CYBV 326: Final Exam

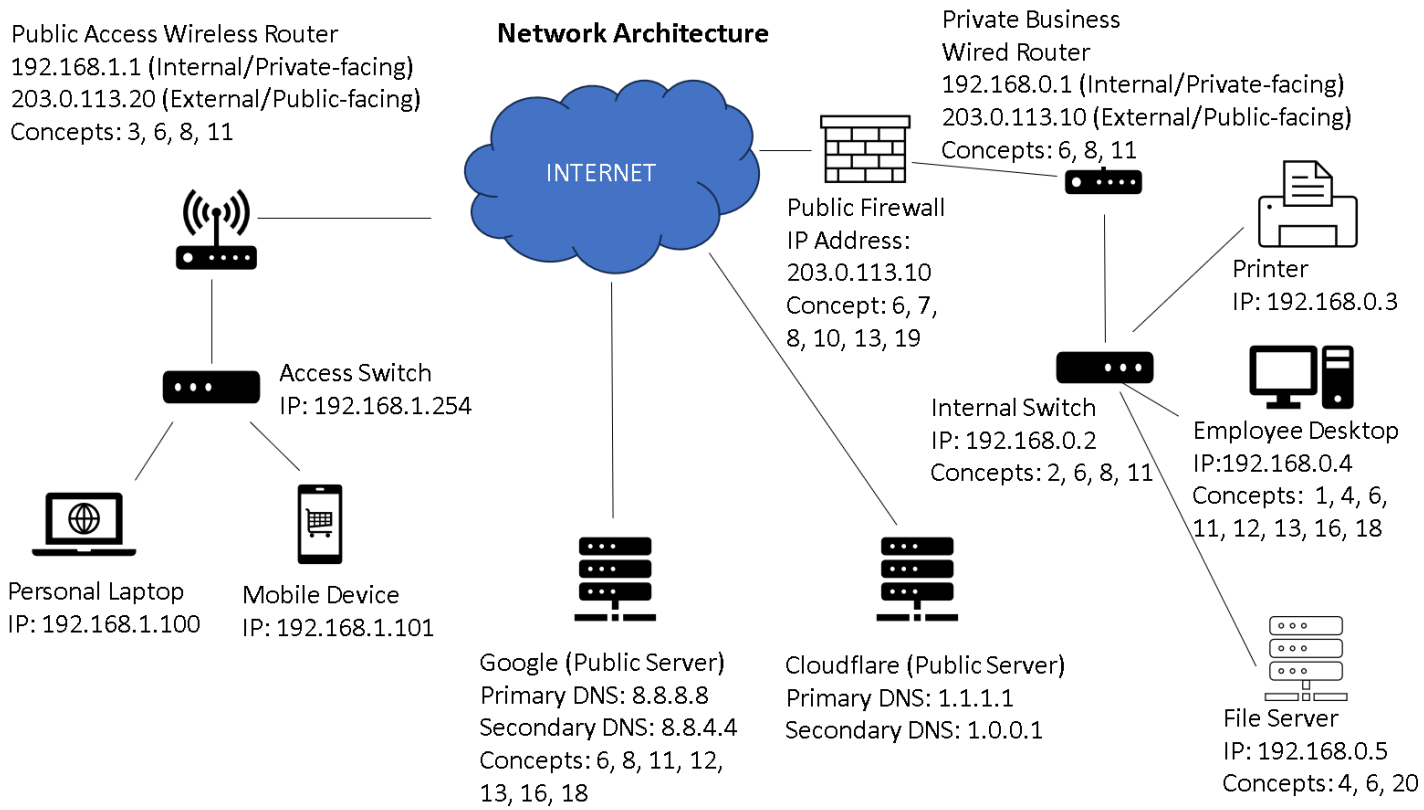
Chas H. Riley

The University of Arizona

CYBV 326: Introductory Methods of Network Analysis

Professor Jonathan Martinez

December 10, 2023


Network Architecture
Public Access Wireless Router
192.168.1.1 (Internal/Private-facing)
203.0.113.20 (External/Public-facing)
Concepts: 3, 6, 8, 11
INTERNET
Private Business
Wired Router
192.168.0.1 (Internal/Private-facing)
203.0.113.10 (External/Public-facing)
Concepts: 6, 8, 11
Public Firewall
IP Address:
203.0.113.10
Concept: 6, 7,
8, 10, 13, 19
Printer
IP: 192.168.0.3
Access Switch
IP: 192.168.1.254
Internal Switch
IP: 192.168.0.2
Concepts: 2, 6, 8, 11
Employee Desktop
IP:192.168.0.4
Concepts: 1, 4, 6,
11, 12, 13, 16, 18
Personal Laptop
IP: 192.168.1.100
Mobile Device
IP: 192.168.1.101
Google (Public Server)
Primary DNS: 8.8.8.8
Secondary DNS: 8.8.4.4
Concepts: 6, 8, 11, 12,
13, 16, 18
Cloudflare (Public Server)
Primary DNS: 1.1.1.1
Secondary DNS: 1.0.0.1
File Server
IP: 192.168.0.5
Concepts: 4, 6, 20

Resource Request

Bob, an IT employee who works for Jurassic Park, decides to use his desktop to log onto the company's private wired router while he's working in the office. Bob needs to log into his employee account to access a file that is stored on the businesses' file server that is in the private employee network. For Bob to access anything in his company's private network, he could also use Wi-Fi access if it's available. Wi-Fi operates on the Network Access Layer and uses the Wi-Fi frame to connect devices to a network using the internet. The only differences between Wi-Fi or wireless and wired is the physical connection of a device to a router.

Chances are that Bob's desktop is a part of a subnet group in the company. A subnet can be used for multiple reasons. For Bob, it's most likely used to create efficiency and for security. A subnet groups devices in a network to a certain set of IP addresses. This separates devices from having access to controls they should or shouldn't have. Subnetting operates on the Network Access Layer.

The flow of data when accessing the internet passes from Bob's desktop to the internal switch, to the private router, to the firewall, to the internet, to a public server (if that server is needed/accessed). That data flow would then move from the public server to the internet, then to the firewall, to the private router, to the internal switch and back to Bob's desktop. When data flow reaches the internal switch, the process of routing takes place. This routing process operates on the Network Access Layer and the Internet Layer. Routing uses the IP datagram, and its purpose is to identify the best possible route for data. This improves traffic efficiency.

