FREQUENTLY ASKED QUESTIONS

WHAT ARE THE PREREQUISITES?

- Acceptance by the ECE Department. Process requires a sufficient background in mathematics and technical undergraduate studies. Applicants with a BSEE degree will usually satisfy the requirements.
- Command/Company Endorsement.

IS THERE A SERVICE COMMITMENT?

Students participating in a program at The Naval Postgraduate School may incur service and/or employment obligations.

WHO IS ELIGIBLE?

Applicants with a US government affiliation, government laboratory engineers, active military personnel, Navy civilians, current NPS resident students, and a limited number of contractors sponsored by Department of Defense (DOD) organizations.

WHEN DOES THE PROGRAM START?

Any quarter.

HOW LONG DOES IT TAKE TO COMPLETE?

Usually 3 or 4 quarters, depending upon elective choices.

CONTACT INFORMATION

Roberto Cristi, Ph.D.
ECE Department
DL Business Manager
(831) 656-2223
rcristi@nps.edu

Monique P. Fargues, Ph.D.
ECE Department
Assoc. Chair for Student Programs
(831) 656-2859
fargues@nps.edu

For more information on the ECE department, go to:
www.nps.edu/ece

For more information on other NPS DL programs, go to:
www.nps.edu/dl

Produced by:
Naval Postgraduate School

Center for Educational
Design, Development, and Distribution
411 Dyer Rd., Knox 120, Monterey, CA 93943

DEPARTMENT OF
ELECTRICAL and COMPUTER ENGINEERING

GRADUATE CERTIFICATE PROGRAM IN WIRELESS NETWORK SECURITY

A DISTRIBUTED LEARNING PROGRAM

NAVAL POSTGRADUATE SCHOOL

THE PROGRAM

The Naval Postgraduate School (NPS) offers a graduate certificate program in Wireless Network Security. The program requires three courses and can be completed in three or four quarters, depending on elective choice.

The Wireless Network Security Certificate Program will provide students with a technical foundation that prepares them for assignments related to research, and management of wireless cyber systems.

Students will also be provided with an educational foundation that prepares them for leadership roles in the design, procurement and management of cyber operations and systems.

"I believe my academic background has prepared me for the challenges of high-level command and complex environments."

- Gen. Keith Alexander, stand-up Commander, USCYBERCOM and NPS alumnus.

Program Overview

Academic Quarter	Required Courses	Elective Courses
Winter		EC4735
Spring		EC4755
Summer	EC4770	EC3860
Fall	EC4745	

THE CURRICULUM

EC4770 Wireless Communications Network Security (3-2)
Summer

Examines the security of wireless communications networks to include wireless PAN, LAN, cellular and mobile broadband technologies.

EC4745 Mobile Ad Hoc Networking (3-2)
Fall

The course presents the fundamental principles, design issues, performance analysis, and applications of infrastructure and ad hoc wireless packet switched networks.

Elective Courses (Choose one)

EC3860 Trustworthy Computer Hardware Analysis and Design (4-1)
Summer

Course focuses on the vulnerabilities of the design, implementation, and manufacturing processes to the covert addition of malicious functionality, as well as the vulnerabilities of the underlying implementation technology. The techniques and methods required to design, implement, and manufacture trusted, high-performance, digital circuits, systems, and computers are studied.

EC4735 Telecommunications Systems Security (3-2)
Winter

Examines underlying technical security issues, policies, standards, implementations, and technologies associated with large-scale commercial telecommunications systems to include mobile networks.

EC4755 Network Traffic, Activity Detection, and Tracking (3-2)
Spring

Network traffic characterization, traffic engineering/management and detection and tracking of traffic anomalies are covered with a focus on statistical and information theoretic concepts, signal processing, and control theory.

THE OUTCOMES

Upon completion of the Wireless Network Security Certificate Program, students will possess:

- the cognitive skills required for vulnerability assessment and evaluation of wireless communications networks and telecommunications systems and the ability to apply these skills to defend cyber systems.
- the ability to apply techniques for securing computer and telecommunications networks.

And, depending upon elective choices,

- the ability to analyze and evaluate wireless activity to identify threats and respond appropriately.
- the ability to analyze, design and evaluate systems for accessing signals of intelligence value in cyberspace.
- the ability to analyze, design and evaluate systems for attack and defense of exploits.
- the ability to analyze, design and evaluate approaches to maintaining situational awareness in cyberspace.

Space communications along with terrestrial microwave and fiber optics provide the core capability required to implement the global cyberspace network.