A Comprehensive Analysis of Spoofing

P. Ramesh Babu
Dept of Information Technology
Rajamahendri Inst. of Engg & Technology
Rajahmundry-533103, INDIA
E-mail:rameshbabu_kb@yahoo.co.in

D.Lalitha Bhaskari
Dept of C.S & S.E
AU College of Engineering (A)
Visakhapatnam-530003, INDIA
E-mail:lalithabhaskari@yahoo.co.in

CH.Satyanarayana
Dept of C.S.E
JNTUK College of Engineering
Kakinada – 533003, INDIA
E-mail: ce@jntukakinada.edu.in

***Abstract*--The main intention of writing this paper is to enable the students, computer users and novice researchers about spoofing attacks. Spoofing means impersonating another person or computer, usually by providing false information (E-mail name, URL or IP address). Spoofing can take on many forms in the computer world, all of which involve some type false representation of information. There are a variety of methods and types of spoofing. We would like to introduce and explain following spoofing attacks in this paper: IP, ARP, E-Mail, Web, and DNS spoofing. There are no legal or constructive uses for implementing spoofing of any type. Some of the outcomes might be sport, theft, vindication or some other malicious goal. The magnitude of these attacks can be very severe; can cost us millions of dollars. This Paper describes about various spoofing types and gives a small view on detection and prevention of spoofing attacks.** (Abstract)

Keywords: Spoofing, Filtering, Attacks, Information, Trust

I. INTRODUCTION

Spoofing can take on many forms in the computer world, all of which involve some type false representation of information. There are a variety of methods and types of spoofing. We would like to introduce and explain following types in this paper:

- IP Spoofing
- ARP Spoofing
- E-Mail Spoofing
- Web Spoofing
- DNS Spoofing

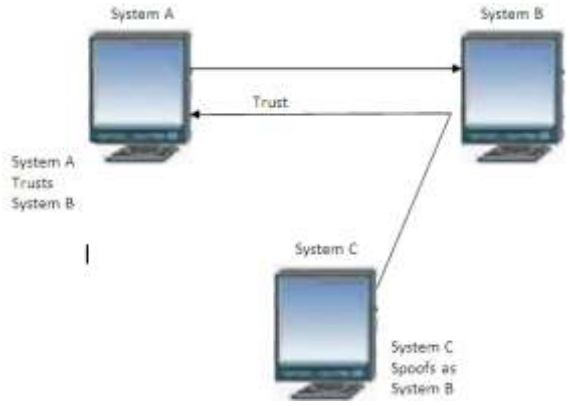
There are no legal or constructive uses for implementing spoofing of any type. Some of the outcomes might be sport, theft, vindication or some other malicious goal. The gravity of these attacks can be very severe, can cost us millions of dollars and should not be overlooked by the Internet security community.

II. IP SPOOFING

IP spoofing is used to gain unauthorized access to a computer. The attacker forwards packets to a computer with a source address indicating that the packet is coming from a trusted port or system. Attackers must go through some complicated steps to accomplish the task [1]. They must:

- Obtain a target.
- Obtain an IP address of a trusted machine.
- Disable communication of the trusted machine (e.g. SYN flooding).
- Sample a communication between the target and trusted hosts
- Guess the sequence numbers of the trusted machine.
- Modify the packet headers so that it appears that the packets are coming from the trusted host.
- Attempt connection to an address authenticated service or port.
- If successful, the attacker will plant some kind of backdoor access for future reference

System A impersonates system B by sending B's address instead of its own. The reason for doing this is that systems tend to function within groups of other ``trusted'' systems. This trust is implemented in a one-to-one fashion; system A trusts system B. IP spoofing occurs in the following manner: if system A trusts system B and system C spoofs system B, then system C can gain otherwise denied access to system A. This is all made possible by means of IP address authentication, and if the packets are coming from external sources- poorly configured routers [2].

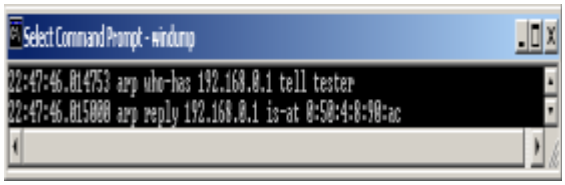


One of the major drawbacks with IP spoofing is that C never "sees" the responses from A. This is completely blind attack, much experience and knowledge of what to expect from the target's responses is needed to successfully carry out his attack.

