ESTD 1845

QUEEN'S
UNIVERSITY
BELFAST

Network Security – Handbook

Dr. Sandra Scott-Hayward

CSC3064 Lecture 01

School of Electronics, Electrical Engineering and Computer Science

Session Overview

- ❑ Lecturer – contact details
- ❑ Module background
- ❑ Course objectives/Learning outcomes
- ❑ Syllabus
- ❑ Assessment
- ❑ Schedule (Lecture/Labs/Assessment)
- ❑ Learning agreement/code of conduct
- ❑ Course bibliography

QUEEN'S
UNIVERSITY
BELFAST

Lecturer

Dr. Sandra Scott-Hayward, CEng CISSP CEH OCSA

Office: Room 08.035, Ashby Building, Stranmillis Road (generally Tues/Thurs/Fri)
Room G.19, ECIT, Titanic Quarter (generally Mon/Wed)

Email: s.scott-hayward@qub.ac.uk

Telephone: 028 9097 1898 (ECIT)

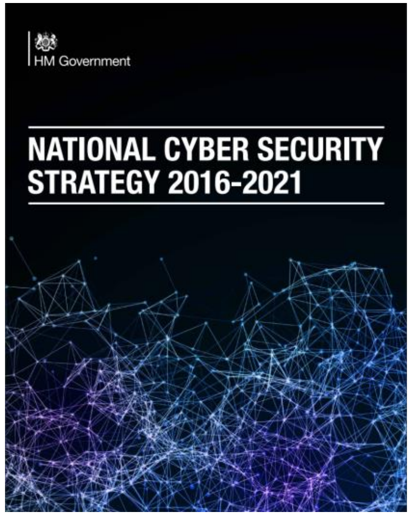
QUEEN'S UNIVERSITY BELFAST

Module Background

- Course Accreditation

- Centre for Secure Information Technologies (CSIT)

- Cybersecurity (N.I., U.K. and globally)



HM Government

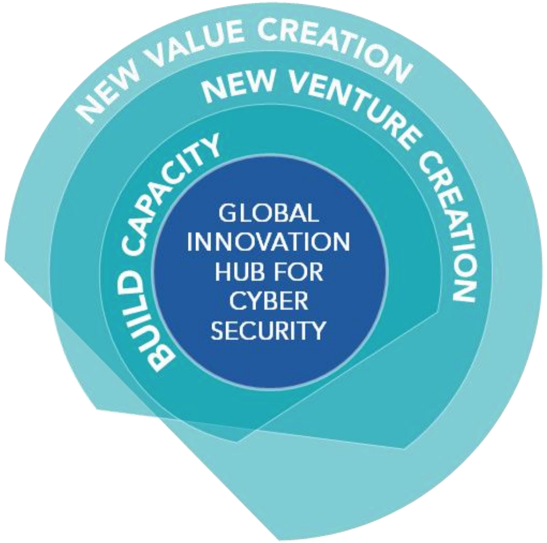
NATIONAL CYBER SECURITY STRATEGY 2016-2021

Course Accreditation

- BCS Accreditation (The Chartered Institute for IT)
    - MEng/BEng/BSc Computer Science, MEng/BEng Software Eng and BSc CIT

- Example criteria:
    - Knowledge of information security issues
    - Methods, techniques and tools for information modelling, management and security

Centre for Secure Information Technologies (CSIT)



Est.2009, Based in The ECIT Institute

Initial funding over £30M (CSIT 2 - £38M)

90 People
- Researchers
- Engineers
- Business Development

Largest UK University lab for cyber security technology research

GCHQ Academic Centre of Excellence

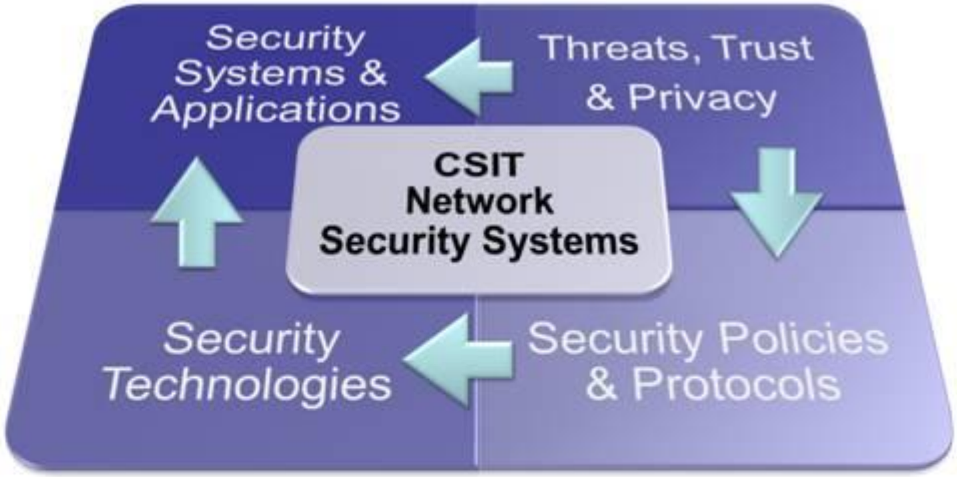
Industry Informed
- Open Innovation Model

