CMPT 320 Intranet & Internet Security
Spoofing: The False Digital Identity by Nekia Brice & Martina Sturdikova

Home
Final Paper
Powerpoint Presentation

Spoofing

"The False Digital Identity"

Martina Sturdikova
Nekia Brice

CMPT 320
Dr. S. Robila
May 2, 2007

Introduction

Spoofing is the action of making something look like something that it is not in order to gain unauthorized access to a user's private information. The idea of spoofing originated in the 1980s with the discovery of a security hole in the TCP protocol. Today spoofing exists in various forms namely IP, URL and Email spoofing.

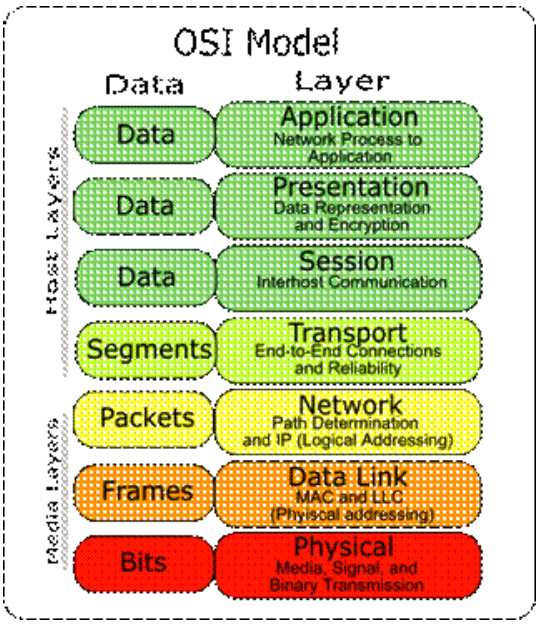
All email users might have received an email asking us to update our profile information for our account in either Paypal or other financial institutions. Some of these users might know that these emails are acts of phishing and thus they avoid/delete emails like these, and others might not be aware of this practice and so they navigate to a spoofed Website by clicking on a link provided in the spoofed email. A spoofed Website is designed to look exactly like the original Website (sometimes even the URL, title bar, and status bar mimic the original Website, this is referred to as a spoofed URL) and a spoofed email appears to be sent from a legitimate source; while in fact it was sent from someone else. Phishing and spoofing are closely related.

The paper will address the issue of spoofing and the negative effects on computer users. It will analyze the various types of spoofing, current prevention methods and current research in new technology to prevent spoofing (site-authentication or Certified Mail Delivery).

Types of Spoofing

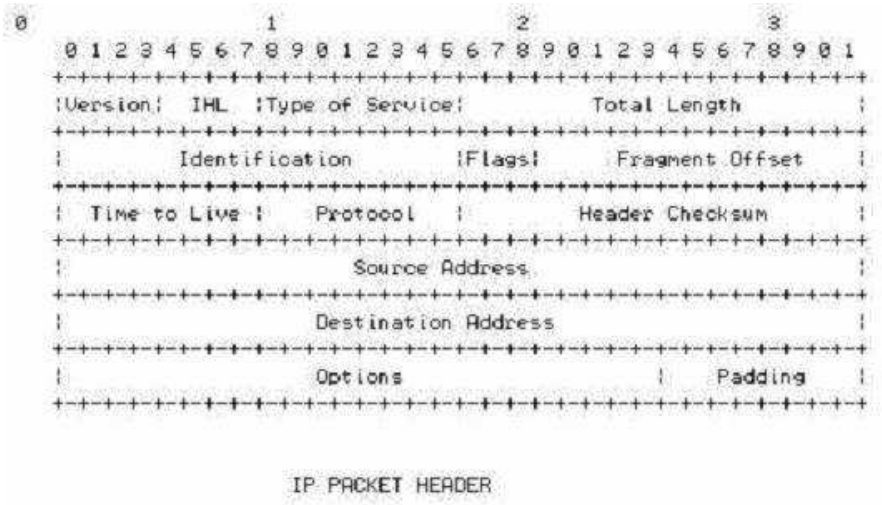
IP Spoofing

Internet Protocol (IP) is the protocol used for transmitting messages over the Internet; it is a network protocol operating at layer 3 of the OSI model.



Source: http://www.3mfuture.com/network_security/arp-guard-arp-spoofing.htm

IP spoofing is the act of manipulated the headers in a transmitted message to mask a hackers true identity so that the message could appear as though it is from a trusted source.



Source: http://www.securityfocus.com/infocus/1674

The hacker manipulates the packet by using tools to modify the "source address" field. The source address is the IP address of the sender of the message therefore once an intruder forges this address and the destination server opens up a connection, this is when numerous attacks can take place.

Attacks

- Man-in-the-Middle attack

In a Man-in-the-Middle attack, the message sent to a recipient is intercepted by a third-party which manipulates the packets and resends it own message.

- Denial of Service (DoS) Attack

A DoS attack is when a attacker floods a system with more packets than its resources can handle. This then causes the system to overload and shut down. The source address is spoofed making it difficult to track from where are the attacks taking place.

Solutions

IP spoofing can be prevented by monitoring packets using network monitoring software. A filtering router could also be installed, on the router an ACL (access control list) is needed to block private addresses on your downstream interface. On the upstream interface source address originating outside of the IP valid range will be blocked from sending spoofed information.

URL Spoofing

URL spoofing occurs when one website appears as if it is another. The URL that is displayed is not the real URL of the site, therefore the information is sent to a hidden web address.

Attacks

- Intrusion

URL spoofing is sometimes used to direct a user to a fraudulent site and by giving the site the same look and feel as the original site the user attempts to login with a username and password. The hacker collects the username and password then displays a password error and directs the user to the legitimate site.
Using this technique the hacker could create a series of fake websites and steal a user's private information unknowingly.

Solutions

Security patches are released by web browsers which add the feature of revealing the "true" URL of a site in the web browser. It is important to check if your internet browser is vulnerable and to perform the necessary updates. See http://secunia.com/advisories/10395/ for more information on URL Spoofing Internet Explorer vulnerability.

Email Spoofing

Email spoofing is the act of altering the header of an email so that the email appears to be sent from someone else.

Attacks

- Cause confusion or discredit a person
- Social Engineering (phishing)
- Hide identity of the sender (spamming)

Recognize spoofed email

- Check the content of the email:

    - Is the content weird in some way, or really unexpected from the sender?
    - Does it contain a form?
    - Does it request to either confirm or update login or any kind of information?
- Check the header of the email

Solutions

Mac Spoofing

Attacks

Solutions

Conclusion

http://www.cert.org/advisories/CA-1995-01.html

http://www.astalavista.com/index.php?section=docsys&cmd=details&id=50

http://www.theage.com.au/articles/2003/12/12/1071125632006.html