Some of the most common ways to avoid this type of attack are to disable source-routed packets and to disable all external incoming packets with the same source address as a local host.

III. ARP SPOOFING

ARP stands for Address Resolution Protocol. ARP is used to map IP addresses to hardware addresses [6]. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address resolution in both directions [3]. When an incoming packet sent to a host machine on a network arrives at a router, it asks the ARP program to find a MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the network to determine if any machine knows who has that IP address. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied. Here is a sample ARP broadcast query:



One might deduct that this addressing scheme could also be spoofed to provide a host with incorrect information "ARP Spoofing involves constructing forged ARP request and reply packets. By sending forged ARP replies, a target computer could be convinced to send frames destined for computer A to instead go to computer B." This referred to as ARP poisoning. There are currently programs that automate the process of ARP poisoning – ARPoison, Ettercap, and Parasite. All three have the capability to provide spoofed ARP packets and therefore redirect transmission, intercept packets, and/or perform some type of man in the middle attack. Either enabling MAC binding at a switch or implementing static ARP tables achieves prevention of ARP spoofing. MAC binding makes it so that once an address is assigned to an adapter; it cannot be changed without authorization. Static ARP management is only realistically achieved in a very small network. In a large dynamic network, it would be impossible to manage the task of keeping the entries updated. ARPWATCH, for UNIX based systems, monitors changes to the ARP cache and alerts administrator as to the changes.

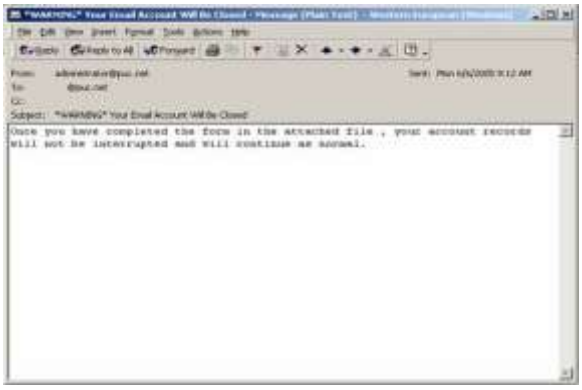
IV. E-MAIL ADDRESS SPOOFING

Spoofing is when an e-mail message appears to come from a legitimate source but in fact is from an impostor. E-mail spoofing can be used for malicious purposes such as spreading viruses, trawling for sensitive business data and other industrial espionage activities [8].

If you receive a snail mail letter, you look to the return address in the top left corner as an indicator of where it originated. However, the sender could write any name and address there; you have no assurance that the letter really is from that person and address. E-mail messages contain return addresses, too – but they can likewise be deliberately misleading, or "spoofed." Senders do this for various reasons, including:

- The e-mail is spam and the sender doesn't want to be subjected to anti-spam laws
- The e-mail constitutes a violation of some other law (for example, it is threatening or harassing)
- The e-mail contains a virus or Trojan and the sender believes you are more likely to open it if it appears to be from someone you know
- The e-mail requests information that you might be willing to give to the person the sender is pretending to be (for example, a sender might pose as your company's system administrator and ask for your network password), as part of a "social engineering" attack
- The sender is attempting to cause trouble for someone by pretending to be that person (for example, to make it look as though a political rival or personal enemy said something he/she didn't in an e-mail message)

Here is an example of a spoofed email made out to look like it originated from administrator@puc.net



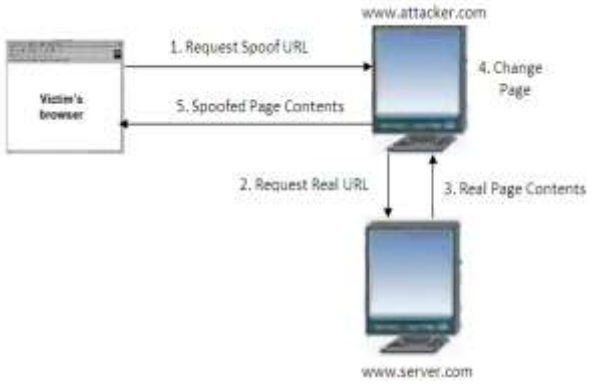
V. WEB SPOOFING

As with the other forms of spoofing Web or Hyperlink spoofing provides victims with false information. Web Spoofing is an attack that allows someone to view and modify all web pages sent to a victim's machine. They are able to observe any information that is entered into forms by the victim. This can be of particular danger due to the nature of information entered into forms, such as addresses, credit card

numbers, bank account numbers, and the passwords that access these accounts [4].

