Journal of Research in Engineering and Applied Sciences

Analyzing the Impact of Data-Driven Insights on Cyber Attacks: Advanced Mechanisms and Emerging Threats

1st Alireza Nik Aein Koupaei
dept. Radio Engineering and Cybernetics
Moscow Institute of Physics and Technology - MIPT
Moscow, Russian Federation
email: anikaeinkoupaei@phystech.edu

***Abstract*—The paper task aims to assess the influence of data-driven insights on cyber attacks, particularly focusing on advanced mechanisms and emerging threats. It involves analyzing how data-driven approaches enhance the understanding and mitigation of cyber threats, ultimately strengthening cybersecurity practices. This abstract explores the synergy between cybersecurity and data-driven insights, emphasizing the critical role they play in countering cyber-attacks and vulnerabilities. The integration of advanced mechanisms and the analysis of emerging threats provide a robust framework for safeguarding critical assets and sensitive information. By harnessing these tools, organizations can detect and respond to threats with greater accuracy and efficiency. The research introduces innovative approaches in advanced mechanisms and emerging threat processes, offers a protection and detection techniques, presents a unique adversarial behavior model for TCP flags ACK, and proposes an original event correlation algorithm for TCP ACK flag detection, contributing to the advancement of cybersecurity practices.**

***Index Terms*—Cyber-security, Data-Driven Insights, Cyber-Attacks, vulnerabilities, Advanced Mechanisms, Threats.**

I. Introduction

In the rapidly evolving landscape of cybersecurity, the utilization of data-driven insights has become increasingly integral in understanding, mitigating, and defending against advanced cyber threats. This dynamic interplay between data-driven insights and emerging cyber attacks underscores the need for comprehensive analysis to grasp the full scope of their impact. The title "Analyzing the Impact of Data-Driven Insights on Cyber Attacks: Advanced Mechanisms and Emerging Threats" encapsulates the essence of this study, which seeks to delve into the transformative influence of data-driven approaches on cybersecurity and their effectiveness in countering sophisticated threats. This introduction sets the stage for an exploration of the intricate relationship between data-driven insights and the ever-evolving landscape of advanced cyber mechanisms, shedding light on the imperative role these insights play in bolstering our defenses against the continuously emerging threats that challenge the digital world. Data-driven insights have emerged as a crucial tool in understanding, detecting, and mitigating cyber threats. This research capitalizes on the power of data analytics, machine learning, and artificial intelligence to extract patterns, anomalies, and trends in cloud-based cyber attacks. Through a rigorous analysis of real-world case studies, historical data, and simulation scenarios, this study aims to provide a comprehensive understanding of the multifaceted impact of these attacks on organizations and individuals. Moreover, the research acknowledges the dynamic nature of cyber threats in the cloud environment. Threat actors are continually adapting, utilizing new techniques, and taking advantage of emerging vulnerabilities. To this end, this study explores the concept of "emerging threats" in the context of cloud-based cyber attacks. By identifying the evolving tactics and potential risks on the horizon, this research equips organizations and security professionals with the knowledge needed to stay ahead of the curve and proactively defend against future threats. In summary, its a timely and essential exploration of the complex interplay between cloud computing and cybersecurity. By providing in-depth analysis, data-driven insights, and proactive strategies, this research aims to empower individuals, organizations, and policymakers to effectively protect their digital assets in an era where the edge technology is both the solution and the battlefield.

II. Background and Related Work

[1] is a research approach or methodology aimed at using data-driven techniques and analytics to enhance the security and protect the integrity of systems that leverage cloud computing technologies. This approach involves collecting, analyzing, and interpreting data related to potential security threats and vulnerabilities in cloud-based systems. It seeks to use empirical data, historical attack patterns, and real-time monitoring to gain insights into emerging threats and the effectiveness of security measures. By doing so, it allows organizations and security professionals to make informed de-

cisions, proactively identify and mitigate threats, and improve the overall security posture of their cloud-enabled systems.

