= COMP9/3441 Final Exam : 2016s1 =
== Total number of marks: 100 plus 1 bonus mark ==
== Total duration: 180 minutes plus 10 minutes reading time ==

Your answers can be submitted by pressing save on this application. You may submit your solutions as many times as you like. ONLY the last submission will be marked.

Write your answers in the computer files as directed in the exam instructions. You may use the supplied paper for your rough working, this will not be marked.

Once the exam has commenced you may not leave the exam.

You may use the GUI calculator and pdf viewer and the exam entry application. You may not use any scripting languages or other software tools. This is an essential examination requirement and any breach of this will be treated as academic misconduct. Be aware that all activity is logged. Also, the toilets are fitted with smoke detectors.

The use of Malachite or unauthorised social engineering is prohibited. Strict exam conditions apply, including that you may not attempt to communicate with any other person, or access other computers or external data or any internet resources.

If you do not follow these instructions you will get zero marks for the exam and a possible charge of academic misconduct.

Phones must be turned off and not visible, either left outside the room in your bag or sealed in an opaque bag placed under your seat. T-shirts with funny logos are permitted. The supervisor's decision about what is funny and what is not is final.

If you think a question is ambiguous, answer the most likely interpretation and state what you have done. Where two or more different answers are possible give the answer which best answers the question. Getting stuck: We suggest you don't spend more than 8 minutes on any of the 5 mark questions. Instead move on and come back at the end in any spare time. Keep answers brief and clear.

There is one bonus mark for following the examination instructions.

<
>
<
>
= Part A =

This part is worth 55 marks and consists of eleven 5 mark questions. Answer all questions.

=== Question 0 ===

Give a specific example demonstrating an attacker using a Denial of Service attack as a key part of a broader attack strategy. What was the purpose of the DOS part of the attack? (Ideally give a real example of an actual and well known attack)

DOS example:
_____
_____
_____

Role the DOS phase played in the overall attack:
_____

=== Question 1 ===

How many bits of security are provided by a passport photo or a thumbprint scan? Pick one of these two identification measures and estimate the number of bits it provides. Give reasoning and calculations to justify your number.

Pick one
 .[A] Passport Photo
 .[B] Thumbprint Scan

How many bits of security does it provide?

_____

Your reasoning and calculations

_____
_____
_____
_____
_____
_____

=== Question 2 ===

Suppose you were part of the original HTTPS protocol design committee
back in the dim distant past.

Why would you not use RSA to encrypt a HTTPS session?

_____
_____
_____

How could you achieve Perfect Forward Secrecy in an HTTPS session?

_____
_____
_____

=== Question 3 ===

Alice and Bob engage in Diffie-Hellman (m=33,g=2) with private secrets 5 and 8 respectively,
but evil Mallory performs a man in the middle attack on them. Write out the steps in the
protocol one step per line in chronological order, each line showing the number which sent
and who it is from, and who it is to.

In your answer write
{{{
A->B 45
}}}
to denote A sending the number 45 to B, where A represents Alice, B Bob, and M represents
Mallory.

State any assumptions you make.

Assumptions

_____

Steps in the protocol

(Use the format of the example below)
{{{
A->B 45

}}}
_____
_____
_____
_____
_____
_____

=== Question 4 ===

Explain how malware could survive the hard drive being reformatted and the operating system being reinstalled.

_____
_____
_____

=== Question 5 ===

You chair the government panel considering the introduction of new mandatory data breach notification requirements for organisations and you have just finished reading all the recent public submissions. What are the main arguments for and against introducing such a requirement?

For
_____
_____
_____

Against
_____
_____
_____

What do you recommend?
(No marks for the recommendation, marks are for the reasoning support it)
_____

Explain why this is your recommendation:
_____
_____
_____

=== Question 6 ===

You are crypt-analysing an unknown ciphering device using a chosen plaintext attack. You know that an Initialisation Vector (IV) is being transmitted in the ciphertext (although you do not know which bytes of the ciphertext contain it). Therefore sending two identical plaintexts usually gives rise to differing ciphertexts. You are not sure if the IV is generated pseudo-randomly, or is a nonce.

You send 2 billion identical single packet plain text messages, and generate 2 billion corresponding cipher text packets before you find a pair of ciphertext packets which are identical to each other.

Is it more likely that the IV is generated pseudo-randomly or is a nonce? How big is it likely to be (in bits)?

Pseudo-random or Nonce?

_____

Give your reasoning

_____
_____
_____
_____

Estimate how big the IV is likely to be (in bits)

_____

Give your reasoning

_____
_____
_____
_____

=== Question 7 ===

Suppose in the future UNSW computing students have spread all over the world and all printf() vulnerabilities and buffer overflow vulnerabilities in all software have been found and patched.

