STUDENT SESSION

REMOTE CONTROL SOFTWARE AND PACKET ANALYSIS

Anđel Petrovski*,
[0009-0004-6336-452X]
Jelena Gavrilović
[0000-0001-6033-1512]

Singidunum University,
Belgrade, Serbia

Abstract:
Modern computers don't have any pre-installed software for remote control. The most important task of remote control software isn't only to allow us to control devices remotely, but to also make it safe as possible. We have worked exactly on that problem of safety during remote control, and we have also made built-in software that tracks the safety of a chosen folder with tracked logs and file paths. Also, we have worked on network traffic analysis while remote control is active. The user whose device is being controlled has an option for restoring the folder, that he previously chose, to its original state before establishing the remote control.

Keywords:
Remote control, Network traffic analysis, Safety.

INTRODUCTION

With the increasing growth and expansion of the Internet, the number of jobs on the Internet has also increased. The easiest way for people to quickly access their client devices and configure them, install software, or work on them, is remote control. The best thing about remote control is that person doesn't have to leave their home or office and they can access any device in the world. For remote control, we need to stay protected from perpetrators who want to intercept data on the network and abuse it. With all this information, Packet analysis became a crucial component of network forensics, offering insights into the complexities of network traffic. In an era marked by new technologies every day, where data requires more security on networks, the ability to analyze packet information holds important significance in the realm of cybersecurity and forensic examination.

Packet analysis stands for the examination of individual packets exchanged between devices inside a network. The packets specifically contain information about what kind of communication protocol was used, what type of data has been transmitted, and who were the participating sides.

Correspondence:
Anđel Petrovski

e-mail:
andjel.petrovski.21@singimail.rs

DOI: 10.15308/Sinteza-2024-413-418

The significance of packet analysis includes tracking cyberattacks, attempts of unauthorized access, finding which ports on the network are open, finding data leaks, and a lot more... The evolution of the packet analysis tool practically admitted noticeable progress within the last decade giving forensic scientists an easier approach to network traffic examination. Today, analysts have a wide range of solutions to capture, filter, and analyze network traffic. It also raises some legal and ethical issues although the utility of prohibiting these activities, on the one hand, seems undeniable. The interception and analysis of network traffic must follow all legal frameworks and ethical guidelines to safeguard user privacy and preserve the integrity of digital evidence.

In summary, packet analysis stands as an essential discipline within the field of digital forensics and cybersecurity. As technology continues to evolve and digital interactions continue to grow, the role of packet analysis in safeguarding digital infrastructures, protecting user privacy, and combating cyber threats remains pivotal.

2. PACKET ANALYSIS

Packet analysis in network forensics involves examining packet details for the reconstruction of network traffic, which helps in identifying cyber criminals such as unauthorized access, malware infection, and data breaches. This technique allows us to get different digital data such as images, documents, and emails sent on the network. Protocols allow communication between two devices, while software specialized for packet analysis enables separation and analysis of network traffic types. Some laws and policies limit the use and sharing of network packet data to protect user privacy and sensitive data. Techniques such as "SafePcap" are used to automatically mask sensitive information in network packets, complying with legal regulations such as GDPR (General Data Protection Regulation) in the European Union [1].

2.1. TYPES OF TOOLS FOR FORENSIC ANALYSIS

Tools used for packet analysis are called packet sniffers. They track and record whole network traffic or only just parts of it. Recorded packets can be analyzed, and raw data is decoded. There are different approaches to wiretapping a network, such as filters, specific hardware devices, and methods like "port mirroring". The standard format for packet files is "libpcap", and there is also a successor "pcapng", which allows different data types [1].

Some of the useful tools for analyzing a network are:

- Wireshark
- Snort
- Scapy
- Fragroute.

Wireshark is the most famous software giving us the best graphic interface for packet analysis. Snort is used for detection and stopping attacks while Fragroute doesn't just allow us to record but also modify and redirect network traffic.

