A Proposed Australian Industrial Control System Security Curriculum

Ernest Foo
Queensland University of Technology
e.foo@qut.edu.au

Mark Branagan
Queensland University of Technology
m.branagan@qut.edu.au

Thomas Morris
Mississippi State University
morris@ece.msstate.edu

Abstract

The security of industrial control systems in critical infrastructure is a concern for the Australian government and other nations. There is a need to provide local Australian training and education for both control system engineers and information technology professionals. This paper proposes a postgraduate curriculum of four courses to provide knowledge and skills to protect critical infrastructure industrial control systems. Our curriculum is unique in that it provides security awareness but also the advanced skills required for security specialists in this area. We are aware that in the Australian context there is a cultural gap between the thinking of control system engineers who are responsible for maintaining and designing critical infrastructure and information technology professionals who are responsible for protecting these systems from cyber attacks. Our curriculum aims to bridge this gap by providing theoretical and practical exercises that will raise the awareness and preparedness of both groups of professionals.

1. Introduction

Industrial control systems are used to automate systems that control factories, electricity substations, transportation systems, sewerage and drinking water systems. All of these systems form the critical infrastructure on which modern Australian society depends. Industrial control systems were designed as isolated communication networks. However, with the advent of cheaper and more efficient information communication technologies and the accessibility of the Internet, these systems have increasingly been connected to corporate information networks. The advantage for doing this for organizations is that it allows operators to monitor and control the system from a central corporate office. Vendors also benefit, as they are able to maintain equipment remotely. The danger of connecting industrial control systems to the corporate network is that these networks are often connected to the Internet possibly exposing them to malicious attackers. Unlike information technology systems industrial control systems are not as prepared to defend against cyber attacks.

The Australian government and other nations around the world have identified cyber attacks against as a major issue to national security [1]. A successful cyber attack has the ability to disrupt and even damage critical infrastructure.

The research community has exposed numerous vulnerabilities in industrial control systems [2,3,4] and government organizations have proposed numerous solutions for improving cyber security measures in control systems [5,6]. However there is a need to provide training and education. The purpose of this paper is to propose a security curriculum for professionals working in the control system industry as well as for graduates hoping to enter the field.

In the control system industry there are two groups of professionals that are involved with the industrial control systems that are the potential targets of attack. The first group is the control system engineers who are responsible for the maintenance and design of the control systems that make up the critical infrastructure. The second group is the information technology professionals who are responsible for maintaining and administering data information and communication networks that make up corporate networks for critical infrastructure providers.

In Australia, there is a cultural gap between the thinking of control system engineers, who are responsible for the efficient and reliable operation of the control systems, and information technology professionals, who are often responsible for protecting these systems from cyber attacks. This paper proposes a postgraduate level curriculum that aims to bridge this gap by providing theoretical and practical exercises that will raise the awareness of issues facing both groups of professionals. This curriculum is especially focused on providing education and local training for Australian conditions. The cost of travelling overseas to undertake this kind of training is prohibitive. A locally offered course will minimize expenses and maximize opportunities for operators to gain critical...
education in this area. Hopefully providing an improvement to the preparedness of Australian infrastructure to withstand cyber attacks.

Up until this year the best opportunity available to Australian operators of critical industrial controls systems for security training has been to attend training provided by the Idaho National Laboratories (INL) in the US. The Australian government has subsidized attendance at this training for selected attendees. While this training is valuable it is limited, from an Australian perspective, in a number of respects. It is not a continuing program and the length of time available limits the areas that can be covered. Further it is unlikely that this training will be available for all Australian operators who would benefit from attending. Ideally the broader aim of providing industrial control systems security training would be to build an awareness and skills base across the industry. Locally based training also allows for the inclusion of more specific local concerns, which may not feature in the INL training. Having a local training base also allows the training to cover a broader range of topics and to delve more deeply into them. The authors do not see the local training course as existing in isolation. Rather over time it would seem vital to establish connections with existing training programs such as INL and Mississippi State University.

