DSV SU

IntroSec
Introduction to Information Security
Autumn Term 2018

Alan Davidson

Written Exam

2019-01-11
1pm – 5pm (4 hours)

Examinees should be clear on the marking principles for this exam. For more details see the next page. Students **should answer <u>all</u> the questions** in order to have a reasonable chance of securing a pass mark.

You are not permitted to have any extra material at this exam.
Dictionaries that do not contain notes are permitted, though electronic dictionaries are not.

Your answers may be in Swedish or English.

Instructions

- Do not answer more than one problem on each separate sheet of paper.
- Write legibly and with clear use of language. Answers that are difficult to read will not be marked.
- Wherever you are unclear on the premises for a problem, clearly document any assumptions that you make in your answer.
- Use by all means both sides of your answer sheets.

Important note on re-sits

Students who do not pass this exam have every right to take resits until a pass is achieved. You will not be penalised for failing an exam and re-sitting it later. Therefore, if you for any reason do not feel that the answers you give at this exam are a true measure of your ability, you may (indeed are encouraged to) choose instead to hand in an empty cover sheet, and re-sit the exam at a later time.

Some Advice...

Please note that these problems call for you to provide various descriptions, discussions and explanations. Your answers should be measured so as to be good descriptions, etc., i.e., you should not make your answers so brief as to leave the examiner guessing at what you are describing. Nor should they be so long as to cloud the central issue. Communicate your understanding of the subject matter as if you were explaining to someone who does not understand. Your ability to communicate on these subjects is part of the exam.

In general, to gain full credit for a problem you must not only show that you understood the terms and concepts involved, but that you can reason around and critically analyse the problem area.

Examination Marking Information

The written examination is comprised of five separate questions. Each of these questions can be graded as follows:

Pass	The answer communicates understanding of the terms and concepts involved.
Pass+	The answer communicates good understanding of the problem and clarity in the answer.
Pass++	The answer communicates good understanding of the problem and gives a complete, balanced and insightful answer.
Fail	The answer does not sufficiently fulfil any of the above requirements.

The written examination as a whole is awarded one of the following grades:

- A All answers are passes where at least four answers are a Pass++.
- B All answers are passes where at least two answers are a Pass++, at least two of the remaining answers are at least Pass+.
- C All answers are passes where at least four answers are at least Pass+.
- D All answers are passes where at least two are are least Pass+.
- E All answers are passes.
- Fx At most one answer is a Fail and at least two are at least Pass+.
- F None of the above criteria have been met.

Where an Fx grade is awarded it can be assumed that the student has proven their ability in most of the course's subject matter, but for some reason failed within a more narrow subject area. The student can then, after the exam, elect to be set an additional task that allows them the opportunity to show that they can meet the course goals within that subject area. Exactly what that task comprises will depend on the individual situation. Students who elect for this alternative and who are judged successful in the additional task are then awarded no higher than an E grade.

Problem 1

A more recent tendency in the security management of computer systems is to accept that the perimeter of the system (as in, for example, at the system's interface with the internet) cannot be perfectly protected. For this reason it makes good security sense to build systems that are resilient even to having malicious actors or malicious code within your system.

Suggest and describe up to three different effective security methods or mechanisms that could assists in providing protection in the face of malicious agents acting within the outer bounds of an IT system.

Problem 2

As authentication methods, both passwords and biometrics have their pros and cons. Discuss and motivate security problems that are inherent to password based authentication where biometric methods might be assumed to be free of these specific problems, and likewise discuss and motivate security problems that are inherent to biometric methods where password based authentication might be assumed to be free of those problems.

Problem 3

An innocent and honest party can suffer security issues in the processes of both sending and receiving e-mails. Describe up to three such separate security issues, as well as measures that one can go to in order to mitigate each of those issues.

Problem 4

Define each of the following IT security related terms. Also, for each of these terms further illustrate the concept by choosing a closely connected IT security concept and explaining the relationship between the concepts. Furthermore, give an example of an application of these tools/threats/concepts. Give concrete examples wherever possible. Structure each of your answers with headings *definition*, *relationship to [your chosen related concept]*, and *example*. **Your answers to each part should contribute to evidence of your deep understanding of the concept. Related concepts and examples should be chosen and explained with care to maximise the depth of your answers.**

Students may find it helpful to use the pre-printed problem 4 answer sheet for their answer. Those who choose not to should take care to follow the above instructions extra carefully.

Please note that in general a 50% complete answer will be required to obtain a pass mark for this problem

- Self Signed Certificate
- Attribute Based Access Control
- DMZ
- Worm

Problem 5

Explain why a set of cooperating hosts (sometimes referred to as a mixnet) can give a more reliable anonymity service than a single anonymising host is able to give when mediating network traffic. Good explanations will include explanations of relevant threats to anonymity that these services have to deal with.