A Research Study on the TCP Three-Way Handshake Mechanism

Aayush Raj
Offensive Cybersecurity Intern, InLighn Tech

06 June 2025

Abstract

The Transmission Control Protocol (TCP) is a fundamental component of the Internet protocol suite, providing reliable, connection-oriented communication over IP networks. A key aspect of TCP is the *three-way handshake*, a mechanism used to establish a connection between a client and server. This paper explores the mechanics, importance, security considerations, and vulnerabilities associated with the TCP three-way handshake. It also highlights its relevance in modern network communications and cybersecurity.

1 Introduction

The Transmission Control Protocol (TCP) plays a pivotal role in ensuring reliable communication across computer networks, particularly the Internet. In an era where digital data exchange underpins everything from simple emails to complex cloud computing, TCP guarantees that data packets arrive intact and in the correct order. Establishing a connection between two endpoints before data transfer is a fundamental necessity in TCP's operation, achieved through a process called the **three-way handshake**. This initial negotiation phase is critical as it synchronizes sequence numbers and prepares both the client and server for data transmission. Understanding this mechanism provides insight into fundamental networking principles and lays the foundation for identifying and mitigating related security risks.

2 Overview of TCP

TCP is a transport layer protocol that ensures end-to-end reliable data delivery between hosts in a network. Unlike connectionless protocols such as UDP, TCP provides mechanisms for error detection, retransmission of lost packets, flow control, and congestion management. It breaks data streams into segments and assigns sequence numbers to each, enabling the receiving end to reorder packets and detect duplicates or losses. TCP's connection-oriented nature requires an explicit handshake to establish and terminate connections, ensuring that both sender and receiver agree on the communication parameters and are ready for data exchange. This reliability has made TCP the backbone of many critical Internet applications.

3 The Three-Way Handshake Process

The TCP three-way handshake is an essential protocol sequence that sets up a connection between two hosts. This process involves three steps—SYN, SYN-ACK, and ACK—which together establish mutual synchronization and confirm readiness for data transmission.

Step 1: SYN (Synchronize)

The connection initiation begins when the client sends a TCP segment with the SYN flag set, indicating a request to establish a session. This segment carries an Initial Sequence Number (ISN), a randomly generated value used to track bytes within the TCP stream and maintain synchronization.

Step 2: SYN-ACK (Synchronize-Acknowledge)

Upon receiving the SYN packet, the server responds with a segment that has both SYN and ACK flags set. This segment acknowledges the client's ISN by incrementing it by one, signaling that the server has received the request and is ready to communicate. Simultaneously, the server sends its own ISN, establishing two-way synchronization.

Step 3: ACK (Acknowledge)

Finally, the client responds with an ACK segment acknowledging the server's ISN by incrementing it by one. This step completes the handshake, confirming that both the client and server have synchronized sequence numbers and are ready to commence full-duplex communication.

4 Purpose and Importance

The three-way handshake establishes a reliable and synchronized connection, ensuring both sides agree on initial sequence numbers and are prepared to send and receive data. This process helps prevent connection conflicts and data corruption. Additionally, it enables negotiation of TCP options, optimizing the data flow. Ultimately, the handshake mechanism is foundational to TCP's reliable communication.

5 Security Considerations

While the handshake is vital for connection setup, it also introduces potential security vulnerabilities.

5.1 SYN Flood Attack

A Denial of Service (DoS) attack can exploit the handshake by flooding a server with SYN requests without completing the handshake, consuming resources and rendering the server unresponsive.

5.2 IP Spoofing

Attackers can forge the source IP address in the SYN packet, causing the server to send SYN-ACKs to unintended hosts. This misdirection can confuse defenses and facilitate attacks.

6 Enhancements and Mitigations

Several mechanisms have been developed to mitigate these vulnerabilities.

6.1 SYN Cookies

SYN cookies allow servers to defer resource allocation until the handshake is complete, mitigating SYN flood attacks.

6.2 Firewalls and IDS

Security devices can monitor traffic patterns, identifying suspicious SYN activity and blocking or rate-limiting it.

6.3 TCP Fast Open (TFO)

TCP Fast Open reduces latency by allowing data transmission during the initial handshake, improving performance.

7 Applications in Offensive and Defensive Cybersecurity

Understanding the handshake is essential for both attackers and defenders.

- **Offensive:** Penetration testers can exploit handshake manipulation to perform stealth scans, map open ports, or test server resilience.
- **Defensive:** Security professionals analyze handshake patterns to detect and mitigate scanning or DoS attempts.

8 Conclusion

The TCP three-way handshake is a cornerstone of reliable Internet communication. Despite its importance, it presents inherent security risks that must be addressed. Techniques like SYN cookies and TCP Fast Open help mitigate these issues. For cybersecurity professionals, a thorough understanding of the handshake is crucial for both protecting networks and assessing security.

9 References

1. Postel, J. (1981). RFC 793: *Transmission Control Protocol.* `https://tools.ietf.org/html/rfc793`

2. Paxson, V. (1997). *An Analysis of TCP Congestion Control with Reno and Tahoe*, ACM SIGCOMM.

3. CERT Advisory CA-1996-21. *TCP SYN Flooding and IP Spoofing Attacks.*

4. Murdoch, S.J., Kohno, T. (2005). *Attacks on TCP/IP Protocols*, IEEE Security & Privacy.