Walk into Starbucks, plop down a laptop, click start, watch the credentials roll in. Enter Subterfuge, a Framework to take the arcane art of Man-in-the-Middle Attacks and make it as simple as point and shoot. Subterfuge demonstrates vulnerabilities in the ARP Protocol by harvesting credentials that go across the network, and even exploiting machines through race conditions. Now walk into a corporation…

A rapidly-expanding portion of today's Internet strives to increase personal efficiency by turning tedious or complex processes into a framework which provides instantaneous results. On the contrary, much of the information security community still finds itself performing manual, complicated tasks to administer and protect their computer networks. The purpose of this publication is to discuss a new Man-In-The-Middle attack tool called Subterfuge. Subterfuge is a simple but devastatingly effective credential-harvesting program, which exploits vulnerabilities in the inherently trusting Address Resolution Protocol. It does this in a way that even a non-technical user would have the ability, at the push of a button, to attack all machines connected to the network. Subterfuge further provides the framework by which users can then leverage a MITM attack to do anything from browser/service exploitation to credential harvesting, thus equipping information and network security professionals and enthusiasts alike with a sleek "push-button" security validation tool.

Abstract:

Christopher M. Shields
r00t0v3rr1d3

Matthew M. Toussain
0sm0s1z

"He who is prudent and lies in wait for an enemy who is not, will be victorious." --Sun Tzu

Enter Subterfuge, a Framework for Man-in-the-Middle Attacks, where credentials are up for the taking.

The MITM Framework

Give me the numbers. How bad is MITM really? The state of security on the Local Area Network and why you should be concerned.

Walk into Starbucks, plop down a laptop, click start, watch the credentials roll in. Now walk into a corporation…

Introduction: Why Subterfuge?

User-friendly network attack tools are quick to make national headlines due to the threat they pose and because, "in truth, the tools and techniques employed by hackers are extremely complex [1]." Firesheep, a Firefox web browser plugin, is just such a tool. It was designed to capture cookies created during the login process for secure web sites, and it does this at the push of a button. Firesheep's push-button simplicity and overwhelming effectiveness led to its ubiquitous use by skilled professionals and non-skilled users alike, thus focusing attention on a fixable yet often-ignored error in web site implementation.

The Subterfuge Project attempts to use the paradigm popularized by Firesheep, Armitage, and other user-friendly network attack tools to create a framework for Man-In-The-Middle (MITM) network attacks. A MITM attack uses eavesdropping to insert a malicious entity into the communication path between legitimate users on a network [2]. This entity can then masquerade as either of the legitimate users in order to capture sensitive information, like login credentials for a protected web site. Typically, a MITM attack requires a significant amount of complex, text-based configuration of numerous software programs. This complexity, combined with the virtually never-ending reports of stolen identities and online credential theft, makes the MITM attack a prime candidate for the creation of a user-friendly, simplified framework.

Thus, we designed this framework to have a simple interface with minimal configuration requirements in order to appeal to skilled and non-skilled network security professionals and users. Subterfuge has a sleek web based interface to allow a user to deploy the software quickly and easily without editing sophisticated text-based configuration files. Subterfuge automates the configuration process or, alternately, streamlines it with a Graphical User Interface (GUI). It also allows the user to view a report of all the different credentials that were harvested. The ease with which the general populace would be able to use Subterfuge will demonstrate to information security professionals the dangers of MITM attacks on a large scale.

Subterfuge is developed with the Python programming language and uses a SQLite database. ARPSpoof from the Dsniff suite is used to poison the target network. Subterfuge also uses SSLStrip to collect user credentials that were sent over a secure socket layer (SSL) web connection.

The Subterfuge Project's purpose is to demonstrate pervasive vulnerabilities in the ARP protocol…

Setting up Subterfuge is Quick, Easy, and Intuitive.

Man-in-the-Middle Threat Analysis

So what is the big deal? Well a study from Cornell University's Center for Hospitality Research stated that over 90% of hotels provide wireless Internet access to their customers, and the vast majority of these access points are susceptible to ARP Poisoning Attacks [9].

There are two significant types of MITM attacks: Passive and Active. In a Passive attack, a hacker can observe what his victim is viewing, which allows the attacker to steal credentials and session cookies. In an Active attack, "the target is entirely controlled by the attacker, rather than being limited by the extent of the victim's browsing activity" [3].

