

# In-Course Assessment Brief

## *Postgraduate Programme Academic Year 2009/2010*

<b>Module:</b>	<b>Building Secure Applications</b>
<b>Assessment Title:</b>	Secure networked application coursework.
<b>Assessment Identifier:</b>	<b>CWK1</b>
<b>School:</b>	CTN
<b>Module Co-ordinator:</b>	Richard Kay
<b>Assessment Details and Deadlines:</b>	See ECMS My Course on the intranet.
<b>Brief Assessment Details</b>	<p>Students will work individually or in pairs either:</p> <ul style="list-style-type: none"><li>i) To develop a secure networked application or</li><li>ii) To install and configure securely a networked application.</li></ul> <p>All students will also write a report providing a record of development or installation/configuration activity and a security analysis of the application developed or installed.</p>

If you should fail this module you will be permitted to be re-assessed on up to three occasions. If you fail to attend or to submit work for re-assessment at the next opportunity you will be deemed to have exhausted one of the opportunities.

## IMPORTANT STATEMENT

**Plagiarism: the presentation of the work of another (from whatever source: book, journal, internet etc) as if it were one's own independent work. This can be anywhere on a continuum ranging from sloppy paraphrasing to verbatim transcription without crediting sources.**

You are advised to refer to the Student Handbook on matters of cheating and plagiarism as they relate to coursework, group assignments, class tests and examinations. Both cheating and plagiarism are totally unacceptable and the University maintains a strict policy against them. It is YOUR responsibility to be aware of this policy and to act accordingly.

The University requires that the following statement is included in all module documents.

*"You are reminded of the University Disciplinary Procedures which refer to cheating. Except where the assessment of an assignment is group-based, the final piece of work which is submitted must be your own work. Close similarity between assignments is likely to lead to an investigation for cheating. It is not advisable to show your completed work to your colleagues or to share and exchange disks.*

*You must also ensure that you acknowledge all sources you have used. Work which is discovered to be the result of collusion or plagiarism will be dealt with under the University's Disciplinary Procedures, and the penalty may involve the loss of academic credits.*

*If you have any doubts about the extent to which you are allowed to collaborate with your colleagues, or the conventions for acknowledging the source you have used, you should first of all consult module documentation and, if still unclear, your module tutor."*

You will be asked to confirm in writing when handing in any piece of assessed work that it is your own by completing the Coursework Submission & Record Form which should be printed from ECMS My-course on <https://mytid.bcu.ac.uk/>.

It is the STUDENT'S responsibility to accurately complete the form and comply with its rules and guidance as described in the student handbook for this academic year.

**Learning Outcomes to be Assessed:****Learning Outcomes to be Assessed:**

a. Contribute towards the development and implementation of a security policy covering the development and use of a distributed application.

b. Be able to investigate weaknesses within an existing distributed application and recommend and implement remediation strategies based on a costs and benefits analysis.

**Assessment Details:**

Students may undertake this assignment either working individually or as a team of 2. When undertaking this assignment as a team of 2, work must be divided intelligently between the 2 students and different areas of agreed responsibility must be clearly indicated in reports submitted.

The project undertaken must be EITHER:

3. A software development project involving development of a networked application, where the data input to, output by and stored within the application will have multiple users and access restrictions based on authentication of users. OR
4. Involve a non-trivial installation and configuration of existing software within a networked application context in order to implement a networked application where the data input to, output by and stored within the application will have multiple users and access restrictions based on authentication of users.

Students working in teams of 2 are required to set more challenging objectives and agree in advance between them a division of effort and investigation.

Students are advised to discuss their initial ideas for project selection with staff and to submit 100-200 words describing the project selected, its objectives and division of work by 23<sup>rd</sup> Feb 2010.

Each student will individually document the technical design of software developed, or the full installation and configuration procedure used. Technical reports may involve diagrams and tables etc, but if entirely textual should involve approximately 2500 words. This report should describe the achievements made in meeting project objectives.

Each student will also write a contextual report concerned with the security analysis of software developed or configurations used, security configurations and options chosen. Any weaknesses identified in the product should be described together with recommendations for remediation. This analysis should also cover the costs and benefits for improvements in the security design of the products developed and/or installed, based on a selection of security requirements. This report may involve diagrams and tables etc, but if entirely textual should involve approximately 2500 words.

**Assessment Criteria:**

See table below

**Table of Assessment Criteria and Associated Grading Criteria**

<b>Assessment Criteria</b> →	<b>1.</b> <b>Technical software design or installation and configuration document (individual report)</b>	<b>2.</b> <b>Selection of appropriately challenging and feasible objectives (group assessment)</b>	<b>3.</b> <b>Progress achieved in meeting objectives selected (group assessment)</b>	<b>4.</b> <b>Context and Analysis (individual report)</b>
<b>Weighting:</b>	<b>40%</b>	<b>15%</b>	<b>15%</b>	<b>30%</b>
<b>Grading Criteria</b>  <b>0 – 29%</b>	No or trivial effort involved in development of or installation/configuration of product, reflected by flimsy report.	Either little or no thought shown concerning feasibility or trivial objectives. No originality demonstrated in project selection	Either a trivial project or little or no progress demonstrated.	Little or no evidence of systematic or analytical thought applied to trivial and confused report.
<b>30 – 39%</b>	Minor effort and report too weak to pass.	Insufficient thought concerning feasibility or too limited objectives. Little evidence of originality in project selection.	Minor progress in connection with weak objectives or trivial progress in connection with more reasonable objectives.	Disorganised and weak report.
<b>40 – 49%</b>	Some effort in design or installation/configuration reported, but substantial gaps in approach.	Some objectives relevant to requirement but lacking in judgement and initiative.	Some progress but with substantial shortcomings.	Just adequate report showing limited evidence of security analysis
<b>50 – 59%</b>	Fair effort reflected in software development or in installation/configuration or development activity reported. Some gaps in approach.	Reasonable objectives relevant to requirement. Some, but incomplete understanding of requirements. Some but limited evidence of initiative demonstrated.	Moderate progress achieved, but with some shortcomings. Evidence of achievement not entirely satisfactory.	Fair report demonstrating some knowledge and analysis but with gaps in security knowledge or application.
<b>60 – 69%</b>	Good effort at development or installation/configuration, but lacking full coverage.	Sound objectives and understanding of requirements & good initiative shown, but objectives not enough to achieve an excellent standard or project feasibility questionable.	Good progress achieved and clearly demonstrated but not of an excellent standard.	Good report demonstrating some effort, understanding and analysis of all main security issues, but with gaps.
<b>70+%</b>	Excellent effort demonstrated in achieving all of a challenging range of objectives set.	Suitably challenging objectives set with sound judgement applied to feasible project selection.	Excellent progress achieved and clearly demonstrated.	Excellent report demonstrating thorough analysis of all relevant security issues.