Besides software solutions, there are also hardware devices such as Cisco Security Packet Analyzer appliances which allow deep analyzing of network traffic. There are also tools for creating network packets, one of which is the Cisco Packet Builder for creating custom network packets for testing networks [1].

2.2. CLOUD IN NETWORK ANALYSIS

With the growth in the use of cloud services, there is a need for packet analysis directly in the Cloud environment instead of wiretapping a network. This method is very challenging because of the complexity of Cloud environments. The government and financial sectors, cyber defense and security applications, cloud-managed services, VoIP services, etc. utilize cloud storage and cloud computing services, with additional complexities on top of the source and destination IPs, protocols, and port numbers [1]. For example, this is the very reason for Amazon introducing virtual private cloud (VPC) traffic mirroring, which allows capturing and inspecting AWS network traffic at scale [1].

3. WIRESHARK AND NETWORK PACKETS

Wireshark is a network protocol analyzer that captures packets from a network connection [2]. A network packet is a unit of data carried by a packet-switched network [3]. It consists of a header and payload [3]. Any processing or receiving device, such as a router or a switch, sees the header first [3]. The header contains information about the packet's source and destination, versions and lengths of the packet, identifier, information about the protocol used, and other metadata necessary for routing and delivering the packet to its destination [3]. The payload contains the actual data being transmitted, which is usually encrypted [3]. When we analyze packets in Wireshark, we analyze hexadecimal numbers.

We can get information about the protocol used to transfer payload, ports used on networks, the size of data that is being transferred, as well as IP addresses used in communication. In Figure 1 we can see an example of one packet being analyzed. In the orange section marked hexadecimal numbers represent Internet Protocol Version 4 and IP addresses for this packet, the green section represents UDP protocol with used ports and the purple section represents encrypted Data.

4. TYPES OF ATTACKS

Some perpetrators try to cover their attacks by making fake network packets, but there are a few techniques with which we can track the source of the packet, such as ICMP monitoring and techniques based on hashing IP Addresses. The most common ICMP attacks are Ping flood or DDoS attacks, and "smurf" attacks.

Ping Flood, also known as an ICMP flood, is a type of distributed denial-of-service (DDoS) attack in which an attacker overwhelms the targeted device or network with continuous request packets (pings) [4]. This can cause network congestion and prevent legitimate users from accessing network resources [4]. The key difference between Ping Flood and Smurf attacks is that Smurf attacks leverage the spoofing of the source IP address [4]. The attacker sends a large amount of ICMP traffic to the broadcast address of the target network but spoofs the source IP address to be the victim's address [4]. When all the hosts on the network receive and respond to the ICMP echo request, it multiplies the amount of traffic flooding the victim [4].

One of the most popular attacks besides DDoS and Ping Flood is the Man-In-The-Middle (MITM) attack [5]. In cloud systems, the attacker intercepts the communication between systems and manipulates data without the knowledge of the provider and the relying party [5]. The attacker mimics the communication between the provider and the relying party pretending to act like them [5]. MITM attack targets to steal personal identifying information such as credentials, account information, and financial data including credit card numbers and bank details [5]. To defend from MITM attacks, PKI (Public Key Infrastructure) is used, as explained later in the paper.

5. TEAMVIEWER

TeamViewer is a leading global technology company that provides a platform to remote access and control laptops and mobile phones to industrial machines and robots [6]. The platform focuses on cloud-based technologies to enable global online remote support and collaboration [6].

6. SIMILARITIES AND DIFFERENCES WITH TEAMVIEWER

When establishing a session, TeamViewer determines the optimal type of connection [7]. After the handshake through master servers, a direct connection via UDP or TCP is established [7]. Network TeamViewer traffic is secured using RSA public/private key exchange and AES (256-bit) session encryption [7]. As the private key never leaves the client computer, this procedure ensures that interconnected computers, including the TeamViewer routing servers, cannot decipher the data stream [7]. For authorization and password encryption, Secure Remote Password protocol (SRP), an augmented password-authenticated key agreement (PAKE) protocol, is used [7]. The PKI effectively prevents MITM attacks [7]. PKI issues certificates, which help in verifying the identity of computers, routers, IoT devices, and other devices in the network [7]. The attacker can receive the same certificate that the server receives from a client that contains the public key and the domain name the server sends to anyone who wants to connect to it [7].