Strong international links
- ETRI, CyLab, GTRI, SRI International
- Cyber Security Technology Summit

QUEEN'S UNIVERSITY BELFAST

CSIT

- Research Groups:
  - Data Security Systems
  - Networked Systems Security
  - Wireless Enabled Security Systems
  - Security Analytics and Event Management


Security Systems & Applications
Threats, Trust & Privacy
CSIT Network Security Systems
Security Technologies
Security Policies & Protocols

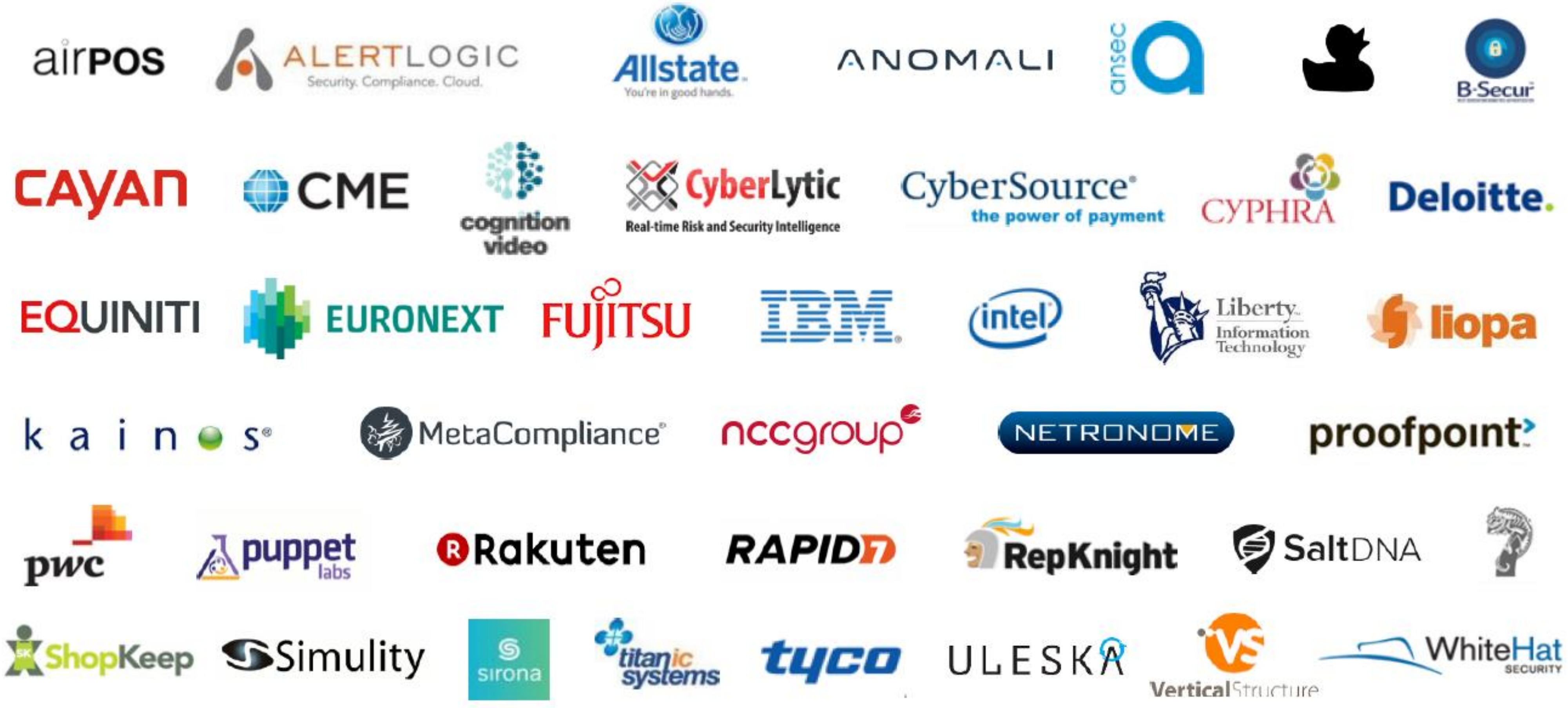
- MSc Applied Cyber Security

- PhD Research Projects

https://www.qub.ac.uk/csit/

QUEEN'S UNIVERSITY BELFAST

N.I. cyber security cluster



Course Description/Objectives

CSC3064 introduces security technologies and policies for the design, development and deployment of secure networks. The module focusses on key topics related to network security, including internet security protocols, network attack and defence mechanisms, network monitoring and analysis, and network security administration.

- To produce students who are employable as professional network security specialists
- To produce students capable of postgraduate study in network security

Learning Outcomes

- Know and understand the administration of network security and the process of incident management;
- Know and understand the technologies involved in the design and deployment of secure networks e.g. AAA, IDS/IPS, secure protocols etc.;
