Written Exam

2019-01-11
1pm – 5pm (4 hours)

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.