CSC8208: Research Methods and Group Project in Security and Resilience

Module Handbook Summary

Academic Year: 2024/2025

Newcastle University

Prof. S Nagaraja, Shishir.nagaraja@newcastle.ac.uk

Chair of Cybersecurity

National Skills Director & Cyber Lead, Newcastle Edge AI Hub

From Newcastle. For the world.

Introduction

- This module focuses on team-based research, design, implementation, and evaluation of a security-related software system.
- It develops critical skills in research methods, security assessment, and project execution.
- You will gain experience in reading and understanding cybersecurity research papers.
- Collaboration is key, as teams must work independently with minimal supervision.

Module Calendar

- Week 1: Module Introduction & Group Formation
- Week 2-4: Literature Review & Threat Model Development
- Week 5-7: High-Level Design & Initial Implementation
- Week 8-10: Full Implementation & Evaluation
- Week 11: Final Report Submission & Project Demo

Lecture Topics

- Lecture 1: Module Introduction & Group Formation
- Lecture 2: Project Briefing
- Lecture 3: How to Read a Research Paper
- Lecture 4: Security & Resilience Fundamentals
- Lecture 5: Research Methods – Side-channels Literature
- Lecture 6: Research Methods – AI & ML
- Lecture 7: Implementation Guidance
- Lecture 8: Writing & Presenting a Project

Office Hours & Tutorials

Office Hours: Prof. S. Nagaraja - Tuesdays 4:30–6:00 PM (Weeks 24-28)

Leadership training: Weeks 24 & 25 (12th and 19th Feb)

Blockchain Track Tutorials: Feb 26, Mar 5, Mar 12, Mar 19 (UBS 4.08, 14:30–15:30)

AI & Security Track Tutorials: Feb 28, Mar 7, Mar 14, Mar 21 (FDC G.56, 10:30–11:30)

Assessment Deadlines

Assessment 1 (30%): Literature Review, Threat Model & High-Level Design

- - Develop Literature Review (~500 words)
- - Submit a Threat Model (250 words)
- - Define a Security Policy (300 words)
- - High-Level Project Design (5 pages max, IEEE format)
  Due Date: 3rd March 2025 (PDF submission)

Assessment 2 (70%): Final Group Report & Video Demo

- - Full project implementation and evaluation
- - Report (10 pages max, IEEE format)
- - Video demo explaining system functionality
- Due Date: 21st March 2025 (PDF & ZIP submission)

Project Brief: Secure ML Computation System

Objective: Design and implement a secure ML system with blockchain integration.

System must support secure communication between multiple entities.

Ensure data confidentiality, integrity, and access control.

Develop and evaluate a machine learning security protocol.

Project Requirements

- System should allow at least 5 entities to securely transmit data.
- Implement ML processing over the collected data.
- Maintain an audit trail of inputs, outputs, and security controls.
- Ensure secure data exchange using encryption and authentication.

Team Responsibilities

- Teams will consist of 6-8 members.
- Each team must nominate a Leader and Deputy Leader.
- Weekly meetings should be held to track progress.
  - Store minutes on Teams
- Team Leader is responsible for organizing meetings and submitting assessments.
  - Leaders must agree contributions with each member beforehand.
  - If there is disagreement, please alert me.
- Teams channel – all comms must be on this channel **only**
- Code on Github

Marking Criteria

Literature Review, Threat Model & Security Policy (30%)

Final Project Report (70%)

Security Implementation (15%)

Resilience & Fault Tolerance (15%)

Innovation & Research Novelty (15%)

Evaluation & Experimental Results (15%)

Presentation (Report 5%, Demo 10%)

Security & Threat Model

- Confidentiality: Protect transmitted messages from unauthorized access.
- Integrity: Ensure data cannot be altered undetected.
- Access Control: Restrict who can modify ML training data.
- Optional Advanced Features: Audit logs, anomaly detection, privacy-preserving computation.