[2], [5] The main objective of these methodologies are to ensure the confidentiality, integrity, and availability of data and services hosted in cloud environments. With the increasing reliance on cloud services for various business and personal activities, it has become paramount to understand and combat the evolving threat landscape. Data-driven threat analysis in cloud-enabled systems provides a systematic and evidence-based approach to achieve this goal, helping to safeguard against cyberattacks and unauthorized access, maintain regulatory compliance, and optimize security strategies for cloud deployments. [6] suggests a research or development effort focused on addressing the security and reliability challenges associated with Internet of Things (IoT) devices in cloud-based sensor systems. [7] This component of the title highlights the core objectives of the study or system. It implies that the research or system aims to establish mechanisms and protocols that ensure the security and reliability of device access within the IoT and sensor cloud context. [8], [9] Cybersecurity attacks continue to evolve in sophistication and frequency, posing significant threats to individuals, organizations, and governments worldwide. Mitigating these attacks is an ongoing challenge that requires constant adaptation and innovative approaches. In this discussion, we will examine some recent cybersecurity attacks and the mitigation approaches that have been employed to combat them. [10], [16] This refers to a system that utilizes machine learning algorithms to continuously monitor and detect unusual patterns or anomalies within an industrial control environment. It adapts and evolves its detection methods to identify unexpected behavior, which can help maintain the security and reliability of critical industrial systems. [17] This refers to a technique for efficiently managing and optimizing the allocation of resources in a cloud cluster that's used for monitoring and processing streaming services. It involves statistical methods to condense or compact the resource allocation, ensuring effective and real-time performance while conserving resources. [18]This is a theoretical framework that outlines an architecture for conducting active cyberattacks on intelligence infocommunication systems. It specifies the use of advanced encryption (AES-512) along with pre-encrypted search tables and pseudo-random functions (PRFs) for conducting secure and covert attacks on these systems. [19], [23] This initiative focuses on leveraging deep learning and machine learning techniques to create a comprehensive and realistic dataset of distributed denial of service (DDoS) attacks, while simultaneously establishing a taxonomy for categorizing these attacks. Additionally, it addresses the management of this dataset, which is critical for training and testing cybersecurity systems. By doing so, it enables the development and enhancement of more effective DDoS attack detection and mitigation strategies, ultimately strengthening network security in the face of evolving cyber threats.

A. *Problem Statement*

The integration of data-driven insights into cybersecurity brings forth a myriad of complex problems and challenges. The sheer complexity and volume of data generated by organizations pose difficulties in collecting, processing, and effectively analyzing this information, potentially leading to both false alarms and missed threats. Advanced cyber threats, such as advanced persistent threats (APTs) and zero-day vulnerabilities, have become more prevalent, making them particularly challenging to detect and mitigate. Privacy concerns are also at the forefront, as the extensive use of data for cybersecurity purposes raises ethical and legal questions about personal information protection. Resource constraints, especially in smaller organizations, hinder their ability to harness data-driven insights effectively and invest in advanced security mechanisms. Furthermore, the dynamic nature of the cyber threat landscape necessitates constant adaptation and vigilance to stay ahead of the ever-evolving tactics employed by cybercriminals.

III. The Advanced Mechanisms and Emerging Threats Processes

This Figure 1 represents a process for managing advanced mechanisms and emerging threats in the context of cybersecurity. Below is a detailed breakdown of the components and steps in the flowchart:

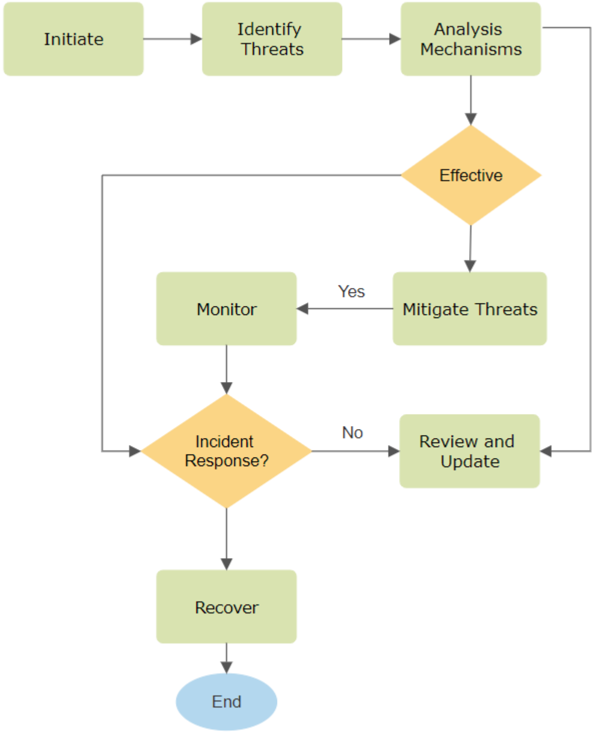

Fig. 1. The advanced mechanisms and emerging threats processes

This architecture, model consists of the following components:

