How Neural Networks Are Reshaping Cybersecurity

As technology and the internet grow at a rapid pace, our lives are moving online, surrounding us with cyber threats and attacks every day.

- Apps track personal data
- Bank information and passwords stored on digital devices
- Life-changing decisions made based on data which can be compromised

What are Neural Networks?

- Multi-layer networks that utilize labeled data sets to mimic how the human brain learns
- Work through formulas containing “weights” and “biases” on hidden layers between input and output

Ex: Facial/voice recognition, social media algorithms, virtual assistants, predictive search

- Different kinds of neural networks
  - Feedword Neural Networks
  - Convolutional Neural Networks
  - Recurrent Neural Networks

What is AI in Cybersecurity Going Forward?

- With the rise of technologies such as AI come new security threats that can only be addressed with modern solutions.
  - Viruses hidden in code of AI applications
  - Adaptable, intelligent malicious attacks
  - Neural networks (NN) provide enhanced approaches for detecting attacks without the need for human supervision.
  - Reduced false positives in Intrusion Detection and Prevention Systems (IDS/IPS)
  - Improved and more efficient malware analysis, preventing network attacks
  - Natural Language Processing (NLP) detects social engineering hacks, ex: spam emails

NN Vulnerabilities and Solutions

- Adversarial Attacks — exploit AI and force them to miscategorize
  - Smooth decision boundaries make it difficult to confuse the neural network
  - A Generative Adversarial Network (GAN) consists of 2 NN working together to produce false data to train against
  - Data Poisoning — injecting inaccurate data into a NN, causing it to function incorrectly
  - Deep Learning-Based Malware — malware hidden in AI-based applications can take advantage of the advanced capabilities and target victims selectively

References


Acknowledgements

Special thanks to:
- The AvenueE program and all its wonderful staff including Shanice Blake, Breidi Truscott Roberts, and Jordan Keys.
- Professor Jennifer Mullen