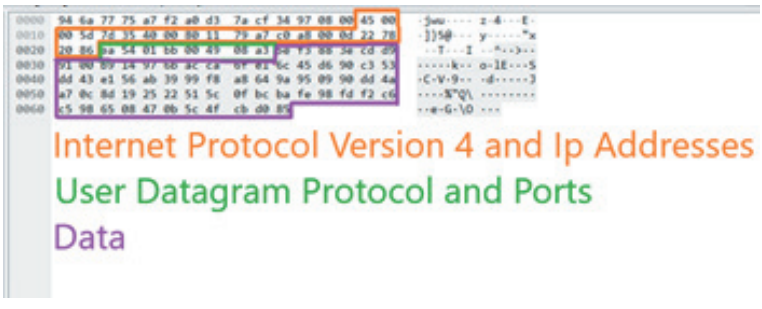

Figure 1. Screenshot example of packet analysis in Wireshark.

However, the attacker can't decrypt the information because only the server owns the matching private key that can decrypt the data [8]. Despite the encryption, the password is never sent directly, but only through a challenge-response procedure, and is only saved on the local computer [7]. TeamViewer uses one port for connection while our software uses two ports. In our software the first port is used for sending and receiving encrypted captured screens, and the second port is used for sending and receiving encrypted mouse coordinates as well as mouse and keyboard inputs.

In our software, only TCP type of connection is used, as well as RSA public/private key exchange and AES (256-bit) session encryption.

The private key never leaves the client's computer. For authorization and password encryption, Secure Remote Password protocol (SRP) is used with Public Key Infrastructure. To receive and send data simultaneously, multithreading is used. In Figure 2 we can see an example of how Remote Control works.

7. PRACTICAL EXAMPLE

For a practical demonstration, We used a Laptop (User B and a Server) and a Desktop computer (User A). At first, the server was run on a Laptop and then we ran users B and A. The Server authenticates user B and waits for user A to enter user's B username and password. The username is always the same but the password is randomly generated every time the app is run. The server authenticates user A and the connection is established. For safe logging users, the Secure Remote Password protocol is used, so the password is never saved and it never leaves the user's device. User B needs to choose which folder security he wants to be tracked. After selecting a folder, the remote control starts.

On User B's device, the screen is being captured, encrypted, and sent to User A. User A is receiving images, decrypting them, and displaying them. Screen sharing is done on one port, and sending and receiving mouse coordinates as well as keyboard and mouse inputs are done on another port. User A only sends mouse coordinates if they are changed to the previous ones, the same

