Chapter 16
Cloak and Dagger:
Man-In-The-Middle and Other Insidious Attacks

Ramakrishna Thurimella
University of Denver, USA

William Mitchell
University of Denver, USA

ABSTRACT
One of the most devastating forms of attack on a computer is when the victim doesn’t even know an attack occurred. After some background material, various forms of man in the middle (MITM) attacks, including ARP spoofing, fake SSL certificates, and bypassing SSL are explored. Next, rootkits and botnets, two key pieces of crimeware, are introduced and analyzed. Finally, general strategies to protect against such attacks are suggested.

INTRODUCTION
Information has always been very valuable. Computers are entrusted to maintain and process massive amounts of information. This makes them valuable targets to attackers. One of the most devastating forms of attack is when an attacker gains access to the information without the victim even being aware of it.

This paper explores some of the means by which this surreptitious access to information can occur. Background material on basics of cryptography, the Diffie-Hellman key exchange, networking, Transport Layer Security and Secure Sockets Layer, and drive by downloads is provided in section 2. MITM attacks are defined in section 3. ARP spoofing, a form of a MITM attack, is explored in section 3.1. Futile defenses to MITM attacks are examined in section 3.2. A MITM attack on SSL using fake certificates is given in section 3.3. Even more forms of MITM attacks are explored in section 3.4. Defenses are discussed in section 3.5. Finally, a new attack known as man in the browser is detailed in section 3.6.

MITM attacks are not the only stealthy means by which information security is breached. Rootkits and botnets, which are capable of doing much more harm, can reside on victim’s computer while evading detection. Rootkits are defined in section 4. An example rootkit, Mebroot, is analyzed in
section 4.1. Defenses against rootkits are discussed in section 4.2. Botnets, which are often used in conjunction with rootkits, are defined in section 5. Attacker’s motivation is examined in section 5.1. The Torpig botnet, and its recent takeover by security researchers, is investigated in 5.2.

We conclude with some general discussion on how to prevent these attacks in section 6.

Background

In this section, we begin with the basics of cryptography, pointing out the difference between symmetric and asymmetric encryption, followed by a description of the Diffie-Hellman key exchange protocol. Next, we present an abstract description of the man-in-the-middle attack. After that, we give some networking details that are necessary to understand a concrete man-in-the-middle attack on modern local-area networks. We first begin with a general discussion on cryptography.

Cryptography

When trying to communicate a message across an untrusted channel, cryptography is a natural solution. The original message, or plain text, is transformed into cipher text by encrypting the plain text with an encryption key, $K_e$. The cipher text will appear meaningless with no apparent relationship to the plain text. This allows the cipher text to be transferred across the untrusted channel with minimal risk of the plain text being intercepted. The cipher text can be transformed back into the plain text by decrypting it with the decryption key $K_d$. Collectively, the methods of encryption and decryption are known as a cipher. This process, illustrated in Figure 1, can be represented symbolically as

$$P = D(K_{priv}, E(K_{pub}, P)).$$

If the decryption key is the same as the encryption key, or efficiently derived from it, the cipher is known as a symmetric cipher; otherwise, it is an asymmetric cipher. Popular symmetric ciphers include the Advanced Encryption Standard (National Institute of Standards and Technology, 2001) and the Triple Data Encryption Algorithm, commonly known as Triple DES (National Institute of Standards and Technology, 1999). Symmetric ciphers suffer from the key distribution problem—getting the communicating parties to agree upon a common key.

In public key cryptography, which use asymmetric ciphers, each communicating entity maintains one private key and one public key, $K_{priv}$ and $K_{pub}$ respectively. Extending the previous notation, public key cryptography is

$$P = D(K_{priv}, E(K_{pub}, P)).$$

As the names imply, the public key is made available freely to anyone who wishes to use it, but the private key is kept secret. If Alice wishes to communicate with Bob, she encrypts the message with Bob’s public key, which is freely available, and sends the encrypted message to Bob. Anyone eavesdropping on this communication cannot decrypt the message unless they have Bob’s private key. Anyone who wants to communicate with Bob can easily get access to his public key,