Violation of Users Privacy By Iptv Packet Sniffing Office Networks

G.S.Geethamani [1], Mansi Goyal [2]
[1]Associate Professor, Dept of IT
[2]Dept of IT
[1, 2]Hindusthan College Of Arts And Science,
Behind Nava India, Coimbatore-641 028, Tamil Nadu, India

Abstract- *On wired broadcast LANs, depending on the network structure (hub or switch), one can capture traffic on all or just parts of the network from a single machine within the network; however, there are some methods to avoid traffic narrowing by switches to gain access to traffic from other systems on the network (e.g., ARP spoofing). For network monitoring purposes, it may also be desirable to monitor all data packets in a LAN by using a network switch with a so-called monitoring port, whose purpose is to mirror all packets passing through all ports of the switch when systems (computers) are connected to a switch port.*

When traffic is captured, either the entire contents of packets can be recorded, or the headers can be recorded without recording the total content of the packet. This can reduce storage requirements, and avoid legal problems, but yet have enough data to reveal the essential information required for problem diagnosis.A technique commonly used by hackers and penetration testers for getting hold of traffic in a switched environment is to use ARP poisoning. Basically ARP poisoning is a technique where two hosts on a network are tricked into sending packets destined for each other to a sniffer machine on the network

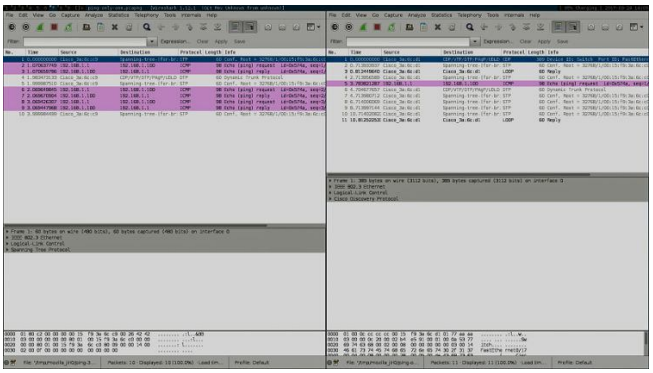
Preventive measures for network traffic from being sniffed are to use encryption such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Encryption doesn't prevent packet sniffers from seeing source and destination information, but it does encrypt the data packet's payload so that all the sniffer sees is encrypted gibberish.

Keywords- session-hijacking, CIA, spoof attack, CSS, SSL, captcha

I. WHAT ARE PACKETS?

When using the internet to send emails, access bank accounts, upload images, or even type in a URL, the data being sent is broken into pieces. These pieces, or packets, are sent from your computer to the receiving end. The receiving end could be another computer or a server.

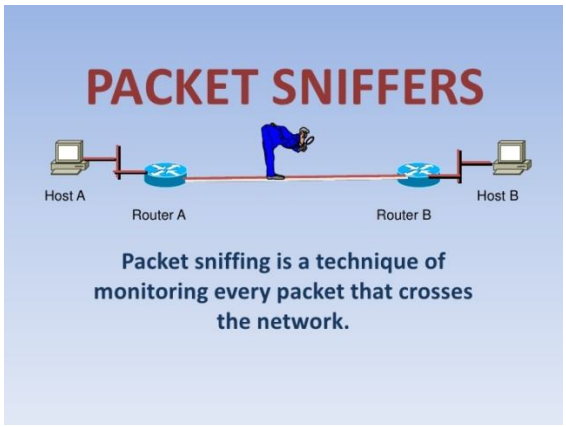
These packets must travel through the Internet to their destination, which could leave the packets vulnerable to packet sniffers.



II. WHAT ARE PACKET SNIFFERS?

Packet sniffing may sound like the latest street drug craze, but it's far from it. Packet sniffers or protocol analyzers are tools that are commonly used by network technicians to diagnose network-related problems. Packet sniffers can also be used by hackers for less than noble purposes such as spying on network user traffic and collecting passwords.

Packet sniffers come in a couple of different forms. Some packet sniffers used by network technicians are single-purpose dedicated hardware solutions while other packet sniffers are software applications that run on standard consumer-grade computers, utilizing the network hardware provided on the host computer to perform packet capture and injection tasks.



