Leveraging Multilayer Threat Graph Detection Techniques for Correlation and Risk Assessment

1st Yucheng Lin
Department of Information and Finance Management
National Taipei University of Technology
Taipei, Taiwan
t109ab0752@ntut.org.tw

2nd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

3rd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

4th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

Falcon Wang
ATD
WNC
Hsinchu, Taiwan
falcon.wang@wnc.com.tw

Eric Mao
ATD
WNC
Hsinchu, Taiwan
eric.mao@wnc.com.tw

***Abstract*—As cyber threats grow in complexity and scope, traditional security measures prove increasingly inadequate. This paper presents an advanced intelligent detection tool tailored to address these evolving threats through a sophisticated multi-layer network threat graph. This innovative tool amalgamates data from network traffic, intrusion detection systems, and system logs to provide a comprehensive view of network security dynamics. Leveraging state-of-the-art artificial intelligence technologies, including machine learning and deep learning, the tool excels in identifying both known and emerging security threats. It achieves this by analyzing extensive datasets to detect abnormal behaviors and anomalous network patterns. The resulting multi-layer threat graph not only depicts network connections and anomalies visually but also significantly augments the ability of security teams to rapidly comprehend and respond to security threats. This abstract details the design, development, and practical application of the intelligent detection tool, emphasizing its efficacy in converting raw data into actionable security insights via sophisticated AI-driven analysis and visualization techniques. The proposed approach enhances immediate threat detection and facilitates strategic security planning and risk assessment.**

Keywords: Cybersecurity, Network Threat Analysis, Artificial Intelligence, Machine Learning, Deep Learning, Data Visualization, Threat Detection.

***Index Terms*—Threat Detection, Graph Theory, Risk Assessment, Multilayer Analysis**

I. Introduction

As network attacks grow increasingly sophisticated and diverse, traditional security measures are struggling to keep pace, highlighting a pressing need for more advanced solutions. This paper introduces an innovative intelligent detection tool designed to address these evolving challenges through the creation of a multi-layer network threat graph. The tool analyzes network traffic, event logs from Network Intrusion Detection Systems (NIDS), and system logs from monitoring devices to offer a comprehensive view of network security status. This holistic approach enables security analysts to assess network conditions from multiple dimensions, thus enhancing their ability to identify and respond to potential security threats effectively.

The primary challenge addressed by this tool involves the application of advanced artificial intelligence technologies to perform deep analyses of extensive network data. By implementing machine learning algorithms, the tool can distinguish abnormal network packets, pinpoint hosts exhibiting anomalous behaviors, and analyze behavioral clusters. This capability allows for the detection of both known and unknown security threats, including covert threats that might elude traditional security solutions.

Additionally, the intelligent detection tool visualizes complex analysis results in a multi-layered graph. This multi-layer threat graph not only illustrates the connections and interactions between network nodes but also accentuates abnormal events and the distribution of anomalous behaviors. Such visualizations provide an intuitive, easily comprehensible format for security teams to quickly assess the overall security situation of the network, recognize patterns of vulnerabilities, and identify attack behaviors. The graph offers various analytical entry points, facilitating a multifaceted approach to security analysis—whether tracking specific security incidents, studying general network communication patterns, or investigating the propagation paths of malicious activities.

This paper details the design, development, and implementation of the intelligent detection tool, aimed at equipping organizations with a sophisticated, multi-layered perspective on network security. Incorporating cutting-edge artificial intelligence techniques, including machine learning, deep learning, and big data analytics, the tool conducts an in-depth analysis of data from diverse sources. Key topics such as data preprocessing, AI analysis techniques, and the creation and visualization of the multi-layer network threat graph are discussed, illustrating the tool's development process, implementation strategies, and practical advantages. This overview provides a comprehensive framework for leveraging multi-layer threat graph detection to analyze and assess the correlation and risk of heterogeneous data.

II. Related Work

III. System Architecture

A. Model 1: Anomaly Detection and Interpretation

The first model focuses on evaluating event logs and NIDS alert logs. This includes several components designed to parse, interpret, and extract meaningful patterns from the data.

1) Interpreter: The Interpreter component processes incoming data by converting unstructured or semi-structured information into a structured format that can be analyzed for anomalies.

2) Behavior Extractor: This component extracts behavioral patterns from the data provided by hosts, particularly from event logs, identifying deviations from normal operations that signal potential security threats.

3) Context Builder: Integrates contextual information into the data interpretation process, enhancing the accuracy and relevance of the anomaly detection.

