DSV SU/KTH

IntroSec
Introduction to Information Security
Autumn Term 2018

Alan Davidson

Suggested Solutions to the Exam 2019-01-11 and Comments on the Marking

(First Incomplete Draft)

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 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.

The problem sets the context of system security. Of the models that we have covered during the course this might suitably remind you of Pfleegers figure 1-12, *Effects of Controls* (Pfleeger et al, p30). That would help you consider ideas such as deterrence, detection and recovery to lead you into methods and mechanisms such as encryption of sensitive data, implementing strict access control policies, IDS, Antivirus, backup, etc, all of which might be suitable to include in your answer.

Note that according to the problem description the threat is already inside the system. What kind of IT system is involved is up to the examinee to define, but we may reasonably consider it to be a network of computers. For that reason we can discount measures such as DMZs. Other possible measures that the examinee could bring up are more numerous to mention here. The quality of the answer will depend on how effective the method might be assumed to be, and how well they are described. A selection of possible subject to expand upon are (only very briefly) listed below.

Access control. For example a stringent MAC based system could be effective at segregating parts of the system, both between network nodes and within individual computers, so that a malicious agent that manages to gain low levels of privileges should be effectively contained.

Encryption of sensitive data.

Logging of activities, (including with intrusion detection systems, and intrusion prevention) can be spread throughout a system. Integrity checks on sensitive data sets (such as by means of well protected hashes) can aid in detecting if something that should not change has been changed.

If we see “the system” as a network of computers then Personal Firewalls could prevent the attack from spreading either to individual personal workstations, or conceivably even stop a threat from spreading out from a compromised station.

One could state that malware protection such as antivirus is a suitable measure, though during the course we have suggested that these might not be as effective as one might assume. That does not mean to say they cannot be valuable though.

Education of users could be cited as a measure, though that is extremely vague unless one can explain what kind of education can be expected to be effective.

A few suggested a sandbox as a possible measure. The descriptions around this suggestion were generally vague. A sandbox, or jail, is normally used to segregate parts of a system that are possibly a threat, such as testing a new program that one is not sure about. If an attacker is within the outer bounds or your system then if you are able to isolate their activity so well so as to be able to put them into a sandbox then you might as well eradicate them. Sandboxes are therefore not a practical means of containing a malicious agent, so without clearer motivation, such answers were assumed to be somewhat confused about what sandboxes are used for.

A honeypot is a kind of sandboxed environment that is more specifically designed to preoccupy and contain a malicious agent while it is being analysed. The honeypot is a well known security measure, but suffers that same problem as a Sandbox, i.e. if one has good enough control over the agent to be able to segregate them, then they are not much of a threat. The difference with a honeypot is that it can be made to look like an attractive target so as to lure an intruder into it.

Some answers cited Saltzer and Schoeder's principles. Since the problem specifically asks for *methods and mechanisms,* citing principles is generally too vague to be called something so specific as a method. Citing principles without explaining how they would be applied to provide protection is too vague as an answer.

The most sensible interpretation of this problem text is that it is about system configuration. The best answers were therefore the ones that saw this, and presented suitable methods and mechanisms in this context. A number of answers drifted into aspect of software security, such as "apply complete mediation in all programs in the system to avoid dangers such as buffer overflows, SQL injection etc". Surely in modern systems I have little control over how all that software that one uses is actually written. I therefore had to assume that such answers showed a confusion about measure that were applied during separate parts of the course that are not so applicable to this problem.

Some wrote very generally about good authentication and strong firewalls, and other such issues that one surely can claim are more about protecting the perimeter of a system. If the threat is within the system one should possible assume that they have already bypassed such measures? There are certainly cases to be made for applying firewalls within the system to help protect different parts from each other (see *personal firewalls* above), or that implementing things like processes of continuous authentication might be able to hinder some malicious actors that already are in a system. However, I have to be suspicious of generally stated answers about authentication, firewalls, etc, assuming that the examinee did not fully understand the context of where such mechanisms are suitably applied.

One student wrote about locking a computer when you leave it. If you can describe what kind of threat that that measure is effective against, I can certainly award points for that.

