Cyber Studies in

Computer Science and Information Sciences

Graduate Certificates
for
Non-Resident Students

DoN, DoD, and U.S. Government Civilians and Non-Naval Military Cohorts

Version 2.2g

Naval Postgraduate School

June 2021

Table of Contents

Cyber Studies Graduate Certificates for Non-Resident Students

DoN, DoD, and U.S. Government Civilians and Non-Naval Military Cohorts

Overview

Intended Audience

This document is intended for those wishing to form reimbursably-funded non-resident student cohorts to enroll in cyber-related certificates. The cohorts may be comprised of the following types of students: DoN, DoD, and U.S. Government civilians, and non-Naval military officers.

Introduction

The Naval Postgraduate School has a long tradition of studies in both cyber security and cyber operations. Starting in the late 1970s faculty and students in the Department of Computer Science (CS) conducted research on in cyber security. By the mid-1990s the CS Department had both introductory and advanced courses that included topics ranging from the use of low-level hardware tin support security objectives to security management at the enterprise level. As a result of the course of study developed by the CS Department, NPS was one of the first universities recognized by the National Security Agency and the Department of Homeland Security as a Center of Academic Excellence in Cyber Security/Defense Education and as a Center of Academic Excellence in Cyber Security Research. In the In 2012, the NSA designated NPS as one of only four schools selected to be a Center of Academic Excellence in Cyber Operations. In 2015, the Department of Information Sciences assumed the management of the newest cyber-related degree program at NPS: Cyber Systems and Operations.

Hundreds of students have completed Master of Science Degrees from the Computer Science and Information Sciences Department having completed focused specialization tracks, certificate programs, and thesis research in cyber security and cyber operations.

The graduate certificates described herein are those offered the Department of Computer Science and the Department of Information Sciences. Students can enroll in certificate programs to meet on-the-job objectives related to the development and operation of systems for which the threat of intelligent adversaries in cyberspace must be considered. Furthermore, because all certificate courses are applicable to specific Masters degrees, the certificates can become a stepping stones toward a full degree.

Cyber Studies Certificates

Graduate certificates provide a way for busy professionals to gain knowledge in specific areas. Certificates are tailored to address topic areas of particular relevance to the DoN and DoD. Case studies and exercises are often based upon real military events and problems. Courses may be either classified or unclassified, depending upon their content. Through a process of continuous updates, the courses that comprise each graduate certificate reflect the latest thinking and innovations in science, engineering and technology in their respective fields. The expert faculty members who design and develop NPS graduate certificates and their component courses work hard to ensure relevant topics in the rapidly changing area of cyber.

For individuals who already have graduate degrees, a graduate certificate can provide an insight into a new area without the cost of engaging in the lengthy process of a second postgraduate degree or the danger of studying tangential material. Those who eventually hope to enroll in a graduate program can use a graduate certificate from NPS as a stepping-stone to a higher-level degree. NPS is a fully accredited graduate school under the Western Association of Schools and Colleges. This means that course credits from NPS are transferable, as permitted by the receiving institution. Course credits associated with NPS graduate certificates are usually applicable toward Masters degrees from the department offering the course. In fact, NPS graduate certificates may be used to incrementally build toward a degree.

Modes of Instruction

NPS has several modes of instruction for its certificates. Sponsors can choose the mode most appropriate for their workforce.

Video Teleconference (VTC)

VTC mode bears the greatest similarity to a traditional class. Remote students are connected via VTC to instructors who provide lectures in real time. VTC classes can be scheduled so that students attend courses at times during the working day that are the most appropriate for the remote sponsor, for example, early in the morning, at lunchtime, or late in the day.

Asynchronous Classes

Asynchronous courses are usually web-based. Students do not attend lectures at a specified time and instead listen to lectures that have been prepared in advance by the faculty. To provide for the discussions that can be key elements of certain courses, a number of network-based technologies are used including: chat, wikis, email, etc. Not all classes are offered in asynchronous mode. Furthermore, the formats for asynchronous mode vary from slides with voice-over recordings of live lectures, to studio voice-over recording with integrated video demonstrations.

Hybrid Option

The "hybrid" option allows NPS faculty and students to meet physically face-to-face for part of the course. These meetings can take place through a trip by the entire student cohort to the NPS campus in Monterey, California. Often this choice is too costly and sponsors opt for the on-site hybrid option in which the NPS faculty member visits the remote site one or more times during the academic quarter for up to a week.

NPS has found that employment of the hybrid option can have considerable benefits including better student-teacher communications throughout the course and significantly reduced student attrition for the duration of the certificate. It can be applied to both VTC and asynchronous mode classes, and is beneficial for both.

Laboratory Facilities

NPS has been at the forefront in the creation of laboratory facilities that permit remote students the same hands-on instructional experience enjoyed by local students. Virtualization

technologies allow students to use personal or a sponsor-furnished PCs or laptops with a browser and a network connection for most of the NPS-based laboratory facilities required for the cyber courses. In fact, students local to NPS use the same mechanisms.

