Research Guide

Introduction

Because this module is part of a Masters programme, it is important that it includes opportunities for you to develop skills that are characteristic of masters-level study. In particular, a key skill for all masters students to develop is that of engaging with scientific literature and being able to critically review it. You should be able to:

- Identify key developments in a given area of study
- Critically analyse them to identify key limitations, and
- Devise and explain ways of improving on prior scientific results.

It is, however, a good idea to research information provided by others. This can include documentation provided by manufacturers, standards bodies, academic journals, and experts sharing their knowledge via websites, blogs, wikis, etc. There is a rich source of information available, but be cautious; quantity and quality are not necessarily the same thing. On this basis it is a good idea to take a planned approach to researching and to use some form of electronic journal to help you assimilate the information found. This document will help you get started with this task, mainly by drawing upon the extensive resources provided by the ITB Library, resources that are made available to you as a student of BN518.

2 Academic skills

2.1 Use of concepts
Concepts (including frameworks, theories and models) are tools that will help you to structure your thinking, but only if used appropriately.

2.2 Finding papers
This is a postgraduate-level module rather than a piece of directed training. As such, you are expected to be able to read and understand academic publications related to the subject you are studying. The advantage of this approach is that it helps you to stay abreast of further developments in the field if you wish to do so (training does not usually have this benefit).

When you are finding papers on a particular theme or topic, you should bear in mind the following points.
- You are expected to find papers that appear in peer-reviewed journals or conferences. You might like to follow these links to find out what a peer review means:http://en.wikipedia.org/wiki/Peer_review, http://www.linfo.org/peer_review.html.
- Papers that appear in databases such as IEEE, InfoTrac and Science Direct are peer-reviewed. These are available in ITB's digital library, which can be found at http://www.blanchlib.itb.ie/screens/databases.html
- Papers from websites will be suitable provided that they appear in peer-reviewed online journals. For example, this paper is online but is from a refereedv(peer-reviewed)
  journal: http://www.ascilite.org.au/ajet/ajet20/williams.html. However, papers that are written as experience stories and that express personal views or

perspectives are not suitable. For example, referring to content from http://www.agilemodeling.com/ would not be suitable. Of course, you can always read such articles to enhance your understanding, but you shouldn't use them in your answer to research questions.

- Usually you will be expected to find 'recent' papers, i.e. ones published in the past five to ten years. The exceptions to this 'rule' are the 'seminal' papers, i.e. papers that present a new idea that forms the basis for later work.

- You need to use a standard format for referring to the papers you have found, normally called Harvard referencing (see Section 3.5). An excellent resource can be found at https://ilrb.cf.ac.uk/citingreferences/tutorial/index.html that gives guidance on how you may cite papers and other resources/sources in your work.

2.3 Analytical styles and techniques

There is a range of analytical styles and techniques that may be used to communicate your ideas. These include description and narration, comparison and contrast, interpretation, explanation, evaluation (or assessment) and synthesis.

Network Security encourages and values a critical perspective, so you should look in particular for opportunities for evaluation and synthesis when answering research questions.

Some different analytical styles and techniques are described below.
- *Compare and contrast*

To compare means to identify, at the level of description, common features of two or more things; to contrast means to identify differences. Comparing and contrasting is often the basis for identifying important dimensions of alternatives. The phrase 'compare and contrast' is conventionally meant to encourage you to perform a comparison of two (or more) views on a subject by identifying, on the one hand, the similarities in the viewpoints presented and, on the other hand, the differences between them in such a way that the comparison shows you have understood the two viewpoints. Thus 'compare and contrast' often provides a basis for objectively preferring one thing among others, e.g. choosing one solution to a problem among a range of alternatives. Tables are often a useful means of documenting comparisons.

- *Critical summary*

A critical summary is a summary of the essential points of a paper in which you identify the author's opinions and comment critically upon them. This does not mean you must say why the author's opinions are wrong; you may agree with them. It means you should examine the evidence that the author provides to support his or her arguments and say how well you think the views are supported. See also Section 2.3.

- *Description and narration*

A description outlines the main attributes or features of something. Narrative does the same, but usually in relation to some time-related framework. There is always an important place for description when seeking to communicate, so most assessments will contain descriptive material.

- *Evaluation*

Evaluation normally involves the assessment of something against a set of criteria. Sometimes the criteria are readily available as an established ideal or benchmark; at

other times, determining – with justification – the appropriate criteria to use can also feature as part of evaluation. See also Section 2.3.

- *Explanation*

Explanation seeks to identify causes behind what we observe. As such, it often refers to theories and underlying principles or natural laws. Some aspects of some questions will draw upon bodies of theory, e.g. with respect to social, psychological and economic behaviour.

- *Interpretation*

Interpretation often involves examining something in a specific context, where the context determines what is relevant or meaningful. Much of the work in your Assignments requires you to take account of what is appropriate for a given scenario. The relevance and value of concepts, techniques and solutions will often be interpreted in relation to the needs of that scenario.

- *Synthesis*

Synthesis involves bringing together more than one body of evidence, or different perspectives or viewpoints. It often involves an attempt to arrive at a unified overview or perspective through a process of integration and/or abstraction.

