**Timeline of Network-Delivered Attacks and Analysis of IP Spoofing C Code**

Laurence T. Burden

Angelo State University

CS6315: Computer and Network Security

Dr. Erdogan Dogdu

November 5, 2024

Table of Contents

[Default Passwords 3](#_Toc181286280)

[Timeline of Network-Based Attacks 6](#_Toc181286281)

[DNS Cache Poisoning 6](#_Toc181286282)

[Spoofing Attacks 7](#_Toc181286283)

[Man in the Middle (MiTM) 7](#_Toc181286284)

[Distributed Denial of Service (DDoS) 8](#_Toc181286285)

[Other Attacks 8](#_Toc181286286)

[References 9](#_Toc181286287)

[Footnotes 11](#_Toc181286288)

[Tables 12](#_Toc181286289)

[Figures 13](#_Toc181286290)

This paper will cover some common network security issues and report on code that is setup to spoof the IP address of a client. First, the dangers of default passwords will be explained and a truncated list of passwords for devices will be provided. Next, a detailed timeline of network-delivered attacks will be reviewed. Finally, the paper will end with an analysis of the IP spoofing C code.

# Default Passwords

Every network device that requires administrative privileges will need to ship with a default password. The majority of these will be a set standard that all similar models share when they are first created. The Open Web Application Security Project classifies default passwords as a security misconfiguration vulnerability and ranks it sixth out of the top ten vulnerabilities (2021).

A simple search on Google will provide many web pages with a list of default passwords for many network devices. One such list can be found on <https://datarecovery.com> and contains 1,252 password and device pairs (2019). A small sample is shown below as a screenshot of the website.

A white sheet with black text

Description automatically generated

Figure 1. A sample screenshot of all listed network devices and default passwords as shown on datarecovery.com.

# Timeline of Network-Based Attacks

Network-based attacks are those designed to degrade the six security goals. These goals are: confidentiality, authentication, non-repudiation, integrity, access control, and availability (Wu & Irwin, 2013). The exact moment when these attacks started is hard to pin down, but one site lists a cyber-attack by Allen Sherr against MIT in 1962 as the first occurrence (Arctic Wolf, 2024).

Many of these attacks rely on more than one attack vector to be successful. Below is a list of recent significant network-based attacks. They are organized by attack type, followed by date of the attack.

## DNS Cache Poisoning

**Description:** This attack relies on the necessity of DNS responses to be cached. This cache enables quick responses on repeat translations. Cache poisoning is carried out by inserting a fake address record for a domain within the DNS. The fake record then sends unwitting victims to the attacker-controlled website (Wu & Irwin, 2013).

**Discovery (2008):** This attack was made easier with a discovery by Dan Kaminsky in 2008 (Wu & Irwin, 2013). He developed a way to reduce the randomness of the query ID and allow attackers to place fake addresses into the DNS on a more consistent basis. Steps were taken to reduce this risk and mitigate possible attacks shortly after the discovery.

**Re-discovery (2020):** Researchers from Tsinghua University and the University of California, Riverside demonstrated a way to make cache poisoning possible again. This new method “…exploits a side channel that identifies the port number used in a lookup request. Once the attackers know the number, they once again stand a high chance of successfully guessing the transaction ID” (Goodin, 2020).

## Spoofing Attacks

**Description:** Spoofing attacks are any instance of an attacker disguising themselves as a trusted entity to deceive the machine or process. The entity could be a software program, network device, website, or any number of cyber related hardware.

**Operation Aurora (2009):** This was a massive, coordinated attack to gain access to Google and 30 other companies. The attack was undertaken by the hackers slowly working their way up from smaller companies to bigger ones. The credentials gained by attacking the smaller companies were used to spoof access to the bigger targets (Moes, 2024).

**DNS Spoofing on Brazilian Banks (2017):** This attack spoofed the websites of a Brazilian bank with the goal of stealing credentials and identities (Moes, 2024). A DNS cache poisoning attack was used to send queries to the bank’s website to attacker owned sites that contained more malicious code.

## Man in the Middle (MiTM)

**Description:**  As the name implies, this attack is accomplished by the attacker inserting themselves in the middle of some network communication and eavesdropping on it. This allows the attacker to use the gathered information for further attacks, or they may use the data captured in other was, such as selling it or holding it for ransom to the victim. Some examples of communications captured can include emails, texts, chat logs, or website credentials being sent over the internet.