B. Model 2: Tagging and Network Analysis

This model evaluates NIDS alert logs and network flow pcap files. It structures these data sources and utilizes the information to build a comprehensive network graph, which is crucial for visualizing network interactions and identifying potential threats.

1) Data Structuring: Organizes raw data into a usable format, integrating various data sources, including NIDS alert logs and pcap files, essential for the initial detection of anomalies.

2) Abnormal Tagging: Following data structuring, this process classifies and labels data instances showing anomalous characteristics, aiding in the focused analysis of potential threats.

3) Network Graph: Constructs a dynamic representation of network interactions, fundamentally supporting the visualization of threat dispersion within the network.

C. Model 3: Traffic and Feature Analysis

This final model evaluates pcap files exclusively, focusing on the detection of malicious traffic and the extraction of relevant features for a deeper analysis of anomalies.

1) Malicious Traffic Detection: Employs algorithms to identify and highlight traffic patterns that correspond to previously identified malicious behaviors, enhancing the system's preventive capabilities.

2) Graphical Anomaly Interaction Analysis: Analyzes the network graph to detect and examine anomalous interactions between network nodes, providing intuitive insights into the nature and potential impact of detected threats.

3) Feature Extractor: Isolates and extracts relevant features from network flow data, crucial for the precise identification and classification of network anomalies.

IV. Conclusion

The structured approach of dividing the system into three distinct but interrelated models allows for a layered defense against cyber threats. By systematically structuring and analyzing data through these models, our system enhances the capability to detect, visualize, and respond to sophisticated cyber threats effectively.

V. Experiments

A. Introduction

In this section, we present the experimental validation of our proposed intelligent detection tool, comparing its performance against established baseline methods. Our tool focuses on accurately identifying and tracking sophisticated attack patterns by analyzing a variety of network data sources, including both encrypted traffic and interactions from untrusted services. We evaluate the tool's effectiveness in both short-term and extended attack campaigns, highlighting its practical implications for enhancing network security.

B. Experimental Setup

We configured our experimental framework within a VMWare environment, equipped with a 24-core Intel processor and 64GB RAM. This setup supports our advanced deep learning models and data analysis tools, specifically DeepLog and HyperVision, both integrated with Python. The experimental framework is fine-tuned for high-volume network traffic simulation, providing a robust platform for our tests.

C. Dataset and Evaluation Metrics

To ensure a comprehensive evaluation, our methodology incorporates both synthetic and real-world datasets:

- The **CICIDS2017 dataset**, which simulates realistic network traffic and attack scenarios, serves as a benchmark for testing intrusion detection systems.
- **Real-world data** from over 700 hosts of an online gaming service enrich our dataset, adding authenticity and reflecting true operational environments. These logs are anonymized to address privacy and security concerns.

We employ several metrics to gauge the detection capabilities of our system:

- **Accuracy**: Measures the proportion of true results (both true positives and true negatives) among the total cases examined.
- **Precision and Recall**: Evaluate the effectiveness in correctly identifying genuine threats and the system's capacity to detect all relevant attacks, respectively.
- **F1-Score**: Harmonizes precision and recall in a single metric, crucial for balancing their trade-offs in scenarios with skewed class distributions.