- Initiate: This is the starting point of the flowchart. It signifies the beginning of the process, where an organization or entity becomes aware of the need to address emerging cybersecurity threats.
- Identify Threats: In this step, the organization identifies potential cybersecurity threats and vulnerabilities. This can involve threat intelligence, system monitoring, and analysis of emerging risks.
- Analyze Mechanisms: Once threats are identified, the organization analyzes the mechanisms and methods used by these threats. This step aims to understand the tactics and techniques employed by malicious actors.
- Effective: This diamond-shaped decision point asks whether the mechanisms used by the threats are effective. If the organization determines that they are, it leads to the "Incident Response" path. If not, it leads to the "Mitigate Threats" path.
- Mitigate Threats: When the mechanisms are not considered effective, the organization takes steps to mitigate the identified threats. This can involve implementing security measures, patching vulnerabilities, or strengthening the defense mechanisms.
- Monitor: This step involves continuous monitoring of the environment for any signs of threat activity. It's essential to ensure that the mitigation measures are effective and that new threats are promptly detected.
- Incident Response: This decision point asks whether an incident has occurred. If there's an incident, it leads to the "Recover" path, indicating the need to respond to and recover from the security incident. If there's no incident, it leads to the "Review and Update" path.
- Recover: In the event of a security incident, the organization initiates incident response procedures. This may include containment, eradication, recovery, and lessons learned from the incident.
- Review and Update: If there is no incident, or after an incident has been resolved, the organization reviews the overall security posture and updates its security measures and practices. This continuous improvement process ensures readiness for future threats.
- End: This is the end point of the flowchart. It signifies the completion of the process for managing advanced mechanisms and emerging threats. The organization should be better prepared to address future threats and adapt to changing circumstances.

This flowchart serves as a visual representation of a cybersecurity strategy that combines threat identification, analysis, mitigation, continuous monitoring, incident response, and ongoing improvement. It helps organizations systematically address the complex challenges posed by advanced mechanisms and emerging threats in the cybersecurity landscape.

IV. Mechanism Formulation Model

This algorithm outlines a systematic approach to address the ever-evolving cybersecurity landscape characterized by advanced mechanisms and emerging threats. It begins by initializing the necessary variables and data structures, setting the stage for threat management.

The process then proceeds with threat identification, where data from various sources is collected and analyzed to recognize potential threats. If no threats are identified, the process terminates, acknowledging that there are no immediate concerns.

Upon threat identification, the algorithm delves into analyzing the mechanisms and tactics employed by these threats. It assesses the effectiveness of these mechanisms, distinguishing between those that are effective (assigned a value of 1) and those that are not (assigned a value of 0).

When ineffective mechanisms are identified, the algorithm moves to the mitigation phase. Mitigation measures are implemented to reduce the risk and impact of these threats. The threat's status is updated to indicate that it has been mitigated.

Continuous monitoring is a critical component of this algorithm. It involves ongoing surveillance to detect any signs of threat activity. If a new threat is detected, the process loops back to the mechanism analysis phase to address the new threat's tactics and tactics.

In the event of a security incident, the algorithm triggers incident response procedures. This can include containment to prevent further damage, eradication to remove the threat, recovery to restore normal operations, and post-incident analysis to learn from the experience.

Finally, the algorithm emphasizes the importance of regular review and updates to enhance the overall security posture. This step ensures that security measures and practices remain effective and adaptable to the changing threat landscape.

In summary, the algorithm offers a structured and adaptive approach to managing cybersecurity threats, providing a framework for identifying, analyzing, mitigating, monitoring, responding to incidents, and continuously improving security measures in the face of advanced mechanisms and emerging threats.

