

In-Course Assessment Brief

Undergraduate Programme Academic Year 2009/2010

Module:	Security Systems Theory UG2
Assignment Title :	Security Investigation and Report.
Assignment Identifier:	1.2
School:	CTN
Module Co-ordinator:	Richard Kay
Set Date:	
Submission Deadline:	See ECMS My Course on the intranet for details
Assessment Weighting:	
Submission Method:	Submitted through the IT Helpdesk on level 3.
Nominal time to complete this assignment:	45 Hours
Assessment Details and Deadlines	See ECMS My Course on the intranet.
Brief Assessment Details	Students will select and register a unique mini-project either from a choice made available through the module website, or will determine aims and objectives themselves and request registration of a project of similar relevance, interest and difficulty. A fair procedure giving all students an equal chance of registering the most popular projects will be implemented on a first come, first served basis. Once the project is registered, students will carry out a technical investigation into the security subject chosen, and will write a report.

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

Demonstrate understanding of principles and technologies for engineering security systems. Demonstrate understanding of security system protocols with attention to legal and ethical requirements. Demonstrate understanding of the techniques used for monitoring, evaluation, risk assessment and management of security systems applied to networks, access systems and communications. Specify solutions using appropriate techniques. Demonstrate understanding of the scope and capabilities of cryptographic techniques.

Assessment Details:

For details of mini project availability and to register one, please see the module website:
<http://bcu.copsewood.net/tic/sectheory>

Students are required to choose a mini project from the selection available on the module website and register this using the web form to be provided. Registration will commence at a date and time to be announced in advance. Students may also choose their own titles for projects concerning a security investigation and report, but aims and objectives of these must be discussed and agreed with the module coordinator in advance of registration, to ensure a suitable scope and investigation target has been defined, and that this is of a similar level of difficulty and relevance to the module content, and that the topic is different from investigations registered by other students. Options for two students who want to investigate the same topic exist, but they must both agree with each other to collaborate on a deeper or wider investigation between themselves, and the additional scope and division of work must be documented and agreed with the module coordinator. In all cases the first student to register their student ID against a topic name on the module website reserves this project title and other students must choose different projects.

A student who chooses and registers a project topic without proper consideration and who subsequently decides they want to change their topic, will lose marks on grounds of poor rationale, lack of initiative and lack of problem solving. Failure to complete registered project choice also unfairly reduces the choices of more capable students by excluding them from investigating the same subject. Students uncertain as to their preferred topic are therefore required to discuss options in advance with the module coordinator to ensure they understand the availability and suitability of appropriate information and technical resources before registering a topic. These discussions are normally expected to occur during timetabled tutorial sessions.

Deliverables

Technical Investigation and report section

Each student will carry out a technical investigation into the security subject chosen. The nature of this will very much depend upon the mini project topic selected. This investigation might involve a review of the mathematical or legislative issues chosen, it might require development of a small program to carry out automated testing of another program or analysis of its log files. The investigation might require installation, configuration and testing of a program. It might result in a user guide or a howto guide. The technical investigation will result in appropriate report sections, which should describe the reasoning behind all decisions taken, as well as the technical investigation itself and the results obtained from this.

Where collaboration involving 2 students is part of a registered project description, it is accepted

that up to 50% of the technical investigation content of this may be submitted as a group report, i.e. as information which may be included within both reports. However, this part and the individual investigation must be clearly marked. This technical investigation must be appropriately documented as part of the report, the additional requirements of which are described below. The nature of the technical report section will vary considerably depending upon the security topic and method of investigation chosen. If it is submitted entirely in writing, 2000 words are suggested for this report part, but the use of screenshots, source listings of student written programs or configuration edits, tabulated test results and diagrams etc. might be appropriate for part of this technical content.

Context and conclusions report section (individual deliverable)

In addition to the sections within the report describing the details of the technical investigation, each student will in addition individually write a 2000 word report summarising:

- a. The rationale for selection of key information resources (books, on-line forums, web information resources) used. The rationale for any investigation choices made.
- b. The context of the security issues addressed, the results of other relevant research carried out by other parties into the security subject, target or issue covered.
- c. The individual discoveries and conclusions resulting from the project undertaken.

Assessment Criteria:

The table below describes the basis on which marks will be given.

Table of Assessment Criteria and Associated Grading Criteria

Assessment Criteria	1. Technical investigation and report section	2. Rationale for experiments carried out and information resources selected.	3. Problems solved, Initiative and originality demonstrated	4. Context and conclusions report
Weighting:	35%	15%	15%	35%
Grading Criteria 0 – 29%	Little evidence that any real investigation was carried out. Entirely derivative work.	No evidence of thought applied to selection of information resources used. Little or no technical work done.	No problems solved. Trivial degree of initiative. Failure to adhere to project choice.	Report not written or trivial and very weak. Little evidence of thought concerning project documentation.
30 – 39%	Weak effort involving a very limited and very derivative investigation.	Very weak effort at choosing information resources or selecting technical approaches.	Minor evidence of initiative or originality of approach. Unclear whether any problems solved	Weak report not demonstrating consistent evidence of thought applied to project.
40 – 49%	Enough of an investigation to pass but still very limited and with large gaps in approach.	Effort at selecting information used and making technical choices but limited and weak.	Some evidence of initiative taken or originality of approach. Minor problems solved	Passable report but only just. Some awareness of security issues covered but this is limited.
50 – 59%	Fair investigation undertaken but with significant gaps.	Some limited success in finding and selecting suitable information resources and designing or understanding relevant experiments.	Fair degree of initiative taken or originality in approaching task at hand. Some problems tackled.	Fair report demonstrating an awareness of security issues, but with significant gaps.
60 – 69%	Good quality investigation including primary and secondary resources but with gaps evident.	Good rationale for all main information sources selected and technical work carried out.	Strong initiative and originality and problem solving demonstrated but with limitations in approach.	Thoughtful and critical report demonstrating good awareness of security issues but with shortcomings.
70+%	Full investigation involving all feasible primary approaches and relevant secondary resources.	Excellent research into information sources and clear and solid rationale behind technical work done.	Excellent degree of initiative and a unique, independent and fully thought through approach. Difficult problems overcome.	Deeply thoughtful and fully critical report demonstrating an excellent standard of security awareness.