In the case of classified courses, remote connection to a classified lab across the network is more challenging. To date, NPS has solved this problem by using unclassified laboratory exercises for remote students, even for classified courses.

Physical contact labs, such as those for biometrics or the lock picking exercises in our units on physical security, require special arrangements.

Sponsorship and Funding Vehicles

To offer a certificate, the minimum cohort size must be funded. This can be accomplished by a single sponsor or by multiple sponsors. The latter allows sponsors who want to support fewer than the minimum required number of students to share the cost of the certificate.

Sponsors must fund the certificate programs described in this document. Funds are transmitted to the Naval Postgraduate School via a MIPR, or, for non-DoD agencies, using an IAA. Additional information is available upon request.

Admission and Graduation Requirements

To be admitted to an academic certificate program, prospective students must meet the master's admissions requirements for NPS and any prerequisites for the courses in the certificate program. Requirements for the latter are:

> A candidate entering any Master's degree program must possess a baccalaureate degree from a regionally accredited institution, or in the case of foreign students, a recognized institution, with a minimum grade point average of 2.2 on a 4.0 system, of which 100 semester-hours must have been taken in residence. If the candidate does not possess an undergraduate degree the following are standards for admission to a program leading to a graduate degree:
> 1. A minimum of 100 semester-hours of in-residence undergraduate work must have been completed at accredited institutions with an average grade of “B”. Courses in which grades lower than “C” were earned will not be counted in the total. Courses which have been duplicated on various transcripts should be counted only once in arriving at the total number of semester-hours to be credited.
> 2. The general education requirements prescribed for the Naval Postgraduate School baccalaureate degree must be satisfied.

Departmental requirements for individual graduate certificates are provided below.

The academic certificate program must be completed within three years of admission to the program. A student must maintain a 3.0 GQPR in the certificate courses to be awarded a certificate. Note that the GQPR is a function of both the number of credit hours associated with each course and the grade received in that course.

Course Credits and Multiple Certificates

For each graduate certificate, students must take a minimum of 12 credit hours of courses that have not been applied to another certificate. Since some courses appear in more than one certificate, sponsors and prospective students should carefully consider the order in which certificates are taken. The NPS staff will be happy to advise sponsors on optimal certificate ordering.

Contact

Those interested in the cyber graduate certificates can contact

Primary

Cecelia Davis
cmdavis@nps.edu
(831) 656 3810

Secondary

Cynthia Irvine
irvine@nps.edu
(831) 656 2461

In all cases, sponsors will be put in contact with the appropriate manager of the certificate of interest.

Cyber Security Fundamentals

Classification:

Unclassified.

Curriculum number:

Resident: 257

Non-resident: 256

Overview

The Cyber Security Fundamentals certificate is a graduate-level, non-degree program designed to enable DoD, U.S. Government and other personnel to gain an understanding of the basic concepts and methods associated with cyberspace.

The program is intended to help you obtain a strong foundational understanding of computer network defense, vulnerabilities, and exploitations. The objective of the certificate is intended to enable students to make choices that will result in better defense of their networks.

As distance learning, the program is typically taken over a three-quarter period: one course per quarter. When students take the certificate in residence, the certificate can be completed in a single quarter.

The Cyber Security Fundamentals certificate can be combined with the Cyber Security Defense certificate to create a program that is a minimum of two quarters in duration.

This certificate program may be applicable toward a Master's degree in Computer Science, Curriculum 368.

Requirements

- Baccalaureate degree
- Basic understanding of computers.
- An Academic Profile Code (APC) of 344 is required.
- Command or company endorsement

Program Length

Resident: One academic quarter, usually more

Non-Resident: Up to three academic quarters

Required Courses

Core (required)	Group A (choose one)
CS3670	CS3600
CS3690	CS4600

We advise working with the Program Manager for the certificate when selecting course options. Certain courses may be more appropriate for a certain set of students. In addition, course availability is a function of several factors, which vary from quarter to quarter.

Course Descriptions

CS3600 Introduction to Computer Security (4-2)

This course provides a comprehensive overview of the terminology, concepts, issues, policies, and technologies associated with the fields of Information and Software Assurance. It covers the notions of threats, vulnerabilities, risks, and safeguards as they pertain to the desired information security properties of confidentiality, integrity, authenticity, and availability for all information that is processed, stored, or transmitted in/by information systems. This is the entry point prerequisite for all other Computer Security Track courses. Perquisites: CS2011 or CS3030.

CS3670 Secure Management of Systems (3-2)

This course provides students with a security manager's view of the diverse management concerns associated with administering and operating an automated information system facility with minimized risk. Students will examine both the technical and nontechnical security issues associated with managing a computer facility, with emphasis on DoD systems and policies. Prerequisites: CS3600.

