Final Exam - Review

COMP9337/9447

T1 2019

Schedule

- COMP4337/9337 Written
- Date/Time/Location: Please check myUNSW
- Calculator – UNSW Approved
- Instructions: see next foil

SAMPLE INSTRUCTIONS TO CANDIDATES:

-
- Time allowed: 2 hours plus 10 minutes reading time
- Total number of sections: 2. Answer all sections and all questions in each section. This exam makes up **40 marks**.
- Answer each section in a separate booklet. Please write down the section number on the top of each answer booklet.
- Total number of pages (including this cover page): Four (4).
- Do not write your answers on this paper. This paper *must be returned* at the end of the examination.
- This is an *open notes* examination. Students are permitted to bring along solutions to sample problem sets and tutorials. Handwritten notes and/or underlining is permitted in typed notes and printed lecture material into the examination room by students.
- For questions that require intermediate steps to reach the final answers, you are advised to show all your intermediate steps in the answer booklet too. Both the intermediate steps and the final answer carry marks.
- Other than your UNSW approved electronic calculator, you are not allowed to use other electronic devices such as laptops, tablets, PDA, mobile phones etc.
- Write all answers in *ink* except where they are expressly required. Pencils may be used only for drawing, sketching or graphical work. To facilitate efficient marking, please make your answers brief and to the point.

Material Covered in Final Exam

- **Lecture topics covered:**
  - Course Intro
  - Wireless Comms and Security Overview
    - no need to know the detailed structure of SHA/HMAC, Feistal function/structure, DES structure.
  - RSA/DH, CA, SSL, Kerberos
  - Network Layer Security, IPsec,
  - EAP, WLAN 802.1X Authentication
  - Broadcast Authentication
  - Bluetooth Security
  - **IDS, IPS**
- **GUEST Lecture topics :**
  - Guest lecture (except IDS/IPS) details are not covered in the exam however, general ideas having reviewed the notes are expected. Please review the lecture recordings as a refresher if you didn't attend these lectures.

Material in Final Exam (contd.)

No direct question on lab commands/programs but design concepts learnt in labs would be useful in answering some questions.

Assignment/Project: No programming in exam but concepts of protocol design either in Assignment/Project or in general covered in other parts of the syllabus.

In-class discussions: You must be aware of these discussion, some of these have extended lecture material and you should cover these.

Exam Format

- Open book: only printed lecture material, Text books, no computers allowed. This is worth **40** marks.
- There will be a number of questions (some with parts a, b, c) which will provide scenario and ask you to design protocols, check if a given design is correct, identify security problems etc.
- You should have a good grasp of basic crypto mechanism, key distribution techniques, and various attacks etc. as learnt through both lecture, discussions and labs. A small part may go beyond notes, i.e. if you aspire to get HD ☺
- *Students must score at least **20** marks in the final exam to pass this subject.*
- Total number of sections: 2. *Answer all sections and all questions in each section.*

Sample Question1

Consider the following pseudo-WEP protocol. The key is 4 bits and the IV is 2 bits. The IV is appended to the end of the key when generating the keystream. Suppose that the shared secret key is 1010. The keystreams for the four possible inputs are as follows:

101000: 00101011010101010011011010100100 . . .
101001: 10100110110010101110100100101101 . . .
101010: 00011010001111000101001010011111 . . .
101011: 11111010000000001010101000010111 . . .

Suppose all messages are 8-bits long. Suppose the ICV (integrity check) is 4-bits long, and is calculated by XOR-ing the first 4 bits of data with the last 4 bits of data. Suppose the pseudo-WEP packet consists of three fields: first the IV field, then the message field, and last the ICV field, with some of these fields encrypted.

- We want to send the message m = 10100000 using the IV = 11 and using WEP. What will be the values in the three WEP fields?

Sample Question-2

这里说要取代公钥加密方法,所以说用实现准备好的对称秘钥来交换session对称秘钥

Suppose Alice wants to communicate with Bob using Symmetric Key Cryptograpy using a session key Ks. In this question we use a Key Distribution Centre in place of Public Key Cryptography. KDC shares a unique secret symmetric key with each registered user. For Alice and Bob, denote these keys by $K_{A\text{-}KDC}$ and $K_{B\text{-}KDC.}$ Design a scheme that uses the KDC to distribute the session key: A message from Alice to the KDC; A message from KDC to Alice; and finally a message from Alice to Bob. The first message is $K_{A\text{-}KDC}$ (A,B). Using the notation $K_{A\text{-}KDC}$, $K_{B\text{-}KDC}$, S, A, and B answer the following questions:

A) What is the second message?

B) What is the third message?

对称秘钥有两个
1 对称秘钥
2 session 对称秘钥

(Exam question may be longer a bit more complex)

Sample Question 3

- Suppose Bob initiates a TCP connection to Trudy who is pretending to be Alice. During the handshake, Trudy sends Bob Alice's certificate. In what step of the SSL handshake algorithm will Bob discover that he is not communicating with Alice?

  在last step trudy这边没有Alice的私钥所以得不到最后一个random num ,

Solutions?

- These questions give you a flavour of how you should approach your preparation.
- Keep an eye on Moodle for solution one week before exam (this gives you opportunity to revise and try yourself).
- Please send your queries related to exam via Moodle.

Final Results 2018

- Total Students attended 59
- HD – 17
- D - 21
- C – 12
- P - 6
- 3 Students failed due to double pass in final exam.
- Final exam of 40: ***Average 28.6, Stdev=5.7***

MyExperience Survey!

- Two new labs (Crytpo and IDS)
- Rewriting of some lab specs
- Lectures
  - New material on Kerberos and IDS/IPS
  - New demo on IoT security
- Guest Lectures:
  - Lot more new guest lectures (Insider Attack, BC, Privacy.)
  - 2 Industry guest lectures.
- New hands-on assignment/project despite being 10 week term

Thank You

- And good luck with final exams.