## INFORMATION SECURITY GROUP
### Course Specification 2017-18

<table>
<thead>
<tr>
<th>Code:</th>
<th>IY5511</th>
<th><strong>Course Value:</strong></th>
<th>20</th>
<th><strong>Status:</strong></th>
<th>Core A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title:</strong></td>
<td>Network Security</td>
<td><strong>Availability:</strong></td>
<td>Autumn term</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Prerequisites:</strong></td>
<td>None</td>
<td><strong>Recommended:</strong></td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Co-ordinator:</strong></td>
<td>Jason Crampton</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Course Staff:</strong></td>
<td>Jason Crampton</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Aims:
- consider information networks and their operation;
- examine the security threats and risks arising in particular types of networks;
- identify and evaluate countermeasures that can be used to enhance the security of networks.

### Learning Outcomes:
- have a systematic understanding of information networks and their operation;
- have a clear understanding of the components of the TCP/IP protocol stack, the OSI 7 layer model, and the associated security architecture as specified in ISO/IEC 7498-2, and be able to analyse the benefits and drawbacks of applying security controls at different network layers;
- have a critical awareness of key security threats and risks faced in network environments, and be able to specify appropriate countermeasures;
- have a comprehensive understanding of the methods by which strong authentication protocols and key exchange mechanisms suitable for use on open networks can be constructed;
- have a comprehensive understanding of the security architecture and design rationale of selected protocols, such as Kerberos, SSL/TLS and the IPSec protocol suite, and how they can be applied in single-sign on, e-commerce, virtual private networking and remote access applications;
- understand the design rationale for the security architecture in GSM and UMTS systems and be able to compare and evaluate the security in the two systems;
- be able to evaluate the security threats in wireless LANs and the strength of security countermeasures offered by current standards;
- be able to assess the security offered by different firewall technologies as well as their limitations;
- understand the value of Intrusion Detection Systems and related network security technologies.

### Course Content:
- Introduction to Reliable and Secure Communication Channels;
- Introduction to Networking and Network Security;
- Introduction to Secure Protocols;
- Secure Protocols – IPSec, SSL/TLS and SSH;
- GSM and UMTS Security;
- Wireless LAN Security;
- Firewalls;
- Intrusion Detection Systems and related network security technologies.

### Teaching & Learning Methods:
- Lectures delivered by ISG staff.
- Small group and individual tutorials.
- Optional exercises to reinforce learning and provide directions for further study. Course website, hosted on Moodle, with teaching materials, links, and bibliography.

### Key Bibliography:

### Formative Assessment and Feedback:
- There will be two compulsory pieces of coursework with deadlines during the first semester. These will be marked and returned to the students. Marks obtained in these assessments will NOT contribute towards the final assessment for this course. However, the content of the assignments is examinable.

### Summative Assessment:
- **Exam:** 100(%)  This course is assessed solely by written examination consisting of a two-hour exam.
- **Coursework:** 0(%) Coursework does not contribute to the final assessment for this course.
- **Deadlines:** The written examination will be held in the Summer term.

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department’s policy of continuous improvement and development. Every effort will be made to notify you of any such changes.