RIT | Golisano College of Computing and Information Sciences
Department of Computing Security

Advanced Computing Security Clusters

A matriculated student in the B.S. in Computing Security needs to take 6 elective courses. It is required to take 3 courses from one of the following clusters, and 3 courses from the approved Advanced Electives. If the course has * next to it, that course is required if it is in your chosen cluster.

Students can create customized clusters for their special interests provided compositions of clusters are vested by one faculty, one student academic advisor, and approved by the department chair. Courses in a customized cluster should be on the list of approved advanced elective courses of Computing Security. To be counted as a cluster course, a GCCIS course not on the list of advanced elective courses of Computing Security needs to be approved by the chair on a case by case basis, or simply such a course can be counted as a free elective for students. A course prepended with an asterisk is a required course for the cluster.

Network and System Security:

- *CSEC 461 Computer System Security
- *CSEC 462 Network Security and Forensics
- CSEC 465 Network & System Security Audit
- CSEC 469 Wireless Security
- CSEC 471 Penetration Testing Frameworks & Methodologies
- CSEC 473 Cyber Defense Techniques
- CSEC 520 Cyber Analytics and Machine Learning
- CSEC 559 Usable Security and Privacy

Forensics & Malware:

- *CSEC 464 Computer Systems Forensics
- *CSEC 476 Malware Reverse Engineering
- CSEC 462 Network Security and Forensics
- CSEC 465 Network & System Security Audit
- CSEC 467 Mobile Device Security and Forensics
- CSEC 470 Covert Communications (WI-GE)
- CSEC 520 Cyber Analytics and Machine Learning

Software Security:

- *SWEN 261 Introduction to Software Engineering
- *SWEN 331 Engineering Secure Software
- CSEC 467 Mobile Device Security and Forensics
- CSEC 468 Risk Management for Information Security
- CSEC 559 Hacking for Defense
- CSEC 559 Usable Security and Privacy
- **CSEC 731 Web Server and Application Security Audits
- **CSCI 622 Data Security and Privacy
- **CSCI 642 Secure Coding
- SWEN 567 Hardware Software Co-Design for Cryptographic Applications

Security Management and Evaluation:

- *CSEC 468 Risk Management for Information Security
- *CSEC 477 Disaster Recovery Planning and Business Continuity
- CSEC 465 Network & System Security Audit
- CSEC 471 Penetration Testing Frameworks & Methodologies
- CSCI 531 Introduction to Security Measurement
- CSCI 532 Introduction to Intelligent Security Systems
- CSEC 520 Cyber Analytics and Machine Learning
- CSEC 559 Hacking for Defense
- CSEC 559 Usable Security and Privacy

Electives:

- CSCI 455 Principles of Computer Security
- CSCI 464 Xtreme Theory
- CSCI 531 Introduction to Security Measurement
- CSCI 532 Introduction to Intelligent Security Systems
- **CSCI 622 Data Security and Privacy
- **CSCI 642 Secure Coding
- **CSCI 762 Advanced Cryptography
- CSEC 461 Computer System Security
- CSEC 462 Network Security and Forensics
- CSEC 464 Computer Systems Forensics
- CSEC 465 Network & System Security Audit
- CSEC 466 Introduction to Malware
- CSEC 467 Mobile Device Security and Forensics
- CSEC 468 Risk Management for Information Security
- CSEC 469 Wireless Security
- CSEC 471 Penetration Testing Frameworks & Methodologies
- CSEC 473 Cyber Defense Techniques
- CSEC 470 Covert Communications (WI)
- CSEC 476 Malware Reverse Engineering
- CSEC 477 Disaster Recovery Planning and Business Continuity
- CSEC 520 Cyber Analytics and Machine Learning
- CSEC 559 Hacking for Defense
- CSEC 559 Usable Security and Privacy
- **CSEC 731 Web Server and Application Security Audits
- SWEN 261 Introduction to Software Engineering
- SWEN 331 Engineering Secure Software
- SWEN 567 Hardware Software Co-Design for Cryptographic Applications