- Be able to demonstrate the use of network security functions e.g. Firewall/VPN;
- Be able to demonstrate the use of network security analysis tools.

Syllabus

- Introduction to Network Security
- Network Security Architecture
- Security of Internet Protocols
- Tunneling and VPNs
- AAA/Firewalls
- Denial of Service
- Intrusion Detection/Protection Systems
- Network Security Administration
- Incident Mgmt./Network Forensics
- Cloud/Virtualization Security
- Wireless/Mobile Network Security

Assessment

Assessment is 100% coursework/continuous assessment:

- Class Tests (40%)
  - 2 * Class Tests, each worth 20% (Individual Mark)

- Assignment (40%)
  - Case Study worth 40% (Group work - Individual Mark)
  - Topics: Security Policy, Incident Management

- Practical (20%)
  - 1 * Practical Test worth 20% (Individual Mark)
  - Possible Topics: Network Analysis, Firewalls, Intrusion Detection and Protection Systems, Tunneling

What you need to do to pass

The compulsory assessment elements are:

- Class Tests
- Practical Test

This means that you must pass each of these elements i.e. get >= 40% on the class test component and get >= 40% on the practical assessment.

The overall pass mark for the module is 40%.

Lectures

All lectures to be held in CSB/02/027

- Tuesday’s lecture is 4-5pm
- Thursday’s lecture is 12-1pm
- Friday’s lecture is 12-1pm

All labs to be held in CSB/01/020 (unless otherwise advised e.g. Green Room for class tests)