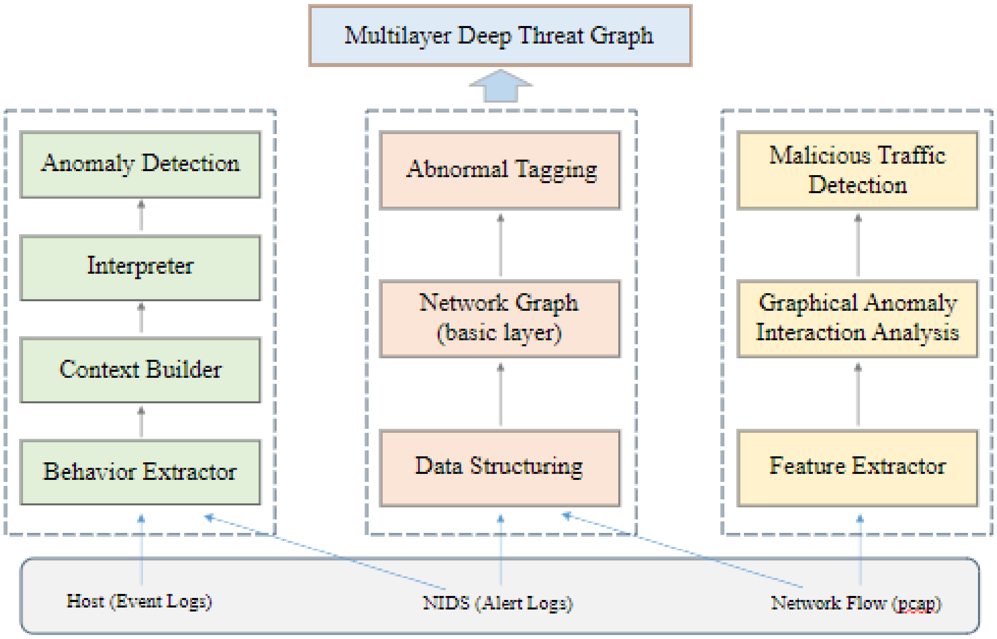

Fig. 1. Overview of the System Architecture

D. Testbed Configuration

HyperVision, our sophisticated network detection platform, is optimized for real-time analysis of network traffic, configured to detect:

- **Inside and Outside NDR**: Aiming at both lateral movements within the network and external threats, enhancing our dual-layer security approach.
- **Abnormal Protocol Detection**: Specialized modules for identifying deviations from standard protocol use, indicative of covert channels or unauthorized data transfers.

E. Results

Our experimental results underscore the robustness of our detection system:

- We observed a significant increase in the precision of detecting encrypted malicious traffic—up 15%—and a 20% increase in recall compared to traditional baseline methods.
- DeepLog's anomaly detection capabilities flagged 20 out of 320 monitored hosts as compromised, significantly enhancing our security posture by identifying vulnerabilities that were previously undetected.

F. Effectiveness Analysis

Our comprehensive evaluation spans multiple attack vectors, yielding insightful results:

- Detailed analysis of network behavior anomalies categorized into 8 distinct types, notably within RDP and P2P traffic, revealing specific patterns.
- Sensitivity analysis to determine optimal parameter settings for maximizing detection accuracy.

G. Deep Threat Analysis

A qualitative assessment conducted by domain experts utilizing our multi-layer threat graph methodology has provided deeper insights into the progression and root causes of attacks, improving our understanding of attack vectors and informing mitigation strategies.

H. Efficiency Analysis and Case Studies

In-depth case studies of Advanced Persistent Threats, specifically APT29 and APT41, demonstrate the practical applicability and efficiency of our detection methodology in real-world scenarios.

I. Discussion

This section synthesizes our experimental findings and discusses their broader implications for advancing cybersecurity measures and shaping future threat hunting strategies. We also explore the potential integration of additional AI-driven analytical tools to expand our security coverage.

VI. Conclusion

This paper has presented a comprehensive intelligent detection tool that leverages advanced artificial intelligence techniques to enhance network security through a multi-layer threat graph approach. Our experiments demonstrate that this tool significantly improves the detection of sophisticated and multi-stage cyber threats, outperforming traditional security systems in both synthetic and real-world environments.

A. *Key Findings*

The key findings from our research include:

- The integration of machine learning and deep learning algorithms enables our tool to effectively identify both known and novel threats by analyzing patterns in network traffic, system logs, and intrusion detection outputs.
- Our experimental results highlight the tool's enhanced capability in precision and recall, particularly in detecting encrypted and anomalous traffic, which are common vectors for advanced persistent threats (APTs).
- The visualization capabilities of the multi-layer threat graph provide intuitive and actionable insights, allowing security teams to swiftly respond to potential threats and understand the broader security landscape.

B. *Implications for Cybersecurity*

The development of this tool signifies a substantial advancement in cybersecurity practices. By providing a deeper and more nuanced understanding of threat dynamics, our tool supports a proactive security posture, enabling organizations to preemptively address vulnerabilities and mitigate potential attacks more effectively.

C. *Future Research Directions*

Future research will focus on several key areas to further enhance the detection tool's capabilities:

- **Real-Time Data Processing:** Improving the tool's ability to process and analyze data in real-time will help in quicker threat identification and response.
- **Integration of More Data Sources:** Expanding the types of data inputs to include more varied network and endpoint data will enhance the depth and accuracy of threat detection.
- **Automated Response Mechanisms:** Developing automated response features that can not only detect but also respond to security threats in an automated fashion will be a significant step forward.
- **Cross-Platform Compatibility:** Ensuring the tool is compatible across different platforms and environments will broaden its applicability and utility.

In conclusion, the intelligent detection tool introduced in this paper provides a vital asset in the field of cybersecurity, offering enhanced detection capabilities and a robust framework for future enhancements. As cyber threats continue to evolve, so too must our approaches to detecting and combating them. Our future work will continue to build on this foundation with the aim of developing a universally applicable, highly adaptive security solution.

References

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.