Assignment 1
ELEC5616: Computer and Network Security

Luke Anderson
luke@lukeanderson.com.au
University of Sydney

May 10, 2019

Date Due:

- 24^{th} May 23:59 - Deadline for feedback.
  Assignments submitted before this time will be marked with feedback before the exam.
- 7^{th} June 23:59 - Final Deadline for assignment.

Instructions:

- You are to work on this assignment in groups of 1 or 2.
  These groups do not have to be the same as those for your project.
- This assignment is to be submitted via e-learning with your answers typed (not handwritten).
- Late assignments will not be accepted.
- Make sure you understand each of your answers well, they are excellent exam preparation.
- Please make sure the names and SIDs of each person in the group are provided.

1 Question 1: Secure Design (25 marks)

A. **Attacks (15 marks)**
How would you design a system to be resilient against each of the following attacks?

1. Brute force of the message space.
2. Buffer overflows.
3. Replay attacks on protocol messages.
4. ARP spoofing.
5. Password sniffing.
6. Timing attacks.
7. Social engineering the network administrators

- *2 marks each.*
- *Explain how and why, no more than two or three sentences each.*
- *1 additional mark for particularly good explainations*

B. **Attacks (5 marks)**
Playing in your regular Friday night poker match, you notice collusion between Slim Jim and Rusty Joe. Every time Slim Jim scratches his left eye, Rusty folds; and every time Slim Jim coughs, Rusty Joe bets the house. Using this information you fleece both of them for their pocket money. What class of attack did you use?

C. **PRNGs (5 marks)**
After Slim Jim and Rusty Joe realise what's going on, the only way you all agree to play is over the Internet. Your first attempt is to download PokerXP from MickySoft. The designers of PokerXP didn't take *ELEC5616*, and it turns out they used the UNIX rand() linear congruential generator to shuffle the deck. How long will it take for Slim and Rusty to get their revenge?

2 Question 2: Cryptosystems (25 marks)

A. **RSA (5 marks)**
Provide a brief description of the RSA algorithm, referring to both its operation and use.

B. **Timing Attack (5 marks)**
What is a timing attack? How can a timing attack be used against naive implementations of RSA.

C. **Mafia RSA (5 marks)**
The Mafia family you belong to is holding elections for a new boss. It is suggested that each member of the family votes privately by encrypting their nomination (either "Sammy the Knife", "Big Kevsta" or "Teflon Hook") with the family's 4096-bit RSA public key (which is well known) and then e-mail the ciphertext in. If everyone can read everyone else's e-mail, is this system still secure?

D. **Avalanche Effect (5 marks)**
Explain the avalanche effect in DES, with reference to the three major building blocks which cause it to occur.
(Hint: two are 'black boxes' and the third is the overall structure).

E. **Attacks on Asymmetric Algorithms (5 marks)**
Is the rate at which we're improving attacks on asymmetric cryptosystems greater or less than symmetric cryptosystems? What is the end game for attacks on asymmetric algorithms?

3 Protocols (25 marks)

Commitment schemes allow Alice to commit a value x to Bob. The scheme is *secure* if the commitment does not reveal any information about the committed value to Bob. At a later time, Alice can *open* the commitment and convince Bob that the committed value is x. The commitment is *binding* if Alice cannot convince Bob that some other value $x' \neq x$ is the committed value.

Consider the following commitment scheme:

Commitment: Alice chooses a random r the same size as x and calculates $y = h(x \| r)$, where h is a hash function (e.g. MD5). She sends the values r and y to Bob.

Open: Alice sends x to Bob, and Bob calculates $y = h(x \| r)$.

A. Show that the proposed scheme is binding. *(7 marks)*

B. Show that the proposed scheme is insecure, i.e. that the scheme reveals information which allows Bob (with some work) to determine the committed value. *(7 marks)*

C. Suggest a modification to the scheme to secure the protocol. *(11 marks)*

4 Question 4: Network and Software Security (25 marks)

A. **Salting Passwords (5 marks)**
Explain how password salting increases the security of password files. What is the difference between a salt and a secret salt?

B. **OS Fingerprinting (5 marks)**
Explain how operating systems can be precisely identified across a network.

C. **Programming (5 marks)**
List 5 common programming mistakes resulting in security problems, and describe with a sentence for each how to avoid them.

D. **Internet (10 marks)**
In a page, address both sides of the following statement: "It would be good for security if everyone on the Internet ran the same operating system".

This is the end of the assignment.