V. Mathematical Modelling

Theorem 1. *Let I be the set of identified threats, and for each $t_i \in I$, let M_i represent the set of mechanisms and tactics associated with threat t_i. Additionally, let S_i be a binary variable representing the effectiveness of the mechanisms for threat t_i, where $S_i = 1$ if mechanisms are effective, and $S_i = 0$ if not.*

The algorithm for managing advanced mechanisms and emerging threats can be described as follows:

1) *Initialize the system with appropriate variables and data structures.*
2) *Identify threats: Collect and analyze data from various sources to identify potential threats. If no threats are identified, the algorithm terminates.*
3) *Analyze mechanisms: For each identified threat t_i, analyze the mechanisms and tactics in M_i. Determine the effectiveness of these mechanisms using the binary variable S_i. A mechanism is considered effective when $S_i = 1$ and ineffective when $S_i = 0$.*

Algorithm 2 Algorithm for Managing Advanced Mechanisms and Emerging Threats

```
Data sources for threat identification Improved cybersecurity posture  Initialize variables and data structures End of the process
True Step 1: Identify Threats  Collect and analyze threat data No threats are identified End the process
Step 2: Analyze Mechanisms  each identified threat Analyze the threat mechanisms and tactics  Determine if the threat mechanisms are effective
Step 3: Mitigate Threats  each threat with ineffective mechanisms Implement mitigation measures  Update threat status as mitigated
Step 4: Continuous Monitoring  Continuously monitor the system for any signs of threat activity  A new threat is detected Return to Step 2 (Analyze Mechanisms)
Step 5: Incident Response  A security incident occurs Initiate incident response procedures  This may include containment, eradication, recovery, and lessons learned
Step 6: Review and Update  Review the overall security posture  Update security measures and practices
```

4) *Mitigate threats: Implement mitigation measures for threats with ineffective mechanisms. Update the threat status as mitigated.*
5) *Continuous monitoring: Continuously monitor the system for signs of threat activity. If a new threat is detected, return to step 3 (Analyze Mechanisms) for analysis.*
6) *Incident response: If a security incident occurs, initiate incident response procedures, including containment, eradication, recovery, and lessons learned.*
7) *Review and update: Regularly review the overall security posture and update security measures and practices.*

This algorithm, when applied, results in an improved cybersecurity posture by systematically identifying, analyzing, mitigating, and responding to advanced mechanisms and emerging threats.

A. Advanced Mechanisms: Protection and Detection Technique

The Karn/Partridge algorithm is used to calculate the retransmission timeout (RTO) in the Transmission Control Protocol (TCP). It is based on the following mathematical expressions:

$$\begin{aligned}\text{Estimated\_RTT} &= (1-\alpha)\cdot\text{Estimated\_RTT}+\alpha\cdot\text{Sample\_RTT}\\ \text{Deviation} &= (1-\beta)\cdot\text{Deviation}+\beta\cdot|\text{Sample\_RTT}-\text{Estimated\_RTT}|\\ \text{RTO} &= \text{Estimated\_RTT}+4\cdot\text{Deviation} \qquad (1)\end{aligned}$$

Where:

Estimated_RTT - Estimated Round-Trip Time
Sample_RTT - Sample Round-Trip Time
Deviation - Smoothed Mean Deviation
α - Smoothing factor for Estimated_RTT
β - Smoothing factor for Deviation
RTO - Retransmission Timeout

The algorithm is used to adapt the RTO value dynamically based on observed network conditions, allowing TCP to efficiently handle varying RTT values and improve data transmission reliability.

VI. Adversarial Behavior Simple Modeling for detecting TCP flags ack

Adversary Profile:

1) Adversary Type: The adversary in this context is a network attacker who seeks to disrupt communication or gain unauthorized access to network resources.
2) Adversary Knowledge: The adversary possesses a moderate level of knowledge about TCP/IP protocol and network communication.

Adversarial Strategies:

1) ACK Flag Manipulation: The adversary may engage in the following strategies related to the ”ACK” flag:

- ACK Flooding: The adversary may flood the target with a high volume of TCP ACK packets, overwhelming the target's resources and causing network congestion.
- ACK Spoofing: The adversary might spoof ACK packets to falsely acknowledge data reception, tricking the sender into continuing to transmit data.
- ACK Suppression: The adversary may selectively suppress ACK packets to disrupt the flow of communication between legitimate parties.

