BURNISHED LAW JOURNAL

Himanshu Sahu

University of Petroleum and Energy Studies, Dehradun

SPOOFING AS A CYBER THREAT: LEGAL REMEDIES

Let's face it: the future is now. We are already living in a cyber society, so we need to stop ignoring it or pretending that is not affecting us.

-Macro Ciapelli

INTRODUCTION

The word cyber and its relative dot.com are probably the most commonly used term of the modern period. In the information era the rapid development of computers, telecommunications and other technologies has led to the evolution of new forms of trans-national crimes known as cyber-crimes. Cyber crimes have virtually no limits and may harm all the nations in the world. The extent of loss involved worldwide of cybercrimes is tremendous as it is estimated that about 500 million people who use the internet can be affected by the emergence of cyber crimes. Cyber crimes are a very serious danger for the times to come and pose one of the most difficult challenges before the law enforcement agencies. Most of the cyber crimes don't involve violence but rather greed, pride, or play on some character weakness of the victims. It is become impossible to recognize the culprit, as the net can be vicious web of deceit and can be access form any part of the world. In a spoofing attack, the interloper sends messages to a computer for showing that the messages have come from a trusted system. To become successful, the interloper must first find out the IP address of a trusted system, and then modify the packet headers to that it appears that the packets are coming from the trusted system. In essence, the interloper is spoofing the distant computer into believing that they are a legitimate member of the network. The object of the attack is to form a connection that will permit the interloper to gain root access to the host, permit the creation of a backdoor entry path into the main target system. Spoofing Internet traffic is tenacious threat, and generally the main reason of agonizing Distributed Denial of Service attacks. While technical aspirations for blocking spoofed congestion subsist they are only effective and applicable near to the edge – computers and other

end devices attached to the net. This demands deployment of anti-spoofing evaluation by a wide majority of networks on a universal scale something that isn't uncomplicated to achieve.

DEFINITION OF SPOOFING

The word 'spoof' came into existence by the British Comedian Arthur Roberts in 1852[1] . Actually in 19th century, Arthur Robert invented a game named spoof which used the tricks and non sense and very soon the word spoof took the general sense of nonsense. Spoofing is a broad term for the type of behavior that involves a cybercriminal masquerading as a trusted user or device to get you to do something beneficial to the hacker and detrimental to us[2] . Spoofing refers to sort of cybercrime that happens when a hacker imitates a known source or it can be described as surrounding a sort of evasive action all relevant to hacker's ability to pass themselves off as someone else[3]. Spoofing in network security involves fooling a computer or network via a falsified IP address, by redirecting internet traffic at the DNS level, or by faking APR data within a local access network. Spoofing influenced to a attacked at a networks rather than individuals, with the aim of growing malware, stealing data, bypassing security systems, or laying the framework for subsequent attacks. Spoofing can be used in such a broad types of ways that it can be a challenge to find out every attack. That's why it's so important for us to equip ourselves with robust, reliable internet security.

TYPES OF SPOOFING

1) ARP Spoofing: The Address Resolution Protocol is a type of protocol which is used to translate IP Address into Media Access Control (MAC) addresses in sequence of proper transmitting. Briefly, the protocol maps an IP address to a physical machine address. This kind of spoofing attacks takes place when a false attacker links the hacker's MAC address with the IP address of a company's network. This permits the intruder to indulge data intended for the company computer. This type of spoofing may lead to data theft and deletion, includes accounts and other malicious consequences. APR may also be work for DoS, hijacking and for many types of attacks.

---

[1] *Techniques of Spoofing Attack,* UKessays, (Dec 11, 2017, 12:35 P.M), https://www.ukessays.com/essays/computer-science/the-process-of-spoofing-computer-science-essay.php

[2] *What is Spoofing?,* Kaspersky, https://www.kaspersky.com/resource-center/definitions/spoofing

[3] *What is Spoofing and how can I defend against it? ,* Avast Academy, (Apr 16, 2020, 12:40 P.M), https://www.avast.com/c-spoofing

2) DNS Spoofing: The Domain Name System (DNS is behind associating domain names to the correct IP addresses, allowing the visitor to connect to the correct server. For a DNS spoofing attack to be affluent, a hostile attacker divert the DNS translation so that it points to another server which is typically damaged with malware and can be used to aid spread viruses and worms. This kind of spoofing is also erratically referred as DNS cache poisoning, due to the enduring effect when a server caches the hostile DNS responses and serving them up every time the identical request is sent to that server.

