Analysis of Traffic Interception Threats and Effective Protection Methods

Israfilov A. Master's Degree, Individual Researcher

Drozdov I.S. Bachelor's Degree, Bauman Moscow State Technical University, Moscow, Russia

Pismenskiy D.A. Bachelor's Degree, Bauman Moscow State Technical University, Moscow, Russia

Abstract

In the contemporary world, where a significant portion of human activity has shifted into the digital space, cybersecurity issues have increasingly gained prominence. A key threat in this context is traffic interception, which may involve both passive methods of monitoring user data without altering it and active attacks aimed at interception, modification, or redirection of digital flows. Statistics show that active and passive traffic interception methods constitute a significant proportion of incidents in the realm of cybersecurity, thereby amplifying the need for the development and implementation of comprehensive protection systems. This paper pays special attention to the study of various approaches to ensuring information security, including data encryption via SSL/TLS protocols, the use of HTTPS to reduce the risks of Man-in-the-Middle attacks, the application of end-to-end encryption to guarantee the confidentiality of transmitted information, multifactor authentication as a means to enhance the reliability of user authentication, and the utilization of intrusion detection and prevention systems capable of timely responding to unauthorized access attempts. The article emphasizes that no single protection method is absolutely reliable in isolation, and true security is achievable only through the integration of various tools and approaches. It analyzes the complementarity of encryption methods, multifactor authentication, and network monitoring systems, illustrated by statistics on the success of countering cyber threats. In conclusion, it highlights the importance of adaptability and flexibility of cybersecurity strategies for effective response to constantly evolving cyber threats, supporting this argument with the necessity of wide adoption of comprehensive solutions at all levels of the information infrastructure of enterprises and organizations. Thus, the article offers a fundamental analysis of traffic interception threats and a review of prevalent methods for their prevention, underscoring the strategic importance of a comprehensive approach to ensuring cybersecurity in the continuously evolving digital space.

Keywords: cybersecurity, traffic interception, data encryption, multi-factor authentication, intrusion detection, prevention systems.

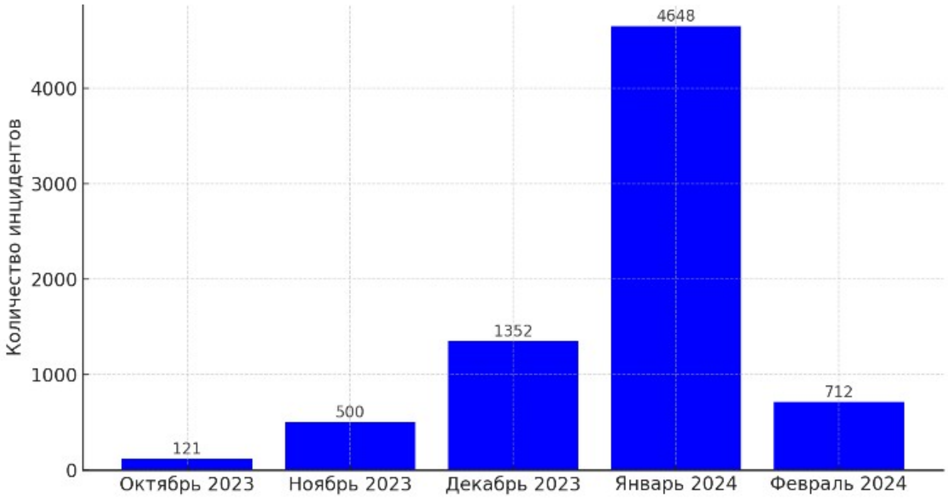
Introduction

One of the central problems in the field of cybersecurity is traffic interception (TI). The variety of TI methods and the complexity of their detection require organizations to pay special attention to ensuring information security (IS). Research on the volume of TI and ways to prevent it is regularly conducted by major international companies. For instance, according to Kaspersky materials (2023), more than 30% of registered IS incidents were directly related to TI [1]. These data highlight the need to analyze mechanisms and classify TI methods, as understanding and systematizing such mechanisms allows for the development of effective strategies for detecting and preventing cyber-attacks.

The purpose of this paper is to analyze existing TI threats, methods for their detection, and the development of comprehensive protection measures. The article examines various data security strategies and analyzes their effectiveness.

