Module Descriptor

Part one: Module leader's section: core module details

1. Module title:	**Network Security and Cryptography**

2. SCQF level: Choose	**3. SCQF credit value 20**	**4. ECTS credit value: 10**

5. Module code CSN09xxx

6. Module leader: Prof. Bill Buchanan

7. School: Computing

8. Napier subject area: Computer Systems (CSY)

9. Prerequisites	To study this modules you will need the learning equivalent to the module listed or to have passed this module
Module code	CSN08102
Module title	Practical Networks 2
Examples of equivalent learning	Level 8 equivalent networking-related module or module in software development.

10. What you will learn and what this module is about

Security is a major concern in technological developments and in business development. This module provides a deep understanding of some key fundamental areas of security, and aims to provide a foundation of the key principles and practiced used in network security and in cryptography. The module uses an advanced cloud infrastructure to virtualize the labs, using both public clouds (including Amazon EC2 and Azure) along with a private cloud. It also has full on-line lectures and a range of related challenges. The main focuses is on:

- Network security architectures and devices.
- Codes and code cracking.
- Network protocols.

The module uses an advanced website (http://asecuritysite.com) which outlines a wide range of security principles, and provides ever-changing on-line challenges. Overall the module presents material to computing-related students, no matter their future intentions, background, or programme, and aims to provide fundamental areas of security in a fun and interesting way.

11. Description of module content

The aim of the module is to develop a deep understanding network security and cryptography, that will allow graduates to act professionally in the design, analysis, implementation, and reporting related to network security. An outline of the main areas includes:

- Network Architectures and Network Device Configuration. Robust, scaleable and secure architectures. Firewalls/IDS/IPS/Log/DMZ Configuration.
- Hosts, servers and services. Configuration of the range of hosts, services and servers used in network architectures, including covering related test/debug tools.
• Intrusion Detection Systems. Techniques, Snort, IDS Rules, Distributed/Agent-based, Signature/Anomaly detection, APT, and signature generation.
- Cloud/grid computing. Principles, virtualisation, distributed architectures, dynamic infrastructures, and layered approaches.
- Introduction to Network Protocols/Forensics.
- Secret Codes. Substitution codes, key-based codes, secret sharing, and a wide range of methods.
- Encryption. Prime Numbers, Weaknesses, Public/private key, CBC/ECB. Coverage of methods: RSA, AES, ElGamal, and so on.
- Key exchange methods. Diffie-Hellman, Kerberos, and so on.
- Hashing methods. Including MD5, SHA-1, and so on. Adding Salt. Collisions, One-time passwords.
- Authentication methods. Authentication methods, Identity Architectures, Digital Certificates.

- Data Integrity. Checksums, Message Authentication Codes (MACs), CRC-32, and other associated methods.
- Code cracking methods. Brute force, rainbow methods, parallel processing, Man-in-the-middle, known weaknesses.

12. Learning Outcomes for module

On completion of this module, students will be able to:

L1: Develop an advanced knowledge of key security/cryptography principles and methods.
L2: Understand the key academic principles and practical skills required to build security architectures.
L3: Design, implement, evaluate and critically analyse a system to a given set of security requirements

13. Indicative References and Reading List

T1: Buchanan WJ, *Security and Network Forensics*, Auerbach Publishers Inc., 2009, ISBN 084933568X.
T2: Buchanan WJ, Advanced Cloud and Virtualisation, CRC Press, Sept 2014, ISBN 1439880379.
T3: asecuritysite.com

Part two: Module leader's section: Versions

✷**14. Occurrence**:

14a. Primary mode of delivery: Blended
14b. Location of delivery: Scotland
Partner: N/A – Napier Delivery
Other partner (if more than one using same version):
14c. Member of staff with primary responsibility for delivering module, if different from module leader:

✷**15. WebCT presence**

Please select **one:**

1. ☐ This version of the module does not require a WebCT presence.
2. ☒ This version of the module requires a WebCT presence that is not shared with any other versions.
3. ☐ This version of the module requires a WebCT presence that is shared with other versions (give details):

✷**16. LTA approach**

Learning & teaching methods including their alignment to LOs

- The coursework will involve the design, implementation, evaluation and critical analysis of a system to a given set of security requirements [L3].
- The module will use an advanced cloud infrastructure which virtualises hosts and devices, and allows complex network architectures to be created.
- The Asecuritysite Web package contains a completely managed learning environment, where the students can track their performance.

Embedding of employability/ PDP/ scholarship skills

The module uses industry-standard methods, protocols, equipment and software.

Assessment (formative and summative)

There will be two methods of assessment:

- **Coursework** [50%]. This relates to a coursework on the design, implementation, evaluation and critical analysis of a prototype of a secure/digital forensics system, based on a range of requirements.
- **On-line tests** [50%]: This involves two on-line tests which cover the key areas of network security and cryptography.

Research/ teaching linkages

The main research group involved in this area has an excellent foundation in research related to security and digital forensics (Centre for Distributed Computing and Security). It has several researchers working in this area, including on the performance evaluation of security devices, enhanced digital forensic frameworks, and in e-Crime. The group also has patents related to next-generation digital forensic system, and works with many industrial companies on security and digital forensics. There are also links with the different domains

such as with the NHS, the Scottish Police, the FSA, and other industrial partners. The module also uses a state-of-the-art teaching framework, which has been published in educational journals and conferences (Buchanan, 2006).

Ref:

Buchanan WJ, *Correlation between academic and skills-based tests in computer networks*, British Journal of Educational Technology, -. doi: 10.1111/j.1467-8535.2005.00476.x, Vol 37, No 1, 2006, pp 69-78

Supporting equality and diversity
The technology can be used by any student, and there are no barriers to equality or diversity. The material will be available in a wide range of formats, including a printed version, and an electronic version. All the lectures will be available on-line, and a narrative of the material covered in the lecture. Email and MSN Messenger support is also available to allow remote working. Student can work at their own pace through the Asecuritysite Web infrastructure, and gain formative feedback on their performance.

Internationalisation
The module uses equipment, techniques, technologies, and methodologies that are standard across the World. Security is also a major issue around the World, and students should be able to understand how a secure system can span across large-areas, and over different countries and continents.

✴**17. Student Activity** (NESH)

Mode of activity	L&T activity	NESH
Face-to-face	Lecture	24
Face-to-face	Practicals/Labs	24
Independent learning	Individual learning activities	152
Mode of activity		
Mode of activity		
Mode of activity		
Mode of activity		
	TOTAL NESH	**= 200 hours**

✴**18. Assessment**

Week	Type of assessment	Weighting	LOs covered	Length/ volume
	Component: Assessment One Enter assessment element(s):			
8,12	Digital exam Other:	50%	1,2	2 hours
14	Project Other:	50%	3	16 hours
	Please select... Other:	0%		
	Component subtotal:	100%		
	Component: Assessment Two Enter assessment element(s):			
	Please select... Other:	0%		
	Please select... Other:	0%		
	Please select... Other:	0%		
	Component subtotal:	0%		
	Module total:	100%		

✶**19. Length of module delivery**.
Over how many trimesters is this module delivered?

☒ One	☐ Two ☐ Three *See Guidance Note 19*

✶**20. Trimester(s) of delivery**. TR2

Admin use

21. Approval **Date of approval**	
Date of approval commencement	
Final date of review	

22. External examiner's name

23. Main Administrator's name

Fiona Sutherland, Assistant Faculty Manager, School of Computing

24. Notes for administrative use only

Admin use (for each version)

24. ✶**Exemptions** awarded from regulations