Impact of Generative AI on Cybersecurity Education

Dulal Chandra Kar

Texas A&M University-Corpus Christi

Challenges Posed by Generative AI in Cybersecurity

- **Generative AI is rapidly transforming computing technology.**
- **It offers both beneficial and harmful applications.**
- **Challenges**
  - Increased ease of malware development for novice attackers.
  - Use of generative AI for creating phishing emails and social engineering attacks.
  - Creation of convincing deepfake videos and fake news using generative AI.
- Cybersecurity education needs to adapt to the impact of generative AI.

Need for Rigorous Cybersecurity Education

- **Cybersecurity community must stay ahead of cybercriminals.**
- **How?**
  - Academic institutions should revise cybersecurity curriculums to address generative AI threats.
  - Revising cybersecurity curriculums with contents on generative AI.
  - Generative AI should be included as a tool for cybersecurity education.
  - Generative AI can provide a safe and controlled learning environment.
  - Collaborating with industry partners to access generative AI tools and resources.

Enhancing Learning with Realistic Training

- More realistic training datasets for practical learning.
- Interactive and dynamic learning experiences.
- Improved engagement and effective learning outcomes.
- Generative AI can be used to create engaging training materials.
  - Virtual simulations and games can be developed for immersive learning.
  - Generative AI can create synthetic data mimicking real-world cyber threats.
  - Can be used by cybersecurity professionals to practice identifying and responding to threats.

A ChatGPT Example on Detecting Deepfake Videos

- **Visual inconsistencies:** Look for blurry edges, unusual facial expressions, mismatched lighting and shadows, or distorted features. Pay attention to unnatural head or body movements that may appear out of sync with the background or other objects.
- **Inconsistent or unusual eye movements:** Watch for abnormal blinking patterns, lack of natural eye reflections, or eyes that appear out of alignment.
- **Uncanny valley effect:** If a person's face appears eerily perfect, too smooth, or lacking natural imperfections, it could be a red flag.
- **Lip-sync accuracy:** Pay attention to lip movements and audio synchronization. Misalignments between speech and mouth movements can indicate a manipulated video.
- **Unnatural head or body movements:** Look for jerky or unnatural motions, especially during rapid movements or when interacting with the environment.
- **Inconsistencies with context or background:** Watch for odd reflections, shadows, or lighting that don't match the surroundings or the person's position.
- **Source analysis:** Cross-reference the video with other reliable sources or contact the original content creator for verification.
- **Use technology-based detection tools:** Researchers and developers are continuously working on tools and algorithms to detect deepfake videos. Stay informed about the latest advancements in deepfake detection technology and utilize reliable detection tools when available.
- **Deepfake technology is constantly evolving.** Exercise critical thinking, be cautious when encountering suspicious videos, and seek expert opinions or forensic analysis if necessary.

Conclusion

- **Generative AI has a significant impact on cybersecurity education.**
- **Addressing challenges posed by generative AI is crucial.**
- **Leveraging generative AI can enhance training**