**Addressing IP Vulnerabilities and the Difference Between “Hollywood Hacking” and Real Hacking**

Robert N. Sago

Information Sciences, University of Arkansas – Little Rock

CSEC 2324

Dr. William R. Cox

November 26, 2024

One of the first things that every student studying Network Security Administration learns is the seven-layer Open Systems Interconnection (OSI) model that sets the standards for system interconnectivity.[[1]](#footnote-1) The third layer, the Network layer, is home to the Internet Protocol (IP) suite. Relaying datagrams across network boundaries, the IP is the glue that holds the entire internet together.

What we call the internet had its beginnings in 1969, in the form of UNIX systems that kept military bases networked to each other to prevent a Pearl Harbor type disaster, and was later used to connect college campuses. The latter obviously made it easier to do research for papers like the one you are currently reading. It was in the 1990s that the modern iteration of the internet finally saw widespread use. As the technology evolved, so did the capacity for criminal misuse. In a 1998 Computer Crime and Security survey conducted by the Computer Security Institute, it was revealed that 64% of respondents reported computer security breaches in the twelve months prior to March[[2]](#footnote-2). Of those respondents, 72% acknowledged suffering financial losses. The dollar figure on these losses added up to approximately $136,822,000. The number of organizations that cited their internet connection as a frequent target of attacks was approximately 54%[[3]](#footnote-3). And this was back when the World Wide Web was still new to the private sector. Nearly 25 years later, things have only gotten worse.

No structure is truly devoid of weaknesses, and the IP suite is no exception. IPs typically contain multiple data packets, which include fragmentation, sequence number fields, and source and destination addresses. The source address is one of the greatest Achilles heels, leading to what is quite possibly one of the most common exploitation of IP weaknesses: Spoofing.

Spoofing is where a hacker forges a source address, thus tricking the destination address into thinking they are receiving a data packet from a trusted source[[4]](#footnote-4). This allows a hacker to trick the target into thinking the malicious data (or deceptive information) they are about to receive is actually coming from a trusted, valid source. It doesn’t even have to be used in an attack. A common scam that targets people during iffy job markets is the “Reshipping” scam[[5]](#footnote-5). A scammer will claim to work from a small shipping company that is understaffed. The jobseeker is offered the opportunity to “be their own boss” by inspecting packages sent to their homes then reshipping them to a designated address (with labels provided by the “employer”). These packages are actually merchandise bought with stolen credit cards or counterfeit money orders. What enables so many people to fall for this scam is the intricate level of IP Address spoofing involved: the jobseeker is directed to a very professional looking website of what they think is a real company[[6]](#footnote-6). It takes a detailed eye, or several minutes of searching on Google, to figure out that the website is a fake; even esteemed institutions like LinkedIn have occasionally been fooled by these phony company websites.

One of the most malicious forms of spoofing is the “Man in the Middle” attack. This is an outright connection hijacking[[7]](#footnote-7). A hacker will intercept a legitimate communication between two hosts, then hijack the connection of either the sender or receiver – effectively stealing their identity for the duration of this scam – to fool their intended target into disclosing confidential information. This type of attack is made possible due to an exploitable weakness known as the “desynchronized state”. When a sequence number in a data packet does not match the sequence number that is expected by the destination address, this results in a desynchronization of the connection. When two hosts are desynchronized enough, they will ignore data packets from each other. This enables a hacker with access to the communication path to create forged data packets with the correct sequence numbers and thereby alter the flow of communication[[8]](#footnote-8).

Another common IP vulnerability exploitation is the “Denial of Service” attack. The DoS attack involves a hacker consuming resources and bandwidth by flooding a target with multiple data packets in a short period of time[[9]](#footnote-9). The hacker will spoof multiple legitimate source address, making it difficult to trace the attack or block the traffic. DoS attacks can dovetail with “Man in the Middle” attacks, cutting off the party that the hacker seeks to impersonate. More often than not, however, it is used in cyberterrorist attacks to deliberate cause target services to crash.

One needs only to read the news to note how many IP vulnerabilities have been exploited by attackers. In December of 2020, the IT Department at the University of Michigan discovered a set of vulnerabilities they labeled Amnesia:33 in four open source TCP/IP stacks (uIP, PicoTCP, FNET, and Nut/Net)[[10]](#footnote-10). Amnesia:33 gave hackers the opportunities to remotely compromise devices, execute malicious code, perform denial-of-service attacks, and steal sensitive information. The UM IT department responded by adding addition network protections and device updates[[11]](#footnote-11). A more recent IP vulnerability, CVE-2024-3273, was discovered earlier this year (2024)[[12]](#footnote-12). This weakness allowed hackers to hijack end-of-life (EOL) network attached storage (NAS) devices. Over 92,000 hosts were exposed to attack[[13]](#footnote-13). Hackers were quick to exploit this vulnerability, sharing affected IP addresses on underground forums. Many of these attacks originated from IP addresses associated with China and Russia.

While most people are aware of the threat hackers pose, there are many common misconceptions about how they operate. The classical image of “Hollywood Hacking” – where a hacker enters a series of code, or just taps a few keys, and says “I’m in” is so prevalent that many people who are not familiar with IP security think this is how real hackers operate. Real hacking is far more tedious and methodical, often relying on social engineering, espionage, or theft to acquire passwords or encryption algorithms. This pop culture misconception has led to an increased emphasis on encryption in cybersecurity. While complex encryption certainly is a good thing to have, it is important for those in the security field to remember, hackers are human and they tend to exploit the human factor to accomplish their goals.