Detection Strategies: To detect adversarial behavior related to the ”ACK” flag, network defenders can employ the following methods:

1) Threshold-Based Anomaly Detection: Set thresholds for the expected rate of ACK packets. Unusual spikes in ACK traffic could be indicative of an attack. Anomaly detection algorithms can be employed for this purpose.
2) Packet Inspection: Examine packet headers for signs of ACK manipulation. Tools like intrusion detection systems (IDS) can analyze incoming and outgoing packets for anomalies and alert administrators to suspicious ACK patterns.
3) Flow Monitoring: Monitor TCP flows and establish a baseline for normal ACK behavior. Deviations from this baseline, such as an unusually high number of ACK packets, can trigger alerts.
4) Behavioral Analysis: Employ machine learning models that learn the typical behavior of ACK packets in your network. Any deviations from learned patterns can be flagged as potential adversarial activity.

Response Strategies: Upon detecting adversarial behavior related to the ”ACK” flag, network defenders can respond by:

1) Traffic Filtering: Implement traffic filtering rules to block or rate-limit incoming ACK packets if they exceed predefined thresholds.
2) Alerts and Notifications: Set up alerting mechanisms to inform network administrators about suspicious ACK flag activity so that they can investigate further.
3) Incident Response: Initiate an incident response process to identify the source of adversarial behavior, mitigate the impact, and remediate the issue.
4) Adaptive Security: Adjust network security policies and controls based on the nature of the attack. For example, adaptive firewall rules may be applied to block IP addresses associated with malicious ACK activity.

VII. Event Correlation Algorithm for Detecting TCP ACK Flag

Let $E_1, E_2, \ldots, E_n$ represent a sequence of network events where n is the total number of events. Each event E_i is defined as a 5-tuple:

$$E_i = (T_i, S_i, D_i, P_i, F_i)$$

Where:

T_i is the timestamp of the event E_i

S_i is the source IP address

D_i is the destination IP address

P_i is the protocol (e.g., TCP, UDP)

F_i is the set of TCP flags associated with the event

The TCP ACK flag is represented as $F_i = \{ACK\}$.

The event correlation algorithm to detect the TCP ACK flag is as follows:

1) For each event E_i, check if P_i is equal to ”TCP.”
2) If P_i is ”TCP,” check if the set F_i contains the ”ACK” flag.
3) If F_i contains ”ACK,” log or alert the event as a TCP ACK flag event.

The algorithm can be implemented in a network monitoring system to identify and correlate events with the presence of the TCP ACK flag.

VIII. The Experimental Results

In cybersecurity and network analysis, examining TCP packets with ”tcp.flags.ack == 0” and ”tcp.flags.ack == 1” involves assessing the state of the Acknowledgment (ACK) flag in the TCP header. The ACK flag plays a crucial role in TCP connections, indicating whether or not a packet acknowledges the receipt of data. Here’s what each condition can mean in the context of cybersecurity and attacks:

tcp.flags.ack == 0:

1) Denial of Service (DoS) Attacks: Packets with ”tcp.flags.ack == 0” typically indicate that the packet does not acknowledge the receipt of data. Attackers can use this flag to flood a target system with unacknowledged packets, potentially overwhelming its resources and causing a denial of service (DoS) attack.
2) Port Scanning and Reconnaissance: In a network scan, attackers may use ”tcp.flags.ack == 0” to identify closed ports. By sending packets with this flag, they can see which ports do not acknowledge their presence, helping them map the target’s network.

tcp.flags.ack == 1:

1) Normal Data Transfer: In the context of legitimate network communication, ”tcp.flags.ack == 1” indicates that the packet acknowledges the receipt of data. This is the expected behavior in most TCP connections during data transfer, and it helps ensure the reliability of the data exchange.
2) Firewall and Intrusion Detection Bypass: Attackers may use the ”tcp.flags.ack == 1” condition in their packets to mimic legitimate traffic, making it more challenging for firewalls or intrusion detection systems to identify malicious activity. This can be part of a technique known as ”packet normalization” or ”protocol evasion.”

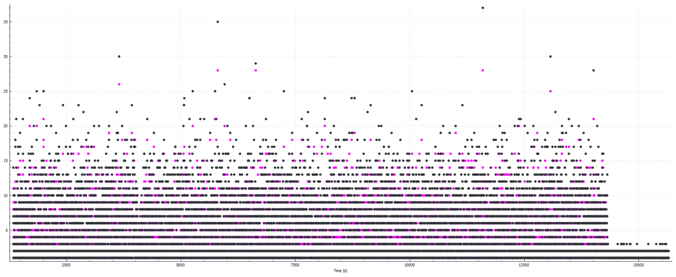

Fig. 2. Analysing and Examining TCP Packets -TCP control flags

Understanding these analysis states is important for cybersecurity professionals when monitoring network traffic and identifying potentially malicious patterns. Analyzing these flag conditions, along with other indicators, can help detect and respond to network attacks, unauthorized access attempts, and other security threats.

