Cody Riggins

Professor Hendricks

CIDS 484

March 9th, 2022

Rough Draft Milestone 2

I - Introduction:

Packet Sniffing has recently become a highly prioritized security protocol within cyber security, as companies such like Target, Walmart, Best Buy, and more begin to offer free Wi-Fi networks for their customers, opportunities arise for people looking to use that network maliciously. Throughout this paper we will discuss, research, and monitor network traffic analysis known as Packet Sniffing. As we unfold the processes of hardware, software, and the uses together we will begin to see what packet sniffing equates to, and why hackers are using this option to uncover information from companies, and consumers alike.

As you begin to journey into packet sniffing, you'll soon find that programs behind packet sniffing are extremely efficient at capturing data and showing the data you are capturing. Packet Sniffing is known as a program or application that hackers will use to grab packets of information within the network such as a public Wi-Fi network that is communicating between two connections such as two computers via email. The packet sniffing program will attempt to pull the information sent from within those packets and report that information back to a hacker's computer, or device that a hacker would be using. Packet sniffing first came to being as early as 1988 known as the Sniffer Network Analyzer, since 1988 this program has been passed through several hands of companies, such as McAfee. The first generation of packet sniffers read the headers of data packets within a network. Within the first many years of packet sniffing being able to grab the header information within a message was a heavily sought-after ability to do, as hackers, or companies could decipher what another company was sending to people and grab that information. Another explanation of packet sniffing is as a method of tapping each packet as it flows across the network, otherwise known as the technique sniffing, in which a user sniffs data belonging to other users of the network. Packet sniffers can operate as an administrative tool, or in most cases, it is used for malicious intent. Network administrators use them for monitoring and validating network traffic. Packet sniffers are programs or applications that travel across the network layer of the transmission control protocol/internet protocol (TCP/IP) layer. As the packets are retrieved from the network layer the data is then interpreted.

As networking and overall computing power began to change in the last twenty years, network administrators have begun to prioritize options that would allow for admins as well as the normal operator within the company to have useful tools that would prevent someone from gaining access to their network and using a packet sniffer inside of a company. A network administrator can employ several protections and techniques inside of their network to protect and prevent data sniffers. They also tend to implement several applications or programs that will detect when a data sniffer is being used on their network. With the ever-expanding network of the internet. The scope of networking, and data security, and data information sent has increased tremendously in the last few years, this has led to the development of sophisticated tools that are useful in the cyber security mitigation but are also widely used by criminals to eavesdrop or gain illegal access. Packet sniffing is a great example of the cyber tools that have been used in both positive, but also malicious intent across the internet world.

While these tools have become a widely used favorite by criminals as they will often scan unprotected data within a network they plan to sniff. A term known as White Hat Hackers, or people who use programs that criminals often use, will often attempt to prevent these criminals from gathering information without being paid, or necessarily related to the company, or person the criminal is targeting, White Hat Hackers will often counteract against those criminals and help prevent them from being able to gain access to information and networking tools such as WireShark, and TCPDump that have become one of the most used packet sniffing tools to date.

II - Hardware – Computer Networks, Routers, and Encryption Devices

A standard company that is operating online with often have computers, laptops, or internet devices they are extremely basic and used solely for business purposes. A good example would be a Mobile Point of Sales (MPoS) system typically used on tablets, or laptops. These MPoS systems are often an application downloaded by the company on an approved device that has a VPN configuration set on these devices that allow it to connect to an internal website/server. Another device would be a computer that is typically built within a monitor, or best known as All-In-One computers, an Apple Mac is a perfect example of these types of computers, but Dell, Samsung, Asus, etc. develop these options as well. These devices will have implementation of VPNs (Virtual Privatized Networks) that would allow a network administrator to access and monitor incoming and outgoing traffic on these devices. During a routine check and sweep of these networks administrators will often monitor the traffic flow, during checks if they or the application they often use notice anything within the check that may seem abnormal such as a device accessing and interpreting an abnormal amount of data inside of the network layer, it will prompt or the user will prompt an investigation of that system, and often times will access that device without the user knowing they are accessing it. This allows for the administrator or the application to monitor and see what is happening during the time of use, to further breakdown this process, an administrator will open the device by remote access and breakdown the traffic flow within that device. The administrator will check the routing information, for example, when an email is sent via an internal emailing system, it will often house the sending IP address of the user, and the receiving IP address of the user who is receiving the email, but it will also include the information of the email, and the users it is being communicated between. An administrator doing a routine sweep investigation will be able to detect if a packet sniffer is being used on these products by checking when, where, and how the packets that are being sniffed, using an application or tools given to them by the company that were developed by the IT team, or a company that develops these network monitor detectors. As companies and IT begins to further develop their security to prevent attacks, they will often use applications or implementation within their network access to reroute information from inside their network to prevent or stop a packet sniff from happening, for example if a device is investigated and is determined to be hacked, or using software to grab information, administration will use a technique known as rerouting, where they are take information that is being sent to a user inside of that hacked area, and further encrypt that data in order to prevent the criminal from accessing company information, or customer information.

Another implementation that administrators will use is known as encryption inside of devices such as credit card readers, mobile point of sales systems, and even computer devices such as laptops. Encryption allows for the company to essentially mix the information inside of random packets of lettering, symbols, and numbers. This can help prevent hackers from gaining knowledge from information if it is leaked, these hackers would ultimately have to reverse engineer that encryption, which if done correctly, makes it extremely difficult for the hackers to decrypt the information.