On entering the exam hall several examinees asked for a clarification of the first exam problem, so in case others were labouring under misinterpretations of the problem text, I explained that "within the outer bounds of the system" means that the threat is already inside. The first paragraph of the problem sets the context that the threat is inside the system. Taken on its own the phrase "within the outer bounds" could possibly be taken to mean "a part of the outer bounds" rather than "on the inside of the system past the outer bounds". In normal English usage I would say that the second interpretation is so clearly the correct one that I did not even consider that one could twist it to mean the former. However, this could be an issue beyond the expected level of English language, so I have to consider that it could be an issue. However, given the context set in the first paragraph I can say that this is the only reasonable interpretation. I have to conclude that a student is only likely to go with the first interpretation if you find it much easier to answer about Firewalls, DMZs etc. and therefore lead ones own self to answer incorrectly.

Grading:

P Showing understanding of some ideas that could be relevant for the issue, but they are unclear on the context of the problem, vague in application, etc.

P+ Good clear answer on the most relevant of methods for protecting a system, but do not show great breadth in the examples shown.

P++ Enough clearly described methods to show a good understanding or the context and the possible solutions. Note that the “complete” in the grading criteria is not interpreted as giving an exhaustive answer, but one that is enough to show reasonable mastery of the subject and perspective within the time available.

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.

In no particular order, here is a list of some of the aspects that one might use to develop arguments. Please note that for brevity here I am only giving hints without discussion and motivation. **Discussion and motivation is however a vital part of the exam answer** to show that you understand the issues and are able to communicate them well.

You can change passwords if they are stolen or eavesdropped, but if biometrics can be replicated (such as through lifting and replicating fingerprints, as demonstrated in the *Mythbusters* clip linked in the course material), then there is no easy way to revoke the fingerprint data to stop the use of the false fingerprint.

You can forget passwords, but presumably not biometrics (well, maybe which finger was used for a fingerprint?).

Cost of implementation - It is certainly true that in general biometric methods will require more specialised hardware to work, though a camera can be used, and that is not specialised equipment for biometrics, and a keystroke measures can be used in biometrics, requiring exactly the same equipment as a password. What is more, card readers have keypads specifically for the purposes of entering a pin code, so I would be wary of assuming that every device that is part of an authentication process can be expected to already have a keyboard.

Privacy can be an issue for biometrics. Biometric data is linked to identity so one must reveal one’s identity when authenticating. There are authentication situations where it may not be necessary to be personally identified, such as having a door code for access to a building.

Passwords are subject to human tendency to choose guessable patterns. Guessable patterns could conceivably be a part of biometric data, but we may suppose that designers of those methods will have greater opportunities to avoid capturing guessable data form biological traits.

One can inadvertently leave traces or otherwise reveal some biometric data in situations outside of the authentication situation. Fingerprints can be left that could allow false facsimile fingerprints to be created. A highly detailed camera might be able to capture iris patterns without the subject deliberately presenting their eye. Though it is possible to inadvertently reveal passwords outside of the authentication process (as well as during that process) that could be put down to carelessness, whereas keeping biological attributes confidential is not a natural part of how we use our bodies.

A number of answers brought up the issue of biometrics being susceptible to false positives and false negatives. There is a case to be made for this, but when compared to passwords there is surely a case to be made that passwords can also suffer badly from the problem of false negatives. Accidentally tying the wrong password is surely a common occurrence, and a faulty keyboard can cause even a correctly typed password to by registered falsely.

If you site the fact that a finger can be cut or burned and spoil authentication, one must surely question if that is more of a problem than occasionally forgetting a password. Surely any authentication method must have an alternative authentication means in order to be able to reset?

Can it be claimed that fingerprints are unique? As Pfleeger (p62) says – there is actually no no definitive scientific scientific evidence for such a claim.

Please note that It has not been claimed on the course that voice recognition will fail if one has a cold. Nevertheless a number of answers claimed that this is a tangible problem with biometrics. In fact research on this subject says that voice recognition systems will use metrics that are not greatly effected by situations such as a having a cold (see e.g. https://whatsnext.nuance.com/customer-experience/five-common-misconceptions-voice-biometrics/). The same applies to facial recognition and claims that smiling, or growing a beard might render them inoperative. Sensible biometric methods would use data that is not sensitive to such changes. One should perhaps check one's preconceptions before using them in exam answers.