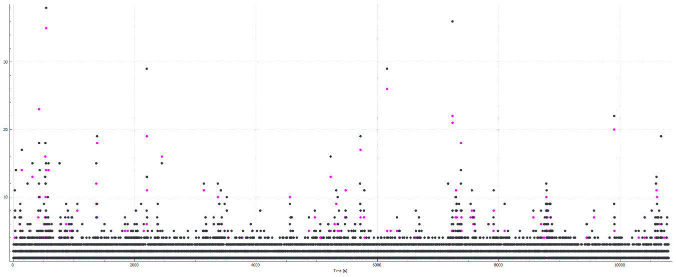

Fig. 3. Analysing and Examining TCP Packets -TCP control flags

Figures 2 and 3 present the outcomes of analyzing packets that often carry non-data information, primarily serving control functions within the TCP protocol. Such packets frequently play essential roles in the establishment and termination of connections, including the initial handshake (SYN, SYN-ACK, ACK) and connection closure (FIN, FIN-ACK). Furthermore, they can signify filtered or irrelevant traffic, as identified by our ”Correlation Algorithm for Detecting TCP ACK Flag.” Lastly, encountering packets devoid of active flags may hint at unusual or potentially malformed packets that deviate from the typical behavior expected of TCP communication.

In essence, a thorough examination of these packets offers valuable insights into the intricate mechanisms governing TCP connections. It not only aids in network troubleshooting and analysis but also showcases the algorithm’s ability to enhance anomaly detection during packet segmentation. In a network packet capture, TLS (Transport Layer Security) alert messages are used to communicate problems or error conditions related to the TLS protocol. These alert messages can be observed in the payload of the TCP packets during a TLS handshake or encrypted communication. TLS alert messages consist of two bytes: a severity level and an alert description. Fig.4 shows analysing network packets,in TLS alert messages as part of a TLS handshake or encrypted communication. These alerts provide valuable information about the health of the TLS connection and can be used for troubleshooting and monitoring the security of a connection. However, it’s crucial to note that the exact content of these messages is encrypted and cannot be directly inspected in the packet capture unless the encryption is decrypted using the appropriate keys. Time sequences can be an essential aspect of understanding network behavior and diagnosing issues. Tools like ”tcptrace” are commonly used for analyzing TCP (Transmission Control Protocol) traffic, and they can help you visualize the time sequence of packets in various ways. Fig.5 provides valuable insights and assist in various aspects of security:

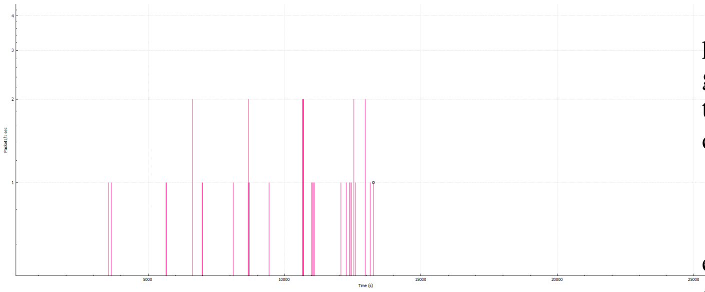

Fig. 4. TLS Alert Message Analysis

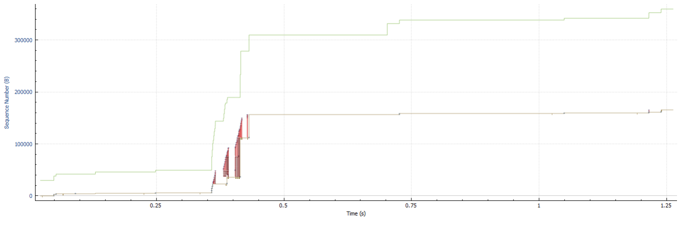

Fig. 5. Traffic Analysis TCP, ”time sequence”

Anomaly Detection: Sudden spikes in traffic, unexpected delays, or irregular packet reordering can be indicative of an ongoing cyberattack or intrusion.

