EC335 - E-Commerce Security

Module designation	**EC335 - E-Commerce Security** The module provides students with: - Attack types, security models, policies and usage contexts. - Encryption algorithms as well as specific applications, weaknesses, strengths and implementation considerations, such as DES, AES encryption techniques, public encryption, - Identify, analyze and evaluate resources, threats and security risks, implement resource access control according to international standards such as ISO27000 - Information security management system, OWASP , and Payment Card Industry Data Security Standard (PCI DSS)
Semester(s) in which the module is taught	4
Person responsible for the module	MEng. Ha Le Hoai Trung, MSc. Tran Thi Dung
Language	Vietnamese, English
Relation to curriculum	Specialization
Teaching methods	Lecture, lesson, assignment, project, seminar, examination.
Workload (incl. contact hours, self-study hours)	(Estimated) Total workload: 165 Contact hours: Lecture: 45 hours, Lab: 0 hours Self-study hours: 120 hours
Credit points	Number of credits: 3 (4.5 ECTS credits) Lecture: 3 Laboratory: 0
Required and recommended prerequisites for joining the module	Introduction to Computer Network

<table>
<tr>
<td>Module objectives/intended learning outcomes</td>
<td>
<table>
<tr><th>Goals</th><th>Module Learning Outcomes</th><th>Intended Learning Outcomes (ILOs)</th></tr>
<tr><td><b>G1</b></td><td>Understand and articulate fundamental concepts: attack, defense, risk, encryption, decryption, firewall, and website security techniques..</td><td>ILO2
(2.2)</td></tr>
<tr><td><b>G2</b></td><td>Identify risks in information systems.</td><td>ILO3
(3.1)</td></tr>
<tr><td><b>G3</b></td><td>Apply encryption, authentication, and access control techniques according to international standards such as ISO27000 on information security management systems, OWASP, and Data security standards for card payments (PCI DSS)..</td><td>ILO3
(3.3)</td></tr>
</table>
<table>
<tr><th>CLO</th><th>ILO</th><th>CLOs description</th><th>Competency level</th></tr>
<tr><td>G1.1</td><td>2.2</td><td>Understand and present fundamental concepts: attack, defense, risk, encryption, decryption, authentication, authentication, identification, ...</td><td>K2</td></tr>
<tr><td>G2.1</td><td>3.1</td><td>Understand and identify the risks and threats of attack from external and internal.
Understand some basic criteria for choosing methods of building defense systems.</td><td>K2</td></tr>
<tr><td>G3.1</td><td>3.3</td><td>Apply algorithms and prevention methods to solve real problems:
Select design requirements based on the goal, scope, and importance of the resource to be protected.
Select a balance between different goals, such as cost and level of security, when considering system protection.
Evaluate the level of security in the database management system (SQL Server, MySQL, …) based on hypotheses. Ensure the privacy of data when aggregated and made public using the open source framework..</td><td>S3</td></tr>
</table>
(<b>Competency level</b> K: Knowledge, S: Skill, A: Attitude)
</td>
</tr>
</table>

<table>
<tr><td>Content</td><td>Theory
<table>
<tr><th>Week / Duration (4 hours)</th><th>Content</th><th>CLOs</th><th>Assessment elements</th></tr>
<tr><td>1</td><td>Chapter 1: Overview</td><td>G1.1</td><td>A1.1</td></tr>
<tr><td>2, 3</td><td>Chapter 2: Crytography</td><td>G1.1, G2.1</td><td>A1.1, A1.2, A4</td></tr>
<tr><td>4</td><td>Chapter 3: Identification and Authentication</td><td>G1.1, G2.1, G3.1</td><td>A1.1, A1.2, A4</td></tr>
<tr><td>5</td><td>Chapter 4: Discretionary Access Controls - DAC</td><td>G1.1, G2.1, G3.1</td><td>A1.1, A1.2, A4</td></tr>
<tr><td>6</td><td>Chapter 5: Mandatory Access Controls – MAC</td><td>G1.1, G2.1, G3.1</td><td>A1.1, A4</td></tr>
<tr><td>7</td><td>Chapter 6: Firewalls</td><td>G1.1, G2.1, G3.1</td><td>A1.1, A4</td></tr>
<tr><td>8</td><td>Chapter 7: ISO27000 - Information security management system</td><td>G1.1, G2.1, G3.1</td><td>A1.1, A4</td></tr>
<tr><td>9</td><td>Chapter 8: Payment Card Industry Data Security Standard – PCI DSS</td><td>G1.1, G2.1, G3.1</td><td>A1.1, A4</td></tr>
<tr><td>10</td><td>Chapter 9: OWASP</td><td>G1.1, G2.1, G3.1</td><td>A1.1, A4</td></tr>
<tr><td>11</td><td>Review</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>Examination forms</td><td>
<table>
<tr><th>Asessment elements</th><th>Details</th><th>CLOs</th><th>Percentage</th></tr>
<tr><td rowspan="2">A1. Practice</td><td><b><i>A1.1 Theoretical assignments</i></b>
Classwork
Homework</td><td>G1, G2, G3</td><td rowspan="2">50%</td></tr>
<tr><td><b><i>A3. Final project</i></b></td><td>G2, G3</td></tr>
<tr><td>Final theory examination</td><td><b><i>A4. Final examination</i></b></td><td>G2, G3</td><td>50%</td></tr>
</table></td></tr>
<tr><td>Study and examination requirements</td><td>Classroom and teamwork formation: Forming a group (maximum of 4 students), conducting group discussion, assigning tasks, creating a work plan for members to track progress, submitting a project report, and delivering a detailed presentation to the lecturer after the module ends (1-2 weeks later).
In-class and at home learning methods: Engaging in hands-on activities and problem-solving during class, as well as completing assignments and module projects at home.
Module’s rules: Attendance policy: Full attendance is required (students who are absent for more than 5 lectures will be prohibited from taking the theoretical exam, and those absent for 3 lectures will not receive attendance points).</td></tr>
<tr><td>Reading list</td><td>[1] Stallings W., Brown L., Bauer M.D. and Howard M. Computer security: principles and practice, 4th Edition, Pearson, 2018.
[2] Matt Bishop. Computer security: art and science, 2nd Edition, Addison-Wesley Professional, 2018.
[3] Mark Stamp. Information security: principles and practice, 2nd Edition, JohnWiley & Sons, 2011.
[4] Hoffman, Andrew. Web Application security: exploitation and countermeasures for modern web applications, 1st Edition, O'Reilly Media, 2020.</td></tr>
</table>