Creating a local training program also has one other important benefit. The proposed curriculum in this paper is intended for continuing professional education or service training. However, having the training locally based allows for the program to be further developed into a university level program.

This paper is divided into the following sections. Section 2 will describe our approach to teaching and learning for the proposed curriculum. Section 3 will describe the four courses in the curriculum in detail. Section 4 describes the laboratory setup for the practical components of the course. In section 5 we briefly examine previous work in security curriculums and discuss how our approach extends this work. Finally in section 6 we discuss the impact of the curriculum in Australia and conclude the paper.

2. Approach to Teaching and Learning

This curriculum is aimed primarily at postgraduate students. However, it is possible to adapt the course for graduates. It is expected though that the majority of students undertaking the proposed curriculum will either be control system engineers or information security professionals. The aim of this course is to provide students with a flexible set of skills that will provide them with the ability to adapt and adjust to the changing threat and vulnerability environment they will face in their day-to-day work.

For most of the courses we endeavor to ensure that there are three types of session. The intent is to provide a theoretical basis for the material, reinforce this with practical application and finally to encourage students to integrate the learning by actively reflecting on the sessions.

The first session is a lecture type session where students are introduced to the theoretical aspects of the material. It is important the students understand what is happening in terms of where issues fit in the bigger picture. Often, cyber security training courses concentrate on particular vulnerabilities without teaching the background theory. This makes it difficult for students to adapt when faced with a new attack or other scenario.

The second session is a practical hands-on exercise relevant to the topic. Some courses provide only theory or lecture based courses. These are good for awareness issues, but it is not until students successfully complete a hands-on exercise that the impact of the security issue hits home. The use of complex full system hands-on exercises such as a red team blue team exercise is particularly good at providing an impact to the student.

Finally the third session occurs after the practical session and we call it the debrief session. In this session the course instructor will encourage students to discuss the impact of the previous exercise and relate it to their previous experiences in industry. These open discussion sessions allow students to share their insights with each other. Ideally course instructors arrange for a break between the practical session and the debrief session. This is to allow students to reflect internally and synthesize the application of the hands on exercise that they have just completed. We have found in previously delivered cyber security courses that the debrief sessions are often described by students as the most useful parts of the course.

Classes are to be conducted in consecutive full day instruction sessions. The decision to deliver classes in this manner is to fit in with full time employed students. However as the curriculum matures it is expected that the courses will be delivered over a normal semester period.

The advanced courses described in this curriculum involve postgraduate level assessment. Students are able to apply for credit towards a masters or graduate certificate award on the completion of these courses.
3. The SCADA Security Curriculum

The philosophy of the course is to provide theoretical and practical instruction for specific roles dealing with cyber attacks in industrial control systems.

The SCADA Security Curriculum consists of four courses that vary in length from one to five days of intensive instruction. The intent is for students to be able to undertake courses in any order except for an initial general awareness short course. It will be highly recommended that this course be undertaken first by all students.

The Control Systems Security Introductory Awareness course is for operators, managers and information technology staff associated with industrial control systems. This course will provide general background information on security issues related to industrial control systems.

The Vulnerability Analysis and System Audit course is aimed at students who are responsible for managing and administering industrial control systems. It will cover the knowledge and skills required for analyzing and auditing existing systems.

The Penetration Testing course is aimed at students who plan on becoming security professionals who will be testing systems to ensure that they are safe from cyber attack. This course is also important for managers and administrators of these systems so they know what to expect when they employ Penetration Testers to examine their systems.

The Forensic analysis and Incident response course is aimed at digital investigators who respond and analyze industrial systems after an incident has been detected. This course is also important for managers and administrators, as it will provide knowledge required to enable forensic readiness in an industrial control system.

3.1 Introductory Awareness Course

The first course in the curriculum is a one-day introductory course that has four main aims. Firstly, to raise awareness of information security issues in general and how they relate to control systems in particular. Secondly, to raise awareness of issues within control systems that IT professionals may not be aware of, such as the need to maintain low latencies, real time requirements and reliability requirements. Thirdly, the course aims to raise awareness, in control system engineers, of the dangers of cyber attacks and the capabilities of attackers in this area. Finally, the course will raise awareness of the particular requirements of deploying information security remediation in the control systems arena.