List four different examples of Data/Control interaction style vulnerabilities which attackers will still be able to exploit. If you can think of more than four put the four most significant at the top of your list.

_____
_____
_____
_____
_____

=== Question 8 ===

Many operating systems and antivirus systems now give preferential treatment to code which is signed (for integrity and authentication) using an X.509 digital certificate.

So malware authors would like their malware to be signed. List four ways they could manage to have their malicious code signed. If you can think of more than four, list the four most important first and the other ones below.

_____
_____
_____
_____
_____

=== Question 9 ===

This Ruby code decrypts any (supposedly "securely" encrypted) Snapchat image in any phone's cache.

(Note: You don't need to be able to program in Ruby, or indeed even to understand the syntax of Ruby, to answer this question. Your background knowledge of programming from Python or C is sufficient)

```
{{{
require 'openssl'
```

```
ARGV.each do|a, index|
    data = File.open(a, 'r:ASCII-8BIT').read
    c = OpenSSL::Cipher.new('AES-128-ECB')
    c.decrypt
    c.key = 'M02cnQ51Ji97vwT4'
    o = ''.force_encoding('ASCII-8BIT')
    data.bytes.each_slice(16) { |s| o += c.update(s.map(&:chr).join) }
    o += c.final
    File.open('decyphered_' + a , 'w') { |f| f.write(o) }
end
}}}
```

You have been hired by Snapchat to improve their security. They ask you if they should move from AES128 to AES256. They have asked you to comment on whether or not an attacker will be able to carry out 128 bits of work.

Prove, showing your calculations and assumptions, whether or not 128 bits of work is too much for an attacker to be able to do, and make a recommendation as to whether snapchat should switch or not.

_____
_____
_____
_____

What are the main two security weaknesses that this code reveals?

Main weakness:

_____
_____

Second weakness:

_____
_____

=== Question 10 ===

This question relates to the film Die Hard 2 which you watched in week13/stuvac.

The Federal Aviation Administration (FAA) is the national aviation authority of the United States, with powers to regulate all aspects of American civil aviation. These include the construction and operation of airports, the management of air traffic, the certification of personnel and aircraft.

Suppose the film was real (!!) and after the events depicted in the film the FAA appoints you to conduct an investigation into the events with the aim of making recommendations on the basis of lessons learned. What are the top 4 recommendations you would make within the scope of the FAA (e.g. so don't make military or drug trafficking recommendations). As usual put the most important recommendation(s) at the top of the list. Briefly justify/explain each.

Recommendation 1

_____

Justification

_____
_____

Recommendation 2

_____

Justification

_____
_____

Recommendation 3

_____

Justification

_____
_____

Recommendation 4

_____

Justification

_____
_____

= Part B =

This part is worth 30 marks and consists of two 15 mark questions. Answer both questions.

=== Question 11 ===

This question relates to the ABC news article
"Singapore prepares to block internet access on government computers"
(see supplied PDF from http://www.abc.net.au/news/2016-06-08/singapore-blocking-internet-access-on-government-computers/7494498)

Suppose the Australian government has set aside 100 million dollars to improve the security of government computers and that you have been appointed chair of the working party recommending how it is to be spent.
The prime minister has asked you to consider this approach taken by Singapore (as reported in the article) and advise if Australia should do the same.

What attacks is this protecting against?
_____
_____
_____
_____
_____

What attacks would not be protected by this?
_____
_____
_____
_____
_____

Give the 3 main factors in favour of Australia doing this:
_____

_____
_____

Give the 3 main factors in favour of Australia NOT doing this:
_____
_____
_____

Make your recommendation

Should Australia do this YES/NO?

_____

(marks are for reasoning not for your particular recomendation)

Explain your reasoning for making this recommendation

_____
_____
_____

If you recommended YES explain with reasons how you would implement such a system within your 100 million dollar budget.

If you recommended NO give with reasons the main alternatives you recommend to do to protect the security of government computers with your 100 million dollar budget.

_____
_____
_____
_____
_____
_____

=== Question 12 ===

Consider the following flawed communications protocol intended to provide a zero knowledge proof to person V that person P knows a solution to a particular sudoku puzzle.

==== Terminology: CELLS, ROW, COLUMN, SQUARE ====
{{{
Say a solution is a 9x9 grid of CELLS each containing a single number.
Say a ROW is a horizontal line of 9 cells in the grid
Say a COLUMN is a vertical line of 9 cells in the grid
Say the grid is divided into 9 non-overlapping SQUARES consisting of 9 cells of the grid arranged 3x3.
}}}

Step 1.
P privately rearranges the cell values in each 3x3 square of their solution by moving each to a random different location in the same square, and then encrypts this into file S.1

Step 2
P privately rearranges the cell values in each 9x1 row of their solution by moving each to a random different location in the same row, and then encrypts this into file S.2

Step 3
P privately rearranges the cell values in each 1x9 column of their solution by moving each to a random different location in the same column, and then encrypts this into file S.3

Step 4.

