Module Descriptor

Refer to the guidance notes as you complete this descriptor

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

1. Module title:	Security and Forensic Computing

2. SCQF level: 09	**3. SCQF credit value 20**	**4. ECTS credit value:**

5. Module code	CSN09105

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	
Module title	
Examples of equivalent learning	Level 8 equivalent networking-related or computing/software development module

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

Security is a major concern in technological developments and in business development, and this module provides a deep understanding of some key fundamental areas of security. The module aims to provide a series of challenges to students, in order for them to solve. This includes code cracking exercises within the assessment and practical elements, along with the creation of a security toolkit. The module will also be virtualised for its labs, including within the Amazon and Azure clouds, and have full on-line lectures. It thus focuses on:

- Intrusion detection.
- Codes and code cracking.
- Network, file and live forensics.

The module uses an advanced Web site (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 provide a foundation in a range of key principles related to security. Its coverage will include:

- **Intrusion Detection Systems**. Techniques, Snort, IDS Rules, Distributed/Agent-based, Signature/Anomaly detection, APT.
- **Secret Codes**. Substitution codes, key-based codes, and a wide range of methods.
- **Encryption**. Prime Numbers, Weaknesses, CBC/ECB. Including RSA, DES, 3DES, Blowfish, AES, and so on.
- **Key exchange methods**. Diffie-Hellman, El-Gamal, Kerberos.
- **Hashing methods**. Including MD5, SHA-1, and so on. Adding Salt. Collisions.
- **One-time passwords**. Time-based, hashing, time stamp.
- **Authentication methods**. Authentication methods, Digital Certificates.
- **Data Integrity**. Checksums, Message Authentication Codes (MACs), CRC-32, and other associated methods.
- **Secret sharing**. Shamir, Secure Functions.
- **Code cracking methods**. Brute force, rainbow methods, parallel processing, Man-in-the-middle, known weaknesses.
- **Introduction to Obfuscation and Steganography**.

- **Network, File and Live Forensics**. This will provide an analysis of a range of network protocols. Introduction to Live Forensics. Magic Numbers. Machine Code and Device Architecture.
- **Investigation tools**. Coverage of a wide range of tools, including EnCase, NetWitness, and so on.

12. Learning Outcomes for module

On completion of this module you will be able to:

L1: Demonstrate an in-depth knowledge of key security principles and methods that related to the areas of intrusion detection, secret codes, and code cracking.

L2: Demonstrate an in-depth knowledge of key security principles and methods that relate to the area of network and live forensics.

L3: Apply a suitable methodology and implement this for the investigation of a security incident, and will use code cracking methods.

13. Indicative References and Reading List

T1: Buchanan WJ, *Security and Network Forensics*, Auerbach Publishers Inc., 2008, ISBN 084933568X.

T2: http://asecuritysite.com

Part two: Module leader's section: Versions

✴**14. Occurrence**:

14a. Primary mode of delivery: Blended

14b. Location of delivery: Scotland

Partner:

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. VLE presence**

Please select **one:**

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

✴**16. LTA approach**

Learning & teaching methods including their alignment to LOs

- The lecture material will present the fundamentals areas of the module, along with practical demonstrations. These will be assessed through graded exercises [LO1 and LO2], with each question broken down into a number of possible answers. A range of multimedia applications has also been developed to show complex methods.
- The coursework will involve the analysis of real-life code cracking and analysis [LO3].
- The module uses a range of networking challenges where students study using the Asecuritysite package, which produces a novel challenge each time the program is run.
- The Asecurity 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 (such as RSA, DES, MD5, and so on), protocols, equipment and software, while covering the key principles of encryption, authentication and intrusion detection systems.

Assessment (formative and summative)

There will be two methods of assessment:

- **Coursework** [50%]. This relates to a coursework on the design, implement and outline evaluation of a prototype of a secure system, based on a range of requirements.
- **Graded exercises** [50%]: This involves two tests which provide a number of questions, which have itemised answers for each of the elements of the question.

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. 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).

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. Student can work at their own pace through the Asecuritysite.com Web site, 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	Lecture	12
Independent learning	Individual learning activities	144
Assessment		20
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):			
	Digital exam Other:	25%	1	1h
	Digital exam Other:	25%	2	1h
	Project Other:	50%	3	18h
	Please select... Other:	%		
	Component subtotal:	100%		
	Component: Assessment Two Enter assessment element(s):			
	Please select... Other:	0%		
	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**.

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

24. Notes for administrative use only

Admin use (for each version)

24. ✴Exemptions awarded from regulations