Attack Identification: Distributed denial of service (DDoS) attacks, can be detected by observing sudden surges in incoming traffic, followed by a decrease in the responsiveness of the network. Analyzing the time sequence helps pinpoint when these attacks began and how they evolved.

Malware and C2 Detection: The timing of connections and the order in which certain commands are issued can help identify communication patterns between compromised systems and command-and-control servers used by malware. Such patterns can be used to detect and mitigate threats.

Response Time Analysis: Analyzing the time sequence of packets shows the network and application responsiveness is getting higher for some specific time. Unusually slow response times or excessive latency may indicate an ongoing attack or compromised system.

IX. Conclusion

The proposed framework of advanced mechanisms and emerging threat processes, accompanied by its supplementary algorithmic components, displays immense potential for the effective identification of cyberattacks and anomaly detection within the realm of cybersecurity, particularly through packet analysis. By harnessing purpose-built algorithms, mechanisms, and data structures tailored to the cybersecurity landscape, this framework enhances threat intelligence management and fortifies overall security. Moreover, this framework offers a robust and comprehensive solution for the detection of cyberattacks and anomalies. Its effectiveness is underpinned by its ability to harness advanced algorithms, adapt in the face of evolving threats, and enable informed decision-making. By integrating this framework into their cybersecurity systems, organizations can augment their capabilities in detecting and responding to cyberattacks, thereby fortifying their overall security stance and safeguarding critical assets and sensitive information.

In conclusion, the analysis of TCP packets, specifically ”tcp.flags.ack == 0” and ”tcp.flags.ack == 1,” reveals essential insights in cybersecurity. The former often indicates potential denial of service (DoS) attacks or port scanning, while the latter signifies normal data transfer or intrusion evasion. Understanding these conditions is crucial for monitoring network security effectively. Additionally, examination of Transport Layer Security (TLS) alert messages in network captures offers insights into TLS protocol health. Monitoring time sequences aids in anomaly detection, identifying attacks like DDoS, recognizing malware patterns, and assessing network responsiveness. This research empowers cybersecurity professionals to bolster network security by proactively responding to threats and anomalies, contributing significantly to the field.

References

[1] Alwaheidi, M.K.S.; Islam, S. Data-Driven Threat Analysis for Ensuring Security in Cloud Enabled Systems. Sensors 2022, 22, 5726. https://doi.org/10.3390/s22155726

[2] Ahsan, M.; Nygard, K.E.; Gomes, R.; Chowdhury, M.M.; Rifat, N.; Connolly, J.F. Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. J. Cybersecur. Priv. 2022, 2, 527-555. https://doi.org/10.3390/jcp2030027

[3] UcedaVelez, T.; Morana, M.M. Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis; John Wiley & Sons: Hoboken, NJ, USA, 2015.

[4] Manzoor, S.; Vateva-Gurova, T.; Trapero, R.; Suri, N. Threat Modeling the Cloud: An Ontology Based Approach. In Proceedings of the Information and Operational Technology Security Systems, IOSec 2018, CIPSEC Project, Heraklion, Crete, Greece, 13 September 2018; Fournaris, A., Lampropoulos, K., Marín Tordera, E., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2019; Volume 11398.

[5] de Azambuja, A.J.G.; Plesker, C.; Schützer, K.; Anderl, R.; Schleich, B.; Almeida, V.R. Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0,A Survey. Electronics 2023, 12, 1920.

[6] Chaudhry, S.A.; Yahya, K.; Al-Turjman, F.; Yang, M.-H. A secure and reliable device access control scheme for IoT based sensor cloud systems. IEEE Access 2020, 8, 139244–139254.

[7] Giannoutakis, K.M.; Spanopoulos-Karalexidis, M.; Filelis Papadopoulos, C.K.; Tzovaras, D. Next Generation Cloud Architectures. In The Cloud-to-Thing Continuum; Lynn, T., Mooney, J., Lee, B., Endo, P., Eds.; Palgrave Studies in Digital Business & Enabling Technologies; Palgrave Macmillan: Cham, Switzerland, 2020

[8] A. N. A. Koupaei and A. N. Nazarov, "A Hybrid Security Solution for Mitigating Cyber-Attacks on Info-Communication Systems," 2020 International Conference Engineering and Telecommunication (EnT), Dolgoprudny, Russia, 2020, pp. 1-4, doi: 10.1109/EnT50437.2020.9431296.

