

CERTIFICATES OFFERED

<https://engineering.pacific.edu/engineering>

Certificates Offered

The School of Engineering and Computer Science offers the following graduate certificates:

Certificate in Cybersecurity Management-Cloud, Mobile and Privacy

Certificate in Cybersecurity Operations

Certificate in Securing Enterprise Systems

General Information

Certificate in Cybersecurity management - Cloud, Mobile and Privacy:

The certificate in "Cybersecurity Management - Cloud, Mobile and Privacy" is a three-course, for-credit, certificate that is designed for students who want to specialize in learning the cloud security fundamentals (AWS focus), privacy controls and overall cyber security management. This certificate gives an edge to students aspiring to move into cyber managerial roles.

Certificate in Cybersecurity Operations:

The certificate in "Cybersecurity Operations" is a three course, for-credit, certificate that is designed for students interested in learning how to identify, triage and resolve cybersecurity incidents. This certificate includes strong fundamentals in network security, system administration, security operations, security information and event management (SIEM) and Endpoint detection and response (EDR).

Certificate in Securing Enterprise Systems:

The certificate in "Securing Enterprise Systems" is a three course, for-credit, certificate that is designed for students interested in learning how to proactively build secure software systems, identify and manage cybersecurity risks, and manage the vulnerability lifecycle.

Eligibility

Students enrolled in a graduate or blended program in the School of Engineering and Computer Science are eligible for the certificates.

Students not enrolled in a graduate or blended program in the School of Engineering and Computer Science must apply for admission. After admission, these certificates can be earned as standalone options independent from any graduate degree.

Admissions Criteria

Students who are not already enrolled in a graduate or blended program in the School of Engineering and Computer Science must apply for admission in order to earn a standalone certificate. The admission requirements are:

- Bachelor's degree
- Official university transcript(s) showing a 2.65/4.0 GPA on the last 60 units of undergraduate study
- Educational qualifications and/or industry experience to satisfy knowledge of computer programming and data structures, equivalent to COMP 053.
- Two letters of recommendation

Certificate Requirements

Students must complete their certificate courses with a minimum Pacific cumulative grade point average of 3.0 in order to earn the certificate.

Certificate Stacking

Students who have completed one of the three cybersecurity certificates described above are eligible, upon written request, will be admitted to the MS in Cybersecurity program without the need to reapply. Courses completed as part of these certificates will count towards satisfying the MS in Cybersecurity degree requirements.

This certificate stacking is subject to university policy regarding residence and time limits. Specifically, a Master's degree must be completed within five years subsequent to admission to the program, which in this case is defined as admissions to the certificate. The five-year period begins the first semester students are enrolled and is calculated from the date of degree conferral. Credit that is more than five years old will not be counted toward a Master's degree.

Student Learning Outcomes

Certificate in Secure Software Systems

Students completing a certificate in Secure Software Systems will be able to demonstrate the following learning outcomes:

- Security Fundamental Principles – Students will possess a thorough understanding of the fundamental principles underlying cybersecurity, how these principles interrelate and are employed to build secure systems.
- Vulnerabilities – Students will possess a thorough understanding of the various types of security vulnerabilities (design and/or implementation weaknesses), their underlying causes, their identifying characteristics, the ways in which they are exploited, and potential mitigation strategies.
- Software Reverse Engineering – Students will be able to deduce the design of a software component, determine how it works, and discover the data and communication protocols it uses, without knowing its design in advance.

Certificate in Cyber Defense and Offense

Students completing a certificate in Cyber Defense and Offense will be able to demonstrate the following learning outcomes:

- Security Fundamental Principles – Students will possess a thorough understanding of the fundamental principles underlying cybersecurity, how these principles interrelate and are employed to build secure systems.
- Cyber Defense – Students will have a sound understanding of the technologies and methods utilized to defend systems and networks. They will be able to describe, evaluate, and operate a defensive network architecture employing multiple layers of protection using technologies appropriate to meet security goals.
- Networking – Students will have a thorough understanding of how networks work at the infrastructure, network and applications layers; how they transfer data; how network protocols work to enable communication; and how the lower-level network layers support the upper ones to enable communications and data transfer.

Certificate in Cybersecurity Management - Cloud, Mobile and Privacy

Students are required to complete the following courses for the certificate.

COMP 285	Mobile and Cloud Security	3
COMP 286	Cybersecurity and Privacy Management	3
COMP 284	Cybersecurity Governance, Risk and Compliance	3

Certificate in Cybersecurity Operations

Students are required to complete the following courses for the certificate.

COMP 276	Security Operations: Incident Response and Digital Forensics	3
COMP 279	Cybersecurity Advanced Topics	3
COMP 275	Network Security and System Administration Essentials	3

Certificate in Securing Enterprise Systems

Students are required to complete the following courses for the certificate.

COMP 283	Vulnerability Management	3
COMP 270	Secure Software Systems	3
COMP 284	Cybersecurity Governance, Risk and Compliance	3