EXPERT DATA FORENSICS
INVESTIGATORS OF DIGITAL EVIDENCE

eForensic Focus is a publication of
Expert Data Forensics, LLC. © June 2014

The Vulnerability Landscape:
Digital Drama with the Man-in-the-Middle

Published by: Leon Mare

June 2014

Is The Man-in-the-Middle Controlling Your Digital Communication?

Case Study: Rob states that he received a text message from Julie; the text reads "Hello". Julie states that she did in fact text Rob, but that her message said "Goodbye" and not "Hello". Both phones are forensically examined; an analysis of incoming/outgoing text messages and deleted data within the time frame was conducted. The analysis confirmed that both statements are accurate. The question is, how?

The forensic analysis suggests that a form of digital hacking known as "Man-in-the-Middle Attack" or MITM was the cause. When a hacker intercepts communications between two people or entities and modifies the communication without anyone knowing, we refer to the attack as the “Man-in-the-Middle” The hacker can modify text messages, emails and data transmissions.

Cyber Security in recent times has evolved rapidly from a stage of technical regulation to a well mapped notion. From breaking into the voice mails of the Duke of Cambridge to hacking the Sony’s Play Station Network, internet related crime is increasing both in severity and frequency with an increasing number of attackers looking to exploit vulnerabilities in software and websites. Sensitive information of individuals and restricted and confidential databases of businesses are at the front line of internet security battles.

While we consider our cell phone calls very secure, our privacy is not always what we think! A cell phone can be hijacked easily too!

Major Security Flaw in Apple iOS 7.06 Opens Users to a Man-in-the-Middle Attack.

Immediately after the release of iOS 7.06, Apple revealed a major flaw in their software – an overlooked SSL (secure socket layer) encryption issue, exposing its users to Man-in-the-Middle attacks. The flaw in the software allowed hackers to alter and intercept communications such as login credentials for numerous Apple hardware users.

Viber, Whatsapp, Flickr - Vulnerable to Man-in-the-Middle Attacks putting millions of users at risk.

More recently a serious flaw in voice messaging and voice calls system was discovered by researchers at UNH Cyber Forensics Research and Education.

Viber app available for Blackberry, Windows phone, iOS, Android and Desktop offers a free Viber to Viber voice calling service to its users in addition to allowing them to share almost everything- from the location to text messages to videos.

It was discovered that this data gets stored in unencrypted form on the Viber Amazon servers. This data could be easily accessed from these servers without any authentication. By intercepting a link from Viber, a hacker can easily access user's data by becoming the "Man-in-the-Middle"

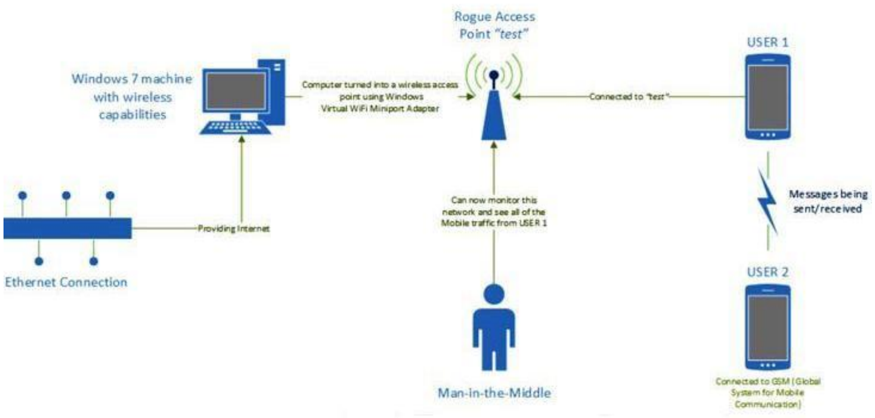

Figure 1: Graphical Illustration of a typical scenario on Viber user. Any attacker can use network testing tools available on the market to sniff the traffic on Viber. (Source: UNH Cyber Forensics Research and Education)

Digital Impersonation: Man-in-the-Middle Attack

The ability to communicate securely has been quite a challenge for millennia. For as long as people tried to exchange confidential information, others have tried to compromise their privacy. In the modern communications environment, radio frequency communications and worldwide digital networks such as the internet, compound the problem.

