

Family Name:

Other Names:

Signature:

Student Number:

This PAPER is NOT to be retained by the STUDENT

The University Of New South Wales
COMP3441/9441 Final Exam

Cryptography and Security

November 2004

Time allowed: **3 hrs**

Number of questions to answer: **14**

Total number of marks: **101**

You must hand in this entire exam paper, the answer booklets, and your reference sheet. Failure to do so will result in zero marks for the subject and a possible charge of academic misconduct.

Do not use red pen or pencil in this exam. You may bring and refer to one reference sheet of A4 paper containing your name, student number, and any notes you wish. Scientific calculators may be used. Computers, programmable calculators, calculators capable of storing text, or devices capable of wireless communication may not be used. Use or possession of a non-allowed device will result in zero marks for the subject and a possible charge of academic misconduct.

before you start: Fill in all of the details on the front of *each* answer booklet, and SIGN each booklet. Do the same for this pink question paper. Check your name and student number are written clearly on your reference sheet. Write *WORKING ONLY* on the front of one answer booklet. Flip the answer booklets over and turn them upside down - you must write your answer on the *last* two pages.

There is one mark for following the examination instructions.

| Examiner's Use Only | | | | | | | | | | | |
|---------------------|------|---|----|----|----|----|----|---|---|-------|--|
| | Inst | A | 12 | 13 | 14 | 15 | 16 | C | D | Total | |

Part A: Short Answer Questions

Answer these questions in the spaces provided below on **this pink question paper**. DO NOT answer these questions in one of the answer booklets!

Write your answers clearly. Keep your answers neat and very brief. Messy or long answers will not be marked.

In this part if you do not wish your answer for a question to be marked clearly write “*1 sympathy mark please*” in the space for the answer. If you do this as well as writing an answer, the answer will **not** be marked. If a question has consists of multiple subquestions writing this for any subquestion will result in one mark being awarded for the entire question.

Each question is worth 5 marks.

Question 1

Compare and contrast the following concepts: *nonce*, *salt*, *cryptographic random number*, *IV*, *shared secret*.

nonce: _____

salt: _____

random: _____

IV: _____

secret: _____

Question 2

Your friend has IP address 208.144.100.203 but they have not told anyone else but you. Explain to them why this secrecy is not going to protect them from attack.

A black hat, who would like to avoid detection, sends an TCP segment to see if there is a computer at this address. Give the packet and explain how it achieves this effect.

Why secrecy is not sufficient: _____

The segment:

Write 4 bits per box, add extra lines if needed. For bits which require non-trivial calculation just write a brief explanation rather than calculating them.

| | | | | | | | |
|--|--|--|--|--|--|--|--|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Explain how it achieves this effect:

Draw arrows to the bits you talk about.

Question 3

Your kid sister in year 11 gets an SMS message saying "i love you", but she doesn't know who it's from. She rang the sender's mobile number but a busy sounding women answered the phone and she hung up in embarrassment. Now she's not sure if that lady sent the message to her number by mistake, or if she has a teenage son who sometimes uses his mom's phone for love messages. How could you use social engineering to help her find out if the lady has a son and, if so, what his name is. Finding more about him (age, location, school, does he have a girlfriend etc) would be even better.

How: _____

Question 4

Explain what you could do to detect passive sniffing on your LAN.

Question 5

How could you use an IDS to detect attempted buffer overflow attacks on an intel-based machine? State, and briefly explain, example snort rule(s) to do so. In your answer you may wish to make use of the fact that the NOP instruction for intel-based machines is 0x90.

How Detect: _____

Example rule(s): _____

Question 7

Describe a non-interactive zero knowledge proof of your ability to sign a particular document (using an RSA private key corresponding to a particular known RSA public key).

Show that the proof is indeed zero knowledge

Question 8

The following is an extract from <http://www.newscientist.com/news/news.jsp?id=ns99996457>

Microchip imperfections could cut cloning

Imperfections unique to every microchip can be used to make them impossible to clone. The techniques inventor claims that this will make banking or ID smart cards impossible to copy, and perhaps halt the illicit global trade in counterfeit computer games consoles.