When Bob's desktop connects to the Private Wired Router, the router uses the Ethernet protocol and switching to ensure efficient data forwarding within the local network. Ethernet protocol and switching both operate at the Network Access Layer and their data unit is in ethernet frames. The Ethernet protocol's purpose is to allow communication between devices that are on the same network.

Switching is used to send data in a network from one device to another based on Media Access Control (MAC) addresses.

Before Bob's desktop can communicate with the file server, it needs to obtain the MAC address of that server. To do this, Bob's desktop sends an Address Resolution Protocol (ARP) request. An ARP is a request/reply protocol that also operates on the Network Access Layer. It helps map out or locate other devices in a network. It also translates Internet Protocol (IP) addresses into a physical MAC address so anything belonging to the network can be found. An IP address operates at the Internet Layer and uses IP datagrams as a measurement. IP datagrams are essentially packets of data that contain a header (source and destination information) and the payload, or all information being sent. Think of IP addresses as a package being sent in the mail. The header is the sender and receiver information, and the payload is what is inside the package. If for any reason the requests sent run into an issue, Bob's desktop might receive an Internet Control Message Protocol (ICMP). An ICMP is a protocol that networks use to communicate an error. This process is also known as error detection and correction, and it's used to transfer information more reliably. The error detection and correction process operates on the Transport Layer.

The ARP data would travel from the desktop to the internal switch, and from the internal switch, it would flow to the file server. Based on the network diagram I made, the office internal network would most likely be located on that file server or through the internet on a 3rd party cloud server that is only accessible by the Jurassic Park employees. The private file server is also connected to the internet and would still send data traffic through the internet and back to the private server before sending it back to Bob's desktop. The file server containing the internal network would then recognize that Bob's ARP request to the device that holds the MAC address of the file server belongs to itself. The file server then responds with an ARP reply, providing its MAC address to the switch and then back to Bob's desktop.