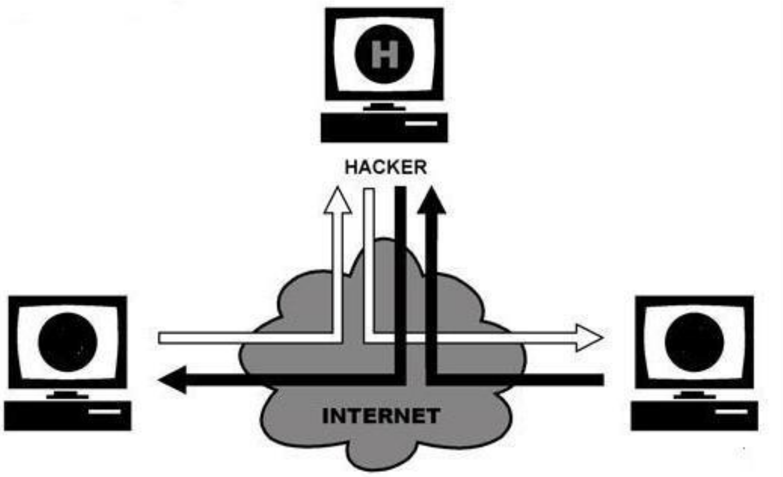

Figure 2: Graphical Illustration of Man-in-the-Middle Attack.

Man-in-the-Middle Attack is a form of digital attack that occurs when a malicious entity inserts themselves without authorization, into a digital exchange taking place between two parties and intercepts the data through a trusted yet compromised system in a way that the original parties still appear to be communicating with each other when in fact the entire communication is controlled by the attacker.

The attacker is actually eavesdropping and disrupting a communication session taking place between individuals and systems. For example, Chris believes he is talking to David but Michelle is listening in and manipulating the conversation.

Typically Man-in-the-Middle Attacks involves usage of a fake security certificate being posed as a legitimate Web service that bypasses browser security settings and intercepts data. Most of the time people are unaware their communication session or data has been tampered with until it is too late.

NSA and GCHQ running Man-in-the-Middle Attacks impersonating Google.

It has been exposed that the US National Security Agency NSA has impersonated Google, and possibly other websites, to intercept, store and read supposedly secure communications. The NSA's top secret program called PRISM has already been accused of mining private information from the servers of reputable companies including Google, Yahoo, Facebook, Microsoft and AOL. Even though, the companies have dismissed the allegations for collaborating in the program, the surveillance program is designed to monitor emails, chat messages, videos and file transfers.

One of the key revelations about GCHQ's (Government Communications Headquarters based in the UK) program called 'FLYING PIG' was that it was using Man-in-the-Middle Attacks on Internet Services like Google.

It is believed that NSA employees log into an internet router – most likely the one used by ISP's. It remains unclear whether this was done with the permission and knowledge of the router's owner or not.

Once the log in was successful, the internet traffic was redirected to an MITM attack – a site that acted as a stealthy intermediary, intercepting communications before they were forwarded to their intended destination.

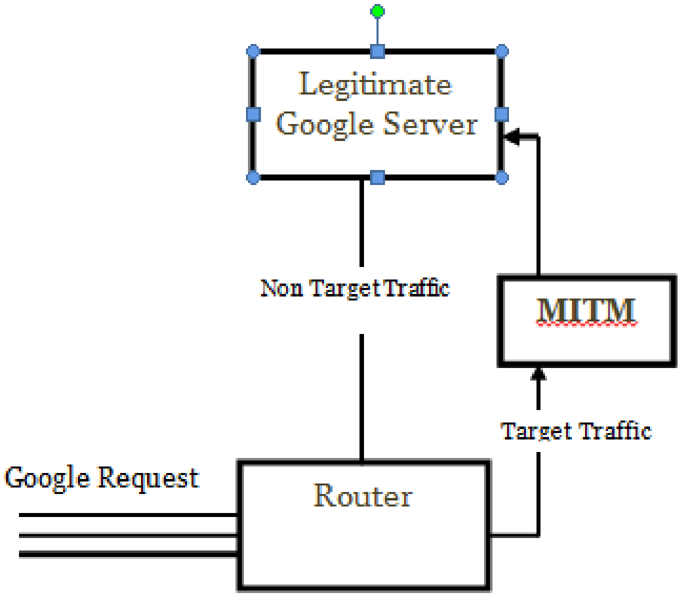

Figure 3: Graphical Illustration of Man-in-the-Middle Attack impersonating Google.

