DSV SU/KTH

IntroSec
Introduction to Information Security
Autumn Term 2015

Alan Davidson

Exam Re-sit 2016-08-16
Hints and Comments on the Marking

Suggested answers are not provided for this exam, only some pointers to help you validate your own exam answers. Do not assume that the comments here are complete examples of how the exam problem can be answered.

Problem 1

> Wikipedia (2016) defines Access Control Matrix as:
>
> "... an abstract, formal security model of protection state in computer systems, that characterises the rights of each subject with respect to every object in the system"
>
> Explain this definition further by breaking the sentence into suitable constituent parts and explaining what each part means, by all means including helpful examples. The result should be a text that could help anybody who does not entirely understand the original definition to gain better insight.

"abstract" – The Access Control Matrix expresses an idea. There may be practical implementations of that idea, but not necessarily.

"formal security model" - The language used to express the matrix follows stringent rules, at a formal level equivalent to mathematical or logical representations.

"protection state" - The purpose of the model is to describe a state in which resources are properly protected. The matrix describes only a single state of a system, and not the possible state transitions, e.g. what happens when an object is added to a system is not described.

"computer system" - The state described is assumed to express protection of any resource that has any place in a computer system. At such it could just as well describe the protection state of a network of computers as a single processor's registers (N.B. it is a mistake to assume that subjects are people and objects are files).

"that characterises the rights of each subject with respect to every object in the system" - each and every subject is mapped to every object with respect to a set of rights (which may be empty). Where subjects are processes and objects are files, typical examples of rights might include *read*, *write*, *execute*. The matrix's mapping of all such subjects to objects in respect of rights is commonly represented as a table where each column represent a single object, and each row a single subject, the intersection cell of which contains the rights for that subject over that object.

Problem

> Give examples that well illustrate how multifactor authentication is commonly used in practical authentication situations. Discuss also why this practice might generally be assumed to be an improvement over single-factor authentication.

The problem asks for examples in plural. Good answers therefore use several examples to illustrate how multifactor might involve diverse kinds of authentication methods, such as something the entity has with something the entity knows, but also other combinations such as "... is & ...knows", "where the entity is & ..has", or "...knows & ...knows".

Good discussions on the motivation might introduce relevant security principles, as well as careful

logical motivation.

Problem 3

a) Characterise and explain what protection simple traffic filtering firewalls (as described in the course literature, and as opposed to the hybrid products that can be obtained on the market under the name “firewall”) may be able to afford a computer network. Be explicit as possible on what kinds of security problems such a firewall best can protect from.

b) Give differing illustrative examples of attacks on a network that it is unlikely that such a firewall will be able to protect against. Include detailed motivation.

Some examinees assumed that the “simple traffic filtering firewalls” was referring specifically to “packet filtering firewalls”. The was not the case, but all the types covered in the course book were included. The question was therefore asking the student to give a general explanation for what firewalls do and how they do it. The interpretation of considering only packet filtering was not regarded as a very serious mistake, so long as the student could properly explain how this type of firewall works.

There is a wide range of discussions on attacks that firewalls are unlikely to be able to protect against. Some are considered to be better illustrations of the failings of firewalls than others. For example, social engineering attacks are indeed difficult to filter out, but this says little about firewalls. On the other hand, traffic being transmitted through an encrypted VPN (and through a firewall) can be a good example to illustrate the limits of the firewall concept.

Problem 4

Describe 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.*

Some 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:

- One-Time Pad
- Replay Attack
- Complete Mediation
- Certificate Authority

Suggested solutions for problem 4 are not complete in this version of the document. Please see the course book and other relevant sources in the reading notes as well as the course video material for definitions and examples.

Suggestions for closely related concepts that can allow for productive discussions on the relationship:

- One-time pad - vigenére cipher
- Replay attack - eavesdropping
- Complete mediation – unvalidated input
- Certificate Authority - PGP

This does not mean to say that naming these concepts is sufficient for an answer. They must be meaningfully related to the given concepts. I suggest that they are close enough to the given concept for the examinee to be able to show deeper understanding of the given concept through their

comparison.

Problem 5

> Consider the following statement and discuss how this position can be justified, based on elements of the course material:
>
> "Spam emails are always an offence to personal rights, and therefore a security issue. Furthermore, spam is sometimes used as a precursor to a type of attack that makes them even more serious a security problem"

This problem invites the student to show their understanding of *spacial privacy* issues as well as such email threats as, for example, *phishing, web-bugs, executable attachments,* etc.

References

Please note that exam answers are not (necessarily) expected to give exact references, but these notes attempt to do the reader the respect of giving references where suitable.

Wikipedia 2016 Wikipedia, *Access Control Matrix,* Available at: https://en.wikipedia.org/wiki/Access_Control_Matrix [last accessed 2016-08-15]