**NSA Data Breach (2013):** Edward Snowden leaked documents that showed that the NSA had the capability to intercept traffic meant for Google. This was accomplished with a spoofed SSL encryption certificate and allowed the agency to obtain search records for all Google users (Fortinet, 2024).

**Comcast Code Injection (2015):** Comcast was found to be replacing third-party advertisements on websites with its own ads. This was done with a combination of a MiTM attack and code injection (Fortinet, 2024). This allowed Comcast to replace ads or even to place ads on otherwise ad-free websirtes.

**Equifax Data Breach (2017):** Equifax suffered a data breach that affected all 100 million of its customers. This attack was accomplished with a vulnerability in the Apache Struts Java framework. This flaw was exploited to insert malicious code into HTTP request content-type headers (Miyashiro, 2021).

## Distributed Denial of Service (DDoS)

**Description:** DDoS attacks are crafted to deny others from reaching resources. This is usually done by creating millions of zombie computers through other malicious attacks. The collection of zombies, called a botnet, are then instructed to flood a website or other resource with too many requests to handle. The resource then fails due to the unmanageable number of requests.

**Mirai Dyn DDoS (2016):** A major DNS provider named Dyn was attacked with a one terabit per second network traffic flood (A10 Networks, 2024). This attack made many sites unreachable. The sites included GitHub, HBO, Twitter, Reddit, Netflix, and many more. Over 10 million unique IP address were found to have been a part of the botnet that caused this DDoS attack.

**AWS Attack (2020):** Many AWS services were rendered unreachable when a DDoS attack was launched against the web giant. This attack used a technique called the Connectionless Lightweight Directory Access Protocol (CLDAP) reflection. This attack spanned three days and saw 2.3 terabytes per second of data being sent (A10 Networks, 2024).

**Multiple Sites (2023):** New methods of DDoS attacks was witnessed when AWS, Google, and Cloudflare were attacked with botnets of unusually small size. Researchers found that the attack exploited a vulnerable feature of HTTP/2 that would allow rapid request cancellation using the RST\_STREAM frame, and the servers would be overwhelmed by the streams being continuously opening and closing (A10 Networks, 2024).

## Other Attacks

**Heartbleed (2014):** An extremely dangerous bug was found in OpenSSL that would allow an attacker to read memory from a webserver, including private keys used for SSL/TLS. After the attacker has these keys, they can eavesdrop on communications between a user and a web server. The bug was fixed by adding a bounds check before a specific memcpy() call in SSL3 (OWASP, n.d.).

**Replay Attacks:** These attacks are accomplished by copying some information and resending it to trick a service into re-accomplishing an action without the victim’s knowledge or consent. The proliferation of NFC chips for credit transactions saw the need to protect against such attacks. The Flipper Zero device has made copying insecure building badges and garage door openers easy for any person.

References

*A05:2021 – Security Misconfiguration*. OWASP Top 10:2021. (2021) <https://owasp.org/Top10/A05_2021-Security_Misconfiguration/>

*List of default passwords*. Datarecovery.com. (2019, May 30). <https://datarecovery.com/rd/default-passwords/>

Wu, C.-H., & Irwin, J. D. (2013). *Introduction to computer networks and cybersecurity*. CRC Press.

Arctic Wolf. (2024, April 19). *History of cybercrime*. History of Cybercrime. <https://arcticwolf.com/resources/blog/decade-of-cybercrime/>

Goodin , D. (2020, November 12). *DNS cache poisoning, the internet attack from 2008, is back from the dead*. Ars Technica. <https://arstechnica.com/information-technology/2020/11/researchers-find-way-to-revive-kaminskys-2008-dns-cache-poisoning-attack/>

Moes, T. (2024, January 25). *Spoofing examples (2024): The 4 worst attacks of all time*. SoftwareLab. https://softwarelab.org/blog/spoofing-examples/

*What is a man-in-The middle (mitm) attack? types & examples*. Fortinet. (2024). https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack

Miyashiro, I. (2021, April 30). *Case Study: Equifax Data Breach*. Sevenpillarsinstitute.org. https://www.sevenpillarsinstitute.org/case-study-equifax-data-breach/

*Five most famous ddos attacks and then some*. A10 Networks. (2024, October 23). https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

*Heartbleed Bug*. Heartbleed Bug | OWASP Foundation. (n.d.). https://owasp.org/www-community/vulnerabilities/Heartbleed\_Bug