global delivery centers and more than 68,000 employees as of September 30, 2009, we combine a unique onsite/offshore delivery model infused by a distinct culture of customer satisfaction. A member of the NASDAQ-100 Index and S&P 500 Index, Cognizant is a Forbes Global 2000 company and a member of the Fortune 1000 and is ranked among the top information technology companies in BusinessWeek's Hot Growth and Top 50 Performers listings.

Start Today

For more information on how to drive your business results with Cognizant, contact us at inquiry@cognizant.com or visit our website at www.cognizant.com.

Cognizant
Passion for building stronger businesses

World Headquarters
500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277
Email: inquiry@cognizant.com

European Headquarters
Haymarket House
28-29 Haymarket
London SW1Y 4SP UK
Phone: +44 (0) 20 7321 4888
Fax: +44 (0) 20 7321 4890
Email: infouk@cognizant.com

India Operations Headquarters
#5/535, Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060
Email: inquiryindia@cognizant.com