Counterfeiters copy smart cards or games consoles by reverse engineering the electronic circuitry within them working out what a circuit does and making another one that does exactly the same. If this is done properly, any software that uses the chip, whether it is in an ATM or a PlayStation, will run as normal.

The trick that Srinivasa Devadas, an electronics engineer at the Massachusetts Institute of Technology in Boston, has dreamed up is to design software that interrogates the hardware to see if the chips inside it are genuine.

Slight variations in the make-up of silicon chips mean that no two are identical. Devadas idea is to use these variations to construct a unique ID code for it that the software will verify.

Exact temperature

A microchips transistors are connected by aluminium or copper tracks a few hundred nanometres wide whose thickness depends on the exact temperature and pressure during the manufacturing process. Due to minute variations in the temperature and pressure, each chips metal tracks are left with a unique thickness profile.

A thicker track lets a signal pass quicker than a thinner one, and Devadas proposes building a small circuit in every chip that picks up these differences and uses them to generate an ID code that is unique to that individual chip.

The circuit will apply a 128-bit signal that Devadas calls a challenge code to some of a chips metal tracks. The signals that cross a track first are fed into a secret algorithm to produce a unique ID code. This is more secure than any system we have right now, claims Devadas.

The technique is designed to defeat hackers who clone smart cards such as those used to authenticate bank transactions, give access to buildings or decrypt pay TV signals.

Smart cards hold their security information on a chip, and determined counterfeiters sometimes take these chips apart and examine the memory under an electron microscope to retrieve the security data. It is then a simple matter to program this data into a blank card to make a clone.

Spoof ID

The new card would not be susceptible to this forensic approach. It would be impossible for a counterfeiter to mimic the precise physiology of the chip to reproduce its ID code.

Analyse the above article from the 2004 October 2 edition of New Scientist. Give the main strengths and weaknesses of Devadas' idea.

(write your answer on the next page)

Strengths _____

Weaknesses _____

Question 9

The following is from <http://www.mail-archive.com/cryptopp-list@eskimo.com/msg01009.html>

Rijndael Encryption with SHA256 hash

- * From: Phillip Allan-Harding
- * Subject: Rijndael Encryption with SHA256 hash
- * Date: Wed, 30 Apr 2003 12:42:19 -0400 (EDT)

I'm relatively new to cryptography and Crypto++, can someone comment on whether what I want to do sounds "correct" (whatever correct means!)

- I want to encrypt data, that is to be transmitted around the inter/intraNet, using Rijndael
- I want to use a key for the encryption that is an SHA128/256 hash based on: -
 {multiple concatenated string data components} + {a nonce}

Regards,
Phil Allan-Harding.
blue 8
Interchange 25 Business Park
Bostocks Lane, Sandiacre
Nottingham NG10 5QG
+44 (0)115 921 0200

Give your comments:

Question 10

Here is a diagram of a network configuration:

Here is the policy about what traffic is permitted on this network and what is not.
blah blah blah

Give firewall rules for all the network adaptors to enforce this policy.

Rules:

Question 11

An internet cafe has asked you to evaluate their security. Outline the threat model you will use.

Question 12

Explain and contrast multi-layered and multi-lateral security models. Give the name of one well known model of each type, and an example of where it is used.

multi-layered: _____

multi-lateral: _____

Part B: Long Answer Topics

Select and answer *TWO only* of the following topics.

Answer each topic in a separate booklet. Clearly write the topic letter on the back of each booklet in big digits AND fill in the two boxes below

Write your answers in the *back* of the answer booklet. (You will need to flip the booklet over and turn it upside down). This lets us mark the booklet without seeing your name first.

Your answer must take no more than two pages. We will only mark the first two uncrossed-out pages of any answer (counting from the back of the book).

Make your answers as clear and easy to understand as possible. Provide diagrams and brief comments where necessary. Confusing, difficult to understand or illegible answers will lose marks.

I have chosen to answer topic and topic
Each topic is worth 20 marks.

Topic A

After the exam you are at a party and get to talking with the IT manager of a medium sized company. You mention some of the questions in the security exam, and this question in particular. The IT manager says “all that security stuff is just a waste of time in the real world. All you really need is a good firewall”.