Web Spoofing works on both Internet Explorer and Netscape and is not necessarily prevented by secure connections. This is due the way that the SSL protocol uses certificates to authenticate websites. The attacker can observe and modify all web pages and form submissions, even when the browser is indicating that there is a secure connection. The attack can be implemented using JavaScript and Web server plug-ins, and works in two parts. First, the attacker causes a browser window to be created on the victim's machine, with some of the normal status and menu information replaced by identical-looking components supplied by the attacker. Then, the attacker causes all Web pages destined for the victim's machine to be routed through the attacker's server. On the attacker's server, the pages are rewritten in such a way that their appearance does not change at all, but any actions taken by the victim (such as clicking on a link) would be logged by the attacker. In addition, any attempt by the victim to load a new page would cause the newly loaded page to be routed through the attacker's server, so the attack would continue on the new page. The attack is initiated when the victim visits a malicious Web page, or receives a malicious email message.

Current browsers do not completely prevent Web Spoofing, and there seems to be little movement in the direction of addressing this problem. I believe that there can be no fully secure electronic commerce on the Web until the Spoofing vulnerability has been addressed.



VI. DNS SPOOFING

A DNS spoofing attack can be defined as the successful insertion of incorrect resolution information by a host that has no authority to provide that information. It may be conducted using a number of techniques ranging from social engineering through to exploitation of vulnerabilities within the DNS server software itself. Using these techniques, an attacker may insert IP address information that will redirect a customer from a legitimate website or mail server to one under the attacker's control – thereby capturing customer information through common man-in-the-middle mechanisms [9].

According to the most recent "Domain Health Survey" (Feb 2003), a third of all DNS servers on the Internet are vulnerable to spoofing.

Operating normally, a customer can expect to query their DNS server to discover the IP address of the named host they wish to connect to. The following diagram reflects this process.

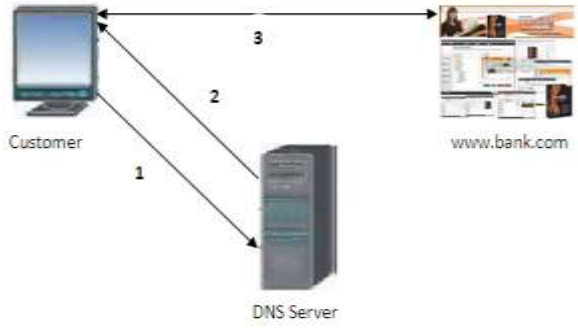


Fig 1: The Normal DNS Motion Process

1. The customer queries the DNS server – "What is the IP address of www.bank.com?"

2. The DNS responds to the customer query with "The IP address of www.bank.com is 150.10.1.21"

3. The Customer then connects to the host at 150.10.1.21 – expecting it to be www.bank.com.

However, with a successful DNS spoofing attack, the process has been altered. The following diagram reflects this process.

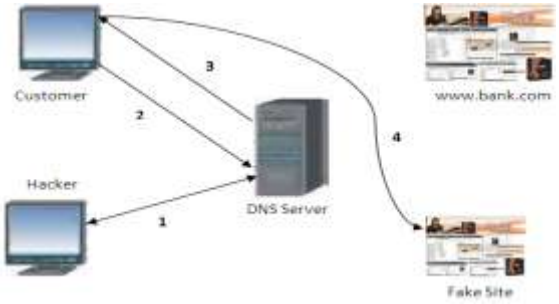


Fig 2: The DNS motion process having fallen victim to a DNS spoofing attack

1. The attacker targets the DNS service used by the customer and adds/alters the entry for www.mybank.com – changing the stored IP address from 150.10.1.21 to the attacker's fake site IP address (200.1.1.10).

