Man in the Browser Attacks

Timothy Dougan, University of Ulster, UK
Kevin Curran, University of Ulster, UK

ABSTRACT

Man-in-the-Browser attacks are a sophisticated new hacking technique associated with Internet crime, especially that which targets customers of Internet banking. The security community has been aware of them as such for time but they have grown in ability and success during that time. These attacks are a specialised version of Man-in-the-Middle attack, and operate by stealing authentication data and altering legitimate user transactions to benefit the attackers. This paper examines what Man-in-the-Browser attacks are capable of and how specific versions of the attack are executed, with reference to their control structure, data interaction techniques, and methods for circumventing security. Finally the authors discuss the effectiveness of counter-Man-in-the-Middle strategies, and speculate upon what these attacks tell us about the Internet environment.

Keywords: Hacking, Internet Banking, Man-in-the-Browser, Man-in-the-Middle, Security

1. INTRODUCTION

In network security terminology, “the Middle” is defined very broadly. In this sense it refers to the domain of action of Man in the Middle (MitM) attacks, in which an unauthorized party inserts themselves surreptitiously at some point along the flow of communication between two or more parties. This is so as to gain the ability to monitor the information that is exchanged, and perhaps also to modify that information, generally without being discovered so doing (Tanenbaum & Wetherall, 2011). In theory, the attack can be performed at almost any point along the communication channel between the victims. The Man in the Middle may attack through a server they control at any point along the data channel, or anywhere along the wire that it is possible to arrange for a physical tap. In practice it is impractical to choose a server or wire somewhere in the immediate vicinity of a targeted party, and it would be ineffective to attack from somewhere at random in the web where traffic is subject to fluctuating routing tables. Therefore, this approach would usually be commenced with a phishing attack to trick the user into bridging the gap, which will be discussed. If either terminating machine is using a wireless connection, the Man could also interpose himself between that machine and its associated wireless router, by picking up their outgoing signal and then posing as the user’s machine to the router. This would also work if they have control over a LAN device on the same bus as the user.

The “Middle” described already encompasses all points from the moment a signal leaves a machine at one end of a transaction right through until just before it reaches its
destination. However, the Man could also breach the integrity of the signal before it even leaves the user’s PC, if he subjects the user to a Man in the Browser (MitB) attack. This is a more recent form of attack in which the user’s browser is corrupted in order to act as the tap in the information stream, an attack which “occurs at the system level, between the user and the browser, [rather than via] the protocol layer” (Litan & Allan, 2006). This, structurally speaking, is “a man-in-the-middle attack between the user and the security mechanisms of the browser” (Gühring, 2006).

Therefore, in network security terms, “the Middle” is every point along the course an information transaction between the initial input and final output device (i.e., anything that is not a keyboard or a monitor etc). In this sense, the MitB attack is a special case of the MitM attack in which the intrusion occurs at the very nearest end of the middle to the user.

2. MitB IN TERMS OF MitM

Let us begin by exploring the places in which MitB differs from MitM. Firstly, MitM intercepts data using an inserted or compromised piece of hardware that is external to the targeted system. MitB on the other hand gains access through the software configuration on that system, generally by way of a Trojan that targets the web browsers on that computer.

Secondly, MitM either has to deal with messages that have already been protected by whatever security is associated with the connection (and read/alter them mid-flight in both directions of communication), or has to present a plausible reason for the user to create their connection with the attacker’s own server. MitB does not need to bother with the extra work this entails. In the outward-bound direction, it is the author of all compromised messages sent. In the inward-bound direction, it does still have to deal with a fully formed message, but it does not need to be concerned with modifying the message itself so as to conceal its actions. This is because MitB directly controls the browser, and therefore needs only to modify the browser display to be as the user expects. Together this means that it works outside of any client-side and server-side encryption and validation, and therefore does not have to be concerned with increased latency arising from hashing overheads or to provide dummy keys for public key encryption.

This implies another advantage of MitB over MitM, in that MitM is only guaranteed to be able to handle public key encryption (and this only up to a point as discussed in the section “Trust”), whereas MitB is “immune” to all forms of encryption, including symmetric key, by being external to it. Finally, MitM is only truly effective a directed or location-based attack, whereas MitB can be spammed to as many computers as its Trojan is able to infect.

If the access point of MitM were somewhere at random in the Internet, it is unlikely for it to be able to extract valuable data or make modifications undetectably. This is because packets can be routed independently, so any data gleaned will probably be fragmentary, and replies to any fraudulent modified messages would not be guaranteed to pass through the same compromised point as the outgoing message, making concealment of modifications almost impossible. To maintain constant contact, the MitM attacker must either be physically close enough to the victim to capture their outgoing data before it has the opportunity to bifurcate, or trick the victim into navigating to the attacker’s own server that will act as a stable mid-point.

This compels the attacker to either directly target or in some other way reach out to individuals or groups, and means that this attack does not scale very well. On the other hand, the only such limitations on MitB are around the level of security that is installed on the systems it attacks or is practiced by the people who use them, and it scales very well. Where MitM is limited to a chosen few targets at a time (most effectively spread by mass spam emails with links to compromised sites), individual MitB Trojans are known to have compromised between hundreds and hundreds of thousands of users’ security concurrently (Finjan, 2009;
Semantic Knowledge Mining Techniques for Ubiquitous Access Media Usage Analysis
[www.igi-global.com/chapter/semantic-knowledge-mining-techniques-ubiquitous/24308?camid=4v1a](www.igi-global.com/chapter/semantic-knowledge-mining-techniques-ubiquitous/24308?camid=4v1a)