CS3690 Network Security (4-2)

This course covers the concepts and technologies used to achieve confidentiality, integrity, and authenticity for information processed across networks. Topics include: fundamentals of TCP/IP-based networking, core network security principles, traffic filtering types and methodology, packet-level traffic analysis, employment of cryptography, tunneling/encapsulation, Public Key Infrastructure (PKI), remote authentication protocols, and virtual private networks based on the IPSec, L2TP, and SSL protocols. Prerequisites: CS3600, CS3502, IS3502, or EC3710.

CS4600 Secure System Principles (3-2)

An advanced course that focuses on key principles of a constructive approach to secure systems. A brief review of operating systems and computer architecture is provided. Major topics include threat characterization and subversion; confinement; fundamental abstractions, principles, and mechanisms, such as reduced complexity, hierarchical relationships, least privilege, hardware protection, resource management and virtualization, software security, secure system composition, mutual suspicion, synchronization, covert and side-channel analysis, secure metadata, secure operational states, usability, and life cycle assurance. Current developments will include advances in security hardware, components, and systems. Prerequisites: CS3600, CS3070, CS3502.

Cyber Security Defense

Classification:

Unclassified.

Curriculum number:

Resident: 259

Non-resident: 258

Overview

The Cyber Security Defense certificate is a graduate-level, non-degree program designed to enable DoD, U.S. Government and other personnel to gain an understanding of the concepts and methods used to defend cyberspace.

The program is intended to help students obtain a strong foundational understanding of computer network defense, vulnerabilities, and exploitations. The objective of the certificate is to enable students to make choices that will result in better defense of their networks.

Through the Cyber Security Defense graduate certificate, students obtain a detailed understanding of and ability to function in real operational situations. Students learn:

- the technical depth required to actively prepare for and respond to attacks,
- to analyze network traffic to extract the observable characteristics of networks and network devices, thus providing a basis for defensive strategies,
- to build tools and configure systems and networks to permit systems to foster resiliency and continuity of operations, perhaps with reduced capacity, through attacks,
- how to construct systems and tools to mitigate the impact of malicious software,
- forensic techniques to retrieve and analyze stored information that may be corrupted or hidden.

Considerable programming and hands-on work with systems and networks is required. Entire courses, or units within them, may be taught at the classified level, thus facilitating classroom discussions on emerging challenges and capabilities.

This certificate program may be applicable toward a Master's degree in Computer Science, Curriculum 368.

Requirements

- Baccalaureate degree
- Basic understanding of computers.
- An Academic Profile Code (APC) of 344 is required.
- Command or company endorsement
- Students entering this program are expected to have a strong foundation in cyber security and networking. In addition, entering students will be expected to understand and use the languages and techniques of operating system and network component

development: the C programming language, assembly, shell scripting, use of linkers, loaders, and debuggers.

Program Length

Resident: One academic quarter, usually more

Non-Resident: Up to three academic quarters

Required Courses

Choose Three Courses	
CS4558	CS4600
CS4677	CS4684

We advise working with the Program Manager for the certificate when selecting course options. Certain courses may be more appropriate for a certain set of students. In addition, course availability is a function of several factors, which vary from quarter to quarter.

Course Descriptions

CS4558 Network Traffic Analysis (3-2)

Explores fundamentals of packet-switched network traffic analysis at the network layer and above as applied to problems in traffic engineering, economics, security, etc. Explores the design and integration of analytic tools and techniques into the fabric of the network including: spatial and temporal anomaly detection, origin- destination matrix estimation, application mix determination, deep- packet inspection, fingerprinting, intrusion detection and insider threat mitigation. Finally, the course covers active defense and offensive methods reliant on traffic analysis. Prerequisites: CS3502 and CS4550 or equivalent.

CS4677 Computer Forensics (3-2)

This course covers the fundamentals of computer forensics in the context of DoN/DoD information operations. Students examine how information is stored and how it may be deliberately hidden and/or subverted. Coverage includes: practical forensic examination and analysis, techniques of evidence recovery, legal preparation of evidence, common forensic tools, principle of original integrity, disk examination, and logging. Prerequisites: CS2011 and CS3600 and CS3670.

CS4600 Secure System Principles (3-2)

An advanced course that focuses on key principles of a constructive approach to secure systems. A brief review of operating systems and computer architecture is provided. Major topics include threat characterization and subversion; confinement; fundamental abstractions, principles, and mechanisms, such as reduced complexity, hierarchical relationships, least privilege, hardware protection, resource management and virtualization, software security, secure system composition, mutual suspicion, synchronization, covert and side-channel analysis, secure metadata, secure operational states, usability, and life cycle assurance. Current developments will include advances in security hardware, components, and systems. Prerequisites: CS3600, CS3070, CS3502.