This course is mainly delivered through instructor led discussions and information sessions. Proposed topics in the course include:

- Introduction to Cyber Security
- Introduction to Industrial Control Systems
- Information Security in Industrial Control Systems
- Attacks on Industrial Control Systems
- Methods for Protecting Control Systems
- Practical Demonstration

The first part of this course introduces the students to case studies of a number of well-documented incidents that have occurred in recent times including the Stuxnet attack on Iranian nuclear facilities [4]. Students will be encouraged to discuss how to identify critical infrastructure information networks and systems. They will also discuss what is defined as an attack on these systems.

The course will provide some basic technical knowledge on selected vulnerabilities that have been exposed by ICS-Cert.

The final session of the day involves a demonstration of a successful attack on an industrial control system that is constructed in our laboratory. The instructors demonstrate how an attacker can access the corporate network externally through an incorrectly configured firewall. After accessing the corporate network the demonstration moves on to show how attackers can then gain access to the control network and view control system data and manipulate the control system itself.

3.2 Vulnerability Analysis and System Audit

The Vulnerability Analysis and System Audit course is an advanced intensive five-day course. The aim of the course is to introduce students to vulnerability analysis and security audits in Industrial Control systems. As a result of completing this course the students should have an understanding of the process that needs to be undertaken to conduct an audit and the practical skills to apply this process to industrial control systems. Students will also gain practical experience with defending industrial control systems from attacks.

Instructors in this course present theory through lecture sessions, but the course also involves four to five practical exercises as well as instructor led discussions. Proposed topics for the course include:

- Standards for Security Audit and Vulnerability Analysis
- Security Governance, Policy and Management
- Classification of Information and Control System Resources
• Threats to Information and Control Systems
• Strategies for dealing with attacks in information and control systems
• Processes for minimizing damage in information and control systems
• Final Exercise - Defend an Industrial Control System

This course begins by providing the student with an overview of vulnerability assessment and how security audit standards have been developed in the information security arena. We then look at how existing security audit standards and methodologies can be applied to industrial control systems. Threats common to both traditional information systems and to industrial control systems will be considered. Students will be introduced to practical strategies and tools for hardening and defending both computer networks and industrial control systems. Special emphasis will be given to areas of commonality.

On the final day of the course students participate in an eight-hour team exercise where they are appointed the role of defending a complex corporate and industrial control system configured in our laboratory. Students will have to apply skills they have acquired in vulnerability assessment and auditing to implement defenses for the network.

Assessment for this course involves a written report covering the final exercise and the discussion workshops.

3.3 Penetration Testing of Industrial Control Systems

The Penetration Testing will also be undertaken as an advanced intensive five-day course. The aim of this course is to introduce students to the process of penetration testing in industrial control systems. This course emphasizes the active process of penetration testing rather than the more passive audit activity covered in the previous course. After completing this course students will be familiar with some tools and techniques used by penetration testers. Students will understand how to adapt these techniques to industrial control systems. Emphasis will be given to the safety of such activities and the special considerations that must be made to undertake any penetration testing on potentially critical control systems. This course will emphasize the implementation of mitigation strategies for the vulnerabilities discussed. The course is focused on developing a useful approach to penetration testing rather than on the development of exploits. Therefore, ‘known’ vulnerabilities and attacks would be the preferred techniques.