Guess who is Whatsapping you! Account hijacking through Man-in-the-Middle Attack.

In order to prevent attackers from impersonating somebody else making use of the victim's phone number, a verification SMS that contains a 4 digit PIN code is sent at the time a new user opens an account on Whatsapp. The code needs to be copied by the user into the app's GUI. The process connects a user account to a physical device.

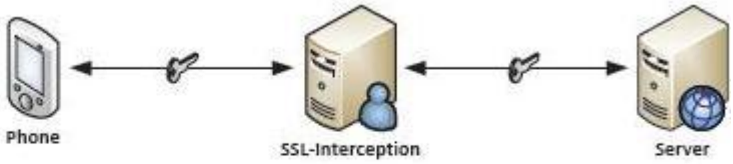

Figure 4: Whatsapp Authentication Process

More recently it was discovered that this verification or authentication process is lethally broken. The 4 digit PIN code used for SMS verification is generated on the phone and sent to the server through an HTTPS connection. An SMS message is initiated by the server through a SMS proxy to the phone. The App then verifies if the code entered by the user is the same as the auto generated PIN code.

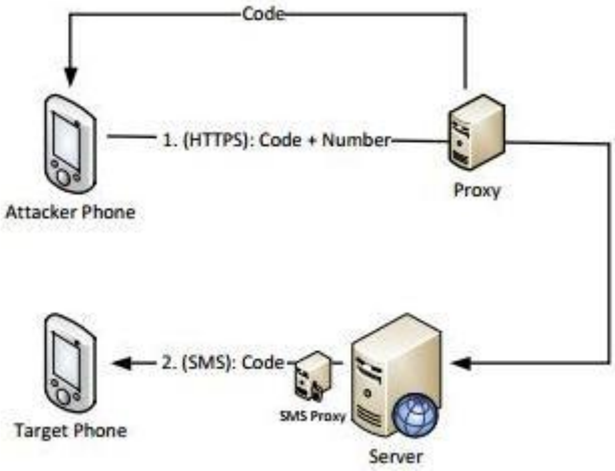

Figure 5: Man-in-the-Middle Attach against Whatsapp Authentication

This mechanism can be easily hijacked by an attacker. The hijacking can be performed by simply typing in the phone number of the target during the authentication stage and interfering with the communication taking place between the server and the user's phone to hack the PIN. While this communication is SSL protected, all that an attacker needs is to intercept the connection between the personal phone and the Whatsapp server.

In order to exploit this vulnerability, it is not difficult to set up an SSL proxy and get the proxy certificates installed on the phone and gain easy access to the encrypted communication. Once the account has been hijacked during the authentication process, the target's phone gets linked with the hacker's phone which enables the attacker to send and retrieve messages from the target's account.

How to Prevent a Man-in-the-Middle Attack: Securing Your Communications.

As organizations rely on modern communication tools and techniques, MITM attacks have broadened to encompass mobile devices as well. Lately, the Apple iMessage protocol was found vulnerable to Man-in-the- Middle and spoofing attacks. Top five ways to stay protected!

1. **Securing your mail**

Ensure that your email contacts have the ability to verify if a particular message was actually sent by you. It is therefore critical that you implement a comprehensive email security solution to prevent your emails from being hacked or attacked.

2. Encrypt Your Data in Transit

It is important to remember that your information is vulnerable even when it is in transit. If the data in transit is not encrypted, it can easily be captured online. To ensure the integrity of your information, such as sending emails or even accessing your Facebook account, it needs to be encrypted.

3. Keep Your Webmail private

The Internet is an open network and the information on it travels in a readable format. If an email message is intercepted on its way to a recipient, its contents can be read. And because the Internet is a large World Wide Network that depends upon intermediary computers to direct traffic, a number of people may have the opportunity to invade your message.

4. Secure your Instant Messaging Software

Instant messaging is also not a secure means of communication and it can be just as susceptible to surveillance as email. Fortunately, there are programs that can help secure the privacy of your chat sessions. Just like with email, you need to have a secure communication channel in order to make sure that your chatting sessions are safe.

5. Secure your Voice Over IP Software

Some of today's more popular VoIP programs include Skype, Google Talk, Yahoo, Voice and MSN Messenger. When using voice communication to exchange sensitive information, it is important to choose a tool that encrypts the call all the way from your computer to the recipient's computer.

– End.