Aims
This module will:

- provide an overview of smart cards/tokens and their properties
- introduce various applications that exploit smart cards/tokens
- examine benefits, threats and attacks
- consider systems for the development, manufacture and management of smart
  cards/tokens
- review smart card standards and security evaluation methodologies.

Pre-requisites
None

Essential Reading
Media-2008

This is included as study material once registered on the module.

Assessment
This module is assessed by a two hour unseen written examination.

Learning Outcomes
On completion of this module students will be able to:

- identify constituent components, analyse strengths and weaknesses and identify new
  applications of smart cards
- identify the steps in the manufacturing/personalisation processes, analyse and evaluate
  potential risks and compare security safeguards
- identify and compare the systems in use, analyse the strengths and weaknesses and
  evaluate interoperability and security issues
- analyse the range of capabilities of SIM/USIM cards and RFID tokens, and apply them to
  new service ideas, evaluate the possible range of services and security measures
• 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
• analyse the key role of the smart card for passports, IDs and satellite TV, evaluate the security measures that have protected past and current cards
• identify and describe “new” technologies, including Trusted Platform Modules (TPMs), Trusted Execution Environments (TEE), Host Card Emulation (HCE), Internet-of-Things (IoT) and apply them to new applications and evaluate the likely suitability/success of approach

• explain how Common Criteria may affect smart card design/development, analyse the different approaches and compare with less formal methods
• identify and describe the classes of attack and notable methods within each class, analyse countermeasures and evaluate practicality of attacks
• identify, compare and evaluate different methods of developing applications for smart cards, and understand the development cycle and the use of practical tools for different technologies like Java Card, Multos, etc.
• analyse the issues concerning smart card lifestyle management, and evaluate and compare methods of local and remote card management
• analyse the differences and similarities of the main multi-application smart card platforms and operating systems.

**Syllabus**

**Unit 1 – An Introduction to Smart Cards**, is based on the presentation by Prof Keith Mayes of the Information Security Group Smart Card Centre (ISG SCC). This unit leads the students through an introduction to the basics of smart card related issues. It reviews the different types of cards and token platforms along with introducing the main types of popular smart card applications. The presentation aims to motivate and provide context for the rest of the units.

**Unit 2 comprises of two different presentations:**

**Unit 2a – Smart Cards Trusted Production Environment**
In Unit 2, Prof Keith Mayes presents various issues associated with the smart card production chain. The unit examines the processes (e.g. production of the card body, chip moulding, personalisation and card delivery) involved in smart card production.

**Unit 2b – Introduction to IoT (Internet of Things)**
In Unit 2, Prof Keith provides an introduction to the subject of Internet of Things (IoTs). The presentation also highlights the privacy issues surrounding the deployment, initialisation and personalisation of these devices, compared with more traditional devices like smart cards.

**Unit 3 – An Overview of Multi-Application Smart Card Operating Systems and Platforms**
is delivered by Prof Konstantinos Markantonakis (ISG SCC). Having examined the basic functionality of smart card technology in the previous two modules, this presentation provides an overview of the most widely utilised multi-application smart card platforms and operating systems.

**Unit 4 – Smart Cards for Secure Banking and Finance**, is delivered by David Main (independend consultant). The presentation examines how cryptography and various other technologies (e.g. cards, tokens, 3D secure, contactless cards) are utilised by major financial institutions in order to safeguard financial payments.

**Unit 5 – Applications & Security for Mobile Communications, USIM/SIM and Services.**
The mobile telecommunications industry utilises more smart cards than any other sector. This unit is delivered by Prof Keith Mayes. He discusses the role of the SIM and USIM in the mobile telecommunications industry. At the same time he reviews the evolution of smart cards, GSM standards
and other technologies (such as the SIM Toolkit, Near Field Communication, USB interfaces, Smart Card Web Servers, large memories and Host Card Emulation) as the main building blocks for offering enhanced and secure services in the telecommunication industry.

**Unit 6 comprises of two different presentations:**
In **Unit 6a – ID Cards and Passports**
Ingo Liersch (Giesecke & Devrient) examines the recent proposals and standards related with the utilisation of secure tokens for the provision of e-passport and e-ID applications. The presentation also covers issues around biometrics and how they affect any proposed solutions.

**Unit 6b – RFID/NFCs Explained.** Dr Gerhard Hancke (University of Hong Kong) provides an introduction to the subject of Radio Frequency Identification (RFID) and Near Field Communication (NFC). The presentation highlights the significance of these technologies along with comparing and contrasting their capabilities and trade-offs.

**Unit 7 - Unit 7 is composed of two distinct presentations:**
**Unit 7a – Advances in Chipcard Technology.**
Chris Shire (Infineon) examines the past and the future of smart card technology. It highlights issues around the future of smart card chips by taking into account various limitations in terms of size, processing power, and cost. Finally, he discusses issues around consumer demand.

**Unit 7b – Security For Video Broadcasting**
Dr Allan Tomlinson (ISG) examines various issues around the protection of digital content in the satellite TV industry. In particular, he examines how smart card technology is utilised as the main security mechanism for the protection of the transmitted content.

**Unit 8 – Evaluating Smart Card Security with the Common Criteria.**
Tony Boswell (Siventure). This unit explains how Common Criteria has evolved and how it is applied in practice to the complex and highly demanding field of smart card security evaluations.

**Unit 9 – Security Attacks, Countermeasures and Testing for Smart Cards,** by Jacques Fournier (Gemalto) focuses on the wide range of smart card security attacks and countermeasures that need to be considered when planning commercial smart card offerings.

**Unit 10 – Application Development Environments for Multos,** Chris Torr from MAOSCO Ltd, provides an introduction to the subject of application development and deployment on MULTOS supported smart cards. The development of an application for a resource constraint device like a smart card is very different than for a resource rich environment like a desktop machine. Also the presentation provides the basic information needed in order to be able to start programming MULTOS smart cards.

**Unit 11 is composed of two distinct presentations:**
**Unit 11a – Overview of Trusted Platform**
Dr Allan Tomlinson (ISG) provides an overview of the Trusted Production Module (TPM) and highlights how it compares with smart cards in terms of technology, overall architecture, management and ownership.

**Unit 11b - Introduction to TEE and Related Processors,** presented by Prof Keith Mayes, introduces the subject of Trusted Execution Environments (TEE) and related processors. This unit provides an insight into the world of the Trusted Execution Environment (TEE) which are increasingly found in mobile devices to provide a safe and trusted user interface for a variety of application including mobile payments. The presentation also briefly covers security economics and the importance of TEEs when using Host Card Emulation (HCE) applications on mobile phones.

Last updated 16 May 2016
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.