DSV SU/KTH ***IntroSec***

Introduction to Information Security

Autumn Term 2015

Alan Davidson

Suggested Solutions to the Exam 2016-01-15 and Comments on the Marking

Some answers suggested here may be more comprehensive than would normally be expected from students in order to cover several relevant aspects of the problem.

Problem 1

a) Explain what aspects of a system are balanced in a risk analysis in order to practically apply reasonable security safeguards.

b) Discuss reasons why this balancing of relevant aspects can in practice be difficult to achieve.

a) As expressed in the course book: “A basic model of risk management involves a user's calculating the value of all assets, determining the amount of harm from all possible threats, computing the costs of protection, selecting safeguards (that is, controls or countermeasures) based on the degree of risk and on limited resources, and applying the safeguards to optimize harm averted” (Pfleeger, Pfleeger and Margulies, 2015, p23). If the costs of protection are too great in the balance of how effective that protection is against the loss of asset value, then one has already 'lost'. There is no such thing as perfect security, unless it is finding the perfect balance in a risk analysis.

b) One way to take this discussion could be:

Values of assets are not necessarily easy to put figures on. Aspects that could be affected in a security situation include such intangibles as public confidence in your organisation. A sense of feeling secure might in some situations be valuable, as separate from the true ability of a security measure to protect an asset, e.g. visible security measures at an airport might make customers more inclined to feel safe and therefore fly, even if they might not be totally effective. How much some aspects of assets are worth could be dependent on the philosophical, religious, ethical, profiteering etc outlook of the parties involved, where there is no clear consensus on what is best. One might for example question why so much security expenditure has followed the 9/11 attacks in USA when americans themselves seem to be responsible for killing some ten times as many people each year on the roads (WHO, 2015) without a comparable expenditure on hindering such deaths compared to deaths attributed to terrorism.

I am puzzled and despondent that so many answers to this question simply brought up the CIA triad. It should be very clear from the course book and lecture discussions that the important element to a risk analysis is that of the value of assets. I have a worrying suspicion that the only reason that students have answered this way is that the keyword “balanced” in the problem text could be associated to a separate discussion from lectures, i.e. where we showed how we should not presume that security is a point of perfect balance in the centre of the CIA triad. Having said this, there are other possible points of association between the CIA triad and risk analysis. In the course book, the authors use the triad as part of a mapping in an illustrative table that they suggest for one single phase in a risk analysis (p674). It would surprise me if this was the source of students' erroneous answers since that part of the book is not part of the course, i.e. it is not within the course reading notes.

Since there was such a distinctive pattern to so many students' wrong answers for this problem I felt obliged to question if anything that had happened on the course could be the source of students getting the wrong idea. If that were the case one might think that this could be seen as an 'unfairly' difficult problem to set. In this perspective I ended up trying to read the most I possibly could into answers to see if they could be said to be worthy the lowest possible passing grade, even when the answer was wrong. I therefore decided that answers that showed capable reasoning around the wrong answer could conceivably be given a pass grade. I nevertheless worry that the real reason for the low occurrence of good answers is that some students might assume that exam problems will not be set based on passages of course book, even when they are covered in the reading notes.

Problem 2

> Even within relatively small organisations it is quite reasonable for a single user's Internet traffic to pass through three separate firewalls before reaching the Internet.
>
> a) Explain in terms of general security design principles why this strategy could be considered good security practice, but identify and explain also any principles that suggest that this could be bad for security.
>
> b) Explain the likely roles of the specific firewall types involved.

a) In the most general terms we can state things like: Redundancy in security mechanisms is a wise strategy, as is Defence in Depth (here in the IT security sense of the term rather than the military one). But since the problem specifically relates to security design principles we associate with such principles as those defined by Saltzer and Schroeder (Pfleeger, Pfleeger and Margulies, 2015, p212), more depth is required. There are all sorts of ways to reasons sensibly around the principles in this context, the following being one attempt.

The Saltzer and Schroeder principle that is most closely associated to the ideas of Defence in Depth is that of Separation of Privilege. If access to all objects should depend on more than one condition, then access of data from the Internet to the local computer (as well as vice versa) will pass through several firewalls on the way, each of which will presumably have their own differing set of access conditions.

We might make the case for the firewalls being an implementation of the principle of complete mediation. It is tricky to claim this without in part answering part b of this problem, since without knowing which resource the firewall mediates the traffic to, it is hard to claim it is complete. If the firewall is on the Internet side of a proxy server then one would expect all traffic from the Internet to be routed through that firewall, and that firewall to in some way check all of the incoming traffic. The firewall can then be said to be implementing complete mediation of Internet traffic for the proxy server. A similar point can be made in case the firewall is of the personal sort. Such a firewall should mediate all network traffic going to that individual computer, i.e. Internet as well as from the local network.

The principle of least common mechanism can also be cited, inasmuch as different network filtering responsibilities can be separated between different firewall devices rather than sharing the same resources.

When it comest to the principle of Psychological Acceptability, three separate firewalls could mean a security problem. If, for example, it is found that legitimate traffic is not being passed, the reasons for this could have one out of three sources. But searching for errors will be difficult. It can also be more difficult work for an administrator to correctly configure three firewalls compared to one.

Some students argued that having several firewalls is likely to slow down network traffic and thereby negatively affect psychological acceptability. In fact, three firewalls would work in parallel, so they presumably would slow things down less than one more complex one.