Packet sniffing is the act of capturing packets of data flowing across a computer network. The software or device used to do this is called a packet sniffer. Packet sniffing is to computer networks what wire tapping is to a telephone network.

Packet sniffing has legitimate uses to monitor network performance or troubleshoot problems with network communications. However, it is also widely used by hackers and crackers to gather information illegally about networks they intend to break into. Using a packet sniffer it is possible to capture data like passwords, IP addresses, protocols being used on the network and other information that will help the attacker infiltrate the network.

A "Packet Sniffer" is a utility that sniffs without modifying the network's packets in any way. By comparison, a firewall sees all of a computer's packet traffic as well, but it has the ability to block and drop any packets that its programming dictates. Packet sniffers merely watch, display, and log this traffic.

Today's networks may already contain built-in sniffing modules. Most hubs support the RMON standard, which allow the intruder to sniff remotely using SNMP, which has weak authentication. Many corporations employ Network Associates "Distributed Sniffer Servers", which are set up with easy to guess passwords. Windows NT machines often have a "Network Monitoring Agent" installed, which again allows for remote sniffing.

Packets sniffing is difficult to detect, but it can be done. But the difficulty of the solution means that in practice, it is rarely done.

The popularity of packet sniffing stems from the fact that it sees *everything*. Typical items sniffed include:

SMTP, POP, IMAP traffic Allows intruder to read the actual e-mail. POP, IMAP, HTTP Basic, Telnet authentication Reads passwords off the wire in clear-text. SMB, NFS, FTP traffic Reads files of the wire. SQL databse Reads financial transactions and credit card numbers.

WHAT IS IPTV?

Internet Protocol television (IPTV) is the delivery of television content over Internet Protocol (IP) networks. This is in contrast to delivery through traditional terrestrial, satellite, and cable television formats. Unlike downloaded media, IPTV offers the ability to stream the source media continuously. As a result, a client media player can begin playing the content (such as a TV channel) almost immediately. This is known as streaming media.

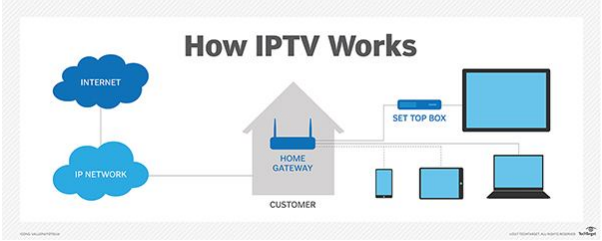
Although IPTV uses the Internet protocol it is not limited to television streamed from the Internet, (Internet television). IPTV is widely deployed in subscriber-based telecommunications networks with high-speed access channels into end-user premises via set-top boxes or other customer-premises equipment. IPTV is also used for media delivery around corporate and private networks. IPTV in the telecommunications arena is notable for its ongoing standardisation process (e.g., European Telecommunications Standards Institute).

IPTV services may be classified into three main groups:

- Live television and live media, with or without related interactivity;

- Time-shifted media: e.g. catch-up TV (replays a TV show that was broadcast hours or days ago), start-over TV (replays the current TV show from its beginning);
- Video on demand (VOD): browse and view items in a stored media catalogue.

III. HOW IPTV WORKS?



IPTV is much similar like browsing the internet than traditional channel surfing. It merely uses IP (Internet Protocol), a transport protocol which is a delivery mechanism to deliver the videos to the viewer. When the viewer clicks on any TV program or requests the video, video from different sources (servers) is divided into data packets and sent over the internet. Video servers transmit programs through fiber-optic cable to existing household via internet connection and requests are sent out and shows are sent back

IV. TYPES OF SNIFFING ATTACK

Your networks and data are vulnerable to any of the following types of attacks if you do not have a security plan in place
.

EAVESDROPPING

In general, the majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.

DATA MODIFICATION

After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if you do not require confidentiality for all communications, you do not want any of your messages to be modified in transit. For example, if you are exchanging purchase requisitions, you do not want the items, amounts, or billing information to be modified.

IDENTITY SPOOFING (IP ADDRESS SPOOFING)

Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed—identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet.

After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data. The attacker can also conduct other types of attacks, as described in the following sections.