[9] Chowdhury, A. (2016). Recent Cyber Security Attacks and Their Mitigation Approaches, An Overview. In: Batten, L., Li, G. (eds) Applications and Techniques in Information Security. ATIS 2016. Communications in Computer and Information Science, vol 651. Springer, Singapore.

[10] R. Derbyshire, B. Green, D. Prince, A. Mauthe and D. Hutchison, "An Analysis of Cyber Security Attack Taxonomies," 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 2018, pp. 153-161.

[11] Sun, N.; Zhang, J.; Rimba, P.; Gao, S.; Zhang, L.Y.; Xiang, Y. Data-driven cybersecurity incident prediction: A survey. IEEE Commun. Surv. Tutor. 2018, 21, 1744–1772.

[12] Jan Vávra, Martin Hromada, Ludek Luká, Jacek Dworzecki, Adaptive anomaly detection system based on machine learning algorithms in an industrial control environment, International Journal of Critical Infrastructure Protection, Volume 34, 2021, 100446, ISSN 1874-5482.

[13] Alazab, M.; Venkatraman, S.; Watters, P.; Alazab, M. Zero-day malware detection based on supervised learning algorithms of API call signatures. In Proceedings of the Ninth Australasian Data Mining Conference (AusDM'11), Ballarat, Australia, 1–2 December 2011.

[14] Junjiao LIU, et al. A novel intrusion detection algorithm for industrial control systems based on CNN and process state transition 2018 IEEE 37th International Performance Computing and Communications Conference (IPCCC), IEEE (2018), pp. 1-8.

[15] Chernenko, E.; Demidov, O.; Lukyanov, F. Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms; Council on Foreign Relations: New York, NY, USA, 2018.

[16] Papastergiou, S.; Mouratidis, H.; Kalogeraki, E.M. Cyber security incident handling, warning and response system for the european critical information infrastructures (cybersane). In Proceedings of the International Conference on Engineering Applications of Neural Networks, Crete, Greece, 24–26 May 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 476–487.

[17] A. N. Nazarov and A. N. A. Koupaei, "An Architecture Model for Active Cyber Attacks on Intelligence Info-communication Systems:Application Based on Advance System Encryption (AES-512) Using Pre-Encrypted Search Table and Pseudo-Random Functions(PRFs)," 2019 International Conference on Engineering and Telecommunication (EnT), Dolgoprudny, Russia, 2019, pp. 1-5, doi: 10.1109/EnT47717.2019.9030541.

[18] A. Nazarov, A. Sychev, A. N. A. Koupaei, S. K. Ojha and H. Rai, "Statistical compaction of a monitoring cloud cluster resource when processing streaming services," 2019 International Conference on Engineering and Telecommunication (EnT), Dolgoprudny, Russia, 2019, pp. 1-5, doi: 10.1109/EnT47717.2019.9030598.

[19] Johnson, L. Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response; Newnes: Oxford, UK, 2013.

[20] Alghamdi, M.I. Survey on Applications of Deep Learning and Machine Learning Techniques for Cyber Security. Int. J. Interact. Mob. Technol. 2020, 14, 210–224.

[21] Sharafaldin, I.; Lashkari, A.; Hakak, S.; Ghorbani, A.A. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October 2019.

[22] Cortes, C.; Vapnik, V. Support-vector networks. Mach. Learn. 1995, 20, 273–297.

[23] John, G.H.; Langley, P. Estimating continuous distributions in Bayesian classifiers. arXiv 2013, arXiv:1302.4964.

[24] Kokila, R.; Selvi, S.T.; Govindarajan, K. DDoS detection and analysis in SDN-based environment using support vector machine classifier. In Proceedings of the 2014 Sixth International Conference on Advanced Computing (ICoAC), Chennai, India, 17–19 December 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 205–210.

[25] Kruegel, C.; Toth, T. Using decision trees to improve signature-based intrusion detection. In Proceedings of the International Workshop on Recent Advances in Intrusion Detection, Pittsburgh, PA, USA, 8–10 September 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 173–191.

[26] lowers, M.; Williams, J. Machine learning applied to cyber operations. In Network Science and Cybersecurity; Springer: Berlin/Heidelberg, Germany, 2014; pp. 155–175.

[27] Li, X.; Chen, D.; Li, C.; Wang, L. Secure data aggregation with fully homomorphic encryption in large-scale wireless sensor networks. Sensors 2015, 15, 15952–15973.