2. The customer queries the DNS server "What is the IP address of www.bank.com"

3. The DNS responds to the customer query with "The IP address of www.bank.com is 200.1.1.10" – not the real IP address.

4. The Customer then connects to the host at 200.1.1.10 – expecting it to be www.bank.com, but in fact reaching the attackers fake site.

VII. AVOIDANCE OF SPOOFING

The Packet filtering is the best method to avoid various spoofing attacks. In this section we have described three packet filtering methods which are used to filter the spoofed packets, they are

A. Ingress Filtering Method - IFM

B. Egress Filtering Method - EFM

C. Spoofing Prevention Method - SPM

A. Ingress Filtering Method

- Ingress filtering is a technique used to make sure that incoming packets are actually from the networks that they claim to be from [7].
- Networks receive packets from other networks. Normally a packet will contain the IP address of the computer that originally sent it. This allows other computers in the network to know where it came from, which is needed for things like sending a packet back to the sending computer [7].
- In certain cases, the sending IP address will be spoofed. This is usually done as part of an attack, so that the attacked computer does not know where the attack is really coming from [7].
- Filtering a packet is when the packet is not processed normally, but is denied in some way. The computer processing the packet might simply ignore the packet completely, or where it is possible it might send a packet back to the sender saying the packet is denied.
- In ingress filtering, packets coming into the network are filtered if the network sending it should not send packets from IP addresses of the originating computer.
- In order to do ingress filtering, the network needs to know which IP addresses each of the networks it is connected to may send. This is not always possible. For instance, a network that has a single connection to the Internet has no way to know if a packet coming from that connection is spoofed or not [7].
- Ingress filtering is a packet filtering technique used by many Internet service providers to try to prevent source address spoofing of Internet traffic, and thus indirectly combat various types of net abuse by making Internet traffic traceable to its source [7].
- Ingress filtering is a "good neighbor" policy which relies on mutual cooperation between ISPs for their mutual benefit.
- There are many possible ways of implementing this policy; one common mechanism is to enable reverse path forwarding on links to customers, which will indirectly apply this policy based on the provider's route filtering of their customers' route announcements [7].

B. Egress Filtering Method

- Egress filtering is the practice of monitoring and potentially restricting the flow of information outbound from one network to another. Typically it is information from a private TCP/IP computer network to the Internet that is controlled [7].
- TCP/IP packets that are being sent out of the internal network are examined via a router or firewall. Packets that do not meet security policies are not allowed to leave - they are denied "egress" [7].
- Egress filtering helps ensure that unauthorized or malicious traffic never leaves the internal network [7].
- In a corporate network, typically all traffic except that emerging from a select set of servers would be denied egress. Restrictions can further be made such that only select protocols such as http, email, and DNS are allowed. User workstations would then need to be set to use one of the allowed servers as a proxy. Direct access to external networks by the internal user workstation would not be allowed [7].
- Egress filtering may require policy changes and administrative work whenever a new application requires external network access. For this reason egress filtering is an uncommon feature on consumer and very small business networks [7].

C. Spoofing Prevention Method (SPM)

A new approach for filtering spoofed IP packets, called Spoofing Prevention Method (SPM). The method enables routers closer to the destination of a packet to verify the authenticity of the source address of the packet. This stands in contrast to standard ingress filtering which is effective mostly at routers next to the source and is ineffective otherwise. In the proposed method a unique temporal key is associated with each ordered pair of source destination networks (AS's, autonomous systems). Each packet leaving a source network *S* is tagged with the key $K(S;D)$, associated with $(S;D)$, where *D* is the destination network. Upon arrival at the destination network the key is verified and removed. Thus the method verifies the authenticity of packets carrying the address *s* which belongs to network *S*. An efficient implementation of the method, ensuring not to overload the routers, is presented [5]. The major benefits of the method are the strong incentive it provides to network operators to implement it, and the fact that the method lends itself to stepwise deployment, since it benefits networks deploying the method even if it is implemented only on parts of the Internet. These two properties, not shared by alternative approaches, make it an attractive and viable solution to the packet spoofing problem.

