**F20CN Computer Network Security**

**COURSE DETAILS**

- **Course Code**: F20CN
- **Full Course Title**: Computer Network Security
- **SCQF Level**: 10
- **SCAF Credits**: 15
- **Available as Elective**: No

**DELIVERY LEVEL**

<table>
<thead>
<tr>
<th>Undergraduate:</th>
<th>Yes</th>
<th>Postgraduate Taught:</th>
<th>No</th>
<th>Postgraduate Research:</th>
<th>No</th>
</tr>
</thead>
</table>

**Additional Information:**

**COURSE AIMS**

Impart critical understanding of key concepts, issues, theories and principles of computer network security.

- Develop detailed theoretical and practical knowledge of foundational issues in computer network security.
- Provide detailed understanding and practical experience with key services and tools used for computer network security purposes.
- Give practical experience of analysing requirements, designing, implementing and testing security solutions for computer network applications

**LEARNING OUTCOMES – SUBJECT MASTERY**

Detailed and critical understanding of the concepts, issues, principles and theories of computer network security

- Critical theoretical and detailed practical knowledge of a range of computer network security technologies as well as network security tools and services
- Practical experience of analysing, designing, implementing and validating solutions to computer network security challenges using common network security tools and formal methods.

**LEARNING OUTCOMES – PERSONAL ABILITIES**

- Ability to deal with complex issues and make informed judgements about network security in the absence of complete or consistent data.
- Demonstrate critical reflection on network security issues. (PDP)
- Exercise substantial autonomy and initiative in addressing computer network security challenges.
- Showing initiative and team working skills in shared computer network security application development. (PDP)

**SYLLABUS**

- Basics of cryptography: principles & algorithms - concepts (classification, symmetric vs asymmetric encryption etc); public-key encryption: challenges
and algorithms. Key Management - key establishment protocols, key management infrastructures. Proof-
carrying-code - concepts (role of trust, 
authentication-based/free certification, logical foundations; case study: PCC for resources. Operating system 
security - concepts (vulnerabilities in: multiuser, 
distributed etc OSs), security-enhanced Linux.

- X.800 network security model - attacks, mechanisms, services. Network service fundamentals - sockets, 
services, threads, base64 encoding. Digests – 
MD5, symmetric ciphers, JCE. Digital signatures, public key certificates. X.509 certificates, certificate 
authorities and hierarchical trust models. Signed 
applets. Secure key exchange – Diffie Hellman, SSL/TLS, SSH. PGP public keys, OpenPGP, web of trust, 
Java APIs for PGP, RMI, JNDI, EJB, RMI 
over SSL, remote class loading, RMI security manager, HTTP authentication, secure web access

Other Information:-

A fundamental knowledge of computer networking, formal methods and Java programming are pre-requisites to this course.

COURSE RELATIONSHIPS

N/A

LOCATION AND ASSESSMENT METHODS

<table>
<thead>
<tr>
<th>Edi</th>
<th>SBC</th>
<th>Ork</th>
<th>Dub</th>
<th>Malay</th>
<th>IDL</th>
<th>COLL</th>
<th>ALP</th>
<th>OTH</th>
<th>Method</th>
<th>Weight</th>
<th>Exam Mins</th>
<th>Type</th>
<th>Diet</th>
<th>Synoptic Course</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Examination</td>
<td>60</td>
<td>120</td>
<td>Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Coursework</td>
<td>40</td>
<td></td>
<td>Assessment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>