Resilience & Innovation

- System must handle large-scale data contributions.
- Consider distributed consensus mechanisms for data validation.
- Reward contributors using blockchain-based incentive mechanisms.
- Innovation can include privacy-preserving ML, tokenized data economy, or smart contract automation.

Project Evaluation

Projects will be evaluated on real-world security threats.

Use of empirical data to justify design choices is required.

Comparison with existing security approaches is encouraged.

Experimental validation and performance analysis will be key factors.

Final Report & Demo

Final report should follow IEEE Computer Society format.

Clearly define research problem, methodology, and evaluation.

Use diagrams and tables to illustrate security architecture.

Demo video should effectively showcase system functionality.

Best Practices for Success

- Use established security libraries – do not create custom cryptography.
- Communicate regularly using Microsoft Teams and GitHub.
- Divide roles effectively – assign members to specific tasks.
- Ensure fair workload distribution to avoid team conflicts.

Example projects

Decentralised Crop Insurance toolkit

- AI based event detection
- App for insurance signup
- Smart contract for automated release of payment if conditions are met

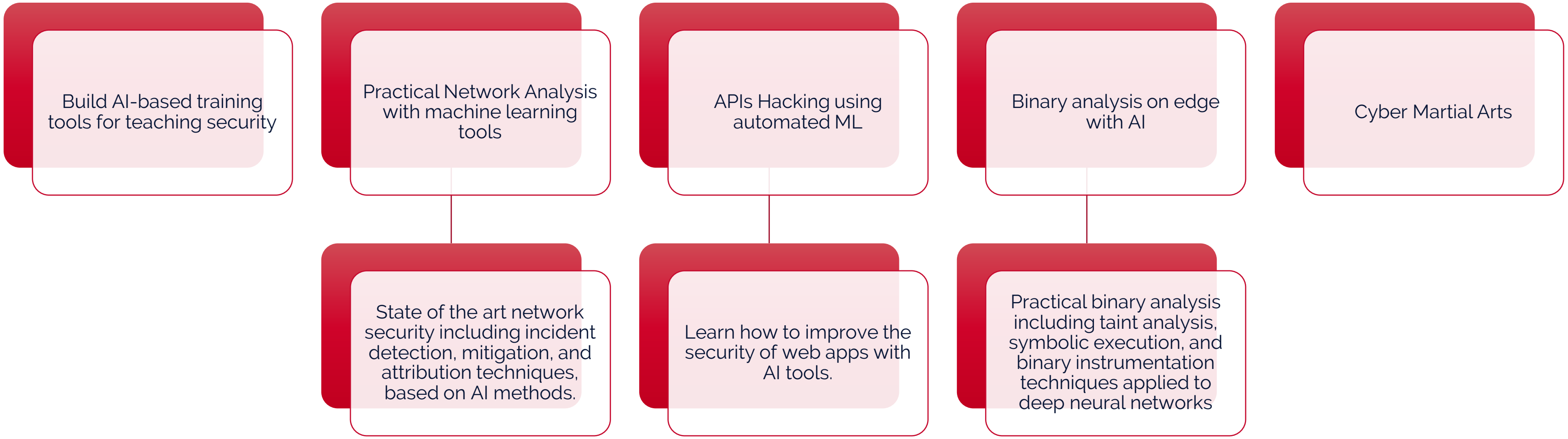
Open Finance: write an area survey and build a training tool

Develop Attack Demonstrators on AI models

- Image models
- Acoustic models

Supply chain traceability: develop tool to detect dependencies of software components and analyse dependency chain for given component. Carry out area study for a regulated market.

Example projects



Build AI-based training tools for teaching security

Practical Network Analysis with machine learning tools

State of the art network security including incident detection, mitigation, and attribution techniques, based on AI methods.

APIs Hacking using automated ML

Learn how to improve the security of web apps with AI tools.

Binary analysis on edge with AI

Practical binary analysis including taint analysis, symbolic execution, and binary instrumentation techniques applied to deep neural networks

Cyber Martial Arts