The University of Sydney
School of Computer Science
Dr Suranga Seneviratne
Senior Lecturer - Security

THE UNIVERSITY OF SYDNEY

INFO3616/CSEC3616/CSEC5616 - Tutorial - 1

1 Programming Satan's Computer

Ross Anderson and Roger Needham infamously described security engineering as "Programming Satan's computer". Explain the metaphor: why, in particular, is it "Satan's computer"? 1-2 sentences are sufficient.

2 Safety/Reliability Engineering vs. Security Engineering

Explain the difference between Safety and Reliability Engineerings and Security Engineering.

3 Security Goals - A

You may wish to revisit the lecture recording to answer the following questions.

a) True or false? Explain your answer in 1-2 sentences

- If you have the choice between secrecy and availability, and your system can only meet one of these goals simultaneously, always go for secrecy.
- Authentication is the process of obtaining permission to access a file.
- Privacy (in the context of internet) is my ability to conduct my online activities whilst being anonymous.

b) Explain in 1-2 sentences.

- Why does non-repudiation require secure timestamping in many cases?
- Why is integrity of logfiles important to achieve accountability?
- Why is it very hard to estimate the complete attack surface of a given system?
- In the context of the last question, why is it important to remind yourself that security is a process?

c) Break a protocol

Danaerys tells Jon how he can enter the city. To enter the city, the guards will question him 'Who goes there?' And Jon must reply with the secret passphrase ('The Lord of Winterfell').
Give a reason why this does not meet the definition of a cryptographic protocol and show how it can be broken.

4 Security Goals-B

Someone tells you that you can "just encrypt data" and you can be sure that the following security goals are achieved: confidentiality, integrity, authenticity, and access control. For each goal, explain if the person is right or wrong.

5 Sydney Opal Card

You are likely familiar with the Sydney Opal Card system: a swipe card is used to 'pay' and allow you to enter and leave the platforms via gates. Let us assume you were in charge when the system was planned. Using our reference framework of Policy, Incentives, Mechanism, and Assurance, please:

- State two policies to achieve. One sentence per policy is fine.
- State two incentives that work against those policies.
- State one attack based on each incentive (see note below). It's fine if the attack is described fairly generically (no need to refer to concrete technology that it attacks).
- Give two mechanisms you can think of that will work against the attack based on the incentive.
- State what assurance you place on each mechanism you have chosen.

This question is intentionally open: you are free to choose policy and incentives, and you are free to make assumptions how the transport system works. You are free to choose the attack based on the incentive (the one that your mechanism protects against). Policies, incentives, mechanism, and assurance do not have to be based on the electronic part of the system—it can also be entirely physical.

6 Designing a New Student Experience

You have recently become the Head of the Higher Education Portfolio at your home university. Your first move is to cancel the subscription to the old "Whiteboard" system used to support lectures, enrolments, and grading. You replace it with something of your own design, called CAMPUS.
In the following, refer to the framework for discussing security aspects that we introduced in the lecture.

a) Incentives

For each of the following actors, give an example *incentive to attack* or *protect the system.* Each incentive must be different.

- The vice Chancellor of the University
- A student enrolled in a course
- A Tutor of the same course
- A Security guard in the CAMPUS data centre

b) Policies

For each of the following actors, give a possible security policy they might want to design and a security goal that relates to it.

- The Vice Chancellor of the University
- A student enrolled in a course
- A tutor of the same course

7 Terminology

a) Person-in-the-middle-attack
What is a Person-in-the-middle aka Man-in-the-middle attack?

b) Distributed Denial-of-Service
What is a Denial-of-Service attack? And a distributed one?

c) Supply Chain Attack
What is a Supply Chain Attack?

d) Security Goals
Tick all that are **not** classic security goals. Explain your choice.

[ ] Authenticity

[ ] Integrity

[ ] Deterrence

[ ] Authorisation

[ ] Confidentiality

[ ] Denial-of-service prevention

8 Homework - ACSC Essential Eight

Essential Eight by the Australian Cyber Security Centre (ACSC) is a series of baseline mitigation strategies recommended for organisations to improve their security posture. Implementing these strategies as a minimum makes it much harder for adversaries to compromise systems.

- Find information about the Australian Cyber Security Centre (ACSC) Essential Eight maturity model.
- Discuss how each strategy is applicable to a new superannuation provider.