Some students also cited the problem of upholding the principle of economy of mechanism in the firewalls. I think this is a tricky argument. The problem text discusses having three firewalls, so I can question why having three firewalls would be more of a problem for economy of mechanism than having one. Each individual firewall could be said to be simpler than a single firewall that tried to do all the filtering, and that seems to uphold economy of mechanism. Some argued that the security problem is complex, so that the firewall mechanism will be complex, which is against economy of mechanism. But once again the problem is about the strategy of using several firewalls, so this argument does not directly address that strategy, but firewalls in general.

b) One reasonable interpretation of the roles could be these are the inner and outer firewalls of a DMZ, and the personal firewall of the user's own workstation. For the sake of brevity in this suggested answer sheet I ask students to refer to the course book for descriptions of these firewalls' roles.

A number of students described the firewall types that we have covered on the course, i.e. packet filters, stateful inspection, etc. I would say that these are more *types* than *roles*. It is unfortunate if students have the idea that these are roles. That breakdown of firewall types is more about showing a historical progression of firewall technology that explains how they functionally are doing things on several layers of abstraction. These days it is unlikely that you would be happy with a firewall that only does packet filtering.

Problem 3

> Describe and motivate useful ways to relatively easily configure and use a personal web browser and mail agent in order to ensure reasonable levels of privacy and security while at the same time upholding reasonable levels of usability.

There are many ways to suggest solutions to this problem, just so long as they are well motivated, and can be said to keep to within the requirements that are set out in the problem text. We have covered several during the course, such as:

- The danger of client-side interpreted script languages such as Java, ActiveX, JavaScript.
- The problem of web page redirects that do not allow the opportunity user to inspect malicious URL content.
- The problem of how links to images in an html formatted email can signal to a server that as specific recipient has read an email at a specific time.

Other things we have studied also become relevant for this problem, such as we understand the advantages of using the https protocol over http, and the dangers involved in accepting (and thereby trusting) self-signed certificates.

In terms of upholding spacial privacy arguments can be made for configuring for spam filtering in an email client and ad blocking in a web browser. In terms of informational self determination one of the simpler and most important configuration options one can expect to be discussed is that of cookies. It is understandable that students propose different strategies based on which browser they are used to, given that what browsers allow one to configure differs.

Arguments that proposed the use of Tor and remailers were generally poor. One can surely hardly cite these as possible mechanisms without addressing the parts of the problem text that says “relatively easily configure and use” and “upholding reasonable levels of usability”. Such tools are for special situations were privacy is needed. You would suffer great problems in your everyday tasks if you were to always use these.

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:

- Ransomware
- Security by Obscurity
- Buffer Overflow
- Cryptanalysis

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 for definitions and examples.

Problem 5

Consider the following IT related ethical dilemma:

You are a security manager who is responsible, among other things, for the education of a number of staff within your organisation. You need them to know about the IT security threats that they and the organisation can be expected to be subjected to, and their responsibilities in the face of these threats. You have ordered a number of IT security textbooks to distribute to the staff to help them to understand the issues involved. However, the books are not available from the distributors, and they say that it will take several weeks for them to obtain new copies from the printers. One of the staff mentions to you that an illicit electronic copy of the book has been found and that several of the staff already have copies of this on their work computers. You find that the situation is not directly covered by any of the current organisational policy rules. You identify the following possible courses of action:

- You allow the staff to make use of the electronic copies while you are waiting for the books to arrive. Once the books have arrived and you have paid for them fully you ensure that all electronic copies are removed.
- You inform the staff that they should ensure that all such illicit material has no place on the organisation supplied computers and must be immediately removed. You do your best to educate the staff without the textbook, and then schedule in some follow-up work once the books are available.
- You cancel the order for the text books and allow the staff to use their electronic copies until you think you have completed their education. You instruct the staff that they must remove all copies from their computers after the end of the course and tell them that they must not tell anyone that they made use of this material. You imagine that this is likely to please the heads of the organisation not least because the overheads for the education of the staff will be less than you budgeted for, though you can think of other reasons.

a) Apply and document accepted basic ethical principles with careful balanced reasoning to motivate a suitable course of action.

b) Suggest how your course of action would be likely to be affected if you were an ISACA certified professional and subject to their Code of Professional Ethics. Suggest in outline what kinds of ethical rules you assume are included in such a code and that effect this decision.

A brief comment on the marking:

Answers to this problem must show an understanding of the principles for ethical reasoning that are well documented in the course book. It is quite possible to make arguments that show that each of the problem's scenarios are quite reasonable depending on whether one interprets the situation in a telelogical egoistic or utalitarian view, or a rule-based view. One cannot satisfactorily answer this problem without referring to which principles on which one bases the interpretation of the scenario.

I had to assume that discussions that held that the student's answer represented the only viable ethical point of view were evidence that the student had not properly studied the course literature on ethics.

For part b marks were given for any discussion that held evidence that the student had a good idea of the kinds of rules that are common in codes of professional ethics, and how they would effect the answer. ISACA is named in the problem since that is the specific example that given in the reading notes, but specific knowledge of any of the ISACA rules were not expected or required. If one did have specific knowledge, one could cite a rule that suggests the second scenario, i.e. “Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association” or else a rule that can be said to contradict the second scenario, i.e. “Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including: audit, control, security and risk management”.

References

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

Pfleeger, C.P., Pfleeger, S.L. and Margulies, J., 2015. *Security in Computing.* 5th ed. Massachusets: Prentice Hall

WHO, 2015. *Global status report on road safety 2015.* http://www.who.int/violence_injury_prevention/road_safety_status/2015/TableA2.pdf?ua=1, last visited 2016-02-01