THE SUFFOLK LAWYER
THE OFFICIAL PUBLICATION OF THE SUFFOLK COUNTY BAR ASSOCIATION
DEDICATED TO LEGAL EXCELLENCE SINCE 1908 www.scba.org Vol. 33, No. 2 – OCTOBER 2018

CYBER

Spoofing

By Victor Yannacone Jr.

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. It can be used to gain access to your personal information, spread malware through infected links or attachments, bypass network access controls; redistribute traffic; or carry out *phishing* attacks.

Email spoofing

Email spoofing is possible because of limitations in SMTP (Simple Mail Transfer Protocol), a technology for allowing emails to be sent from one person to another but which doesn't verify whether the email address in the "From" field is genuine.

Sender information is easy to spoof and can include mimicking a trusted email address or domain by using alternate letters or numbers to appear only slightly different than the original or disguising the "From" field to be the exact email address of a known and/or trusted source

Caller ID Spoofing

Caller ID Spoofing makes it appear as if phone calls are coming from a known and/or trusted source or from a specific geographic location. Attackers can then use social engineering to convince their targets to, over the phone, provide sensitive information such as passwords, account information, social security numbers, and more.


Victor Yannacone Jr.

This technique is widely available today and very much legal. It is only a crime if the spoofer uses it to defraud victims.

Basic defense includes hanging up and calling the number yourself. You can also use *Trapcall* (https://www.trapcall.com/) a paid service that reveals the true identity of a caller. While not foolproof, it is a reasonable starting point for safe caller-ID.

IP Address Spoofing

IP Address Spoofing, also called IP address forgery, IP spoofing or host file hijacking, occurs when an attacker alters the Source IP Address headers, the IP (Internet Protocol) address that a data packet is sent from, so that it appears that these packets originate from the legitimate source address that they have hijacked.

Having masked themselves as a trusted host, the attacker is free to impersonate a web site, gain access to networks to spy, launch attacks, or hijack web browsers. Servers and networks that authenticate based on IP, and not accounts and passwords are particularly vulnerable and at risk.

If a user types a web address (URL or Uniform Resource Locator) into a hijacked browser, they may be misdirected to a spoofed web site designed to look just like the legitimate URL that the user typed in. There, they may unknowingly interact with malicious content concealed on the bogus page that could log their key strokes (keylogging), act as a pipeline for attackers to steal or corrupt sensitive data, install malware, or take over infected systems.

Protecting yourself from IP spoofing is not easy since the malicious hacker takes advantage of IT infrastructure weaknesses that you do not have control over. You can, however, apply ingress and egress filtering on your Wi-Fi router to ensure incoming data packets aren't spoofed and verify that data packets leaving your device are authorized to do so.

- Always encrypt your Wi-Fi network and change the default password of your router!
- Passwords should be at least 10 characters long, contain a special character (such as *, &, or %), a number, and both uppercase and lowercase letters.

ARP (Address Resolution Protocol) Spoofing

ARP is used to steal data, modify it in transit, or interfere with traffic on a LAN (local area network).

DNS (Domain Name System) spoofing

DNS reroutes a domain name to an IP address of the attacker and redirects users of that domain name to a server maintained by the attacker.

Website Spoofing

Website Spoofing mimics an existing site known to and/or trusted by the user to gain login and other personal information from users.

Pharming

Pharming attacks redirect legitimate URLs to spoofed web sites that are designed to look exactly like the real thing where user credentials and

(Continued on page 25)

Spoofing *(Continued from page 6)*

financial information may be stolen or demands for money made.

Phishing

Phishing is an email scam to get unsuspecting recipients to click on links to *pharming* websites where malware can be ported onto the user's system or the recipient will be directed to enter confidential or sensitive information.

The sender's name on the fake email and text messages is usually someone known to the recipient, or the name of an organization with which they're familiar. Subject lines and body text may be intimidating or enticing.

Prevent spoofing attacks by immediately adopting these cybersecurity best practices:

- Two-factor authentication.
- Install firewalls on all networks; then set policies restricting the flow of traffic to and from each system to block false IP addresses.
- Use packet filtering to inspect data as it is transmitted across your network.
- Install whatever anti-spoofing detection software is available for your operating system.
- Use secure network protocols with encryption, such as HTTP Secure (HTTPS), Secure Shell (SSH), and Transport Level Security (TLS).
- Only visit sites with proper SSL certification.
- Avoid so-called "trust relationships," where data transfer protocols with third parties only require IP addresses to authenticate them.
- Avoid providing personal information online, particularly email and social media.
- Don't open attachments in unsolicited emails, and get verification from the sender in person, or on the phone before opening any unsolicited attachment.
- Continuously update your network and upgrade to the latest cybersecurity software.
- Use penetration testing to identify vulnerabilities in your network.
- Provide cybersecurity training to employees.

Note: Victor John Yannacone Jr. is an advocate, trial lawyer, and litigator practicing today in the manner of a British barrister by serving of counsel to attorneys and law firms locally and throughout the United States in complex matters. Mr. Yannacone has been continuously involved in computer science since the days of the first transistors in 1955 and actively involved in design, development, and management of relational databases. He pioneered in the development of environmental systems science and was a cofounder of the Environmental Defense Fund. He can be reached at (631) 475–0231, or vyannacone@yannalaw.com, and through his website https://yannalaw.com.