ANALYSIS OF MODERN CYBER ATTACKS AND METHODS FOR THEIR PREVENTION

Tuxtanazarov Dilmurod Solijonovich

Associate Professor, PhD, International Islamic Academy of Uzbekistan, Tashkent, Uzbekistan.

Ergashev Giyosjon Jurayevich

Associate Professor (Acting), PhD, International Islamic Academy of Uzbekistan, Tashkent, Uzbekistan.

Abstract: This study provides a comprehensive analysis of the evolution of modern cyberattacks, their technical and organizational characteristics, and advanced architectures for combating them. Within the scope of the study, the Zero Trust Security Architecture, Artificial Intelligence (AI)-based threat detection systems, the Cyber Kill Chain model, and the MITRE ATT&CK framework are comparatively analyzed, and their effectiveness and areas of application are evaluated. This information includes an abstract definition of Zero Trust Architecture (ZTA) and presents general deployment models and use cases in which the Zero Trust approach can improve an organization's overall information technology security posture.

Keyword: Cybersecurity, Cyberattacks, Zero Trust Architecture (ZTA), Artificial Intelligence (AI), Machine Learning, Cyber Kill Chain (CKC), MITRE ATT&CK Framework, Threat Detection, Anomaly Detection, Behavior Analytics, Real-time Monitoring, Identity Provider (IdP), Policy Engine (PE), Policy Enforcement Point (PEP), Threat Intelligence Platform.

Introduction: The rapid global development of information and communication technologies has significantly expanded digitalization processes across all sectors. It is not an exaggeration to state that banking and financial

systems, public administration, healthcare, education, and industrial automation systems have fully or partially transitioned to digital infrastructures. At the same time, cybercrime has also become more complex, and new-generation cyberattacks have emerged. Modern cyberattacks are no longer limited to traditional viruses or simple malicious code; instead, they are evolving into complex systems that are multi-stage, adaptive, stealthy, and optimized with the assistance of artificial intelligence.

The main issue caused by cyberattacks is that they no longer exploit only technical vulnerabilities, but also effectively utilize the human factor, system errors, and architectural weaknesses within systems. For this reason, traditional perimeter-based security models are losing their effectiveness.

The analysis of the main literature shows that in NIST SP 800-207 (Zero Trust Architecture), the Zero Trust model is described as a modern security paradigm. The MITRE ATT&CK framework, on the other hand, structurally represents attackers' tactics and techniques. In the literature, AI-based anomaly detection and behavior analytics systems are identified as key directions in cybersecurity.

Currently, cyberattacks are developing through the following stages:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control (C2)
7. Actions on Objectives (final objective)

This model is called the Cyber Kill Chain, and it represents the complete lifecycle of an attack process. This approach enables the analysis of the step-by-step development of cyberattacks and allows detection at each phase of their progression.

Therefore, it is considered one of the important analytical frameworks for modeling attacks in the field of cybersecurity.

From this perspective, in modern cybersecurity, it is important not only to understand the attack process but also to respond to it in a dynamic manner.

The Cyber Kill Chain (CKC) is used in developing effective defense mechanisms aimed at preventing attacks at specific stages. In this regard, through the Cyber Kill Chain model, the stages of attacks can be analyzed in depth, and it becomes possible to develop effective protective measures against them. This very need has made the implementation of proactive and dynamic approaches in modern cybersecurity, as well as more advanced models—particularly the Zero Trust Architecture—a necessity.

Zero Trust Architecture. The Zero Trust model is based on the principle "Never Trust, Always Verify." In this model, all entities inside and outside the network are considered untrusted. Every access request is verified in real time. The components of Zero Trust include Identity Provider (IdP), Policy Engine (PE), Policy Enforcement Point (PEP), Continuous Monitoring System, and Threat Intelligence Platform. The integration of these components ensures comprehensive system security and serves to maintain all access processes under continuous control. At the same time, the use of artificial intelligence–based analysis and detection mechanisms is of significant importance for the more effective operation of this infrastructure.

AI-based cybersecurity. Artificial intelligence-based systems utilize behavior analytics and machine learning algorithms. They analyze parameters such as login time, IP address, traffic patterns, and user behavior. AI systems detect anomalous activity in real time and perform automatic blocking. This reduces dependence on the human factor in cybersecurity processes and increases the speed of decision-making. As a result, the efficiency of early threat detection and prevention of system damage is significantly improved.

Comparative analysis. The following table presents a systematic comparison of the main differences between modern cybersecurity architectures and attack models. Through this table, the specific characteristics and application areas of each model are more clearly illustrated. At the same time, it expands the possibility of evaluating their effectiveness and selecting an optimal approach.

Criterion	**Zero Trust Architecture**	**SASE**	**MITRE ATT&CK**	**Cyber Kill Chain**
Model type	Protection model	Network security integration	Attack tactical map	Attack cycle
Core principle	Continuous verification (Never Trust)	Cloud-based security	Classification of attack techniques	Step-by-step attack
Direction	Defensive Security	Network Security	Offensive Security Mapping	Attack Lifecycle
Flexibility	Very high	Very high	Medium	Low
Real-time monitoring	Yes	Yes	Partial	No
AI integration	High	Medium	High	Low
Main objective	Prevention of unauthorized access	Unified cloud security platform	Attack modeling	Explanation of attack stages

Recent analyses show that the combination of Zero Trust + AI is the most optimal model, as it enables adaptive, dynamic, and context-based decision-making.

Each model has its own advantages and disadvantages. The traditional model is static, whereas Zero Trust and SASE are dynamic and adaptive. Therefore, they

enable real-time detection of modern threats and rapid response to them. As a result, organizations achieve a significant increase in security levels and strengthen the effectiveness of attack prevention.

Conclusion

According to the overall results, modern cyberattacks are complex and multi-layered, and it is impossible to provide complete protection against them using traditional security systems. The highest level of security can be achieved when Zero Trust Security Architecture, artificial intelligence-based threat detection systems, the MITRE ATT&CK framework, and SASE architecture are used together. The most optimal approach is considered to be a hybrid model based on the integration of Zero Trust + AI + real-time monitoring.

References

1. Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, *NIST Special Publication 800-207 – Zero Trust Architecture*, National Institute of Standards and Technology (NIST), August 2020.

2. Mateusz Kazimierczak, Nuzaira Habib, Jonathan H. Chan, Thanyathorn Thanapattheerakul — Impact of AI on the Cyber Kill Chain: A Systematic Review, 2024.