How Neural Networks Are Reshaping Cybersecurity

UC DAVIS UNIVERSITY OF CALIFORNIA

Computer Science/Engineering Team
Anelise Cho, Ashley Li, Eden Tadesse, Leila Jadoon

AvenueE
Roadmap to Your Career in Engineering & Computer Science

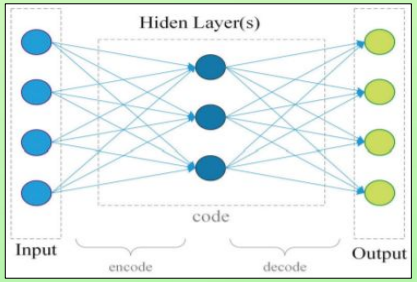
Are We Safe in a Digital Age?

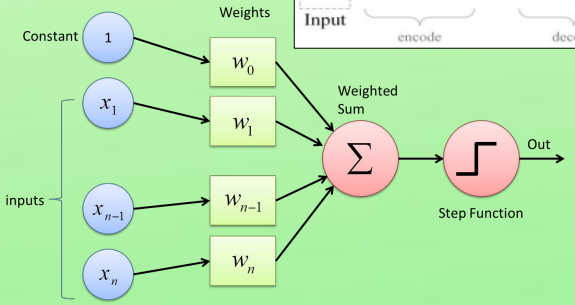
As technology and the internet grow at a rapid pace our lives are moving online, surrounding us with cyber threats and attacks every day.

- 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





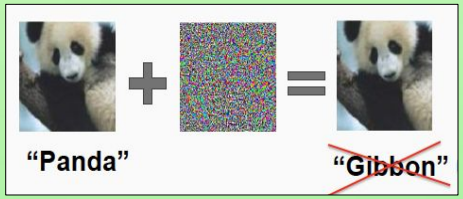
- Ex: Facial/voice recognition, social media algorithms, virtual assistants, predictive search
- Different kinds of neural networks
  - Feedword Neural Networks
  - Convolutional Neural Networks
  - Recurrent Neural Networks

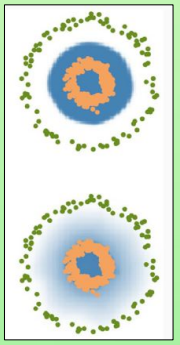
Neural Networks in Cybersecurity

- 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

Main Takeaway

- AI has made daily life more convenient through utilizing an individual’s data for a personalized experience
- As AI moves into prominence in fields such as criminal justice and HR, the data it trains on is increasingly valuable
- Vulnerabilities in AI can have far-reaching consequences and must be addressed

AI in Cybersecurity Going Forward

- GAN and smoothing detection boundaries to protect against Adversarial Attacks
- Higher data integrity to combat Data Poisoning
- Optimization of Neural Networks

References

- R. U. Khan, X. Zhang, M. Alazab and R. Kumar, "An Improved Convolutional Neural Network Model for Intrusion Detection in Networks," *2019 Cybersecurity and Cyberforensics Conference (CCC)*, Melbourne, Australia, 2019, pp. 74-77, doi: 10.1109/CCC.2019.000-6.
- G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," *2018 10th International Conference on Cyber Conflict (CyCon)*, Tallinn, 2018, pp. 371-390, doi: 10.23919/CYCON.2018.8405026.
- J. Lee, J. Kim, I. Kim, and K. Han, “Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles,” IEEE Access, vol. 7, pp. 165607–165626, 2019.
- N. Jamil, S. Lqbal and N. Iqbal, "Face recognition using neural networks," Proceedings. IEEE International Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century., Lahore, Pakistan, 2001, pp. 277-281, doi: 10.1109/INMIC.2001.995351.

Acknowledgements

Special thanks to:

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