As with the previous vulnerability analysis course, this course will consist of theory, practical and discussion sessions. Proposed topics for this course include:

• Introduction to Penetration Testing Methodologies
• Network Discovery Techniques
• Network Vulnerabilities and Attacks
• Attack Tools and Scanners
• Network Exploitation
• Network Defense Techniques
• Common Industrial Control System Vulnerabilities
• Final Exercise - Penetration Test of an Industrial Control System

This course starts by introducing the role of penetration testing in the information security industry and in industrial control systems. The course would cover education in traditional penetration techniques such as network discovery and the theory and practice of exploiting host and network vulnerabilities. For each of these topics we also discuss issues unique to industrial control systems. There would be special emphasis on exploiting vulnerabilities in corporate networks to ‘piggyback’ to the actual control systems. Aside from the actual education on penetration testing this would help in highlighting the importance of considering the interconnectedness of the corporate and control systems for security.

The final day of the course consists of an eight-hour exercise where student teams are tasked with conducting a penetration test on a prepared control system configured in our laboratory. Students must attempt to gain access to the control system through a corporate network or some other back door and disrupt the control system process. Students will have to apply the penetration testing skills they have acquired in the previous sessions.

The laboratory environment will be configured with a known set of vulnerabilities in order to aid in assessment and the controllability of the exercise. Students will be provided with a profile of the organization on which they are nominally running the penetration test in order to allow them to frame their recommendations realistically.

Assessment for this course includes a written penetration tester’s report covering the final exercise. The report must detail the steps taken to exploit vulnerabilities in the system and the results of these exploits. The majority of the weighting for the report will be for recommendations on how to mitigate the attacks found in the system. These recommendations will have to take into account the profile of the organization that has been provided to students. The emphasis will be on creation of a realistic set of recommendations according to the profile.
Details of this course outline are included as an appendix.

3.4 Forensic Analysis and Incident Response

The Forensic Analysis and Incident Response course is the final five-day advanced course in the curriculum. The other courses in the curriculum are designed to be pre incident, activities that can be undertaken before an incident occurs to help minimize the likelihood of an occurrence. This course is designed to provide insight into activities that can be undertaken once an incident has begun and or after an incident has occurred. We are unaware of any courses that offer these topics applied to industrial control systems. Students who complete this course will have a practical understanding of the digital forensic investigation process and how it can be applied to industrial control systems. Students will also have an applied knowledge of incident response procedures and planning processes.

Proposed topics for the course include:
- Introduction to Digital Forensic Investigations
- Digital Forensic Analysis Tools and Techniques
- Live Forensics
- Forensic Readiness in Industrial Control Systems
- Incident Response Planning
- Identification of incidents
- Containment of incidents
- Recovery Processes
- Final Exercise - Incident Analysis

This course has two main topics. The first topic is forensic analysis of industrial control system. Students will initially be introduced to the standard digital investigation process and practical exercises will provide experience with standard digital forensic analysis tools. However, in industrial control systems that are part of critical infrastructure, there are likely to be constraints on the means by which evidence can be collected. Standard digital forensic practices require systems to be fully taken offline to conduct analysis and this will probably not be possible for critical infrastructure. Therefore, this course will also cover live digital forensic techniques and forensic readiness in industrial control systems. The second topic that is covered is incident response. Students are introduced to this topic in terms of the traditional incident response process for information systems, but instructors also discuss issues unique to industrial control systems.

The final day of the course consists of an eight-hour team exercise where students role-play forensic investigators who are asked to examine a control system which has been configured in our laboratory. Course instructors play the role of control system owners. For this scenario there has been a suspected incident involving the control system and the students must investigate and collect evidence. Students are also tasked with designing an incident response process for the system after taking into account the findings of their investigation.

This course could potentially be extended to include a ‘live’ incident response exercise. For this exercise students would be in charge of a control system in the lab. Instructors would initiate an incident and the students would be required to respond in real time to the incident as it unfolds.

Assessment for this course includes a written report to the owners of the system describing any evidence that was found of a security incident and how it was found. Students must also submit their recommended incident response plan.

4. Laboratory Facilities

Practical exercises play a key part in the security curriculum for industrial control systems. The equipment in the laboratories must reflect equipment that is found in the field. However, we are restricted by cost and physical space.

Our laboratory consists of a number of industrial Programmable Logic Controllers (PLC), a Dell R710 server with VMware ESXi installed and various network routers and switches.

