CA306: Security of Emerging Intelligent System

27 Instructional Hours 33 CPEs 6 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE

This course provides a comprehensive and practical exploration of securing modern intelligent systems, including artificial intelligence, autonomous platforms, and cyber-physical infrastructure. It examines how these systems integrate sensing, decision-making, and physical actuation, and how vulnerabilities across these layers can lead to real-world consequences. Learners are introduced to foundational concepts such as system architecture, trust modeling, and threat analysis, as well as advanced topics including adversarial machine learning, supply chain security, IoT ecosystems, and resilience engineering. The course emphasizes a consequence-aware approach to cybersecurity, equipping learners with frameworks and methodologies to analyze, defend, and design secure, resilient intelligent systems operating in dynamic and high-risk environments.

You Will Be Able To

- Analyze the architecture of intelligent systems across physical, sensing, control, decision, and coordination layers
- Identify and evaluate security risks in AI, autonomous systems, and cyber-physical environments
- Assess adversarial threats such as evasion attacks, data poisoning, and model exploitation
- Design secure deployment strategies and resilient defenses for AI and IoT systems
- Apply threat modeling techniques considering state, timing, and real-world consequences
- Evaluate supply chain risks and implement trust and provenance mechanisms

Who Should Attend

This course is designed for cybersecurity professionals, AI practitioners, engineers, and students with a foundational understanding of computing or security who want to specialize in securing intelligent systems. It is particularly suitable for individuals seeking to expand into areas such as AI security, IoT, autonomous systems, and critical infrastructure protection. The course is also valuable for researchers and technical analysts aiming to understand how digital vulnerabilities translate into physical-world risks and operational consequences.

Relevant Combat Roles

- AI Security Engineer
- Cyber-Physical Systems Security Analyst
- Threat Intelligence Analyst (AI/IoT focus)
- Autonomous Systems Security Specialist
- Industrial Control Systems (ICS/OT) Security Engineer
- Red Team / Adversarial ML Specialist

Topics Covered

Foundations & Architecture: Layered system design, trust and threat modeling, and consequence-aware security.

AI/ML Risks: Vulnerabilities across the lifecycle—from data to deployment.

Adversarial & Agentic AI: Attacks like evasion/poisoning and risks from autonomous decision-making.

Autonomous & Cyber-Physical Systems: Securing navigation, control, sensors, and critical infrastructure.

IoT & Supply Chain: Hardware trust, secure updates, and SBOM/HBOM transparency.

Monitoring & Resilience: Anomaly detection, automated response, and fail-safe system design.

Labs

Intelligent System Threat Modeling & Attack Surface Analysis
(system architecture mapping, attack path identification, and consequence surface analysis)

Adversarial Machine Learning & Model Security Testing
(evasion attacks, data poisoning simulations, and defensive technique evaluation)

IoT Security Assessment & Protocol Analysis
(protocol weaknesses, trust analysis, and IoT botnet exposure assessment)

Autonomous System Incident Response & Compromise Analysis
(navigation spoofing investigations, command injection analysis, and incident response operations)