3) IP Spoofing: IP Spoofing is the popular type of spoofing attacks which is used most commonly. This attack is successful in order to send out IP packets using a trusted IP address when a malicious attacker copies a legal IP address. The duplicate IP address compels the systems to believe the source is trustworthy, opening any victims up to different types of attacks using the trusted IP packets and shut down the marked servers. If there are various data packets which are reaching the server, the server will unable to manage all of the requests.

4) Email Spoofing: This sort of spoofing involves things like requests for private data or commercial transactions. The emails appear to be from trustworthy senders like customers, coworkers, or managers but they are generally from cyber criminals. In 2019, Mumbai based Paint Company Asian Paints fell victim to a massive email spoofing attack in which the hackers pretend to be one of the company's suppliers. It is the most popular hacking practice due to the way email is designed. It is an open and relatively unsecured system that permits the people around the globe to send messages to each other without any complications.

In United States v. Machado[4] , the defendant had sent threatening e-mail to Asian Students at University of California at Irvine based on race. The defendant contended that the e-mails were sent idly and without intention to act on threats. The court, however, didn't accept his contention and held accused liable for violating federal hate-crime law.

5) Website Spoofing: When a hacker makes a false version of a real website, they're performing website spoofing. The duplicate sites look just like the real one, and when users log in to the duplicate websites, the hackers obtain their credentials.

[4] C.D. Cal. 2/10/98 USA

6) Caller ID Spoofing: This one is most popular type of spoofing when robocallers can make their calls appear as though they are coming from either a trusted number of particular geographic region. Once the victim answering to the fake call, the attacker will attempt to convince them to divulge sensitive data. Caller ID Spoofing can also be send to use fake spoofed text messages also. Spam and scam calls are so frequent, our Truecaller Insights estimated that in 2018, 24.9 million Americans lost $8.9 billion in phone scams with a 22% increase in spam calls than the previous 12 months[5] .

LEGAL REMEDIES FOR SPOOFING

According to a report from India, Department of Telecommunications, the government of India has taken the following measures against the spoofing service providers:

Websites subscribing caller ID spoofing services are banned in India as an instant measure. According to the Department of Telecommunications (DOT), by using spoofed call service is illegal according to the Section 25(c) of the Indian Telegraph Act, 1885 provides using such services may lead to fine and three years of imprisonment or both.

There have been a number of cases filed by the sufferer of spoofing attacks. Almost all the cases are filed under the Sections 43, 43A and 72A of the Information Technology (Amendment) Act, 2008. The Act provides for the various liabilities and remedies depending on where the spoofing activity has been take place.

Unauthorized Access- Section 43 of the Information technology Act 2000 provides that if any person accesses a computer network where the permission is not permit by the owner, or downloads, copies and develop any information, or causes destruction of any system; among all the other things they will be liable to pay damages through compensation to the sufferer. The offence of spoofing is covered under the above mentioned acts.

Section 66 of the Act also provides that if any person, dishonestly or fraudulently, commits any act referred to in Section 43, he will be punished with imprisonment for a term up to 3 years or with fine up to five lakh rupees, or with both.

[5] Lindsey Lamont, *How to avoid call Spoofing and Neighbor Spoof Scam,* TrueCaller Blog, (Jul 09, 2018, 12:52 P.M), https://truecaller.blog/2018/07/09/how-to-avoid-call-spoofing-and-neighbor-spoof-scam/

It is also regarded as punishable offence under Section 1030(a) (5) (A) of the cyber law of United States. In case of USA v. Robert Tappan Morris[6], it was held that the accused was found guilty for an offence of unauthorized access to protected system and was sentenced to three years of probation, 400 hours of community service and fine of 10,500 dollars.

Failure by an organization to implement cyber security measures- Section 43A of the IT Act, 2000 provides unbarred compensation for failure to take proper steps to preserve any sensitive private data or information held by an organization in a computer resource which it owns, controls and operate.