Figure 1. National Instruments Water Reservoir Simulator

The laboratory also contains several control process simulators. These control process simulators are small-scale tabletop models of a control process controlled by a PLC. The first of these simulators is a water reservoir simulator containing two water tanks run by a National Instruments CompactRIO device as
shown in Figure 1. This simulator contains a pump, a flow control valves and a heating element as well as level, pressure and temperature sensors. All of these devices are monitored and controlled from a PC running a HMI written in Labview. The simulator has Ethernet connectivity allowing us to integrate it into a broader critical infrastructure simulation. Instructors will use the National Instruments simulator during our demonstrations in the introductory awareness course and various practical exercises during the advanced courses.

![Figure 2. Water Reservoir, Pipeline, Smart Meter and Conveyor Laboratory Simulators](image)

There are four other simulators in the laboratory as seen in Figure 2. The simulators model a water reservoir system, a pressurized pipeline, a conveyor belt system and a smart meter system with meter and base station. The smart meter simulator monitors load from a number of attached electrical appliances and light bulbs. A Siemens S7-300 PLC controls the smart meter simulator and acts as a central controller for the other three simulators. The other simulators are controlled by Siemens S7-1200 PLCs. All of these simulators are flexible enough to be connected to a single control system or can represent separate systems depending on the exercise being conducted. These simulators can once again be linked into a wider critical infrastructure simulation.

The Dell R710 server is installed with VMware ESXi virtualization software. The Dell server with 24 virtual processors and 128 Gb of RAM is used to create up to five virtual networks with over ten virtual machines in each. The Dell server is used extensively in the practical exercises and the virtual networks are used to simulate corporate networks in the final day exercise of the three advanced courses. The Dell server allows access from the laboratory PCs through an openvpn server. This allows us to enable access to our laboratory server from other computer laboratories on and off campus.

The entire laboratory has a patching and switching infrastructure that allows it to be networked in various ways allowing a flexible combination of hardware and virtual machines. The laboratory can be configured so that, for example, students are able to access the simulators via the virtual networks enabled on the server. This effectively simulates the corporate network to control system connection. Various dual homed PCs can be configured to act as HMIs for the simulators and PLCs. The network infrastructure also allows for connection of other devices and services such as traffic monitoring equipment and so on. By use of a combination of virtual and hardware devices complex control systems infrastructures can be configured and simulated.

As well as the simulators, the laboratory contains various trainer PLCs from other manufacturers such as DirectLOGIC, Allan Bradley, and Mitsubishi. We will use these PLCs to develop further training exercises and research activities. The trainer PLCs can also be integrated into the simulated control system infrastructures allowing us to increase the complexity of the simulated infrastructure.

### 5. Previous Work

The development of security curriculums is not new. For the last ten years universities and training organizations have provided practical security courses to students with varying levels of success [7,8]. Cyber security courses that include industrial control systems are also not new [9,10]. For example, the Department of Homeland Security provides a famous course from the Idaho National Laboratories.

While there have been a number of proposed critical infrastructure cyber security curriculums the content of these programs has been mainly to address awareness issues in industry.

There has also been a number of SCADA security testbeds proposed [11,12], however these testbeds have been developed for research purposes. Our testbed is also capable of conducting research in the area of industrial control system security. However, it is flexible enough to be reconfigured to allow realistic practical exercises to be conducted.

### 6. Discussion and Conclusion

From an Australian perspective the fact that existing training is not locally based is problematic. While there is substantial commonality in the components of control systems worldwide the local environment must also be taken into account. Establishing a local facility to both provide training
and research into industrial control systems security should have substantial benefit. The fact that this curriculum and laboratory are being established in Australia gives more opportunity for local systems owners to provide feedback so that local conditions can be more easily taken into account.

The contribution of this curriculum is that we will provide advanced level courses for postgraduate students and industry professionals as well as awareness courses for operators and managers. Further, in designing this curriculum, we have attempted to explicitly deal with the differing concerns, knowledge and experience of information technology professionals and control systems professionals.