CS4684 Cyber Security Incident Response and Recovery (3- 2)

This course defines the nature and scope of cyber security incident handling services, including intrusion/incident detection, damage control, service continuity, forensic analysis, service/data

restoration, and incident reporting. Material covers policy, planning, operations, and technology issues involved in related cyber incident handling plans; i.e., Business Continuity, Disaster Recovery, and Continuity of Operations. Specific incident types addressed include, natural disasters, denial of service, malicious code, malicious misuse of hardware and firmware, unauthorized access, data compromise and inappropriate use, including insider attacks. Emphasis is given to the detection and analysis of infiltration and exfiltration techniques employed during cyber attacks, thus enabling the incident handler to detect low noise attacks, and to deconstruct particularly insidious attacks. Based upon the choice of case studies, this course will be taught at either the unclassified or TS/SCI levels. Prerequisites: CS3690 or consent of instructor.

This page is intentionally blank

Cyber Security Adversarial Techniques

Classification:

Unclassified.

Curriculum number:

Resident: 261

Non-resident: 260

Overview

The Cyber Security Adversarial Techniques certificate is a graduate-level, non-degree program designed to enable DoD, U.S. Government and other personnel to gain an understanding of the concepts and methods used in offensive cyber operations.

In this program you will gain a strong foundational understanding of computer and network vulnerabilities, and how they may be exploited to gain an advantage in contested environments. The objective of the certificate is to enable you to understand the concepts behind, as well as the construction of, tools for offensive cyber operations.

Through the Cyber Security Adversarial Techniques graduate certificate, you will

- Obtain a detailed understanding of and ability to function in real operational situations in which adversarial techniques are being used,
- Use overarching principles, computer and network architectural concepts, and exemplar cases to analyze current and future malware,
- Learn how to use network traffic analysis to extract the characteristics of ongoing attacks and to identify exploitable vulnerabilities,
- Learn how to decipher subtle, clandestine host-based attack mechanisms and how these mechanisms are inserted into target systems,
- Learn, in detail, how attack and exploitation software mechanisms are built and deployed, including the distributed command and control techniques used to manage large-scale malware networks.

Considerable programming and hands-on work with systems and networks is required.

This certificate program may be applicable toward a Master's degree in Computer Science, Curriculum 368.

Requirements

- Baccalaureate degree
- Basic understanding of computers.
- An Academic Profile Code (APC) of 344 is required.
- Command or company endorsement
- Students entering this program are expected to have a strong foundation in cyber security and networking. In addition, entering students will be expected to understand and use the languages and techniques of operating system and network component

development: the C programming language, assembly, shell scripting, use of linkers, loaders, and debuggers.

Program Length

Resident: One to three academic quarters

Non-Resident: Up to three academic quarters

Required Courses

Core (required)	Elective (choose one)
CS4678	CS4558
CS4679	CS4648

We advise working with the Program Manager for the certificate when selecting course options. Certain courses may be more appropriate for a certain set of students. In addition, course availability is a function of several factors, which vary from quarter to quarter.

Course Descriptions

CS4558 Network Traffic Analysis (3-2)

Explores fundamentals of packet-switched network traffic analysis at the network layer and above as applied to problems in traffic engineering, economics, security, etc. Explores the design and integration of analytic tools and techniques into the fabric of the network including: spatial and temporal anomaly detection, origin- destination matrix estimation, application mix determination, deep- packet inspection, fingerprinting, intrusion detection and insider threat mitigation. Finally, the course covers active defense and offensive methods reliant on traffic analysis. Prerequisites: CS3502 and CS4550 or equivalent.

CS4648 Advanced Cyber Munitions (3-2)

This course will explore how malware is constructed through the analysis of existing malware. Techniques to provide attribution to malware will be explored. Topics include: malware obfuscation, insertion, dynamic updates, encryption and key management, and the use of malware to drive covert channels. The construction and operation of malware such as large scale distributed Botnets will be used in case studies. Prerequisites: CS2011, CS3070, and CS3140 or consent of the instructor.

CS4678 Advanced Vulnerability Assessment (4-2)

This course provides a basis for understanding the potential vulnerabilities in networked systems by applying a problem-solving approach to: (1) obtaining information about a remote network, (2) possibly exploiting or subverting systems residing on that network, (3) understanding the theory of operation of existing tools and libraries, along with how to measure the effectiveness of those tools, and (4) understanding tools and techniques available for vulnerability discovery and mitigation. Labs provide practical experience with current network attack and vulnerability assessment tools as well as development of new tools. Foot printing, scanning, numeration, and escalation are addressed from the attacker's perspective. A final project that demonstrates skill and knowledge is required. Prerequisites: CS3140 and CS3070 and CS3690, or consent of the instructor. Classification: UNCLASSIFIED FOUO, U.S. only.