Several major websites, such as Google and Facebook, have recently realized a significant blunder on their part in terms of browsing security for their users. Facebook used to encrypt solely the login traffic, which contained the username and password of the individual. Afterwards, the session returned to a regular, plain-text browsing session which could be intercepted and easily read by anyone who might be performing a MITM attack. In a paper on the security issues which are challenging Facebook, the need to "educate Facebook users about using secure socket layer (SSL) applications" is discussed as a prerequisite to protecting their users from identity theft [4].

In addition to web site design and implementation errors, the network Address Resolution Protocol (ARP) itself has residual vulnerabilities that are commonly exploited during a MITM attack. The extent to which computers on a local network rely on, and inherently trust the responses of, ARP messages is alarming. If ARP message processing remains uncontrolled, ARP sniffing and poisoning can occur, which means that an attacker can begin the process of masquerading as a legitimate user [5]. Current steps that the security community has made to secure ARP are woefully inadequate. Heightened awareness of the threat implicated by MITM attacks should become more commonplace amongst both computer users and security professionals.

Current Deployment Complications

The primary reason MITM is not seen as a greater threat to network security is because it is not as easy to implement as other attack vectors. There is no simplistic point-and-click framework to execute a standard MITM attack. Hacking tools in this arena are either very easy to use but difficult to configure and update (Firesheep), or they require a significant amount of configuration and are not intuitive (Ettercap). Therefore, such exploitation is not as commonplace as other, more popular attack vectors. Our framework will use the software ARPSpoof and SSLStrip, and will further automate the attack process and make it as simple as pushing a button.

Software: ARPSpoof

ARPSpoof is a simple tool that allows a user to masquerade as the network gateway by spamming ARP Packets. This causes their MAC Address to be associated with the IP address of the default gateway thereby initiating a MITM connection. ARPSpoof is unsupported as of 2001; however, it does have a Win32 port for cross-platform compatibility [8]. In the future Subterfuge will include its own module to ARP Cache Poison. The Subterfuge module will allow for more attack configuration options.

Software: SSLStrip

SSLStrip is another useful tool due to its ability to hijack HTTP (Hypertext Transfer Protocol, or web) traffic on a network, watch for HTTPS (HTTP-Secure) links and activity, and then map those links into look-alike HTTP links [7]. SSLStrip also provides a feature to supply a favicon which looks like a lock icon, giving the impression that the web connection is secure. SSLStrip is used transparently (i.e., without the user's knowledge) to convert an encrypted SSL session into a standard, plaintext web session that can then be easily monitored. Stealing credentials and sessions becomes trivial at this point. SSLStrip is a difficult piece of software for the average security researcher to set up quickly, let alone an average web user. The configuration process requires the user to perform intricate changes to files on the host operating system in addition to setting up network routing rules with a separate program.

Traceroute while under Man-in-the-Middle Attack:

ARP: It's Like Stealing Candy from a n00b

Motivation

Man-in-the-Middle Attacks are a category of vulnerability against which most applicable systems are susceptible. They are and will remain this way because of their obscurity. Until MITM attacks are simplistic enough that even aspiring security professionals can easily leverage them against networks, manufacturers will continue to develop and distribute vulnerable equipment. With Subterfuge, it is possible to make knowledge of these vulnerabilities mainstream, beyond even the security community. Subterfuge can be the motivation that manufactures like Cisco need to build the protections that they have provided to their enterprise customers for years into the systems they sell the average consumer.

The overall goal was to develop a tool that is sufficiently effective and easy to use in order to encourage the security community to focus on the massive vulnerability inherent in the Address Resolution Protocol. To achieve this result, we created a framework called Subterfuge, which allows even an average user to exploit the vulnerabilities in ARP on a local network.

The most basic implementation of Subterfuge collects information and user credentials across an entire local area network and organizes the collected data into a SQLite Database. It does this through the automated utilization of the ARPSpoof and SSLStrip programs, both of which are publicly available.

Subterfuge automatically manages its configuration file, yet allows more advanced users the ability to delve deeper into the MITM settings. This requires Subterfuge to detect the hardware and network configurations needed to initiate the attack. Additionally, Subterfuge is able to properly configure, set up, and deploy the SSLStrip software with little or no input required from the user.