We are designing the curriculum to deal with situations that may occur in industry. A key part of the design is that the curriculum does not simply provide guidelines or theoretical knowledge. By including a substantial practical component students are provided with experience to help them integrate the theoretical knowledge.

The curriculum provides instruction for students across the broad range of activities required for undertaking long term security of industrial control systems. The curriculum provides knowledge and experience in preparatory activities such as forensic readiness, incident response planning and vulnerability assessment. Students will gain experience in activities required to deal with incidents and to carry out after incident investigations. Students will also gain knowledge in ongoing requirements for good security practice audit activities. Students will also be provided with a skill set to allow them to understand the basics of activities such as vulnerability assessment and penetration testing allowing them to further develop proactive security strategies in their own control systems.

While this curriculum is initially being developed as a service offering it has the potential to be further developed as a set of university level subjects. These subjects could either form a self-contained graduate certificate course or form part of a graduate diploma or masters level course. Alternatively the subjects could form a minor at an undergraduate level or simply serve as a set of elective subjects at the undergraduate level. Extending this curriculum in this manner is a long-term goal rather than a short-term aim. In the initial case the authors believe the immediate need is for education and training for those already working in the industry.

There are limitations in our curriculum. It is still under development and has not been extensively tested with a wide range of students. Much of the material is primarily based on our standard IT cyber security course and we are still exploring the effectiveness of the industrial control system security components of the curriculum.

The final issue is that we intend to build in processes to ensure that practical exercises are relevant and kept up to date. Understanding of the range of security issues for control systems is still being developed. Similarly, understanding of effective security measures that do not compromise the operational requirements of control systems is still being developed. Consequently, this curriculum must be considered as a work in process. As more knowledge comes to hand then the courses will have to be adjusted to integrate this new knowledge. This will be especially important in the practical components of the curriculum.

7. References


8. Appendix

Unit Outline

Unit Code: INN607
Unit Title: Penetration Testing and Industrial Control Systems

<table>
<thead>
<tr>
<th>Credit Points:</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites:</td>
<td>None</td>
</tr>
<tr>
<td>Corequisites:</td>
<td>None</td>
</tr>
<tr>
<td>Equivalents:</td>
<td>INN651</td>
</tr>
<tr>
<td>Assumed Knowledge:</td>
<td>Students should have a basic knowledge of network protocols and programming.</td>
</tr>
<tr>
<td>Coordinator:</td>
<td>Ernest Foo</td>
</tr>
</tbody>
</table>

Rationale

The actions of malware and malicious attackers are an increasing threat to industrial control systems administered by government and private organisations. The unprecedented level of malicious activities faced today comes from a wide range of sources including individual hackers, activist groups, organised crime syndicates and nation states.

As a control system security professional you are expected to have an understanding of the vulnerabilities and threats that industrial control systems under your protection may be exposed to. As a result it is important that you are familiar with general system exploitation techniques and tools that may be used against your system services and applications. The knowledge and skills you will gain in this course will allow you to better defend your system services and applications.

This unit will discuss design and testing principles that produce secure applications. This unit will also introduce techniques and tools that demonstrate how to exploit system services and applications.

Aim

The aim of this unit is to give you an understanding of the fundamental concepts and major issues in the area of industrial control system cyber security. You will be able to identify critical application and system service vulnerabilities and determine the information security implications of those vulnerabilities. You will have knowledge of a range of techniques for exploiting and mitigating the impact of threats and vulnerabilities to networks and systems.

Learning Outcomes

On completion of this unit you should be able to:

1) Describe a wide range of vulnerabilities and threats to networked applications and industrial control systems (GC1, GC3, GC6).
2) Define major requirements and techniques for developing, installing and configuring secure networked applications and industrial control systems. (GC1, GC2).
3) Recognise, analyse and describe threats to the security of industrial control systems in a range of practical situations (GC1, GC2, GC3).
4) Evaluate complex industrial control systems through penetration testing to discover and mitigate vulnerabilities and threats. (GC1, GC2, GC3, GC5).
5) Discuss mitigation strategies for a range of vulnerabilities in networked control systems and applications. (GC1, GC3).