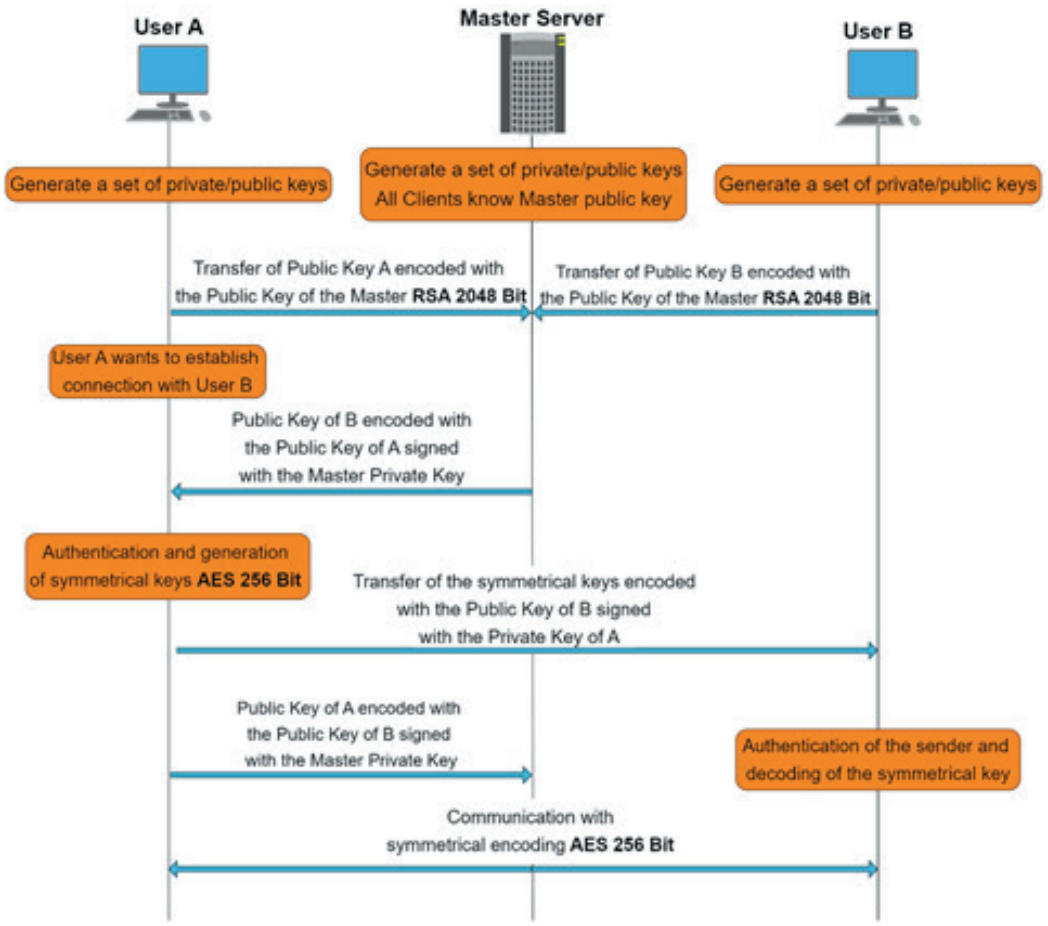

Figure 2. Remote Control Protocol Scheme.

goes for mouse and keyboard inputs. Every information sent through the port is encrypted and needs to be decrypted on the other side. For exchanging RSA public keys, the Diffie-Helman protocol is used with PKI (Public Key Infrastructure). Screen sharing, mouse coordinates, and all keyboard and mouse inputs are encrypted with an AES 256-bit key. If anything is changed in a previous folder we selected for tracking the security, it will be reported. Built-in „File Checker" program shows a file path and if the file is added, deleted, or changed. Before connection, the program hashes all the files in the folder we selected and backs them up. If the user selects the restore option, the folder will be returned to its original state.

7.1. SIMILARITIES AND DIFFERENCES IN FORENSIC ANALYSIS WITH TEAMVIEWER

Two important users in analyzing connection are User A and B. User A is connecting with User B and gains control of User B's device. Only the user's B side is analyzed as its device is being controlled. In Wireshark, we can see the following line:

"192.168.0.23 → 192.168.0.13 TCP 50937 → 10003 [PSH, ACK] Seq=1118 Ack=1118 Win=261632 Len=686".

Every line consists of the next parameters: IP addresses used in packet transfer, protocol and ports used, and information about this packet transfer. The IP address of B is 192.168.0.23 and A is 192.168.0.13. We can see that port 10003 is open on the user's B side for packet transfer. After this line, when A connects to B, A is waiting for B to select a folder for tracking its security. After selecting a folder, A starts to control B's device. Before that, a few seconds after user A logs in to user B, we can find a line that says:

"Who has 192.168.0.23? Tell 192.168.0.13". The next line is "192.168.0.23 is at 7c:10:c9:43:c9:a0".

Here we can see IP addresses used in remote control. "7c:10:c9:43:c9:a0" is a MAC address, because the remote control is done in the local network. When user B finally selects a folder, A starts to control B's device. We can see that user A controls user B in Wireshark with a large block of lines that are all similar to this line:

"192.168.0.13 → 192.168.0.23 TCP 58 10003 → 50937 [PSH, ACK] Seq=9396 Ack=7638 Win=131328 Len=4".

