Module Descriptor

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

1. Module title:	**Advanced Cloud and Network/Live Forensics**

2. SCQF level: 11	**3. SCQF credit value 20**	**4. ECTS credit value: 10**

5. Module code CSN11123

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	

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

This module is relevant to a wide range of students who want to learn new methodologies for enhanced distributed computing. It analyses two main research changes within computing: the move towards distributed infrastructures (Cloud-based and grid computing) and the usage of network/live forensics. The scope of the module will cover all the major Cloud/Virtualised infrastructures including Amazon Web Services and VMWare ESXi.

The module covers an in-depth analysis of data loss protection and detection using a completely virtualised infrastructure, including the coverage of data at-rest, data in-motion, and data in-use. The module will also investigate the key challenges with Cloud and Virtualised Infrastructures, including a focus on security and network/live forensics.

11. Description of module content

The aim of the module is to develop a deep understanding of advanced areas related to security and live/network forensics, with a strong focus on virtualised and Cloud-based environments, that will allow graduates to act professionally in the design, analysis, implementation, and reporting of enhanced software systems, security strategies, and in forensic computing investigations. An outline of the main areas includes:

- **Cloud-based Security Threats, Security Models, Security Evaluation, and Mitigation Strategies.** This involves an in-depth analysis of a range of current cloud-based threats, such as DoS, Botnets, scanning, and so on.
- **Cloud-based System Architectures and Devices**. SoA, Business Continuity, Failover, Secure Architecture, Disaster Recovery, Distributed Storage/Clustering, Load Balancing, SIEM, Virtualised Device Configuration (Firewall/IDS/IPS). Coverage of a range of cloud infrastructures such as Amazon Web Services (S3/EC2); VMWare ESXi/vCenter; Open Nebula; Google Cloud; and Microsoft Azure. Identity infrastructures (OAuth, WS-*).
- **Big Data Storage and Analysis**. Creating large-scale data infrastructure and analysis methods such as Hadoop, security analysis using Big Data, and cross-log analysis (such as Splunk).
- **Performance Evaluation**. Evaluation of cloud-based infrastructures and test frameworks.
- **Cloud-based Cryptography**. Relevant cryptography methods for security-, authentication- and identification-in-the-cloud, including tunnelling, federated identity and secure cloud-based storage.
- **Live Forensics**. Code Analysis, Host/Network Analysis, Malware Analysis, Reverse Engineering. Mobile/x86 architecture, Machine Code Analysis, Vulnerability Analysis, Sandboxed Analysis.
- **Network Forensics**. Advanced Network Protocol Analysis, Advanced Trace Analysis, and Security Threat Network Traces.
- **e-Discovery**. Cloud-based trails for evidence. Cross-correlation, Log analysis and cracking.
- **Data Loss Detection/Prevention.** This part of the module will virtual a complete networked infrastructure in order to investigate the key data loss elements and methods used within Data Loss

Detection/Prevention, including: network/host detection: cryptography protection/detection; and data at-rest, data in-motion, and data in-use.
- **Current Related Research**.

12. Learning Outcomes for module
On completion of this module, students will be able to:
L1: Develop an advanced knowledge of key security/digital forensic principles and methods.
L2: Develop analytical skills related to the key academic principles and practical skills required to understand data loss within a virtualised networked infrastructure.
L3: Research, design, implement, evaluate and critically analyse an advanced system to a given set of security and/or digital forensic requirements, with a focus on virtualised and Cloud-based environments.

13. Indicative References and Reading List
T1: Buchanan WJ, *Advanced Cloud and Virtualisation*, CRC Press, Jan 2015, ISBN 1439880379.
T2: Buchanan WJ, *Introduction to Security and Digital* Forensics, CRC Press, June 2010, 084933568X.
T3: Thomas Erl, Cloud Computing: Concepts, Technology & Architecture, Prentice Hall, 0133387526

Part two: Module leader's section: Versions

✴**14. Occurrence**:
14a. Primary mode of delivery: Blended
14b. Location of delivery: Scotland
Partner: N/A – Edinburgh 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. 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):CSN11124 (DL)

✴**16. LTA approach**

Learning & teaching methods including their alignment to LOs
- The coursework will involve the research, design, implement, evaluate and critically analyse a complex system to a given set of security and/or digital forensic requirements [LO3].
- Full on-line lectures are provided which support deep learning, and with an extensive range of on-line challenges [LO1 and LO2].
- Virtualised cloud infrastructure which implements a corporate infrastructure [LO1, LO2 and LO3]
- Students can download the simulator software at the start of the module, along with an e-Book, teaching pack, and so on. Full on-line support is integrated in the simulator. [LO1 and LO2] The package also contains tests, stimulating challenges, demonstration movies, and automated updates.
- On-line support is given through Skype Messenger and email.

Embedding of employability/ PDP/ scholarship skills
The module uses industry-standard methods, protocols, equipment and software. Along with this the academic and practical skills for advanced security and digital forensics will considerably enhance future employment, as many related industries require both an academic foundation and key practical skills.

Assessment (formative and summative)
There will be two methods of assessment:

- **Coursework** [50%]. This relates to a coursework on the research, design, implementation, evaluation and critical analysis of a complex system to a given set of security and/or digital forensic requirements (LO3).
- **MCQ knowledge-based test** [50%]: This involves two MCQ tests which relate to the fundamental material covered by the core academic material. The results of the tests will be graded, and fed-back to students to indicate their performance (LO1&2).

Research/ teaching linkages

The main research group involved in this area has an excellent foundation in research related to distributed computing, 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, next generation Web infrastructures, 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.

Three new research projects relate to next generation infrastructures for service-oriented systems, including for intelligence frameworks, e-Commerce infrastructures and in health care authentication/authorization (Fan, 2011). The module also uses a state-of-the-art teaching framework, which has been published in educational journals and conferences (Buchanan, 2006). Along with this the research group have developed a lead within teaching within Cloud-based infrastructures (Buchanan, 2011a, 2011b).

Ref:

Buchanan W, *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

Buchanan, W., Macfarlane, R., Flandrin, F., Graves, J., Fan, L., Ekonomou, E., Bose, N., Ludwiniak, R. (2011a). Cloud-based Digital Forensics Evaluation Test (D-FET) Platform. Cyberforensics 2011.

Buchanan, W., Graves, J., Bose, N., Macfarlane, R., Davison, B., Ludwiniak, R. (2011b). Performance and Student Perception Evaluation of Cloud-based Virtualised Security and Digital Forensics Labs. HEA ICS Conference.

Fan, L., Buchanan, W., Thuemmler, C., Lo, O., Khedim, A., Uthmani, O., Lawson, A., Bell, D. (2011). DACAR Platform for eHealth Services Cloud, IEEE Cloud 2011, Washington, USA.

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 virtual images of labs, 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. The service used will also relate to international applications, along with an investigation of local and international customisation.

✴**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	Digital exam Other:	25%	1,2	1 hours
12	Digital exam Other:	25%	1,2	1 hours
15	Project Other:	50%	3	16 hours
	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