Key: Graduate Capabilities
GC1 - Knowledge and Skills
GC2 - Critical and Creative Thinking
GC3 - Communication
GC4 - Lifelong Learning
GC5 - Independence and Collaboration
GC6 - Social and Ethical Responsibility
GC7 - Leadership and Change.

Content

The content of this unit is based on guidelines described by the Information Technology security sections of the Information Security Manual (ISM) Controls document produced by the DSD. The following timetable is only an indicative outline. Instructors will adjust topics according to your progress.

Day 1
Secure Design Principles
Secure Development and Testing
Industrial Control System and Cyber security
Industrial Control System Protocols and Web Services
Revision

Day 2
Buffer Overflows
Format String Overflows
Cross Site Scripting
SQL Injection

Day 3
Session Management
Cross Site Request Forgery
DNS Poisoning
Email Spoofing

Day 4
Malware and Viruses
Day 5
Full Day Penetration Test Exercise

Approaches to teaching and learning
Dependant on the content, a mix of lectures and practical workshops are used. Lectures address theoretical aspects of the field of system and application vulnerabilities, and explain the technical content, which forms the basis of the practical sessions. You are expected to consult reading material such as reference manuals and on-line documentation to enhance your understanding of the technical concepts introduced in this unit.

Practical exercises performed in a computer laboratory environment will allow you to gain experience in a variety of advanced technical tasks required to be performed by Information Security Professionals and Penetration Testers, as well as enhance essential problem solving skills whilst working in teams. Laboratory practical sessions will enable you to perform technical tasks while staff are present to provide limited guidance. You will also be expected to become accustomed to looking up relevant resources on your own initiative and through reading and hands-on experimentation, which may involve trial and error, investigate and find ways of solving computer system and network problems.

Assessment
General Assessment Information
The major assessment for this unit will be the submission of a workbook that discusses the tutorials and workshops conducted during the unit. The workbook should also include student reflections of each topic addressed in the unit.

<table>
<thead>
<tr>
<th>Assessment Item No. 1</th>
<th>Workbook Submission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment Name</td>
<td>Students are to keep a workbook that discusses the tutorials and workshops conducted during the unit. The workbook should also include student reflections of each topic addressed in the unit.</td>
</tr>
<tr>
<td>Description</td>
<td>This assessment item relates to all learning outcomes.</td>
</tr>
<tr>
<td>Relates to learning outcomes</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100%</td>
</tr>
<tr>
<td>Due date</td>
<td>Workbook to be submitted to instructors at the end of the intensive course or 1 week after the completion of the course.</td>
</tr>
<tr>
<td>Individual/group</td>
<td>Individual and Group</td>
</tr>
</tbody>
</table>

Academic Honesty
Academic honesty means that you are expected to exhibit honesty and act responsibly when undertaking assessment. Any action or practice on your part, which would defeat the purposes of assessment, is regarded as academic dishonesty. The penalties for academic dishonesty are provided in the Student Rules. For more information you should consult the QUT Library resources for avoiding plagiarism.

This unit may use the SafeAssign tool in BlackBoard. SafeAssign is a text-matching tool that assists students to develop the academic skills required to correctly use and cite reference material as well as to check citations and determine possible instances of plagiarism. You may be asked to use SafeAssign, in which case you will be expected to submit draft and/or final versions of one or more assignments and may be asked to answer a short online survey about the tool. Using SafeAssign does not constitute formal submission of an assignment. Your Unit Coordinator will provide detailed information on how the software will be used for individual assignments. The use of the tool is for educative purposes and is entirely voluntary.

Resource Materials
Australian Government Information Security Manual (ISM), Defence Signals Directorate, [annual release].

Risk Assessment Statement
There is minimal health and safety risk in this unit. It is your responsibility to familiarise yourself with the Health and Safety policies and procedures applicable within campus areas.