- Friday’s lab is 1-3pm

Note: No lab 18/25 January, 15/22/29 March, 05 April

Lecture Schedule

Week 1 (14): Introduction to Network Security

Week 2 (15): Network Security Architecture

Week 3 (16): Security of Internet Protocols

Week 4 (17): Tunneling and VPNs

Week 5 (18): AAA and Firewalls

Week 6 (19): Denial of Service

Week 7 (20): Intrusion Detection/ Protection Systems

Week 8 (21): Network Security Administration

Week 9 (22): Incident Mgmt./ Network Forensics

Week 10 (23): Cloud/Virtualization Security

Week 11 (24): Wireless/Mobile Network Security

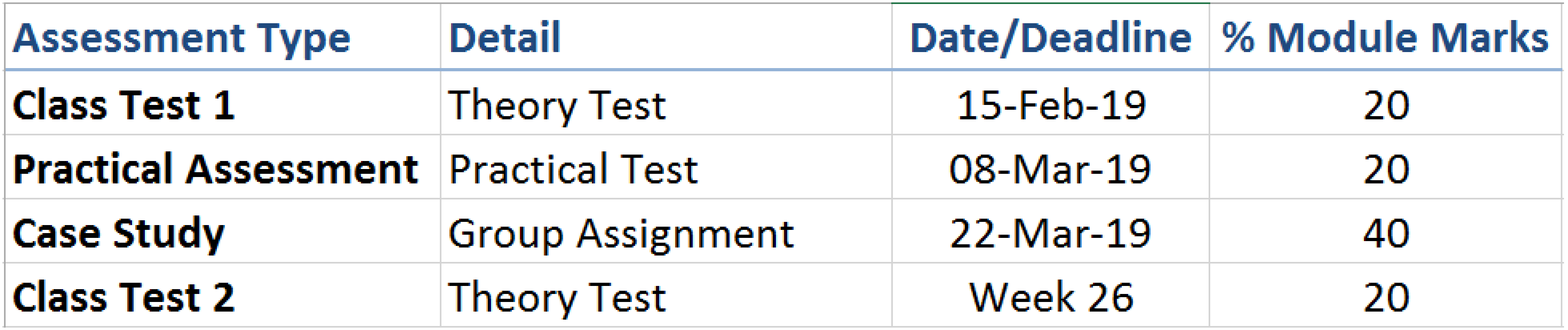
Week 12 (25): Review/Q&A

QUEEN'S UNIVERSITY BELFAST

Lab Schedule

Date	Activity	Submission Deadline (SD) / Assessment (A)
18 January	No Lab	
25 January	No Lab	
01 February	Practical 1 – Network Analysis	
08 February	Practical 2 – Tunneling	
15 February	Class Test	A
22 February	Practical 3 – Firewalls	
01 March	Practical 4 – Intrusion Detection	
08 March	Practical Test	A
15 March	No Lab	
22 March	No Lab	Case Study SD
29 March	No Lab	
05 April	No Lab	
Week 26	Theory Test	A

Assessment Schedule



Assessment Type	Detail	Date/Deadline	% Module Marks
Class Test 1	Theory Test	15-Feb-19	20
Practical Assessment	Practical Test	08-Mar-19	20
Case Study	Group Assignment	22-Mar-19	40
Class Test 2	Theory Test	Week 26	20

Lecture Material

Lecture slides will be available to download from Queen's Online

- http://www.qol.qub.ac.uk

Additional information will be given at lectures:

- Attendance is necessary
- You must be able to demonstrate understanding of the material i.e. understand, not memorize …
- You must apply independent learning
- The university expects that each module will require at least 200 hours of study

Learning Agreement

What you can expect of me:

- I’m here to help you learn about network security
- I’m happy to answer questions
- I will assess your work fairly and consistently

What I expect of you:

- You will attend lectures, take notes, and ask, if you have a question or if you don’t understand something
- You will attend labs and work on the assignments

Code of Conduct

DO NOT PEN-TEST THE QUB NETWORK OR ANY OTHER PUBLIC NETWORK

- Studying network security means it is necessary to learn about offensive actions and attack techniques. You must use this knowledge responsibly. Such experiments must be confined to the virtual machines provided for the practicals.
- The University has policies relating to information security and acceptable use of computer systems. Breaches of the security policies will be investigated in accordance with the University's disciplinary procedures. You should make yourself aware of these policies: http://www.qub.ac.uk/directorates/InformationServices/Services/Security/#Policies

Course Bibliography

- Jacobson, Douglas. *Introduction to network security*. CRC Press, 2008.
- Schäfer, Günter, and Michael Rossberg. *Security in Fixed and Wireless Networks*. John Wiley & Sons, 2016.
- Stallings, William. *Network security essentials: applications and standards*. Pearson Education India, 2014.

Networking Fundamentals References

Fall, Kevin R., and W. Richard Stevens. *TCP/IP illustrated, volume 1: The protocols*. Addison-Wesley, 2011.

http://www.tcpipguide.com/

http://nmap.org/book/tcpip-ref.html

Networking 101: The Basics of Protocols https://www.youtube.com/watch?v=ISrJ5ojvOgA

- From here, there are links to a wide range of related presentations and recorded lectures

