Abstract

Man-In-The-Middle is the term used to refer to the great threats facing internet or networks security. These individuals try to intercept data or information moving from one network or computer to another. These cases are common between internet providers, application developers, and business rivals.

This essay writing service paper will describe various tools used by these hackers when intercepting data and how they pose threats to the internet security. The paper also describes some of the most famous Man-In-The-Middle attacks on various developers' applications. The paper also describes various methods, which can be used to eliminate or reduce the Man-In-the-Middle activities. The paper also describes the threats faced by various businesses because of the "Man-In-The-Middle" activities and how entrepreneurs can protect their clients from these threats.

Introduction

The Man-In-The-Middle attack is abbreviated as MITM. It is mainly an active attack on the internet where the hacker or attacker tries or intercept communications by reading or altering data exchanging between two or more computers. Man-In-The-middle attacks are commonly associated with wireless networks as well as communications systems, which are wired. These types of attacks are commonly known to work hand in hand with 802.11 network security (Combs, 2010).

Man-In-The-Middle attacks are known to exploit weaknesses in the Boarder Getaway Protocol commonly known as BGPs. The weaknesses are mainly created by massive internet traffic experienced with increased innovations in the information technology sector across the world. This is because of continued use of wireless networks in transferring data or information between different users. The World Wide Web is another factor known to

contribute a great deal in the increased cases of Cybercrimes commonly known as the Man-In-The–Middle attacks. This is as result of increased communication through the internet hence hackers find it easier to access people's information on the internet (Moses, 2004).

These attacks take the form of impersonation, forgery or even to an extent, a complete blackmail to customers or clients of a particular network or internet services providers. The hackers access client's private information from the company's servers and use it for the purposes of personification. This might help them to carry out dubious business activities using the names of specific clients. Man-In-The-Middle attacks are known to cause disputes and misunderstandings between companies and their clients especially in the banking industry. Internet traffic has been rerouted manipulatively mainly for eavesdropping purposes. These attacks are also known to come from trusted government authorities especially in their quest to get any security threat tips by users of specific internet browsers and services. This is clearly shown in the attempts by the National Security Agency to interfere with the internet protocols of various internet browsers in search of security threats in the country (Moses, 2004).

Other national security agencies in different parts of the world have been known to attack various bloggers' cites in search of sensitive information that may be a threat to their respective country security. There are several tools used by attackers to carry on with their dubious activities, which are based on weaknesses on integrity, confidentiality and availability (Keizer, 2012).

Wireless Attack tools

The Man-In-The-Middle attacks are mainly based on security flaws in the wireless communication tools. The reason is because most of the tools used in wireless attacks are developed with the main aim of compromising 802.11 networks. Some of these tools include

the Wi-Fi, Bluetooth and wireless connectivity of computers. Wi-Fi is a common wireless tool used by many hacklers due to its widespread popularity across the world. The Wi-Fi provides the hacker with the best platform to cause most of their disruption (Moses, 2004).

Development of new technologies in the market leads to increased development of attack tools. This is because latest technologies are the most endorsed by the largest population hence provides the best platform for hackers to operate on. The case of the great popularity of wireless technology with main emphasis put on Wi-Fi and Bluetooth is a clear example of how latest technologies are used by hackers to perform their activities. Wireless attack tools are known to interfere with the integrity and confidentiality of a person's information hence are categorized as some of the most dangerous Man-In-The-Middle attacks of the century (Combs, 2010).

Other tools used by hackers are the internet and the wide spread use of home group networking of computers. Research shows that internet provides the largest platform through which successful hackers operate. Some of these activities focus on revealing business practices of rival companies and bank information especially with the rise of online banking services. Other cases of manipulative use of the internet are seen on the mailing services. Hackers obtain email account details of various and they hence use them as marketing platforms by sending them as swindle messages. These are mainly used by conmen and most illegal companies whose aim is to make maximum profits by creating traffic on their websites (Dooly, 2012).

Examples

Some of the famous cases cited by various developers on attacks on the activities of hackers on their websites are: the case of Nokia Express browser developers interfering with the Nokia browser protocols, the issue of National security Agency and its interference with

Tor and Firefox browsers, the case of hacklers interfering with the Microsoft operating system development and finally the Indians attacks against Google servers (Moses, 2004).

The National Security Agency has been famous for use scrupulous mechanisms to source security information. The NSA is known to interfere with the Https protocols of Firefox and Tor users in 2004 in their attempt to obtain security information. The NSA was also in the news in 2003 for several attempts of accessing Google servers. Other companies, which have been serious victims of these attacks, are Nokia and Microsoft. Nokia servers were intercepted by Nokia express developers hence making it appear as a genuine product from Nokia Company (Combs, 2010).

Microsoft also announced massive attacks on its servers in 2008 by unknown developers. According to Microsoft, this was because of business rivalry with the attacker intending to identify Microsoft's business secrets (Keizer, 2012).

Remedies

The remedies for curbing the issue of hackers are; the use of recent browsers by users, the users is also advised to keep track of unknown email addresses on their mail inboxes and finally use of encrypted communication techniques when online or on wireless network (Dooly, 2012).

Businesses and end users should ensure that they have active and strong firewalls in their computers. This prevents fake or impersonated addresses from accessing the computers. Businesses should provide their clients with useful information on how to keep their systems secure to prevent cyber-attacks. Business should also ensure that their systems are up to date with genuine security software. This clearly prevents any sort of unknown addresses from accessing the systems (Dooly, 2012).

References

Combs, G. (2010, february 1). *wireshark.* Retrieved February 16, 2013, from Wireless attacks: http://www.wireshark.org

Dooly, T. (2012). *Remedies for cyber crime.* New York: Communications security Inc.

Keizer, G. (2012). Microsoft warns of Hackers. *Computer World* , 1-4.

Moses, M. (2004, April 1). *Automatic Wireless client.* Retrieved february 16, 2013, from Hotspotter: http://www.remote-exploit.org/codes_hotspoter.html