Denial of service attacks – By causing denial of services or access to any person authorized to use a computer network is punished under Section 43(f) of the IT Act, 2000 with imprisonment for a term not exceeding 3 years or with a fine not exceeding five lakh rupees, or with both.

Spoofing – Section 66C of the IT Act, 2000 could be used to prosecute a person for spoofing attacks. It yields that whoever corruptly or dishonestly, makes use of the electronic signature, password or any other exclusive identification aspect of any other person, shall be punished with imprisonment of up to 3 years and also be liable to fine of up to 1 Lakh rupees. In addition to it, Section 66D of the Act provides that any person uses a computer resource for cheating by personation will be punished with imprisonment of up to 3 years and will also be liable to a fine of up to 1 Lakh rupees.

Identity theft or fraud through spoofing – Section 419[7] provides the punishment for offence of cheating by personation for imprisonment up to three years or a fine or both. Section 66D[8] particularly provides for the offence of cheating by personation using a computer resource. This section provides imprisonment for 3 years and a fine up to 1 Lakh rupees.

In case of CBI v. Arif Azim[9], Sony India Private Limited operated a website enabling NRIs to supply Sony Products to their friends/relatives in India after paying for it online. An individual gained acquire the credit card number of an American National and booked Sony products by

[6] (1991) 23 928 F. 2d. 504 (US)
[7] Indian Penal Code, 1860, No. 45 of Acts of 1860 (India)
[8] The Information Technology Act, 2000, No. 21 of Acts of Parliament, 2000 (India)
[9] Talwant Singh Addl. Distt. & Sessions Judge, Delhi, *CYBER LAW & INFORMATION TECHNOLOGY: Sony.Sambandh.com (2000),* 12-13

using her name and specification. It was held that he was convicted under Section 419 of Indian penal code, 1860.

MODES OF PREVENTION AND MITIGATION AGAINST SPOOFING

There are number of techniques and practices that an organizations can employ to decrease the danger of spoofing attacks. Following are some common measures or steps than an organization can take for spoofing attacks includes:

1) **Packet filtering** - Packet filters searches packets as they are transmitted throughout the network. These are beneficial in IP address spoofing attack prevention because they are proficient of finding out and blocking packets with contaminated source address information (packets from outside network that reveal source addresses from the internal network and vice versa).
2) **Avoid Trust Relationship** – All the organizations should develop protocols that based on trust or fiduciary relationships wherever possible. It is efficiently simple for attackers to run spoofing attacks when trust relationships are used because trust relations only use IP address for authentication.
3) **Operate Spoofing detection Software:** Various software and programs are available that helps organizations to detect spoofing attacks, like ARP Spoofing. These type of software works by inspecting and certifying data before it is transmitted and blocking data that appears to be spoofed. Also we can use some software's to prevent IP Spoofing like StopCut, Find Mac Address Pro, Security Gateway for Exchange, Packet Creator and Responder Pro.
4) **Apply cryptographic network protocols:** Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other reliable communications protocols bolster spoofing attack preservation measures by encoding data before it is sent and authentication data as it is accepted.
5) **Report Spoofing Attacks:** When receiver receives any spoofed email and other communications, the sender suppose that the receiver have been spoofed. This can help to stop future spoofing through reporting on the main page of website and report spoofing and other security issues.

As with most aspects of mitigation against cybercrime, the basic object is self – protection is awareness. Generally, trust is good thing, but blind trust specially in the field of virtual world is rarely a good thing but often dangerous.

CONCLUSION

The internet is analogous to the high seas. No one owns it, yet people of all countries utilize it. It may be ideal if synthesis of internet laws could be so achieved so as to lessen the inconsistency in application of such laws. This is essential in the view of the growth of commercial activities on the internet. In IP Spoofing there is a less risk of danger at present due to the patches to the Unix Operating System and the extensive utilization of random segment counting. Many security experts are predicting a shift from IP spoofing attacks to operation related spoofing in which hackers can undertaking a weakness in a specific service to send and receive information under fake identities. A number of changes and new challenges are impassive as the hacker group continues to investigate susceptibility and weaknesses in our system and our networks.