CS4679 Advances in Cyber Security Operations (4-1)

Unfettered by rules, ethics, or government acquisition politics, the cyber underground has created sophisticated and innovative mechanisms for digital crime. Spanning all layers from hardware and firmware to human-computer interfaces, these command and control systems are both clandestine and dynamic. Using case studies, this course explores the techniques, tactics and procedures of cyber security operations used to identify and track emerging adversarial behavior. By addressing computer network attack, defense, and exploitation topics associated with disruptive technologies, students will gain an understanding of the threats, vulnerabilities, and appropriate mitigating security controls. Sample topics include: supply chain attacks; driving forces of the cyber underground; operations involving a variety of cyber technologies and infrastructures; tracking, location, and identification: security implications of new hardware and firmware interfaces; and covert and side channels. Based upon the choice of case studies, this course will be taught at either the unclassified or TS/SCI levels. Prerequisite: CS3690 or consent of instructor.

This page is intentionally blank

Identity Management

Classification:

Unclassified

Curriculum number:

Resident: 228

Non-resident: 227

Overview

Identity Management (IDM) is a growing concern throughout defense, government, and private sector organizations. It includes an infrastructure that supports the identification of humans in physical space, and the logical identification of human and non-human subjects, hardware, and software in cyber space. IDM can be used to address and be applied to ongoing and emerging challenges required to support the recognition of authorized personnel and entities, including their use of DOD facilities and systems. Also, IdM assists in solving the problem of creating synonymy between unknown entities, which can include both people and equipment, and possible or known threats.

The Identity Management Certificate Program is intended to provide busy government professionals a way to continue in their regular jobs while learning details of many facets of identity management.

Upon completion of the courses with adequate grades, students may apply IDM course credits toward Identity Management specialization tracks in either the Computer Science or Information Sciences degree programs.

Requirements

- Baccalaureate degree
- Command or company endorsement

Program Length

Non-Resident: Up to four academic quarters

Required Courses

Identity Management Certificate Courses	
CS3699	IS3710
CS3686	IS3720

Course Descriptions

CS3686 Identity Management Infrastructure (3-0)

This course covers a broad range of topics related to the standards, protocols, technology, and management infrastructure necessary to field an enterprise-level identity management (IdM) solution. Lecture and reading assignments span the gamut of IdM issues: from low-level authentication protocol mechanics, to high-level identity federal initiatives. This course is one of several that will collectively compose the requirements for Identity Management specialization tracks in the Information Science and Computer Science degree programs. Completion of four courses: CS3686, CS3699, IS3710, and IS3720, will meet the requirements for earning the Federal/DoD Identity Management Certificate offered by NPS. Prerequisites: None.

CS3699 Biometrics (3-0)

This course reviews the technical details of biometric identification and verification. The major biometric approaches (fingerprints, irises, etc.) are covered in detail with respect to acquisition of biometric data, matching techniques, anti-spooking techniques, and current standards. The uses and limitations of biometrics are covered, as well as some of the legal, ethical, and privacy concerns of maintaining and using biometric data. This course is one of several that will collectively comprise the requirements for Identity Management specialization tracks in both the Information Science and Computer Science degree programs. Completion of four courses, CS3686, CS3699, IS3710, and IS3720, will meet the requirements for earning the Federal DoD Identity Management Certificate offered by NPS. Prerequisites: None.

IS3710 Identity Management Operations (3-0)

This course will integrate theory with practice to help prepare students with ways of thinking about how to leverage Identity for competitive advantage in operational environments. The focus of this course is on the design architecture for integrated systems which will allow for the collection, analysis, storage, and dissemination of information related to the identity of a person. This course is one of several that will collectively comprise the requirements for Identity Management specialization tracks in both the Information Science and Computer Science degree programs. Completion of four courses: CS3686, CS3699, IS3710, and IS3720, will meet the requirements for earning the Federal/DoD Identity Management Certificate offered by NPS. Prerequisites: None.

IS3720 Identity Management Policy (3-0)

The goals for the Identity Management Policy Course are to provide the student with the necessary ways to think about the creation or implementation of Identity Management policies. The focus is to provide students with a background on the approaches to the verification of personal identity and the implications in a digital environment. As individuals become more conscious of the collection of data regarding their actions, the student must understand the implications of privacy in this changing environment. There will be a strong, case-based focus on the laws, ethics, and moral implications of the collection, analysis, storage, and dissemination of personal data so that the student can prudently apply the appropriate policy. Additionally, the policies and procedures for the provisioning, propagating, maintaining, and removal of personally identifiable information will be discussed. The student will be required to develop a case study for a scenario that will address the policy implications and create a solution to meet the operational requirements. Prerequisite: None.

Information Systems Security Engineering

Classification:

Unclassified

Curriculum number:

Resident and non-Resident: 270

Overview

The role of Information Systems Security Engineering (ISSE) is to help ensure that the security requirements of systems are met. Lacking proper security engineering, systems fail to be certified and accredited, causing costly delays or failures. Ideally the Information Systems Security Engineer (also known as an ISSE) will be a member of the system development team throughout its lifecycle; however, for preexisting systems, the ISSE may be required to assess existing system vulnerabilities and determine mitigating strategies.

