The Impact of Man-in-the-Middle Attacks on Common Network Protocols

Nguyễn Văn Hiếu
Thai Nguyen University of Information and Communication Technology
Thai Nguyen University, Thai Nguyen, Vietnam
student537@ictu.edu.vn

***Abstract*—This undergraduate thesis investigates man-in-the-middle interception of network traffic. Unprotected network exchanges may expose credentials or permit messages to be altered between a sender and recipient. The author reviews network protocols and attack mechanisms, describes a laboratory setup using Ettercap and address-resolution spoofing, and compares insecure web traffic with encrypted web traffic. The report also surveys authentication, integrity checking, and network configuration measures. The examples and discussion show how interception and modification can affect insecure HTTP exchanges. The report presents HTTPS and other protective measures as ways to reduce exposure. It does not demonstrate a production network intervention or provide a controlled comparison of all proposed defenses. The investigation is a student laboratory study. Protocol behavior depends on the exact configuration, certificate handling, and endpoint security. A demonstration of interception should not be generalized to every deployment of the same protocol. The contribution is a documented student study or prototype whose stated scope can guide further testing.**

***Index Terms*—man-in-the-middle, network protocols, HTTP, HTTPS, network security**

I. Introduction

Unprotected network exchanges may expose credentials or permit messages to be altered between a sender and recipient. This thesis investigates man-in-the-middle interception of network traffic. It begins from a practical engineering need and explains the technologies and workflow chosen for the case. The objective is to document a student implementation or comparative investigation, together with the evidence available in the manuscript. Broader operational or economic effects require separate measurements and are not assumed from the existence of a prototype [1]. Earlier ICTU student work on related designs is included here for context [2], [3]. Related published studies provide context for the subject and methods [4], [5], [6], [7], [8], [9], [10]. These contextual works were selected for this English summary; they are not asserted to appear in the original thesis bibliography.

II. Methods

The author reviews network protocols and attack mechanisms, describes a laboratory setup using Ettercap and address-resolution spoofing, and compares insecure web traffic with encrypted web traffic. The report also surveys authentication, integrity checking, and network configuration measures. The source is summarized through its stated design, implementation material, examples, and conclusion. Features shown in the manuscript are distinguished from proposals for later development. This review does not add a new experiment, fill missing measurements with estimates, or treat a planned capability as an observed result. The source thesis remains the provenance for the reported work [1].

Supervisor: Trịnh Minh Đức, Thai Nguyen University of Information and Communication Technology (tmduc@ictu.edu.vn).

III. Results

The examples and discussion show how interception and modification can affect insecure HTTP exchanges. The report presents HTTPS and other protective measures as ways to reduce exposure. It does not demonstrate a production network intervention or provide a controlled comparison of all proposed defenses. The report's screens, configurations, examples, or measurements constitute the evidence for this summary. A capability described only as a design intention is not counted as a validated operational outcome. No additional performance, adoption, financial, or safety figure has been introduced here. The result is interpreted within the scope of the student's documented setup [1].

IV. Discussion

The investigation is a student laboratory study. Protocol behavior depends on the exact configuration, certificate handling, and endpoint security. A demonstration of interception should not be generalized to every deployment of the same protocol. Future work could test the proposed safeguards in a repeatable network environment and record detection rates, false alarms, and resistance to changes in attacker position. These limitations affect how the evidence should be read. The current manuscript can support understanding of the design and reported demonstration, while independent tests would be needed for stronger claims. Any later deployment should document its environment and separate observed outcomes from intended benefits [1].

V. Conclusion

The thesis documents man-in-the-middle interception of network traffic. The examples and discussion show how interception and modification can affect insecure HTTP exchanges. The report presents HTTPS and other protective measures as ways to reduce exposure. It does not demonstrate a production network intervention or provide a controlled comparison of all

proposed defenses. The investigation is a student laboratory study. Protocol behavior depends on the exact configuration, certificate handling, and endpoint security. A demonstration of interception should not be generalized to every deployment of the same protocol. Future work could test the proposed safeguards in a repeatable network environment and record detection rates, false alarms, and resistance to changes in attacker position. Accordingly, the present contribution is a source-grounded account of the student work and its tested or illustrated scope. Claims about broader effectiveness should be assessed in later work using explicit evaluation conditions [1].

References

[1] Nguyễn Văn Hiếu, ”The Impact of Man-in-the-Middle Attacks on Common Network Protocols,” internal undergraduate thesis (original in Vietnamese), Thai Nguyen University of Information and Communication Technology, 2024.

[2] ICTU Student 105, ”Design of a Secure Network Using Cisco PIX Firewall for a Technical College,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[3] ICTU Student 152, ”Implementing Java Encryption for File Transfer,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2010.

[4] Franco Callegati et al., ”Man-in-the-Middle Attack to the HTTPS Protocol,” IEEE Security & Privacy Magazine, 2009. doi:10.1109/msp.2009.12.

[5] Muneer Alwazzeh et al., ”Man in The Middle Attacks Against SSL/TLS: Mitigation and Defeat,” Journal of Cyber Security and Mobility, 2020. doi:10.13052/jcsm2245-1439.933.

[6] Peng Zhou et al., ”HTTPAS: active authentication against HTTPS man□in□the□middle attacks,” IET Communications, 2016. doi:10.1049/iet-com.2016.0331.

[7] Vyron Kampourakis et al., ”Revisiting man-in-the-middle attacks against HTTPS,” Network Security, 2022. doi:10.12968/s1353-4858(22)70028-1.

[8] Yadagiri V et al., ”Enhanced Security for the Prevention of Man-In-The-Middle Attacks,” IJARCCE, 2017. doi:10.17148/ijarcce.2017.63190.

[9] Arnab Dey, ”Innovative Approach to Mitigate Man-in-the-Middle Attacks in Secure Communication Channels,” International Journal of Science and Research (IJSR), 2022. doi:10.21275/sr24320191712.

[10] Dragoș Glăvan, ”Man in the middle attack on HTTPS protocol,” Scientific Bulletin of Naval Academy, 2020. doi:10.21279/1454-864x-20-i1-026.