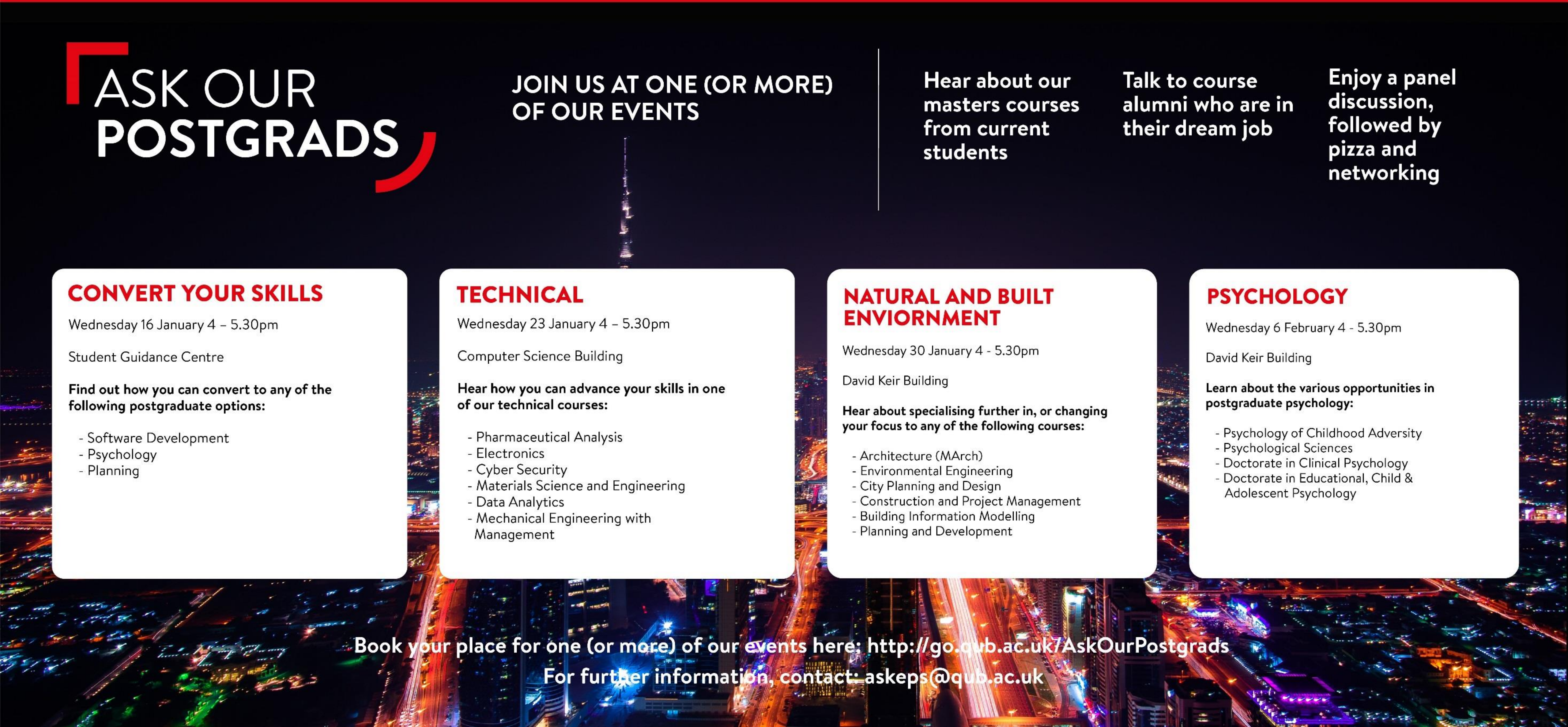
Summary

- Lecturer – contact details
- Module Background
- Course Objectives/Learning Outcomes
- Syllabus
- Assessment
- Schedule (Lecture/Labs/Assessment)
- Learning Agreement/Code of Conduct
- Course bibliography

ToDo

- If you’re not already enrolled on the module, make sure that you’re enrolled by Friday, 18 January.

QUEEN'S UNIVERSITY BELFAST | FACULTY OF ENGINEERING AND PHYSICAL SCIENCES



ASK OUR POSTGRADS

JOIN US AT ONE (OR MORE) OF OUR EVENTS

Hear about our masters courses from current students

Talk to course alumni who are in their dream job

Enjoy a panel discussion, followed by pizza and networking

CONVERT YOUR SKILLS

Wednesday 16 January 4 – 5.30pm

Student Guidance Centre

Find out how you can convert to any of the following postgraduate options:

- Software Development
- Psychology
- Planning

TECHNICAL

Wednesday 23 January 4 – 5.30pm

Computer Science Building

Hear how you can advance your skills in one of our technical courses:

- Pharmaceutical Analysis
- Electronics
- Cyber Security
- Materials Science and Engineering
- Data Analytics
- Mechanical Engineering with Management

NATURAL AND BUILT ENVIORNMENT

Wednesday 30 January 4 - 5.30pm

David Keir Building

Hear about specialising further in, or changing your focus to any of the following courses:

- Architecture (MArch)
- Environmental Engineering
- City Planning and Design
- Construction and Project Management
- Building Information Modelling
- Planning and Development

PSYCHOLOGY

Wednesday 6 February 4 - 5.30pm

David Keir Building

Learn about the various opportunities in postgraduate psychology:

- Psychology of Childhood Adversity
- Psychological Sciences
- Doctorate in Clinical Psychology
- Doctorate in Educational, Child & Adolescent Psychology

Book your place for one (or more) of our events here: http://go.qub.ac.uk/AskOurPostgrads

For further information, contact: askeps@qub.ac.uk

Questions?

Next Session: Thursday, 17 January 2019

Introduction to Network Security – Part 1

QUEEN'S UNIVERSITY BELFAST