As soon as Bob's desktop has received this ARP reply, it would then send a Hypertext Transfer Protocol (HTTP) request to the file server using a Transmission Control Protocol (TCP). HTTP is the most basic form of communication for the World Wide Web. This protocol connects a host with a website or server. The easiest way to think of an HTTP is to think of it as the telephone that connects between two people having a conversation. A benefit used by TCP is flow control. Flow control operates at the Transport Layer and its purpose is to regulate the amount of data sent from point A to point B. This keeps either side from being overwhelmed. Another benefit that TCP provides is Secure Sockets/Transport Layer Security (SSL/TLS). SSL/TLS operates on the Application Layer and uses the port 443 in the form of a TCP. The purpose of SSL/TLS is for security in the form of encrypted communication.

When accessing domain names of websites, the Domain Name System (DNS) will take those domain names and translate them into IP addresses, so communication is possible. The DNS uses the protocol port of 53, which is a User Datagram Protocol (UDP). The data sent is a DNS inquiry/response across the internet to allow communication. Think of DNS as a phone book for websites, servers and devices accessing the internet. DNS operates on the Application Layer. UDP operates on the Transport Layer and utilizes the port 53, which is used for DNS inquiries.

Port 80 is what would be accessed on the file server, which is listening for incoming HTTP requests. Port numbers are used to communicate with devices in a network. All protocols are associated with specific port numbers. The HTTP request from Bob's desktop passes through the public firewall that separates the private employee network from the public internet. The firewall can operate on multiple layers, but this firewall functions as a traffic controller. Since the firewall is inspecting and controlling data that is transmitted, it would be active on the Application Layer. This firewall is a security measure that ensures only authorized traffic is allowed to enter or leave the private network.

If the file server's response needs to leave the private network and go to the public internet, the private wired router performs Network Address Translation (NAT) to translate the internal IP

address of the private file server to the public IP address that was given to the router for communication with external networks. A NAT is a process performed by the private wired router (usually performed by a router in general). This process involves the router taking the private IP addresses of devices on a network and assigning them a public IP address on the internet. The NAT process operates on the Internet Layer and helps with communication on the internet.

The file server completes Bob's request and then sends back an HTTP response with the requested file data. This response travels through the private network, through the internal switch, back through the router, through the public firewall, to the internet, back through the firewall, the router, the switch and finally back to Bob's desktop. This file data sent will come in the form of a File Transfer Protocol (FTP). FTP utilizes ports 20 or 21 and is sent using TCP. The data unit sent is a command or response and is followed by the FTP data. The main purpose of FTP is to transfer files securely through a network.

Concepts Used

Network Access Layer (Layer 1):

1. Ethernet Protocol
2. Switching
3. Wi-Fi (802.11)
4. MAC Address
5. ARP (Address Resolution Protocol)

Internet Layer (Layer 2):

6. IP (Internet Protocol)
7. ICMP (Internet Control Message Protocol)
8. Routing

9. Subnetting

10. NAT (Network Address Translation)

Transport Layer (Layer 3):

11. TCP (Transmission Control Protocol)

12. UDP (User Datagram Protocol)

13. Port Numbers

14. Flow Control

15. Error Detection and Correction

Application Layer (Layer 4):

16. HTTP (Hypertext Transfer Protocol)

17. DNS (Domain Name System)

18. SSL/TLS (Secure Sockets Layer/Transport Layer Security)

19. Public Firewall

20. FTP (File Transfer Protocol)

Research and Analysis

SQL Injection (Application Layer Attack)

In October 2012, a group of hackers named “Team GhostShell” breached 53 universities worldwide, including prestigious institutions like Harvard, Stanford, and Cornell. They published thousands of personal records, which included the names, email addresses, usernames, passwords, addresses, and phone numbers of students, faculty, and staff on the website “Pastebin.com”. While

some of the information leaked was already available to the public, other records contained sensitive data such as dates of birth and payroll information.

Attack Method: The method used by this hacker group is known as SQL Injection. SQL Injection is a type of attack that occurs when malicious code is inserted into input fields of a web application. This type of input is a form of code that tells a web application what to do. If someone can manipulate the application's SQL database, they can gain access to a website or server as if they owned it.

Attackers' Goal: It's unclear on the motives of this hacker group. The group claims that their motive was to raise awareness about changes in education Universities which would line up with hacktivism ideology.