D. Some other plans to avoid spoofing in web applications:

- Use cryptographic signatures to exchange authenticated email messages. Authenticated email provides a mechanism for ensuring that messages are from whom they appear to be, as well as ensuring that the message has not been altered in transit. Similarly, sites may wish to consider enabling SSL/TLS in their mail transfer software. Using certificates in this manner increases the amount of authentication performed when sending mail [7].

- Configure your mail delivery daemon to prevent someone from directly connecting to your SMTP port to send spoofed email to other sites [7].

- Ensure that your mail delivery daemon allows logging and is configured to provide sufficient logging to assist you in tracking the origin of spoofed email [7].

- Consider a single point of entry for email to your site. You can implement this by configuring your firewall so that SMTP connections from outside your firewall must go through a central mail hub. This will provide you with centralized logging, which may assist in detecting the origin of mail spoofing attempts to your site [7].

- Educate your users about your site's policies and procedures in order to prevent them from being "social engineered," or tricked, into disclosing sensitive information (such as passwords). Have your users report any such activities to the appropriate system administrator(s) as soon as possible [7].

VIII. CONCLUSION

With the current implementations of spoofing, the network security community needs to be aware of the magnitude and potential cost of these types of attacks. People can effectively maintain patching and monitoring of logs to minimize the potential damage.

Professionals must remain current with the Operating Systems that we use in our day to day activities. A steady stream of changes and new challenges is assured as the hacker community continues to seek out vulnerabilities and weaknesses in our systems and our networks.

The authors have stated that the paper they presented will cater the needs of novice researchers and students who are interested in information security.

REFERENCES

[1] Daemon, Route, Infinity, “IP Spoofing Demystified”, Phrack Magazine; 1996;

[2] “IP Address Spoofing and Hijacked Session Attacks”; 1/23/95 http://ciac.llnl.gov/ciac/bulletins/f-08.shtml;

[3] Neil B. Riser “Spoofing: An Overview of Some Spoofing Threats” from SANS Reading room.

[4] Felten, Balfanz, Dean, Wallach D.S., “Web Spoofing, An Internet Con Game”; http://bau2.uibk.ac.at/matic/spoofing.htm;

[5] A. Bermlerand H. Levy. “Spoofing prevention Method,” INFOCOM’05, 2005.

[6] Whalen, Sean; “An Introduction to ARP Spoofing”;packetstorm.security.com/papers/protocols/intro_to_arp_spoofing.pdf;6/25

[7] www.wikipedia.com

[8] http://www.puc.net/email_spoofing.htm

[9] http://www.technicalinfo.net/papers//index.htm

[10] Whalen, Sean; “An Introduction to ARP Spoofing”; packetstorm.securify.com/papers/protocols/intro_to_arp_spoofing.pdf; 6/25/01.

[11] DNSAbuse; http://packetstorm.securify.com/papers/protocols/mi004en.htm; 6/30/01.

AUTHORS PROFILE

Ms. Dr D. Lalitha Bhaskari is an Associate Professor in the Department of Computer Science and Engineering of Andhra University. She did her PhD from JNTU Hyderabad in the area of Steganography and Watermarking. Her areas of interest include Theory of computation, Data Security, Image Processing, Data communications, Pattern Recognition and Cyber Forensics. Apart from her regular academic activities she holds prestigious responsibilities like Associate Member in the Institute of Engineers, Member in IEEE, Associate Member in the Pentagram Research Foundation, Hyderabad, India. She is also the recipient of “Young Engineers” Award from the prestigious Institution of Engineers (INDIA) for the year 2008 in Computer Science discipline.

Dr. Ch. Satyanarayana working as Associate Professor in the Department of Computer Science & Engineering, University College of Engineering, JNTU Kakinada for the last 12 years. He obtained his Ph.D from JNTU Hyderabad. He published 22 research papers in various International Journals and Conferences. Under his guidance 12 Research scholars working on different areas like Image Processing, Speech Recognition, Pattern Recognition.

Mr. P. Ramesh babu is an Assistant Professor in the Department of Information Technology of Rajamahendri Institute of Engineering & Technology - Rajahmundry. His research interests include Steganography, Digital Watermarking, Information security, Network communications and Cyber Forensics.

Mr.Ramesh babu did his M.Tech in Computer Science & Engineering from JNTU Kakinada University. He has 6 years of teaching and industrial experience.