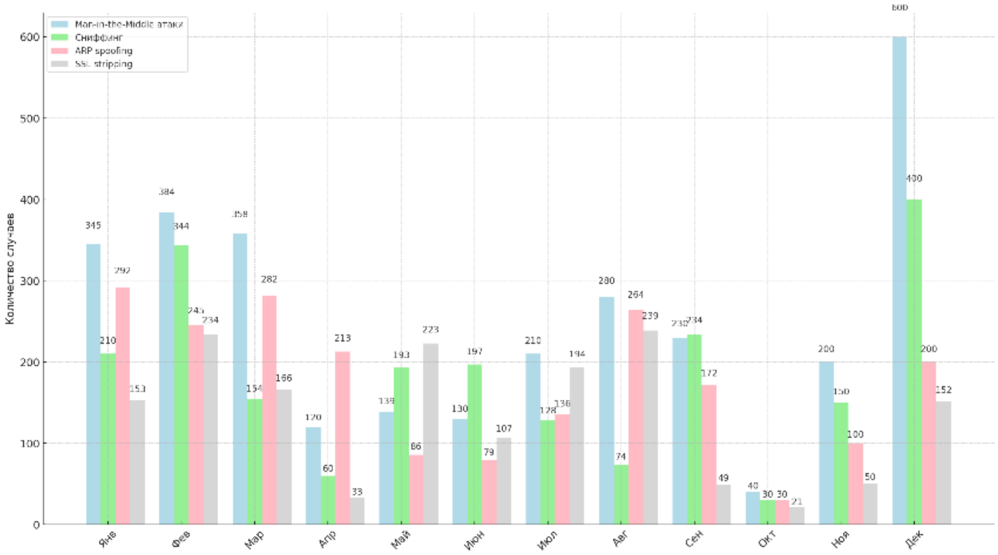
Main Body

The international consulting company IT Governance published a report [2] indicating that from November 2023 to January 2024, the number of publicly disclosed TI incidents increased by 830% (Fig. 1). According to IBM [3], the average global cost of a data breach in 2023 was about $45 million, which is 15% more than in the previous three years.



Images. 1. Dynamics of TI incident growth [2]

Research (Images. 2) shows [6] that a significant portion of TI-related incidents throughout the year were MitM attacks, accounting for up to 40% of all IS incidents. In December, sniffing attacks spiked, making up about 60% of all TI types. ARP spoofing and SSL stripping accounted for about 10% and 15% of incidents, respectively, throughout the year.



Images. 2. IS incident statistics involving TI methods in 2023 [6]

To minimize TI risks and subsequent unauthorized data access, the following protection methods (PM) should be considered:

1. **Data Encryption via SSL/TLS Protocols:** This creates a secure channel between the user and the server, ensuring confidentiality and integrity of transmitted information. Modern studies [7] indicate that using HTTPS reduces the risk of MitM attacks by more than 80%, providing reliable web traffic protection.
2. **End-to-End Encryption (E2EE):** This PM encrypts information on the sender's side, keeping it encrypted throughout transmission until it reaches the intended recipient, who has a unique key for decryption. E2EE is widely used in messaging apps (e.g., WhatsApp and Signal), emails, and file-sharing systems.
3. **Multifactor Authentication (MFA):** This PM requires the user to provide two or more pieces of evidence of identity, significantly complicating the attacker's task. According to [8], implementing MFA can reduce the number of successful phishing attacks by up to 99%.
4. **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):** These monitor network traffic for anomalies, allowing timely responses to potential TI threats. IDS analyze traffic copies for suspicious actions, while IPS actively block detected attacks, preventing their spread. IPS effectiveness can reach 95% in blocking network-level attacks [9].
5. **Secure Configuration of Network Equipment:** This PM includes routers and switches to counter TI. Proper configuration and software updates can reduce the risk of hacking by up to 60%, eliminating most attack vectors related to outdated software vulnerabilities [10].

Table 1. Comparative Analysis of PM against TI Threats [7, 8]

Threat Type	Protection Method	Description	Advantages	Disadvantages
Man-in-the-Middle (MitM)	SSL/TLS and HTTPS	Data transmission encryption	Reliable encryption, global support	Vulnerable to some forms of attacks (certificate spoofing, phishing, and pharming)
ARP Spoofing	Network Equipment Configuration	Network-level protection	High effectiveness in preventing ARP spoofing	Requires complex setup, infrastructure management
Sniffing	E2EE	Creates a secure channel for users	Ensures anonymity, protects data interception	Reduces connection speed due to encryption
SSL Stripping	HSTS	Forces use of encrypted connections	Prevents security level downgrading	Requires browser and server support

The analysis presented in Table 1 highlights the effectiveness, strategic importance, and necessity of integrating these PM into an overall cybersecurity system. Examining various PM against TI threats allows for a comprehensive analysis of their cost and efficiency based on the organization size. Data encryption via SSL/TLS and using HTTPS can be implemented with minimal costs, especially considering free solutions like Let's Encrypt. These solutions are financially accessible, and the protection probability against TI can reach up to 80-90% [10]. Such factors make these PM a preferred choice for small and medium enterprises. Network equipment configuration to prevent ARP spoofing may require more significant funding. Implementing this method can reduce the risk of ARP spoofing by 70-80% [6]. HSTS implementation requires additional server support costs and can be challenging to manage for some organizations. However, this method reduces the likelihood of successful data interception to 10-20% [11].

Enterprise security data analysis has revealed that effective IS protection is achieved through comprehensive use of PM, with data encryption, multifactor authentication, and network traffic monitoring being key elements. This approach not only significantly enhances security levels but also leads to a noticeable reduction in successful cyber-attacks on corporate systems.

The combined use of the examined PM significantly raises the security level of IS compared to their individual use. Strengthening one method should be accompanied by strengthening others, thus creating a comprehensive barrier against potential data interception threats. This approach emphasizes the possibility of ensuring comprehensive IS protection, and a clear understanding of each threat's specifics allows for effective adaptation of these tools to current threats.

Conclusion

The constant growth in the number of TI-related incidents highlights the need for continuous improvement and adaptation of protective mechanisms. Statistics show that a comprehensive approach involving encryption, multifactor authentication, and network traffic monitoring significantly reduces system vulnerabilities. This underscores the necessity for widespread adoption of comprehensive cybersecurity solutions at all levels of information infrastructure.

Maintaining detailed statistics on incidents within each company and analyzing cybersecurity trends will enable management to respond promptly and proactively to changes in attacker methodologies. Protection strategies should be flexible and multi-layered to enhance the effectiveness of defense against cyber threats.