As systems have grown more complex and adversaries continue to successfully exploit numerous vulnerabilities, the need for improved secure system engineering and the formation of a larger cadre of skilled ISSEs has become more acute. The ISSE course sequence will provide the knowledge and analytical skills required to contribute productively in system developments and assist in building a larger cadre of skilled ISSEs to combat adversaries.

This course of study may be applicable toward an MS degree program in Curriculum 368.

Requirements

- Baccalaureate degree
- Basic understanding of computer architecture, computer networking, operating systems and fundamentals of computer and network security
- Command or company endorsement

Program Length

Non-Resident: Up to four academic quarters

Required Courses

ISSE Certificate Courses	
CS3690	CS4650
CS4600	CS4652

Course Descriptions

CS3690 Network Security (4-2)

This course covers the concepts and technologies used to achieve confidentiality, integrity, and authenticity for information processed across networks. Topics include: fundamentals of TCP/IP-based networking, core network security principles, traffic filtering types and methodology, packet-level traffic analysis, employment of cryptography, tunneling/encapsulation, Public Key Infrastructure (PKI), remote authentication protocols, and virtual private networks based on the IPSec, L2TP, and SSL protocols. Prerequisites: CS3600, CS3502, IS3502, or EC3710.

CS4600 Secure System Principles (3-2)

An advanced course that focuses on key principles of a constructive approach to secure systems. A brief review of operating systems and computer architecture is provided. Major topics include threat characterization and subversion; confinement; fundamental abstractions, principles, and mechanisms, such as reduced complexity, hierarchical relationships, least privilege, hardware protection, resource management and virtualization, software security, secure system composition, mutual suspicion, synchronization, covert and side-channel analysis, secure metadata, secure operational states, usability, and life cycle assurance. Current developments will include advances in security hardware, components, and systems. Prerequisites: CS3600, CS3070, CS3502.

CS4650 Fundamentals of Information Systems Security Engineering (3-1)

This course presents the fundamental principles and processes of information systems security engineering (ISSE). The ISSE life cycle model consists of five stages: requirements definition, design, implementation, testing and deployment. The processes involved in these stages are explained in the context of a Defense-in-Depth protection strategy, with an emphasis on the role of security requirements engineering (SRE) in the construction of a secure system. This course covers the concepts and techniques needed to systematically elicit, derive and validate security requirements. It introduces how these techniques can be used in practice, and addresses the relationship between SRE and secure system design. Course work will be a combination of lectures, case studies and a team-based SRE project. Prerequisite: CS4600.

CS4652 Applied Information Systems Security Engineering (3-2)

This course focuses on the key concepts and practices of information systems security engineering from a system life cycle perspective. Core topics include security architecture and design analysis, system implementation assessment, requirements/implementation traceability correspondence, security test and evaluation strategy, certification and accreditation (C&A) requirements analysis, and risk management. The Systems Thinking approach is introduced for assessing system security behaviors based on dependencies, interactions and emergent properties of its components in the context of functionality, scalability, interoperability and maintainability. Case studies and laboratory projects will demonstrate security engineering practices through the life cycle of a secure system. Prerequisite: CS4650.

Cyber Operations Infrastructure

Classification:

TS/SCI

Curriculum number:

Resident: 228

Non-resident: 227

Overview

The Cyber Operations Infrastructure certificate is a graduate-level, non-degree program designed to enable DoD and U.S. Government personnel to differentiate the various components of the infrastructure underpinning cyber operations for its effective use in all aspects of cyber operations.

The objective of the program is to prepare students to deploy cyber-specific assets appropriately within the DoD cyber infrastructure. Students will be able to assess how differing elements of the underlying cyber infrastructures impact cyber operations. Students will learn about the communications systems that support cyber operations and will be able to choose communications modes most suitable for a given cyber mission. They will be able to develop information usage strategies across distributed platforms and will be able to adapt their choices based upon the capabilities of these data-centric systems. They will be able to evaluate the benefits and weaknesses of infrastructure-dependent choices and will be able to integrate these choices in cyber mission planning. Students will be able to develop strategies for cyber operations in contested situations based upon their understanding of the infrastructure.

The program consists of four courses to be taken over a minimum of a four-quarter period in the case of distance learning students. Resident students may be able to complete the certificate in three academic quarters. The total number of NPS graduate credits obtained for the certificate is 15, depending upon the choice of courses. This certificate program may be applicable toward a master's degree program in Curriculum 326, Cyber Systems and Operations.

Requirements

- Baccalaureate degree
- Recent completion, viz. within the past 5 years, of courses in computer and network security, computer and communications networks. Students lacking these prerequisites may be acceptable to the program through their undergraduate records and other indicators of success.
- An Academic Profile Code (APC) of 334 is required.
- Command or company endorsement
- TS/SCI clearance

Program Length

Resident: Three academic quarters

Non-Resident: Up to four academic quarters

Required Courses

Core (required)	Group 1 Electives (choose one)	Group 2 Electives (choose one)
CY3300	CY4600	CS3670
CY4400	EC3760	CY3650

We advise working with the Program Manager for the certificate when selecting course options. Certain courses may be more appropriate for a certain set of students. In addition, course availability is a function of several factors, which vary from quarter to quarter.