The tedious and difficult problem of properly configuring and executing these multiple pieces of software in unison is eased by the automation developed and included in the Subterfuge Project.

This tool is deemed successful if a user is able to execute Subterfuge to collect user information and credentials on the network to which they are connected. Specifically, a Subterfuge user ought to be able to steal user credentials, without the victim's knowledge, even when using a "secure" protocol such as HTTPS.

Outcomes

So what can it do? During preliminary testing, Subterfuge was able to capture login credentials from many websites to include:

Yahoo
Ebay
Amazon
Facebook
Twitter

In our test cases, the tool was even able to steal information transmitted over HTTPS. During these captures, sessions were successfully and near transparently degraded from HTTPS to HTTP. The victim, who was using the Google Chrome web browser, logged into Facebook.com and had their credentials stolen and displayed by the tool in plaintext. Indication of foul play was limited to a Uniform Resource Locator (URL) that stated www.facebook.com as opposed to https://www.facebook.com. No certificate errors were presented to the victim, and the victim was able to login just as they normally would. Thus, their login information was still stolen with effective transparency.

Web Code Injection

The Subterfuge Project includes a modified version of SSLStrip that takes advantage of its web proxy capabilities. Subterfuge's modification allows the data to be tampered with before reaching the victims browser. In essence this allows us to inject arbitrary code into a victim's browser session. This can be anything from a JavaScript alert message to an exploit like ms10_aurora.

Extensibility and the Framework

Naturally, Man-in-the-Middle Attacks are not limited to mere credential fraud. Neither is Subterfuge. Basic usage of the tool will be to ARP Poison the LAN; however, from this perspective it is possible to initiate many attacks. The Framework will automatically gather credentials, but it can also do more. Subterfuge's Plugin System allows for the usage of additional MITM functionality without the need to develop another security tool from scratch.

Future Work

There are numerous areas of future advancement for this framework. At a fundamental level, the framework can be expanded to include additional features to increase its effectiveness in testing and exploiting the vulnerabilities in the ARP protocol.

This tool can also be modified to work as a payload to an exploitation framework such as Metasploit. Subterfuge could be deployed on a remote network to harvest the credentials of legitimate users silently and transparently and then report the information back to a command and control server.

Current Progress

The Subterfuge Project is currently in its beta phase. Plans for future development include modules for:

Session Hijacking
Race Conditions
DNS Spoofing
Wireless AP Suite
Evilgrade Update Exploitation

Module – Session Hijacking

The session hijacking plugin will allow a user to masquerade as a victim within the session that was hijacked.

Module – Race Conditions

The race condition plugin will allow Subterfuge to return its own version of the web page that a user attempts to view. This modified version of the web page will contain a browser exploit, which can be used to attain arbitrary code execution on the victim's machine.

Module – DNS Spoofing

The DNS spoofing plugin will allow Subterfuge to supply false DNS information to a victim's machine causing them to be redirected to an alternate location.

Module – Wireless AP Suite

The Wireless AP Suite will have a number of extremely useful features, which will increase the functionality of Subterfuge. A user will be able to setup a fake access point through which a victim will connect, successfully creating a MITM situation. An advanced option would even listen for what computers in the nearby area are probing for and setup an access point spoofing networks the victims have previously connected to. This will allow the victim computers to connect to and route their traffic through Subterfuge without any user input.

Module – Evilgrade Update Exploitation

Evilgrade is a tool that allows a user to spoof an update server on the network. When a victim starts up a program such as iTunes it automatically looks to see if updates exist. Evilgrade steps into this process and sends the victim a malicious payload. Subterfuge will include a module that simplifies the process, and incorporates it into the framework.

OS Compatibility

The beta version of Subterfuge runs on Linux only; however, the creation of installer packages for the Windows and Mac operating systems will ensure the widespread use of the Subterfuge MITM Framework.

Custom ARP Spoof Tool

The final version of Subterfuge will incorporate a custom-built Python ARP Spoofing Tool using Scapy to improve performance, increase stealth, and provide better MITM protection avoidance. This tool will replace ARPSpoof and allow for more advanced configurations and dynamic options to increase effectiveness, and engender the ability to thwart certain configurations of Cisco's Dynamic ARP Inspection protection. It will also decrease network load and will allow the attack to hide more effectively amongst normal network traffic.

