Designing A New Graduate Course on Artificial Intelligence for Cybersecurity

Ping Wang, PhD, CISSP
University Professor
Robert Morris University
Pittsburgh, PA, USA
wangp@rmu.edu

Presenter Brief Bio

- **Education/Degrees**
  - PhD in Information Systems
  - MCIS (Master of Computer & Information Science)
  - BA & MA in Linguistics
- **Academic Positions**
  - Current:
    University Professor, Computer Information Systems & Cybersecurity
    PoC, National Center of Academic Excellence in Cyber Defense (NCAE-CD)
    Robert Morris University
    PI, NSF and DoD grant projects in Cybersecurity
  - Previous:
    Professor & Program Director, MS Cybersecurity
    University of Maryland University College
- **Recent Research Topics**
  - Cybersecurity capstone project design. Springer, 2025.
  - AI-assisted pentesting using ChatGPT. Springer, 2024.
  - Privacy challenges and risks in AI-enabled healthcare app. IEEE Computer Society, 2023.

Overview

- **Focus**
  Integrating AI in Cybersecurity for a new graduate course design
- **Significance**
  - Fast-growing role/benefits of AI: automation, efficiency, interactivity
  - Gen AI impacts (positive) on Cybersecurity:
    - Network traffic analysis
    - Threat detection/analysis
    - Risk assessment and mitigation
  - Gen AI risks for Cybersecurity:
    - Malicious use
    - Hallucinations
  - Continued demand for cybersecurity professionals
    - Cyber workforce shortage and demand
    - Skills gap in using AI for Cyber
- **Goal**
  Explore the benefits and risks/limitations of AI for cybersecurity in a graduate/master's level cybersecurity course design for cyber workforce development

Research Background (1)

- ❑ AI/LLM benefits to Cybersecurity
  - ➢ Early detection of and response to cyber threats
  - ➢ Improved efficiency/accuracy in vulnerabilityanalysis and risk assessment
  - ➢ Automated incident response and preventive and secure software development
  - ➢ Improved accuracy in security mitigation and countermeasures
  - ➢ Efficient knowledge discovery and training of cybersecurity professionals
- ❑ Security benefits of AI and LLM applications and models will help prepare/develop qualified cyber workforce in the age of AI
- ❑ NCAE-CD new PoS in CyberAI (AI for Cyber & Secure AI)

Research Background (2)

- ❑ Double-edged sword: Risks/limitations of AI for cybersecurity
  - ➢ Malicious misuse for more powerful and automated cyber attacks
  - ➢ Potential disclosures of private/sensitive/copyrighted information
  - ➢ Hallucinations with misleading misinformation
- ❑ Students/future cyber pros should be aware of the AI risks and limitations to address them
- ❑ Major limitation for further research:
  Unknown gap between AI and human intelligence/creativity in defense decision making?

Research Background (3)

- ❑ Effective curriculum and course design should consider cognitive development process and levels of learning objectives
- ❑ Bloom's Taxonomy levels of progressive learning objectives
  - ➢ Recall information, facts, terms, and basic concepts
  - ➢ Describe and interpret facts and ideas to demonstrate comprehension
  - ➢ Apply knowledge and techniques learned to solve problems in new situations
  - ➢ Analyze information to identify causes, motives, and relationships
  - ➢ Evaluate information or ideas based on certain criteria to make judgements
  - ➢ Develop and propose new or alternative solutions
- ❑ Graduate/master's level course design should emphasize and reflect more of the higher levels of learning objectives

Course Proposal: Learning Outcomes

- ❑ Proposed leaning outcomes
  - ➢ Identify and describe AI-powered cyber threats and attacks
  - ➢ Evaluate AI-powered cyber threats and attacks and security implications and solutions
  - ➢ Identify and describe positive impacts of AI in cybersecurity
  - ➢ Identify and apply AI-driven solutions, techniques, and tools for cybersecurity
  - ➢ Evaluate secure development practices for protecting applications in the age of AI
  - ➢ Assess and evaluate AI-powered cybersecurity risks and solutions
- ❑ Course emphasis on more advanced level learning objectives of analysis, evaluation, and solution development in Bloom’s taxonomy.

Course Proposal: Learning Activities

- ❑ Discussions
  - ➢ Gen AI implications for cybersecurity
  - ➢ Impacts of AI on cybersecurity (positive & negative)
  - ➢ AI technologies and solutions for cybersecurity (pros and cons)
- ❑ Case Studies of AI in Cybersecurity
  - o Sutherland Global Services
    Using automation & AI in IBM's QRadar Suite to enable faster, more targeted, and more effective responses to threats
  - o Credico USA
    Using IBM Security® MaaS360® with Watson®, a cloud-based, AI-infused unified mobile device management (MDM) solution for security & tablet policy compliance
- ❑ Comprehensive Project
  - ➢ Project Plan (to be approved by instructor)
  - ➢ Project Presentation (progress report)
  - ➢ Project Final Report

Project Rubric for Assessment

	Excellent	Good	Satisfactory	Below Expectations
AI-related Security Risks with Documented Case Examples (Weight: 60%)	**55-60 Points** Excellent identification and description of AI-related security threats, vulnerabilities, and risks supported by case examples and data	**48-54 Points** Good identification and description of AI-related security threats, vulnerabilities, and risks supported by case examples and data	**42-48 Points** Adequate identification and description of AI-related security threats, vulnerabilities, and risks supported by case examples and data	**Below 42 Points** Inadequate identification and description of AI-related security threats, vulnerabilities, and risks supported by case examples and data
Solutions and AI Technologies/Products (Weight: 30%)	**27-30 Points** Excellent description and discussion of the security solutions and AI technologies/products	**24-26 Points** Good description and discussion of the security solutions and and AI technologies/products	**21-24 Points** Adequate description and discussion of the security solutions and AI technologies/products	**Below 21 Points** Inadequate description and discussion of the security solutions and AI technologies/products
Writing & Formatting (Weight: 10%)	**10 Points** Excellent writing and formatting with no errors	**8-9 Points** Good writing and formatting with few minor errors	**7 Points** Acceptable writing and formatting with a few errors	**Below 7 Points** Poor writing or formatting with frequent errors

Discussions & Conclusions

- Recap of AI significance to Cybersecurity
- Recap of AI Limitations in Cybersecurity
- Need for integration of AI in Cybersecurity curriculum
- Work in progress of this research
  - Course design & development
  - Preliminary implementation
- Further research
  - More in-depth course(s) on AI for Security & Secure AI
  - More implementation data
  - Gap between AI and human intelligence/creativity in security decisions/strategies
- Questions/suggestions
- Thank you!