PASSWORD-BASED ATTACKS

A common denominator of most operating system and network security plans is password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password.

Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user.

When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time.

After gaining access to your network with a valid account, an attacker can do any of the following:

- Obtain lists of valid user and computer names and network information.
- Modify server and network configurations, including access controls and routing tables.
- Modify, reroute, or delete your data.

DENIAL-OF-SERVICE ATTACK

Unlike a password-based attack, the denial-of-service attack prevents normal use of your computer or network by valid users.

After gaining access to your network, the attacker can do any of the following:

- Randomize the attention of your internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.
- Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.

MAN-IN-THE-MIDDLE ATTACK

As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying *as you* to keep the exchange going and gain more information. This attack is capable of the same damage as an application-layer attack, described later in this section.

COMPROMISED-KEY ATTACK

A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key.

An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack.With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

SNIFFER ATTACK

A *sniffer* is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted *and* the attacker does not have access to the key.

Using a sniffer, an attacker can do any of the following:

- Analyze your network and gain information to eventually cause your network to crash or to become corrupted.
- Read your communications.

APPLICATION-LAYER ATTACK

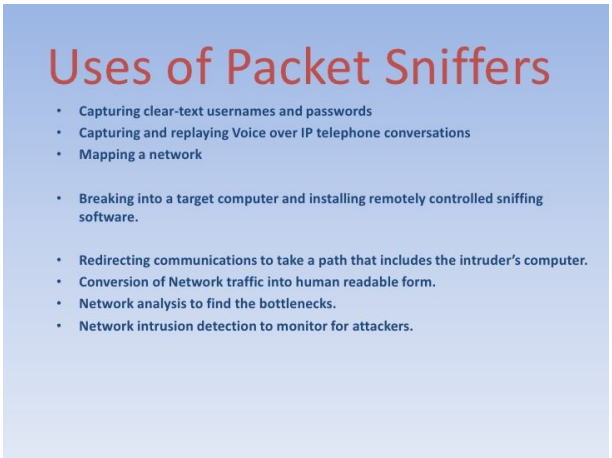
An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:

- Read, add, delete, or modify your data or operating system.
- Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.
- Introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or to corrupt your systems and network.
- Abnormally terminate your data applications or operating systems.
- Disable other security controls to enable future attacks.

USAGE OF PACKET SNIFFER

Packet sniffer software has a number of uses and all of them are of critical nature

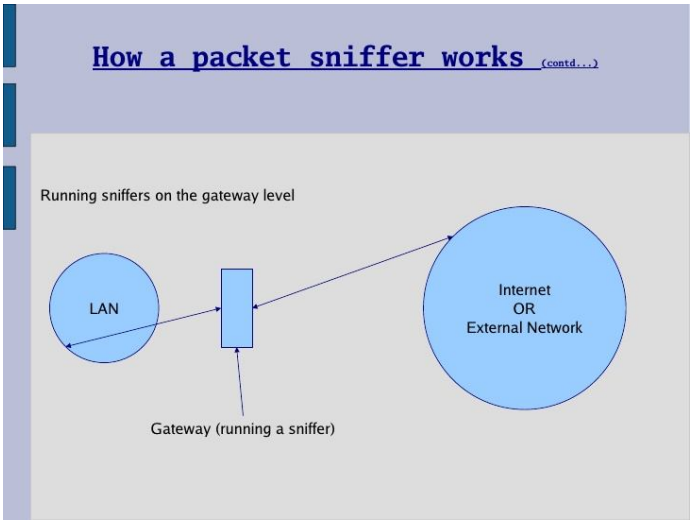
.



