Computer Lab 05

Australian Government Cyber Security Guidelines

Networked Information Systems (COMP2410/ COMP6340), 2022 Semester 1

A/Prof Hanna Suominen

School of Computing,

College of Engineering and Computer Science (CECS)

The Australian National University

Canberra ACT 2601 Australia

www.anu.edu.au

CRICOS Provider No. 00120C

Contents

Australian Cyber Security Guidelines

Summary

The *Australian Cyber Security Centre* (ACSC) has produced the *Information Security Manual* (ISM) in order to outline a cyber security framework that organisations can apply to protect their information and systems from cyber threats, using their own approaches to managing risks. Its latest (2022) version is available at https://www.cyber.gov.au/acsc/view-all-content/ism. The intended audience of the ISM is Chief Information Security Officers, Chief Information Officers, information technology managers, and cyber security professionals.

Learning Objectives

After completing this lab based workshop, students should be aware of and able to learn more about cyber security principles and related guidelines for incident prevention and management in Australia in general and in particular in applying them to cyber-physical systems and network management, including, for example, email and encryption.

Cyber Security Principles

We can follow the cyber security principles by the ACSC to better understand how to protect data and systems. They are available at https://www.cyber.gov.au/acsc/view-all-content/advice/cyber-security-principles.

Questions:

- What is the purpose of these principles?
- How are the five govern, fourteen protect, two detect, and three respond principles targeting this purpose?
- Why is maturity modelling included on the website?

Guidelines for Cyber Security Incidents

The ISM includes cyber security guidelines, available at https://www.cyber.gov.au/acsc/view-all-content/ism/cyber-security-guidelines, to help organisations protect their systems and data from cyber threats. These cyber security guidelines cover not only security matters related to information and communications technology but also personnel security, physical security, and governance. Their chapters are as follows:

- Guidelines for Cyber Security Roles,
- Guidelines for Cyber Security Incidents,
- Guidelines for Outsourcing,
- Guidelines for Security Documentation,
- Guidelines for Physical Security,
- Guidelines for Personnel Security,
- Guidelines for Communications Infrastructure,
- Guidelines for Communications Systems,
- Guidelines for Enterprise Mobility,
- Guidelines for Evaluated Products,
- Guidelines for Information and Communications Technology Equipment,
- Guidelines for Media,
- Guidelines for System Hardening,
- Guidelines for System Management,
- Guidelines for System Monitoring,
- Guidelines for Software Development,
- Guidelines for Database Systems,
- Guidelines for Email,
- Guidelines for Networking,
- Guidelines for Cryptography,
- Guidelines for Gateways, and
- Guidelines for Data Transfers.

Questions:

- Which chapters do you think are the fist ones to be updated? Why?
- Which chapters do you think are likely to remain fairly stable (i.e., do not need updates so often)? Why?
- What does system hardening refer to in the guidelines? Give three more specific examples of guidelines related to system hardening.
- How do system management and system monitoring differ in the guidelines? Give three examples of key differences.
- How do system management and network management differ in the guidelines? Give three examples of key differences.
- How would you summarise the guidelines for cyber security incidents?
- What are the key guidelines for physical security? Why?
- What are the key guidelines for personnel security? Why?
- What is a detail related to guidelines for enterprise mobility that you would be willing to remove if you had to leave one detail out? Why?
- In what ways was can we apply our lessons learnt from the Encryption Lab to Guidelines for Using Cryptography? Did we learn anything relevant to these guidelines?
- Do you notice something missing? What? Why would it be important to include this topic?

A Case Study

Let us consider the “Incident report on the breach of the Australian National University's administrative systems”, available at https://apo.org.au/node/262171, as a case study from 2018–19. This case provides a chronological account of the data breach at the ANU based on available forensic data.

The two key hallmarks of the case study were as follows:

1. The high degree of operational security that involved file and log erasure.
2. Measures designed to defeat forensic analysis and hide activities.

Consequently, the forensics available (and subsequent analysis) were incomplete, although enough detail was available to provide insight into the actor’s activities. Broadly speaking, there were three categories of activities undertaken by the actor during the campaign:

Credential theft: The actor sent out four spearphishing emails, to ANU users, to try and gain credentials (i.e., passwords, usernames, hashes). The aim of these emails was to gain the credentials of an administrator or someone with the right level of access to targeted systems. The actor also tried to gain a broad set of credentials to work around expiring credentials or compromised accounts getting exposed. In the case of ANU, administrator credentials deliberately expire quickly. The actor used software designed to “sniff” credentials from network traffic as well.

Compromised infrastructure: The actor built a shadow ecosystem of compromised ANU machines, tools and network connections to carry out their activities undetected. Some compromised machines provided a foothold into the network. Others, like the so-called attack stations, provided the actor with a base of operations to map the network, identify targets of interest, run tools and compromise other machines.

Data theft: The actor used a variety of methods to extract stolen data or credentials from the ANU network. This was either via email or through other compromised Internet-facing machines.

In the intervening two weeks between the detection of the breach and the public notification, the ANU detected repeated attempts to gain or possibly regain access to its systems and data (see the timeline below). Investigations into the nature of these attempts, which were blocked, were still ongoing at the time of the incident reporting. Within an hour of the Vice-Chancellor’s notice informing the ANU community and public of the data breach on 4 June, the ANU network was subject to a botnet attack. This attack was also successfully stopped by the ANU.

Timelines and Attacks (details will be found in the aforementioned incident report):

- **9 November 2018**: spearphishing email one.
- **12−14 November 2018**: webserver infrastructure compromised.
- **16 November 2018**: compromise of legacy infrastructure.
- **20−21 November 2018**: the creation of attack station one.
- **22 November 2018**: the creation of virtual machines on attack station one.

- **23 November 2018**: exfiltration of network mapping data.
- **25−26 of November**: spearphishing email two.
- **27 November**: access to Enterprise Systems Domain (ESD) file shares achieved.
- **29 November 2018**: third spearphishing attempt.
- **29 November−13 December 2018**: clean-up operations and loss of attack station one.
- **21 December 2018**: fourth spearphishing attempt and loss of attack station two.
- **22 December 2018 – March 2019**: C2 activity and second intrusion attempt.

Considering the aforementioned context, your task is to prepare answers for the following questions.

a) What parts of the guidelines above are relevant to this case? How can we use them to support our answers to the following questions?

b) Outline the major security threats in this context. Be sure to identify those that you think are major threats and those that are minor threats.

c) Prepare a risk assessment that includes the major assets, threats, and controls.

d) How do you ensure the service continuity at the ANU by mitigating or preventing various levels of threats and intruders?

e) Design your network by addressing the location of the security threats in the communication flow with necessary diagram.