I found that a number of answers stated many facts about the respective authentication methods without regards to how they compared to the other. For example, if you state that users tend to reuse passwords for several systems, I do not know what you want to say about how that compares to biometrics. Surely biometrics will force you to re-use your bodily data to authenticate on different systems, so it is not at all clear what comparison students hoped to draw with such an argument.

Some claimed that biometric authentication could not be prone to social engineering attacks as compared to passwords. I do not see how one can be categorical in such a claim. If a social engineer can convince someone to use their BankID to transfer their savings, I am sure that a good social engineer could convince someone to use their biometric data in situations that are against their own best interests.

Pfleeger et al has quite an extensive discussion on the pros and cons of biometrics, so much material for an argument could be found there. It was however fairly common for students to repeat such arguments yet with some dubious reasoning. Though as examiner I understand where your arguments might have come from, if I found the description and motivation to be less than stringent you may well find that I have dotted your exam papers with comments that question whether you are uncritical or even mistaken in your interpretation of what Pfleeger wrote.

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.

It is possible to include attachments to emails that are a threat to the recipient's systems, in particular if such attachments are executable files that are possible to run within the recipient's system, with the privileges of the user.

Mitigation may be through education of users that it can be extremely dangerous to save and execute attached files that come for a source that one does not have implicit trust for, so that a recipient knows what allowing an attachment to run code involves, and how to avoid letting it do so.

Emails that contain rendered html code can be a security threat. Web bugs are links to external servers that make use of the fact that if that if included images are linked to an external source for the image contents then the html renderer will normally fetch that image as the page is being rendered. The URL that is used can be a link to a server-side process that registers who requested to fetch the image, and when, thereby revealing data on those who view the email.

Html mails can also contain other kinds of harmful elements, such as links to external websites together with exhortations to click on such links. This could be the means of implementing a phishing attack, or a non-persistent XSS attack.

Problems in sending are primarily connected to inadvertently revealing information that can be to the sender's detriment. The SMTP protocol sends emails in clear, so any relaying party along the path of delivery, as well as any party who manages to eavesdrop SMTP traffic along the way, would have access to the content of emails. Mitigation – use additional mechanisms that allow for end to end encryption of email content.

Spam and Spacial privacy. Mitigation through spam filters and legal measures.

More to come later...

P++ Three well described problems with mitigation methods

P+ Less than three relevant problems and mitigation are well described (implying that less than three have been attempted, or that some part of the descriptions is vague or confused).

P An attempt to describe problems and mitigation that might mean something to a person who already understands.

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*. **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.**
>
> 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:
>
> - Self signed certificate
> - Attribute Based Access Control
> - DMZ
> - Worm

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.

Self signed certificate

Definition

A public key certificate that has been signed with the aid of its matching private key, thereby allowing no more trust for this certificate than the simple data integrity check that an untrusted digital signature affords.

Relationship to

E.g. A CA signed certificate. (This part of the suggested answer sheet is not yet complete.)

Example

When creating a PGP asymmetric key pair the private key is automatically self signed by the PGP system. In this system one would tend not to trust any such certificate unless it has been verified by the owner through some alternative channel. Other PGP users may choose to add their signatures to the self-signed certificate, therefore bestowing it with greater validity within a so called *web of trust*.

Attribute Based Access Control

Definition

Attribute Based Access Control is an access control mechanism whereby one represents rights in terms of attributes that are may be present in either subjects or objects, or both, also allowing elements of context to define rights.

Relationship to

e.g. RBAC (This part of the suggested answer sheet is not yet complete.)

Comment

MAC and DAC are policies that define how rights should be updated when the system changes. They therefore have only a tenuous relationship with ABAC which is difficult to make sense of in the limits of this exam question. ABAC is closer to ideas of ACL, Capabilities and RBAC, so those comparisons make more sense.

Example

ABAC could be used to simulate a Bell LaPadula type of policy if the subjects and the objects are given attributes signifying their levels. A single line in an ABAC specification could then signify that subjects with Top Secret clearance may read all objects with a Top Secret label as well as all objects with a lower level.

DMZ

This part of the suggested answer sheet is not yet complete.

Definition

Relationship to

e.g.

Example

Comments

Worm

Definition

Relationship to

e.g. (This part of the suggested answer sheet is not yet complete.)

Example

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.

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 fifth ed.

https://whatsnext.nuance.com/customer-experience/five-common-misconceptions-voice-biometrics/