MORGAN STATE UNIVERSITY
DIVISION OF RESEARCH AND ECONOMIC DEVELOPMENT
OFFICE OF TECHNOLOGY TRANSFER

Executive Summary

Multi-Layer Hidden Markov Model Based Intrusion Detection System

Innovation

Intrusion Detection Systems (IDS), which rely on machine learning and artificial intelligence, can significantly improve network defense against intruders. This technology can be trained to learn and identify uncommon patterns given a massive volume of traffic and notify system administrators for investigation. This enhanced IDS design makes use of machine learning algorithms such as Hidden Markov Model (HMM) using a multi-layer approach. This approach has been verified to resolve common flaws in the application of HMM to IDS. It factors the key problem of dimensionality to a discrete set of manageable elements. The multi-layer approach can be expanded beyond two layers to capture multi-phase attacks over longer spans of time. A pyramid of HMMs can resolve disparate digital events and signatures across protocols and platforms to actionable information where lower layers identify discrete events (such as network scan) and higher layers identify new states that are the result of multi-phase events of the lower layers.

Market Need

Systems which automate intrusion detection have been the subject of interest the past few decades as interest in information security has grown. Expanding volume of encrypted traffic has created challenges for security teams trying to monitor malicious network traffic. Encryption is meant to enhance network security, but also allows intruders to hide command-and-control activities, giving time to launch attacks. The IDS market is estimated at $4.6 billion in 2020 and anticipated to grow to $6.2 billion by 2025. The potential of this technology to significantly enhance defense against the ever-growing army intruders and hackers presents an intriguing opportunity to impact this industry.

Intellectual Property

A non-provisional patent was filed in May 2020.

Stage of Development

Current results confirm that our Markov Model can: 1) include multiple dimensions of information; 2) be retrained to identify new network states based on the robustness of the training data; and 3) can be implemented in a large-scale IDS based on this model.

Technology Transfer Opportunity

To keep up, security teams from government, industry and other organizations need modern tools with machine learning and AI to supplement threat detection, prevention, and remediation. This technology addresses vulnerabilities that cannot be detected by existing traffic monitoring tools and improves the state of intrusion detection systems and applies it in layered form to cover multiple forms of attacks over longer durations.

Key Investigators:
- Dr. Farzad Moazzami
- Dr. Wondimu K. Zegeye
- Dr. Richard Dean

Field(s) of Use:
- Computer Engineering
- Cybersecurity
- Business

Key Words:
- Network Defense
- Multi-layer
- Hidden Markov Model
- Dimensionality

Advantages:
- Multi-layered approach
- Factors in key problem of dimensionality
- Uses machine learning to adjust to more potential intrusions

Status:
Patent Filed

Links:
Patent application

Reference Number:
079/2019

Tech Transfer Contact:
Ray Dizon