Course Descriptions

CY3300 Cyber Communications Architectures (Same as EO3730) (4-0)

The purpose of this course is to develop literacy and familiarity with Navy, DoD, and allied enterprise information systems and emerging technology trends. It presents basic concepts in conventional and military telephony and telecommunication networks; examines DoN implementations from intra-ship, ship- to-ship and long haul and discusses architectures and components of the GIG including both classified and unclassified networks. It discusses interoperability of diverse network architectures and the impact of mobile platforms on operations. Classification: SECRET. Prerequisites: CY3100, CY3110, CS3030, or consent of the instructor.

CY4400 Cyber Mission Planning (3-0)

This course details the process of mission planning in the cyber are domain and its integration of cyber with other warfare domains. All phases of mission planning and execution for cyber missions in both direct and supporting roles are covered. Topics include requirements development/solicitation, managing expectations, targeting considerations, munitions development and selection, preparation of the environment, mission deconfliction in the cyber battlefield, balancing the needs of offensive and defensive stakeholders, and cyber battle damage assessment. Classification: U.S. citizenship and TOP SECRET clearance with eligibility for SCI access. Prerequisites: CY4700 or consent of the instructor.

CY3650 Cyber Data Management and Analytics (4- 0)

This course surveys the use of information technologies and data analytics, with emphasis on case studies relevant to cyber operations and to the DoD. Topics include technologies and trends for Big Data management (e.g., distributed cloud file systems, NoSQL data stores); major themes and technologies in cloud computing (SaaS, PaaS, IaaS), distributed computation frameworks (MapReduce); and case studies focusing on how cloud infrastructure is used to enable services and analytics (e.g., mining, matching filtering and translating data). PREREQUISITE: CY3520 or CS3502 or IS3502 or consent of instructor.

CY4600 Network Operations in a Contested Environment (3-2)

This is a course in offensive cyber operations and effects achievable by cyber means in a contested environment. It examines the network environment as a domain under contention and related information operations. Existing architectures and infrastructures for conducting offensive

operations are studied. This course develops the literacy and competencies necessary to understand potential problems and realistic solutions for critical non-kinetic, cyber-related warfare issues for the United States. Classification: U.S. citizenship and TOP SECRET clearance with eligibility for SCI access. Prerequisites: CY3520. Co-requisite: CY4400, or consent of the instructor.

CS3670 Secure Management of Systems (3-2)

This course provides students with a security manager's view of the diverse management concerns associated with administering and operating an automated information system facility with minimized risk. Students will examine both the technical and nontechnical security issues associated with managing a computer facility, with emphasis on DoD systems and policies.

EC3760 Information Operations Systems (3-2)

This course examines the Network-centric Environment that is the focus of the Information Operations (IO) infrastructure with emphasis on current and future implementation models. A Signals Intelligence (SIGINT) approach is taken in which the adversary's computer network system architecture is examined and evaluated for the purpose of exploitation, protection, and/or attack. A thorough review of the fundamentals of communications, computer networks, and advanced digital technologies is discussed. This course works closely with the Department of Defense to reinforce realistic approaches for solving critical IO issues within the community. Classification: U.S. citizenship and TOP SECRET clearance with eligibility for SCI access. Prerequisites: EC2500 OR EO2512 or consent of instructor.

This page is intentionally blank

Applied Cyber Operations

Classification:

Unclassified

Curriculum number:

Resident: 226

Non-resident: 225

Overview

The Applied Cyber Operations certificate is a graduate-level, non-degree program designed to enable DoD and U.S. Government personnel to effectively employ cyber capabilities in an operational context and to prepare students to maintain a high state of readiness for cyber operations in the face of hostile action. Students will be able to utilize their understanding of cyber capabilities and their employment to achieve or support both cyber and overall mission objectives while accounting for adversary activity and environmental constraints. The program consists of three courses to be taken over a minimum of a three-quarter period. The total number of NPS graduate credits obtained for the certificate is 13 or 13.5, depending upon the choice of courses. This certificate program may be applicable toward a master's degree program in Curriculum 326.

Requirements

- A baccalaureate degree is required.
- Recent completion, viz. within the past 5 years, of courses in computer and network security, computer and communications networks. Students lacking these prerequisites may be acceptable to the program through their undergraduate records and other indicators of success.
- An Academic Profile Code (APC) of 334 is required.
- Command or company endorsement

Program Length

Three academic quarters

Required Courses

Basic (choose one)	Core (both required)
CY3520	CY4700
CY3602	CY4710
CS3690	
DA3104	

We advise working with the Program Manager for the certificate when selecting course options. Certain courses may be more appropriate for a certain set of students. In addition, course availability is a function of several factors, which vary from quarter to quarter.

