Embedded Solutions
Network Applications

1D Convolutional Neural Networks for Bit Net Sentry

Integration of Neural Networks for Attack Detection in Industrial Control Systems with invisible Bit Net Sentry

Introduction

- BNS
  - Existing field-proven network appliance
  - An only invisible network security appliance acting at a data-link layer with negligible latency (few nano-seconds)
  - BNS is able to inspect every incoming/outgoing frame and to apply threat detection algorithms in real time
- Why 1D CNNs?
  - 1D CNNs are particularly suited for sequential data. Given that ICS data often consists of time series information (e.g., sensor readings over time), 1D CNNs can capture local patterns and temporal dependencies in the data, making them effective for anomaly detection

Implementation Steps

- Data Collection and Pre-processing
- Model Architecture
- Training
- Evaluation
- Deployment
- Integration of the trained 1D CNN model into the BNS product
- Continuously feed real-time ICS data into the model, flagging sequences that are deemed anomalous
- Integration with Other BNS Features:
  - Use the 1D CNNs in conjunction with other security features in BNS, such as White Box Cryptography and deep packet inspection
  - Use extensive set of BNS' alerts, triggering, redirection to honey ports etc to improve the user experience

Challenges and Considerations

- Ensure that the deployment of 1D CNNs doesn't introduce significant latency into the system, given the real-time requirements of ICS environments
- Continuously monitor the model's performance and be wary of "model drift“, where the model's performance degrades over time due to changing patterns in the data
- Incorporating 1D CNNs into BNS will require a combination of data science expertise, a deep understanding of the specific ICS environment, and rigorous testing to ensure the system remains robust and effective

Reference

Efficient Cyber Attack Detection in Industrial Control Systems Using Lightweight Neural Networks and PCA

by Moshe Kravchik and Asaf Shabtay

IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 19, NO. 4, JULY/AUGUST 2022