In point form set out arguments supporting his position, and then set out arguments you could give to oppose it. Be well structured and compelling but brief (remember this is at a party...)

Note that a good response could get you a job as the firm’s new security consultant.

Topic B

ARP cache poisoning attacks are a concern for privacy on Local Area Networks. How could you write a daemon that analyses a network stream and is able to determine when an ARP attack is occurring. What assurances of privacy could this provide? Explain the theoretical premises upon which your defence is based. What actions should your program take upon detecting an attack?

Topic C

Outline proposed and attempted attacks on the AES/Rijndael algorithm. In your response include an analysis of a range of types of attacks including Side Channel attacks as discussed in lectures. For each attack or type of attack explain whether or not it is feasible. Finally, contrast how susceptible to attack Rijndael is in comparison to the other 4 finalists of the AES competition.

Topic D

Describe three possible *different* attacks on firewalls.

Analyse the merits of each, what weaknesses of firewalls they exploit, and discuss what could be done by a system administrator to either prevent the attacks or minimise their impact on the system.

Select which attack is the most effective against current firewall technology and briefly state why.

Topic E

Give an example of a normal PseudoRandom Number Generator (PRNG) such as a simple LCRNG, and give an example of a cryptographic PRNG.

Set out the properties a cryptographic PRNG needs to have and show that the cryptographic PRNG you gave above has these properties.

Explain, and illustrate with examples, the dangers of using a a PRNG without these properties in a cryptographic protocol.

Topic F

Suppose you are working in a very large company with thousands of computers with Internet access which is considering adding IDS to boost its security. You have been asked to write a report about this and make recommendations. Give your report in point form.

In your report you should address the following:

What parameters do you consider in the design of the IDS?

Explain your recommendation with an example and details of your rules, policies and any other considerations you think are relevant.

State the issues for which need to be considered in the selection of any commercial IDS products and complementary systems.

Topic G

Impressed by your knowledge of honeypots you have just been offered a job by the School of Computer Engineering and Science at the University of South Wales.

Your first task is to write a report about the advantages of honeypots at three possible locations: (1) outside their firewall, (2) in the DMZ, and (3) in their internal network. For each location set out what benefit (if any) they could get from placing a honeypot there. They have also asked (4) if you can think of any useful ways they could use honeytokens.

For each of the four parts of the report you should include any relevant issues they should consider, including any potential disadvantages.

tip: devote roughly equal space to each of the four parts of this question

Topic H

You are a consultant and have been approached by the sysadmin for the Prime Minister's fan club webserver. She is worried that unAustralian intellectual elite communists might launch a Distributed Denial of Service attack against the server.

You have been asked to write a report describing: the workings of such an a attack, how to detect it, how to respond to it, and how to prevent it. Set out the points you will include in your report.

Topic I

The sysadmin for a large law firm has approached you to write a report on how the firm can stop its senior partners being bombarded by spam (they are getting very grumpy about it!) You should outline the various courses of action open to the firm, describing each, and setting out their advantages and disadvantages.

In your conclusion you are to combine the various courses of action open to the company into three alternative strategies the firm might follow - low, medium, and high cost. Present the information in a well organised and coherent way so that the company can make an informed choice about what they are to do.

Set out your report in abbreviated or point form.

Topic J

A simple online election protocol is: the voter sends their vote (encrypted with the tallier's public key) and their identity details to the validator. The validator checks they are eligible to vote and, if so, sends the vote to the tallier who decrypts it and adds it to the tally.

What are the problems with the simple protocol?

Explain how you could tweak this simple protocol to stop the tallier being able to deduce the contents of the encrypted vote without adding extra communication steps.

Explain the FOO protocol.

List and explain which of the above problems are fixed by the FOO protocol, and which are not.

Topic K

Describe all the replication mechanisms used by the Internet Worm. You are a sysadmin for a medium sized company employing a mixture of unix and windows boxes. Briefly set out those parts of your security policy relating to the threat posed by malware.

tip: devote roughly equal space to each of the two parts of this question