

**MODULE SPECIFICATION**

|  |
| --- |
| **Part 1: Information** |
| **Module Title** | Embedded systems security |
| **Module Code** | CY203 | **Level** | 5  |
| **For implementation from** | September 2020  |
| **UWE Credit Rating** | 30 | **ECTS Credit Rating** | 15 |
| **Faculty** | Environment and Technology | **Field** |  |
| **Department** | Computer Science and Creative Technologies |
| **Contributes towards**  | BSc (Hons) Cyber Security Technical Professional Compulsory |
| **Module type:**  | Standard  |
| **Pre-requisites**  | None |
| **Excluded Combinations**  | None  |
| **Co- requisites**  | None  |
| **Module Entry requirements** | None |
|  |
| **Part 2: Description**  |
| page1image12755776This module aims to provide apprentices with an in-depth appreciation of embedded devices and their security. An embedded system is a combination of processor, memory, I/O and the OS that forms a device. Embedded systems get infrequent or never get software updates. They are very many identical devices installed, often in critical facilities and systems. Because of this the devices must be made secure. Delivery will cover modern system architecture, key technologies, and the security implications of implementing these technologies. In addition, essential low-level malware techniques will be examined. Lecture sessions cover the technical knowledge required. Designated practical work is included to ensure that apprentices have absorbed and understood the key principles involved. This module will be based on ensuring that apprentice’s practical skills and knowledge gained in the block release sessions are carried into the workplace to inform their employment and generation of evidence of competency. You will cover: * Architecture of low powered mobile systems
* The nature of security in embedded and network systems
* Networking technologies
* Boot processes, BIOS, file systems and embedded operating systems
* interaction between microprocessor software and signals from sensors, actuators, etc
* exploitation of external environment or software-hardware interface and mitigations that may be employed
* security challenges of embedded systems, for example:
	+ size, power, processor, memory, bandwidth limitations
	+ Internet of Things
* low level mechanisms used by current malware
* machine level instruction set
* reverse engineering techniques
* reverse engineering for malware analysis
* de-obfuscation of obfuscated code
* anti-debugging mechanisms
 |
| **Part 3: Assessment**  |
| **Assessment 1 – Component A** During the college sessions the apprentices will complete a series of tasks in a workbook. These will challenge them to develop independent skills in using and securing embedded systems. **Assessment 2 – Component B** Apprentices will be required to prepare a 30 minute presentation on malware threats, engineering and the techniques required for analysis  |
|  |
| Identify final timetabled piece of assessment (component and element) | Component B1 |
| **% weighting between components A and B** (Standard modules only) | **A:**  | **B**:  |
| **60%** | **40%** |
|  |
| **First Sit** |
| **Component A** (controlled conditions)**Description of each element** | **Element weighting****(as % of component)** |
| 1. Signed off and completed workbook | 100% |
| **Component B** **Description of each element** | **Element weighting****(as % of component)** |
| 1. Presentation (30 minutes) | 100% |
| **Resit (further attendance at taught classes is not required)** |
| **Component A** (controlled conditions)**Description of each element** | **Element weighting(as % of component)** |
| 1. Signed off and completed workbook | 100% |
| **Component B Description of each element** | **Element weighting(as % of component)** |
| 1. Presentation (30 minutes) | 100% |
|  |
| **Part 4: Learning Outcomes & KIS Data** |
| **Learning Outcomes** | On successful completion of this module apprentices will be able to: Understand the characteristics of secure, embedded systems (component A) Develop software for selected embedded devices (component A)Analyse and evaluate security threats and vulnerabilities with regards to embedded systems and identify how these can be mitigated (components A and B) Construct software to interact with the real world and analyse for security exploits (component A)Analyse malware & identify its mechanisms (component B)  |
| **Key Information Sets Information (KIS)****Contact Hours****Total Assessment** |  The table below indicates as a percentage the total assessment of the module which constitutes a;**Written Exam**: Unseen or open book written exam**Coursework**: Written assignment or essay, report, dissertation, portfolio, project or in class test **Practical Exam**: Oral Assessment and/or presentation, practical skills assessment, practical exam (i.e. an exam determining mastery of a technique)  |
| **Reading List** | To be added |

***FOR OFFICE USE ONLY***

|  |  |
| --- | --- |
| **First Approval Date (and panel type)** | *Date of first {panel} approval*  |
| **Revision ASQC Approval Date** *Update this row each time a change goes to ASQC* |  | **Version**  | *1* | *Link to RIA*  |
|  |  |  |
|  |  |  |
|  |  |  |