

**INFORMATION SECURITY GROUP**  
**Course Specification 2016-17**

<b>Code:</b>	IY5606	<b>Course Value:</b>	20	<b>Status:</b>	Option
<b>Title:</b>	<b>Smart Cards, RFIDs and Embedded Systems Security</b>			<b>Availability:</b>	Spring Term
<b>Prerequisites:</b>	Core courses			<b>Recommended:</b>	None
<b>Co-ordinator:</b>	Keith Mayes				
<b>Course Staff</b>	Keith Mayes plus invited ISG and industry experts				
<b>Aims:</b>	<p>This course will:</p> <ul style="list-style-type: none"> <li>• provide an overview of smart cards/RFIDs/Near Field Communications (NFC) and properties</li> <li>• introduce applications exploiting smart cards/RFID/NFC including the Internet of Things (IoT)</li> <li>• examine benefits, threats and attacks when used as assets for Cyber Security</li> <li>• consider development, manufacture and management of smart cards/RFID/NFC</li> <li>• review related standards and security evaluation methodologies for embedded security</li> <li>• consider/compare related technology e.g. TEE, TPM &amp; Android Host Card Emulation (HCE)</li> <li>•</li> </ul>				
<b>Learning Outcomes:</b>	<p>On successful completion of the course students will be able to:</p> <ul style="list-style-type: none"> <li>• identify constituent components, analyse strengths and weaknesses, identify new applications of smart cards/security tokens and their use as assets in cyber security</li> <li>• identify the steps in the manufacturing/personalisation processes, analyse and evaluate potential risks and compare security safeguards</li> <li>• identify and compare current systems/business applications (plus future IoT), analyse the strengths and weaknesses and evaluate interoperability and security issues</li> <li>• analyse the range of capabilities of SIM/USIM cards in Smartphones and apply them to new service ideas, evaluate the possible range of services and security measures</li> <li>• understand the main standards and applications of smart cards for banking and finance, compare with earlier card solutions and analyse strengths and weaknesses of approaches</li> <li>• analyse the key role of the embedded smart card/RFID for passports, IDs and satellite TV, evaluate the security measures that have protected past and current cards,</li> <li>• identify and describe new technologies, including NFC, TPM, TEE, HCE; and apply them to new applications and evaluate the likely suitability/success of approach</li> <li>• explain how common criteria may affect smart card design/development, analyse the different approaches and compare with less formal methods</li> <li>• identify and describe the classes of attack and notable methods within each class, analyse countermeasures and evaluate practicality of attacks and the effects on cyber security</li> <li>• identify, compare and evaluate different methods of developing applications for smart cards, and understand the development cycle and the use of practical tools</li> <li>• analyse the issues concerning smart card/embedded-security lifecycle management, and evaluate and compare methods of local and remote card management</li> </ul>				
<b>Course Content:</b>	<ol style="list-style-type: none"> <li>1. Introduction to Smart Cards/Chips &amp; RFID/NFC; Embedded Assets for Cyber Security</li> <li>2. Smart Cards – Trusted Production Environment &amp; Advances in Smart Chips/Tokens</li> <li>3. Applications &amp; Security for Mobile Communications, USIM/SIM and Services</li> <li>4. Smart Cards for Secure Banking &amp; Finance</li> <li>5. Smart Card Operating Systems, Interoperability and Security</li> <li>6. Smart Cards in eIDs/Passports &amp; Transport for London System Case Study</li> <li>7. An Introduction to the Internet of Things &amp; Practical IoT Attacks</li> <li>8. RFID/NFC explained &amp; Common Criteria Evaluation of Embedded Security</li> <li>9. Security Attacks, Countermeasures and Testing for Smart Cards/RFIDs/NFC/HCE</li> <li>10. Application Development Environments for JAVA and SIM Toolkit</li> <li>11. Comparing Alternative Security Tokens/Environments; including TPM, TEE and HCE</li> </ol>				
<b>Teaching &amp; Learning Methods</b>	<p>Lectures delivered by ISG-SCC staff &amp; industry experts; with some practical demonstrations Private study: Students are expected to read the course text book and encouraged to read other texts and review international standards</p>				
<b>Key Bibliography:</b>	<p><u>Course Text book:</u> Keith Mayes, Konstantinos Markantonakis, "Smart Cards, Tokens, Security and Applications", Springer-Verlag New York, January 2008, ISBN: 0387721975 <b>NOTE:</b> A 2<sup>nd</sup> edition is due to be published late 2016, and this is preferred text.</p> <p>W. Rankl and W. Effing – "Smart card handbook" 2<sup>nd</sup> edition John Wiley 1997 Klaus Finkenzerler, "The RFID Handbook", John Wiley and Sons 2003 Zhiqun Chen, "Java Card Technology for Smart Cards", Addison- Wesley 2000.</p>				

	Konstantinos Markantonakis, Keith Mayes, "Secure Smart Embedded Devices, Platforms and Applications", Springer-Verlag New York, 2013, ISBN 978-1-4614-7914-7
<b>Formative Assessment and Feedback:</b>	There are formative feedback quizzes that are set within one lecture and answers provided at the following lecture. Some lectures also have sample questions/problems that the student may optionally answer. Feedback is given at the lectures, via e-mail and sometimes one-to-one as requested by the student.
<b>Summative Assessment</b>	<b>Exam</b> 100(%) This course is assessed solely by written examination consisting of a two-hour-exam. <i>(3 out of 5 questions)</i> <b>Coursework</b> 0(%) Coursework does not contribute to the final assessment for this course. <b>Deadlines:</b> 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.