Conclusion

In conclusion, the Subterfuge Framework allows a user to circumvent many security protocols and policies on a computer network with ease and with devastating results to the victims. Credential harvesting can be one of the most difficult attacks to recover from as a corporation or an individual because the attacker has the legitimate information that is entered to authenticate a user. Furthermore, the modular structure of Subterfuge makes it extremely extensible. The simplicity and effectiveness offered by Subterfuge should drive the rate of its incorporation into the toolbox of network security practitioners. If this tool is released to the public and distributed, the wide-spread ease in which anyone on a computer network could be victimized by a non-technical user will have the desired effect of forcing the information security community to come up with a solution to the underlying problem – the trusting nature of the Address Resolution Protocol.

The Framework: Poking Holes in ARP one Starbucks at a Time

Subterfuge's web based GUI uses AJAX and JQuery to leverage user input as commands. It then converses with a Django Backend to allow for the seamless execution of the python code that embodies the core of the project.

The Command Line Interface (CLI) for Subterfuge allows users to quickly configure and run a MITM attack against a network.

VLANs can provide network segmentation, which can prevent MITM attacks. Some routers put different hosts on different VLANs. In these cases the devices may be independent of MAC Addresses thereby preventing an ARP Poisoning Attack from occurring. If however, multiple hosts are on the same VLAN no additional protection is provided.

An ARP Cache Poison can modify a victim's ARP Table:

"Creativity is inventing experimenting, growing, taking risks, breaking rules and having fun."
~ Mary Lou Cook

[1] Barber, R. (2011, August 30). *Security Science*. Retrieved from Computer Fraud & Security Volume 2001, Issue 3.

[2] Kurose, J. and Ross, K. *Computer Networking: A Top-Down Approach*. 5th Edition. Addison-Wesley. Page 61

[3] Saltzman, R. (2011, August 30). *Security Science*. Retrieved from OWASP: http://www.security-science.com/pdf/active-man-in-the-middle.pdf

[4] Leitch, S. (2009). *Security Issues Challenging Facebook*. Retrieved from Edith Cowan University Research Online: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1017&context=ism&sei-redir=1#search=%22facebook%20secure%22

[5] Wagner, R. (2011, August 30). *Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks*. Retrieved from http://savannah.gatech.edu/people/lthames/dataStore/WormDocs/arppoison.pdf

[6] Norton, D. (2011). *An Ettercap Primer*. SANS Institute, 1-27.

[7] Marlinspike, M. (2011, August 30). *Blackhat*. Retrieved from http://blackhat.com/presentations/bh-europe-09/Marlinspike/blackhat-europe-2009-marlinspike-sslstrip-slides.pdf

[8] Song, D. (2012, January 1). *Dsniff Frequently Asked Questions.* Retrieved from http://www.monkey.org/~dugsong/dsniff/faq.html

[9] Ogle, J. and Wagner, E. (2012, March 8). *Hotel Network Security: A Study of Computer Networks in U.S. Hotels.* Retrieved from http://www.hotelschool.cornell.edu/research/chr/pubs/reports/abstract-14928.html

References

References

Legacy: Demonstrating Need and Spurring Change

There is an obvious need for change in routing equipment. While routers that incorporate VLANs and are thus protected against ARP Spoofing do exist, they are uncommon commodities. Manufactures have no real incentive to improve their equipment because the arcane art of Man-in-the-Middle Attacks is obscure enough that the average consumer is unconcerned, but they are not safe. Subterfuge uncovers the faults in ARP so easily that consumers of routers will be able to point at products and ask themselves, "Does this product protect me from Subterfuge? "This just might provide the impetus that manufactures should have had a decade ago. Hopefully, through demonstration of the pervasive vulnerabilities inherent in the ARP Protocol router manufacturers will be spurred into utilization of existing technologies to protect their users.

Hopefully through demonstration of the pervasive vulnerabilities inherent in the ARP Protocol router manufactures will be spurred into utilization of existing technologies to protect against ARP Poisoning attacks.