We know that the connection ended when a large block of these similar lines ended. The best option is also to use log files. User B has two log files, a log file history of all connections, and a log file for the File Checker program.

Log file for File Checker stores when the program is started, it stores Status if the folder is safe or not every second with the date and time stamp. If the folder is not safe, it tracks the file path of corrupted, added, or deleted files, and it also tracks if the restore option has been done. In comparison to TeamViewer, we can track the start and end of the connection the same way by looking at a large block of similar lines said before. We can also find a line saying:

"Who has 192.168.0.13? Tell 192.168.0.17". Next line is "192.168.0.13 is at fe80::58af:68ff:fe2c:feb0".

In this case, we have two IP addresses, 192.168.0.17 – The phone used to connect to the Laptop and gain control, and the Laptop's address is 192.168.0.13. In these two lines, we can find, in this case, local IP addresses used in the TeamViewer session. As for the TeamViewer log file, several important lines can be tracked. One where the session is started with written destination ports and IP address, and a session token is created. The next step is "handshake", server and client exchange information so the secured connection can be established. Next is "punch" via UDP protocol. "Punch" in this context is used to exchange information so a peer-to-peer (P2P) connection can be established between two Network Address Translation (NAT) devices. Source punch is an IP address of a source that attempts to get remote control on our device.

The end of the connection can be tracked by several lines. First says that the session to TeamViewer ID ended. The next step is ending "DesktopProcessControl". Client Web API stops accepting requests through ports. The last step is destroying components of VoIP (video and audio communication).

8. CONCLUSION

The research proposed in this paper helps to conduct a systematic study of secure remote control protocols and forensic analysis procedures. Moreover, the actual example described contributes valuable experience to the matter of remote control connections and forensic artifacts.

The usage of encryption methodologies, like RSA and AES, adds another secure tunnel level, which protects all data sent via the network with encryption protocols. Therefore, forensic analysis is one of the key concepts described in this paper, which is of great help in restoring the essence of connection packets and identifying security risks associated with improper activity.

Furthermore, the additional "File Checker" program helps to identify all the unnecessary changes within the monitored folder, which relates to the higher system integrity.

This research adds to the existing knowledge of the area of digital forensics by revealing the forensic artifacts that are created by secure remote control protocols. Moreover, it offers a practical guide for forensic experts and investigators.

9. ACKNOWLEDGEMENTS

This research was supported by the Science Fund of the Republic of Serbia, Grant No. 7502, Intelligent Multi-Agent Control and Optimization applied to Green Buildings and Environmental Monitoring Drone Swarms - ECOSwarm.

10. REFERENCE

[1] L. F. Sikos, "Packet analysis for network forensics: A comprehensive survey," *Forensic Science International: Digital Investigation*, vol. 32, 2020.

[2] "Wireshark," [Online]. Available: https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs. [Accessed 10 March 2024].

[3] K. Yasar and A. Zola, "TechTarget," July 2022. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/packet. [Accessed 14 April 2024].

[4] "Imperva," [Online]. Available: https://www.imperva.com/learn/ddos/ping-icmp-flood/. [Accessed 27 February 2024].

[5] I. Indu, P. R. Anand and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms," *Engineering Science and Technology, an International Journal*, vol. 21, no. 4, p. 574–588, 2018.

[6] JenW, "What is TeamViewer?," 26 April 2023. [Online]. Available: https://community.teamviewer.com/English/kb/articles/33184-what-is-teamviewer. [Accessed 27 February 2024].

[7] JenW, "Security Statement," 23 February 2024. [Online]. Available: https://community.teamviewer.com/English/kb/articles/4619-security-statement. [Accessed 21 March 2024].

[8] G. Dionisie, "SSL Dragon," 29 February 2024. [Online]. Available: https://www.ssldragon.com/blog/ssl-prevent-mitm-attacks/. [Accessed 13 April 2024].