P gives files S.1, S.2, and S.3 to V

Step 5.
V asks P for the key to one of the files and decrypts it, verifying that each digit 1-9 appears exactly once in each square/row/column (depending on which file they have chosen to decrypt)

Step 6.
Repeat 1-5 until V is convinced.

Is this a zero knowledge protocol YES/NO?

_____

If YES prove it is, if no state what the problem is.

_____
_____
_____
_____

Does this protocol demonstrate that P knows a solution YES/NO?

_____

If YES explain why it does; if no state what the problem is.

_____
_____
_____
_____

Give a correct communications protocol to provide a zero knowledge proof to person V that person P knows a solution to a particular sudoku puzzle. (Note we want a communication protocol not a physical protocol. It must be able to be conducted over the internet and cannot require P and V to be in the same physical location.)

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Prove your protocol is indeed zero knowledge:

_____
_____
_____
_____
_____
_____

_____
_____
_____
_____
_____
_____

<
>
<
>
= Part C =

This part is worth up to 15 marks and consists of two questions.

Answer ONLY ONE of the questions. They are not worth equal amounts.

You are to choose which of these two questions, 13a or 13b, to answer but ONLY ONE ANSWER WILL CONTRIBUTE TO YOUR MARK. So don't waste your time and answer them both!

(If you do provide partial answers for both questions just write at the top of your answer for Q13a which one you want us to mark. If you do answer both questions (please don't) and it is unclear which question you want us to mark we will mark 13b.)

Remember answer ONE only of the following two questions.

=== Question 13a ===

(15 Marks)

ONLY ANSWER ONE OF THE TWO QUESTIONS IN THIS PART.
HEY!! YES - TALKING TO YOU!

A bank branch in the wild west of the Blue Mountains communicates with head office in Sydney using a telegraph wire that can be intercepted and which can be cut. So messages can be read, blocked and injected. To address this the bank uses a keyed MAC to guarantee authentication and integrity of the messages. The hacker Ned Kelly Junior intercepts some messages from the branch telling head office of deposits made by customers:

{{{
25052016130902105DEPOSITTODONALDKNUTH 16
10062016090600100DEPOSITTOBUCKAROOBANZAI 31
13062016191100042DEPOSITTOUNSWCOMPUTING1 3
}}}

He performs some transactions himself at the branch and his gang intercept these messages:

{{{
13052016090100025DEPOSITTONEDKELLYJUNIOR 5
12062016090100100DEPOSITTONEDKELLYJUNIOR 22
}}}

He deduces that the messages are of the form

{{{
8 Digits : Date DDMMYYYY
4 Digits : Time HHMM
5 Digits : Transaction Amount DDDDD (in whole dollars ie no cents shown)
The Phrase "DEPOSITTO"
The Name of the Client (perhaps with digits on the end if there are more than one client with that name) this is of variable length
A space
The keyed MAC code in the range 0..32
}}}

The date and time are the approximate date and time of the transaction.

After bribing some staff Ned Junior learns that the MAC is produced by appending a secret key to the end of the message and then computing a proprietary hash algorithm on the resultant combined message. The hash used by the bank is computed as follows:

{{{
0. initialise the variable "hash" to be 0.
1. compute the "value" of the first letter of the combined message.
 * the value of a digit is that digit e.g. the value of "9" is 9.
 * the value of a character is the ASCII value of that letter e.g. the value of "A" is 65.
2. update the hash variable using
      hash = (hash * 2 + value) mod 33
3. repeat 1..2 for the second letter of the combined message, then the third, and so on until you reach the end of the combined message.
}}}

Ned Junior is not sure how often the key changes, there may be a new key each day, or it may only change at the start of each week, or each month.

At 9am he deposits $100 into the branch and his gang intercepts this message:

13062016090100100DEPOSITTONEDKELLYJUNIOR 26

What is the likely security purpose of including the date and time in the message?

_____
_____

What is a fake deposit message which could be injected by his gang which has the same keyed MAC value as this intercepted message, but which states that Ned has deposited $90000 not $100?

_____

=== Question 13b ===
ARE YOU SURE YOU WANT TO ANSWER THIS QUESTION?

ONLY ANSWER ONE OF THE TWO QUESTIONS IN THIS PART.
HEY!! YES - I'M TALKING TO YOU!

(8 Marks - marked as pass/fail - no partial marks are awarded)

Decipher the message below to work out what to type into the answer field.

HQEET UTOII SNAEP MSRTT AOUIC DOINE

OEPOH YCNAE UDIHP RCETH TAIES EWINR

SCERS UNTGE IHUUT EFR

Your Answer:
_____