# Prerequisite/Corequisite Change Request

## (Existing Courses)

### General Information

<table>
<thead>
<tr>
<th>Date:</th>
<th>6/22/21</th>
</tr>
</thead>
<tbody>
<tr>
<td>College/Department:</td>
<td>Engineering/Computer Science</td>
</tr>
<tr>
<td>Course Designator and Number (Cross-listed Course Designator and Number):</td>
<td>CS 5584</td>
</tr>
<tr>
<td>Title of Course:</td>
<td>Network Security</td>
</tr>
<tr>
<td>Instructor and/or Department Contact:</td>
<td>Trey Mayo - Director of Graduate Programs</td>
</tr>
<tr>
<td>Contact Phone:</td>
<td>X0780</td>
</tr>
<tr>
<td>Contact E-mail:</td>
<td><a href="mailto:treymayo@vt.edu">treymayo@vt.edu</a></td>
</tr>
</tbody>
</table>

### Prerequisite Enforced

| Enable prerequisite enforcement? | Yes | No |

### Add the following Prerequisite/Corequisites:

- Graduate standing in CSA

*Attach department letter of support to include a non-departmental course as a prerequisite/corequisite.*

### Drop the Following Prerequisites/Corequisites:

- CS 5560 OR ECE 5560

### List Course Prerequisites/Corequisites after change:

- Graduate standing in CSA

### Justification (Justify prerequisite/corequisite changes and remaining prerequisites/corequisites after change)

Lead instructor for the course has determined that CS 5560 does not have to be a hard pre-req for the course and students who did not have a background in network security were still successful in the course.

*If adding a minimum grade as a prerequisite for a course, data must be provided to clearly show the need for that minimum grade in order to be successful in the course. Minimum grade requirements may not be used as a way to limit enrollment.*

*If request is being processed for the upcoming effective term:*
- Requests to ADD prerequisite requirements (i.e., turn enforcement ON, add grade restriction, add course) must be processed prior to the opening of “course request” for the applicable effective term.
- Requests to REMOVE prerequisite requirements (i.e., turn enforcement OFF, remove a grade restriction, drop course) may be completed at any time, unless the removal causes the course to be more restrictive.

### Approval Signatures

<table>
<thead>
<tr>
<th>Department Head/Chair</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6/22/2021</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>College Curriculum Committee Representative</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6/24/21</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>College Dean</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6/24/21</td>
</tr>
</tbody>
</table>

Office of the University Registrar • Student Services Building, Suite 250, Virginia Tech
800 Washington St., SW • Blacksburg, VA 24061 • (540) 231-6252 • acadgov@vt.edu
Network Security
CS 5584 / ECE 5584
CS is the Home Department

I. Catalog Description


Course Number: 5584/ECE 5584

ADP Title: Network Security

II. Learning Objectives

Having successfully completed this course, the student will be able to:

• Distinguish among network security objectives of confidentiality, integrity, authentication, non-repudiation and availability.
• Apply design principles of authentication systems.
• Analyze the objectives of real-time secure handshake protocols and locate design pitfalls.
• Compare the key management problems for symmetric cryptography-based and asymmetric cryptography-based security protocols.
• Appraise the architecture and functionality of the Kerberos authentication system.
• Assess the objectives of network security protocols such as Internet Protocol Security (IPsec) and Transport Layer Security (TLS); compare security mechanisms used to meet these objectives.
• Distinguish threats to email and threats enabled by email; choose among various security mechanisms employed to protect email security.
• Specify the basic principles of network intrusion detection systems.
• Compare the unique security challenges in wireless networks; apply various wireless network security standards.

III. Justification

Cybersecurity has become a national priority because it is critical to a broad array of societal concerns, including personal privacy, financial accountability and national security. Security problems represent an enormous challenge to the safety and functionality of modern networked computing systems. Many career paths open to
computer science and engineering graduates require them to have a good understanding of cybersecurity challenges arising in the context of networking. This course is part of a set of three new courses and one revised course in cybersecurity from the departments of Computer Science (CS) and Electrical and Computer Engineering (ECE). The revised course is CS/ECE 5560 (new title, “Fundamentals of Information Security”), which provides necessary background in cybersecurity principles and techniques. The proposed CS/ECE 5584 focuses on more advanced security issues in the context of networking.

The course will be taught at the 5000-level because it requires advanced knowledge of computer science and engineering topics (e.g., operating systems and networking) as provided by an undergraduate degree in computer science or computer engineering, and because it requires an appropriate background in cybersecurity as provided by CS/ECE 5560.

IV. Prerequisites and Corequisites

Pre: 5560/ECE 5560

V. Texts and Special Teaching Aids


VI. Syllabus

- Fundamental concepts
  - Network security architecture, basic security concepts, cryptographic techniques, networking concepts and attacks 20%
  - Overview of authentication systems, authentication of people 10%
  - Security handshake principles and common pitfalls 10%
- Security standards
  - Key Management Fundamentals 5%
  - Network Authentication Protocol 10%
  - Public Key Infrastructure 5%
  - Real-time communication security 5%
  - Network Security Protocols 15%
- Other network security topics
  - Email Security 5%
  - Firewalls, Intrusion detection 5%
  - Wireless security 10%

Total 100%