Vulnerability Exploited: The breach involved the use of SQL injection, exploiting software vulnerabilities to access databases. This attack took advantage of poor input validation and lack of parameterized queries in the web application of these universities which led to allowing attackers to inject SQL commands with ease. The leaked data was analyzed by a firm specializing in identity theft prevention and deemed legitimate, with evidence suggesting the hackers had been inside the university systems for at least four months. The group did acknowledge that some of the breached servers already had malware injected (Perlroth, 2012).

Recommendations: The attackers typically aim to gain unauthorized access to sensitive data, modify or delete data, or perform other malicious actions within the database. Seeing that universities are attractive targets for hackers due to the vast amount of personal records they store, it only makes sense to increase measures to secure their servers. Attackers input SQL commands into web forms or URL parameters to gain unauthorized access to the application's database or to manipulate the database in unintended ways. To mitigate this, developers should use parameterized queries, input

validation, and output encoding to prevent malicious SQL code from being executed. Additionally, implementing proper access controls and least privilege principles can help limit the impact of a successful attack.

MAC Address Spoofing (Network Access Layer)

MIT has released a report on its actions in the Aaron Swartz case, which found no wrongdoing on MIT's part but raised concerns about certain policies and procedures. The report was led by Professors Hal Abelson and Peter Diamond and offers forward-looking questions for the Institute to address. MIT's position throughout the prosecution was one of neutrality and it did not seek federal prosecution or oppose a plea bargain. However, the report notes that MIT's neutrality did not take into account certain factors, such as Swartz's contributions to Internet technology and the questionable application of the law. MIT President L. Rafael Reif encouraged the MIT community to read the report in its entirety and acknowledged that there will be further discussion and reflection on the matter.

Media Access Control (MAC) Address Spoofing is an attack that involves a cybercriminal changing their device’s network interface to impersonate another device on that network.

Attack Method: Attackers modify the MAC address of their network interface to mimic the MAC address of an authorized device, allowing them to bypass access controls and gain unauthorized network access. - Attackers' Goal: The attackers typically aim to gain unauthorized access to the network, bypass network access controls, or conduct man-in-the-middle attacks by intercepting traffic intended for the legitimate device. - Vulnerability Exploited: This attack takes advantage of the inherent trust in MAC addresses within the local network environment, as well as the lack of robust mechanisms to authenticate MAC addresses. - Recommendations: To mitigate MAC Address Spoofing, organizations can implement port security features on network switches to restrict the number of MAC

addresses allowed on a port. Additionally, deploying network access control solutions that authenticate endpoints based on more than just MAC addresses, such as 802.1X authentication, can help prevent unauthorized network access and mitigate the risk of MAC Address Spoofing.

Man-in-the-Middle (MitM) Attack (Transport Layer Attack)

The DigiNotar incident, the first digital disaster in the Netherlands. DigiNotar was a Certificate Authority (CA) that issued digital certificates for secure digital communication. In 2011, it was discovered that DigiNotar had been compromised, leading to the generation of falsified certificates. The Dutch government revoked its trust in all certificates issued by DigiNotar, as the authenticity of the certificates could no longer be verified. The article analyzes the underlying weaknesses that allowed the situation to escalate into a disaster, including lack of oversight, lack of security attention and risk awareness, and the absence of an effective mitigation strategy. It also highlights the need for better coordination between the government as a protector and as a service provider, improved oversight of CAs, and the development of better mitigation strategies. The DigiNotar incident is discussed in the broader context of attacks on information security companies, which have introduced a "meta vulnerability" in the cyber security landscape. The article concludes by emphasizing the importance of better preparedness, response capacity, and resilience to future digital disasters.

References

Abelson, H., & Diamond, P. (2013, July 30). *MIT releases report on its actions in the Aaron Swartz case*. MIT News | Massachusetts Institute of Technology. https://news.mit.edu/2013/mit-releases-swartz-report-0730

Capitol Technology University. (2020). *AWS Shield Threat Landscape Report -Q 1 2020*. https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf

Perlroth, N. (2012). *Hackers Breach 53 Universities and Dump Thousands of Personal Records Online*. https://security.research.ucf.edu/Documents/News/Hackers%20Breach%2053%20Universities%20and%20Dump%20Thousands%20of%20Personal%20Records%20Online.pdf

van der Meulen, N. (2013). DigiNotar: Dissecting the First Dutch Digital Disaster. *Journal of Strategic Security*, *6*(2), 46–58. https://doi.org/10.5038/1944-0472.6.2.4