III - Software – Encryption

Encryption software has helped maintain and prevent hackers, or competing companies, from accessing and stealing information such as financial information, company secrets, such as product that is not released, etc. Encryption allows for these companies to safely send and receive information over a public network if needed, or even when using a private network that may or not be breached. Encryption software is just another way for companies to further protect themselves from attacks, and breach of information. Encryption has many options, but the most sought-after option for technology in our current universe of technology is Cryptography, where the operating user will maintain a private key, and send its public key to user it is going to be communicating with and allow for each user to trust each other by operation.

Cryptography allows for multiple users to communicate inside and outside of their privatized network at a company, or from home, by using “keys”. These keys which are generated by a program, are sent to the users through their IP address, or communication address, which often is their email address that is used inside of the company. The sender will then use plaintext data, or a simple email, and lock it behind their public key which then encrypts or ciphers data, is sent to the other user, who than uses their private key, which was accepted by the previous user, to decrypt and unlock the information within that data. For example, a user could encrypt a message like “Hello, how are you today?” and send it to the user across the company, which would use their key to decrypt the message, and allow them to respond to the message and encrypt their message back to the user, who would than be able to decrypt the senders message using their private encryption key.

Another method that companies, and IT administrators are using is known as Symmetric Encryption, which is very similar to the previous method listed known as Asymmetric Encryption, but instead of using a private key and a public key, or 2 keys in total. One total key is used between two communicators. This option is another protected option that companies and people will use when communicating private information, but ultimately could fall short of protection if a user that is inside of the trusted realm of the communication is hacked or breached. While this method is safer than just sending a base email through a privatized network if one of the trusted users is hacked, the hacker would be able to decrypt the data instantly as the user is already approved for the encryption, and decryption process.

IV - Preventative Measures – Stopping attacks

In this portion of the paper, we will begin talking about the prevention and software implantation, that would stop packet sniffers from being able to monitor traffic flow inside of both private and public networks. We will also talk about how to prevent hackers from being able to implement software inside of your network when they gain access to trusted devices.

When developing security for your company, or just to protect yourself at home, you’ll want to consider the options you have before in order to protect information. Packet sniffing being the most easily accessible and used tool by criminals, and hackers. This is a high priority for people who want to protect their information whilst surfing the web on both private and public networks. Prevention of packet sniffers is usually a simple task companies, and people can do to prevent hacker accessing their information being sent out and received. The first and easiest task the people will use, is known as a VPN or a virtualized private network, this would allow a user to hide, or change, their IP address by using of an application that generates one for them, and places their IP in a different geological location, for example, you could live in River Falls, Wisconsin, but set your VPN address to Saint Paul, Minnesota. This often will prevent a hacker from being able to see your true IP address that often contains information about yourself, and your network. Another step users can take is by implementing encryption when communicating with someone regarding sensitive information, like banking information, social security numbers, or any information that may contain information people could use to solicit and steal assets. The average internet user will almost never have to use this option unless they are suspicious about the network they are using, most often public networks.

Another preventative option companies will use is prevention or implementation of software that prevents third-party software to be added to company assets, or trusted devices that a company uses. A good way to prevent these applications from getting downloaded or added into their network is use of an authentication process, often companies will use a configuration that would go through a 1 to 3 step process of getting applications added to their trusted device. If a user wanted to add Safari or Google Chrome instead of Internet Explorer, the application would be sent to the IT Administrator by notification through the software, the administrator would than look into the application by use of security tools, or informational tools companies have on hand about applications, and decline or approve the download request. This method is the easiest, and most cost-effective process to do inside of a company but could ultimately lead to their demise if the administrator becomes lazy, or malicious towards the company they are working for. When a company implements these options they often have more than one person approving and denying requests, as reports have shown that companies will often be attacked or breached due to a malicious employee within the company, instead of an outright random attack on the company.

V – Utilization of Hardware & Software

Work In Progress – Implementing personal experience by use of WireShark.

VI – Resources Used & Citations

Citations:

S. Ansari, S. G. Rajeev and H. S. Chandrashekar, "Packet sniffing: a brief introduction," in IEEE Potentials, vol. 21, no. 5, pp. 17-19, Dec. 2002-Jan. 2003, doi: 10.1109/MP.2002.1166620.

P. Goyal and A. Goyal, "Comparative study of two most popular packet sniffing tools-Tcpdump and Wireshark," 2017 9th International Conference on Computational Intelligence and Communication Networks (CICN), 2017, pp. 77-81, doi: 10.1109/CICN.2017.8319360.

Ibrahim Ali Ibrahim Diyeb, Anwar Saif, Nagi Ali Al-Shaibany
International Journal of Computer Network and Information Security 10 (7), 12, 2018

Z. Zhao, W. Huangfu and L. Sun, "NSSN: A network monitoring and packet sniffing tool for wireless sensor networks," 2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC), 2012, pp. 537-542, doi: 10.1109/IWCMC.2012.6314261.

D. Álvarez Robles, P. Nuño, F. González Bulnes and J. C. Granda Candás, "Performance Analysis of Packet Sniffing Techniques Applied to Network Monitoring," in IEEE Latin America Transactions, vol. 19, no. 3, pp. 490-499, March 2021, doi: 10.1109/TLA.2021.9447699.