As spoofing in particular is a fairly old strategy, numerous countermeasures are available to us in the Cybersecurity field. Host based defense mechanisms are centered on end hosts that can identify spoofed IP data packets[[14]](#footnote-14). They are easily deployable and compatible with most network infrastructures. However, there is a delay in detecting the spoofed packets, as they need to reach the end host[[15]](#footnote-15). Router based mechanisms are implemented on the intermediate routers of the internet’s preexisting infrastructure. They are more complicated and difficult to deploy, but they have been consistently better than host based mechanisms at stopping spoofed data packets from reaching the intended target[[16]](#footnote-16). One of the oldest and router based defense mechanisms is Martin Address Filtering. This filter checks the IP field for any “red flags”. However, it can only detect and defend against simple, common attacks. A more advanced technique is Reverse Path Forwarding (RPF). With RPF, the router will search for the reverse path of a data packet. If the RPF check proves suspicious, the data packet is then dropped, breaking the chain[[17]](#footnote-17).

Defense against attackers who exploit TCP/IP vulnerabilities is a constantly evolving battle. Fortunately, as technology evolves, so have the options available to those in the Cybersecurity field to prevent attacks.

REFERENCES:

* [*ISO/IEC 7498-1:1994 Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*](https://www.iso.org/standard/20269.html). June 1999. Introduction. Retrieved 26 August 2022.
* Sahni, S., & Jagtap, P. (2017). *A survey of defence mechanisms against IP Spoofing.* *IARJSET*, 4(7), 20–27. <https://doi.org/10.17148/iarjset.2017.4704>
* Harris, B., & Hunt, R. (1999). *TCP/IP security threats and attack methods*. Computer Communications, 22(10), 885–897. <https://doi.org/10.1016/s0140-3664(99)00064-x>
* *Work-from-home scams and reshipping schemes* – United States Postal Inspection Service. (2022, October 6). <https://www.uspis.gov/news/scam-article/work-from-home-scams-and-reshipping-schemes-2>
* *Threat actors actively exploiting CVE-2024-3273 : Underground forums share IP addresses of vulnerable D-Link NAS devices - CYFIRMA*. (2024, May 29). CYFIRMA. <https://www.cyfirma.com/research/threat-actors-actively-exploiting-cve-2024-3273-underground-forums-share-ip-addresses-of-vulnerable-d-link-nas-devices/>
* *TCP/IP stack vulnerabilities affect millions of devices / safecomputing.umich.edu*. (2020, December 10). <https://safecomputing.umich.edu/security-alerts/tcpip-stack-vulnerabilities-affect-millions-devices>
* Zorz, Z. (2021, February 11). Vulnerable TCP/IP stacks open millions of IoT and OT devices to attack - Help Net Security. Help Net Security. <https://www.helpnetsecurity.com/2020/12/09/vulnerable-tcp-ip-stacks/>

1. [*ISO/IEC 7498-1:1994 Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*](https://www.iso.org/standard/20269.html). [↑](#footnote-ref-1)
2. Harris, B., & Hunt, R. (1999). *TCP/IP security threats and attack methods* [↑](#footnote-ref-2)
3. Harris, B., & Hunt, R. (1999). *TCP/IP security threats and attack methods* [↑](#footnote-ref-3)
4. Sahni, S., & Jagtap, P. (2017). *A survey of defence mechanisms against IP Spoofing.* *IARJSET* [↑](#footnote-ref-4)
5. *Work-from-home scams and reshipping schemes* – United States Postal Inspection Service [↑](#footnote-ref-5)
6. *Work-from-home scams and reshipping schemes* – United States Postal Inspection Service [↑](#footnote-ref-6)
7. Sahni, S., & Jagtap, P. (2017). *A survey of defence mechanisms against IP Spoofing.* *IARJSET*, [↑](#footnote-ref-7)
8. Sahni, S., & Jagtap, P. (2017). *A survey of defence mechanisms against IP Spoofing.* *IARJSET*, [↑](#footnote-ref-8)
9. Sahni, S., & Jagtap, P. (2017). *A survey of defence mechanisms against IP Spoofing.* *IARJSET*, [↑](#footnote-ref-9)
10. Zorz, Z. (2021, February 11). Vulnerable TCP/IP stacks open millions of IoT and OT devices to attack - Help Net Security. Help Net Security. [↑](#footnote-ref-10)
11. *TCP/IP stack vulnerabilities affect millions of devices / safecomputing.umich.edu*. (2020, December 10) [↑](#footnote-ref-11)
12. *Threat actors actively exploiting CVE-2024-3273 : Underground forums share IP addresses of vulnerable D-Link NAS devices - CYFIRMA*. (2024, May 29) [↑](#footnote-ref-12)
13. *Threat actors actively exploiting CVE-2024-3273 : Underground forums share IP addresses of vulnerable D-Link NAS devices - CYFIRMA*. (2024, May 29) [↑](#footnote-ref-13)
14. Sahni, S., & Jagtap, P. (2017). *A survey of defence mechanisms against IP Spoofing.* [↑](#footnote-ref-14)
15. Sahni, S., & Jagtap, P. (2017). *A survey of defence mechanisms against IP Spoofing.* [↑](#footnote-ref-15)
16. Sahni, S., & Jagtap, P. (2017). *A survey of defence mechanisms against IP Spoofing.* [↑](#footnote-ref-16)
17. Sahni, S., & Jagtap, P. (2017). *A survey of defence mechanisms against IP Spoofing.* [↑](#footnote-ref-17)