Course Descriptions

CS3690 Network Security (4-2)

This course covers the concepts and technologies used to achieve confidentiality, integrity, and authenticity for information processed across networks. Topics include: fundamentals of TCP/IP-based networking, core network security principles, traffic filtering types and methodology, packet-level traffic analysis, employment of cryptography, tunneling/encapsulation, Public Key Infrastructure (PKI), remote authentication protocols, and virtual private networks based on the IPSec, L2TP, and SSL protocols. Prerequisites: CS3600, CS3502, IS3502, or EC3710.

CY3520 Practical Network Operations (3-3)

This course develops fluency in applying computer security principles in the context of deploying and configuring network services and architectures. Emphasis is placed on utilizing an understanding of network protocols and their vulnerabilities to defend and construct a network. Students will gain hands-on experience building a network, analyzing the interaction of network and host based security mechanisms, and maintaining continuous awareness of security relevant events. Prerequisites: CY3110, CS3502, or consent of instructor.

CY3602 Network Operations II (3-2)

This course is a sequel to Network Operations I, with a focus on how to deal with network attacks and compromises. The goal is a resilient network that can meet operational and mission needs even in the face of attacks. Students will learn how to detect and respond to attacks and compromises while keeping the network operational to the extent possible. Topics covered include self-assessment through vulnerability and penetration testing, using firewalls and intrusion detection and prevention systems to monitor network traffic and system activity; and an introduction to established processes for cyber forensics and attribution, incident response, and recovery. Prerequisites: IS3502, CS3600, or consent of the instructor. Co-requisite for students in Curriculum 326: CY4700.

DA3104 Computer Network Attack and Defense (4-1)

This course introduces the basic principles of attacking and defending computer networks. On the attack side, it covers system intrusions, denial of service attacks, viruses, worms, and Trojan horses. On the defense side, it covers security policies and objectives, access control, authentication, firewalls, intrusion detection, cryptography, security management, and incident response. Basic networking concepts, including TCP/IP, are also covered. No background in computer science or networking is required. The course includes some hands-on work with hacking and security technologies. Pre- requisite: DA3101.

CY4700 Applied Defensive Cyberspace Operations (3-3)

This course explores methods for discovering adversarial presence in a network and defending against adversarial TTPs (tactics, techniques, and procedures). Topics include, but are not limited to the cyber kill chain, techniques the adversary uses to remain hidden within a compromised network, adversarial command and control, malware triage, mitigation of malware, and eviction of an adversary from an operational network. Lab assignments will reinforce material taught in class. Prerequisites: CY3000 and CS3690; or consent of the instructor

CY4710 Adversarial Cyberspace Operations (3-3)

This course explores the underlying principles and TTPs (tactics, tools and procedures) of offensive cyberspace operations, and considers the campaign-level advantages achievable through delivery of cyber effects. It examines the use of cyber capabilities against target networks, based on a methodology of cyber reconnaissance of network defenses and vulnerabilities, analysis of viable options for exploitation, preparation and delivery of cyber effects, and post- delivery impact assessment. Students will gain experience using the latest tools and techniques for penetration-testing against target networks. Prerequisites: CY3000 and CS3690; or consent of the instructor

This page is intentionally blank

Student Application Procedures

Applications for the Naval Postgraduate School (NPS) are completed via an online system called the Applicant Management System (AMS) located here: https://www.nps.edu/Admissions/AMS/

First time applicants will need to create an AMS account prior to completing an online application to NPS.

Required Information:

In order to be considered for admission to NPS, students need to complete an online application.

The application consists of a short form requiring the applicant's demographic information, the name of the program being applied for, and official transcripts from all schools (undergraduate and graduated) attended.

Transcripts should be sent directly to NPS to the following address:

Admissions Office
(Official Transcripts)
Naval Postgraduate School
1 University Circle, He-022
Monterey, CA 93943-5100

Some institutions deliver transcripts electronically through secure means. If your institution uses this delivery method, the email address for electronic transcripts is admissions@nps.edu

Acceptance Process:

Once an application is complete and the Admissions Offices has conducted a preliminary review, it is released to the academic department for consideration. At this point, the application is reviewed by the departmental Academic Associate and Program Officer. Incomplete applications will not be reviewed.

NPS requests 2-3 weeks to review complete applications.

If an applicant is accepted, the NPS admissions office will then email the student and official acceptance letter.

Participant Agreement:

All Distributed Learning students must complete a Participant Agreement. This can be accomplished in either of two ways:

1. Each student may complete the agreement and submit it via email to admissions@nps.edu, with a copy to the NPS certificate program manager (Cecelia Davis cmdavis@nps.edu).
2. Alternatively, when a cohort of students is being sponsored by an organization, a manager at that organization can submit a completed blanket Participant Agreement, which must be accompanied by a list of all students in the cohort. These documents are submitted to admissions@nps.edu , with a copy to the NPS certificate program manager (Cecelia Davis cmdavis@nps.edu)P.