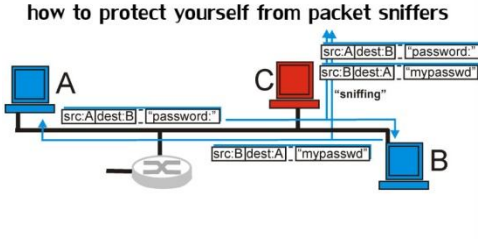
1. Whenever there is a network related problem, we need some basic clues so that we can start addressing the problems. We will be able to get these clues from the packet sniffer software that is installed in the network. Therefore, packet sniffer software will not only help us monitor the network, but it will also help us analyze the network traffic so that we can identify any problem that crops up in the shortest time possible.
2. If there are any unauthorized intrusions, we will be able to detect the intrusions in good time. This will help us protect our network from the hackers.
3. We will be able to monitor the usage levels of the network at any given time. This will help us optimize the usage if we need to.
4. Using packet sniffer software we can keep a tab on each user in the network and gather sensitive information including passwords.
5. Packet sniffers will also be useful to monitor 'on the fly' network traffic to determine what is going on in the network at any given time.
6. Packet sniffers are not only useful for network administrators, it is also useful for programmers and security professionals to study the network traffic and possible loopholes so that they can be sealed.
7. Parents can keep a tab on their children's online PC usage.
8. For those who are in learning stages packet sniffer will help them understand various protocols of the network such as HTTP, POP3, STMP, etc.
9. The reports generated can be used to build reliable statistics about the network use.
10. You will be able to find reasons for system slowdown. Using the packet sniffer software you will be able to troubleshoot the problem in the shortest time possible.

V. HOW DOES A PACKET SNIFFER WORK?

For wired networks, a packet sniffer is able to have access to all or a portion of the traffic being transmitted depending on the configuration of the network switches.
For wireless networks, a packet sniffer is only able to scan one channel at a time. If the host device running the packet sniffer has multiple wireless network interfaces then it is possible to scan multiple channels.



PROTECTING YOURSELF FROM PACKET SNIFFERS



Aside from refraining from using public networks, encryption is your best bet to protect yourself from potential packet sniffers. Using HTTPS, the secure version of HTTP, will prevent packet sniffers from seeing the traffic on the websites you are visiting.

To make sure you are using HTTPS, check the upper left corner of your browser.
One effective way to protect yourself from packet sniffers is to tunnel your connectivity a **virtual private network**, or a VPN.

A VPN encrypts the traffic being sent between your computer and the destination. This includes information being used on websites, services, and applications. A packet sniffer would only see encrypted data being sent to your VPN service provider.

Some of our customers' preferred VPN providers include **NordVPN** and **PrivateInternetAccess**.

VI. CONCLUSION

Packet sniffing process has been successfully defined and designed in systematic manner. We have learned about what is packet , what is packet sniffing , how does packet sniffing work , Usage of packet sniffing , types of packet sniffing. We seen that there are two ways of using packet sniffing one is positive way and other one is negative way. Now in positive way we may see that it is used for monitoring , analyzing , detecting and etc. It is use to capture data while data is transferring through network from one part to other. And in other way we can see that it is use in negative way to steal confidential information, password, user id, documents, etc. The other meaning of sniffing is "sniffe". Which means "theif ".

We are using packet sniffing technology in IPTV . Here IPTV stands for Internet protocol Television . IPTV is a system through which tv services are delivered using the internet protocol suite over a packet-switched network such as a LAN or the internet, instead of being delivered through traditional terrestrial, satellite signal, and cable television formats.

REFERENCE

[1] "Packet sniffing: A brief introduction" S.Ansari, S.G. Rajeev, H.S. Chandrashekar-2002.
[2] "GSM over Ethernet" R.Dettmer.
[3] "An equalized error back propogation algorithm for the on-line training of multilayer percaptrons" J.P. martens, N. Weymacre.
[4] "Mobile Satellite Communication Networks" by E. Ekicl.
[5] "Network Management in Wired and Wireless Networks" by R.Chwastek.
[6] "Ethereal Packet Sniffing" by Angela Orebaugh with GregMorris, Ed Warnicke, Gilbert Ramirez(Technical editor).
[7] "Security and Privacy in Dynamic Environments" by Darko Kirovski, Nebojsa Jojie, and Paul Roberts(Microsoft Research)
[8] "Laws Of Internet Security And Privacy" by Kevinj Connolly-2004, httt://books.google.co.in./books.
[9] "Network Security Tools: Writing, Hacking, and Modifying Security Tools"
by Nitesh Dhanjani, Justin Clarke.
[10] "Packet Analysis With Wireshark" by Anish Nath.
[11] "Packet Guideline to Core Network Protocols" by Bruce Hartpence.
[12] "Attacking Network Protocols:A Hacker Guide to Capture,Analysis, and Exploitation" by James Forshaw.