2.4 Critically evaluating a paper and summarising it

Research is not something done in isolation. It is a discourse between researchers, each providing evidence and argument that contributes to knowledge and understanding, and each critiquing the available evidence. Research is about the articulation and analysis of phenomena observed and investigated through a variety of techniques. It's about 'making sense' of the world: not just describing it, but analysing and explaining it, and from those explanations making testable predictions about it. As more evidence is presented, earlier analysis and explanations are re-evaluated. Knowledge claims can be small but still have a role in the research discourse.

Evaluating a paper

Evaluation normally involves the assessment of something against a set of criteria. Sometimes the criteria are readily available as an established ideal or benchmark; at other times, determining – with justification – the appropriate criteria to use can also feature as part of evaluation. Evaluating a paper and the research it presents involves taking a critical approach to what the authors write. It is wisely said that 'not all that is written is true'. Authors (and researchers) vary, from the excellent to the abominable. Even the best make mistakes. And, in turn, mistakes range from the minor to the horrendous. How can you evaluate whether a paper is good, bad or indifferent?

First, apply external criteria: you need to compare what an author says with everything else you know about the subject so far and also with your own experiences. Does the author make sense when compared with what others have written and what you know? Is the question being addressed significant for the subject area, and is the work original (as far as you know)?

Then apply internal criteria – those that exist within a particular piece of writing. Here is a list of possible questions to ask about the paper:
- Examine the author's methods (that he or she has applied to answer the question) as he or she describes them. Do they appear to be sound methods? Were they rigorously applied? Were they effective methods in this situation?
- Does the author appear to be impartial?

- Are there ambiguities, contradictions or inconsistencies in what the author writes?
- Are the author's assumptions made clear, or has mention of them been omitted?
- Are the assumptions, if stated, acceptable to you given your knowledge of the topic?
- Does the author provide evidence to support the arguments being made? How well do you think the views and opinions of the author are supported?

If, when reading a paper as part of a CA question, you come across a term or idea that is poorly explained or contradictory to what you have learned from the module (or other papers), make sure to highlight and discuss this as part of your answer.

Critically summarising a paper
A critical summary requires you to assess the evidence that is available, either within the paper itself or from the other sources you are referencing (including your own experience), to either support or contradict the points being made in the paper. Any opinion you put forward must be supported by evidence from other sources, except where you believe that the paper is either inconsistent or contradictory, or where you believe that the paper provides evidence to support the argument being presented. In each of these cases, you should cite the relevant parts of the paper itself. A critical summary involves articulating:
- the importance of the question (why is it worth asking?)
- the significance of the findings to the area of information security (why do they matter?) – for example, do the findings contribute towards improvement of the information security practices of an organisation; is it a 'new' technique for the assessment of information security risk; do the findings propose a better way ('better' than the research previously published and that you are aware of) to identify errors in firewall configurations, and so on
- the implications for theory (do the findings help to explain the phenomenon under study and make predictions about it?)
- the limitations to generalisation (are the findings true only for the particular example studied, or is there reason to believe they will apply in other cases?)
- whether the paper provides a significant contribution to the subject area. 'Making a significant contribution' means 'adding to knowledge' or 'contributing to the discourse' – that is, providing evidence to substantiate a conclusion that's worth making.

2.5 Argument
A key skill is the ability to build a coherent and consistent argument (or line of reasoning). This should draw on the conclusions from your analyses and on evidence from all the appropriate module materials, from your discussion and consideration of appropriate theories and concepts, and from practical activities, examples or cases. You should avoid unfounded assertions and cite your sources appropriately (see Section 2.5).

Ensure that assumptions are expressed and justified, appraise the validity and usefulness of concepts you use, consider counter-arguments, and identify strong and weak parts of any argument. For example:
- assertions about the value of a given information security policy may lack supporting evidence, or quoted opinions may be at odds

- theories or concepts may contradict each other
- you may be aware of empirical research findings that do not agree with theoretical propositions
- a theoretical framework may fail to provide a good fit with empirical findings, indicating limits to its applicability.

2.6 Citations
Every time you make use of material from websites, books or other sources in your assignments, you should provide a citation in the body of the assignment and a full reference at the end. The purpose of an accurate citation is to allow a reader access to the materials upon which you have drawn. A reader will then be able to form their own critical view of your work and of the implications you have drawn from it. From the perspective of your own learning, accurate citations allow you to identify and access work that you have found useful during your studies. The use of other people's work also requires proper acknowledgement. Correct citation is therefore an issue of good practice in all forms of technical writing. Failure to incorporate proper citation into your Assignments could result in the loss of the question.

Citations should generally be made using the Harvard system. To cite a piece of work under the Harvard system, it is sufficient to give the author's family name and date of publication, for example:
- Bloggs (1990) claims that the Earth is flat

or
- It has been suggested that the Earth is flat (Bloggs, 1990).

When a work has two authors, both should be named. For example:
- Bloggs and Jones (1995).

Three or more authors can be shortened in the text using 'et al'. For example:
- Bloggs et al. (1996).

If you quote directly from a source, you should give the page number (or some other appropriate reference, such as a clause number) for the actual text you are using. For example:
- 'The earth is flat' (Bloggs, 1990, p. 2).

Full details of the works cited should be given in the list of references at the end of the Assignment.

The secret of efficiency in citation is to record the reference accurately, and in full, at the time your notes are made. Chasing up poorly recorded, half-remembered sources at the last minute can cost valuable time as a deadline approaches (so speaks the voice of bitter experience!). You should also be careful to cite primary and not secondary sources: for example, if citing material in the CISSP Book that itself relates to another source, cite the other source directly and not the CISSP Book.