DSV SU/KTH — ***Säk1B/IV2024***
Information and Computer Security
Autumn Term 2009

Alan Davidson

Suggested Solutions to the Exam 2009-10-20 and Comments on the Marking

Note that since these answers can cover several aspects of possible answers and also discuss these answers, they can contain more than would normally be required for full credit. Indeed, it is normally a strength if the student can give concise exam answers, whereas the following text seeks to be a thorough, comprehensive discussion.

Problem 1

> Bruce Schneier has coined the term *Security Theatre* which he describes thus:
>
> "Security theater consists of security countermeasures[1] intended to provide the feeling of improved security while doing little or nothing to actually improve security." [Schneier03,p38]
>
> a) Discuss what influences in society may encourage security theater.
>
> b) Suggest in outline a more methodical approach to implementing security measures that would hopefully avoid the negative effects of security theater.

We might hope that any resources that are spent on security would help to improve security, but if Bruce Schneier is correct that is not always the case. In general we could surmise that where security theater[2] occurs the parties that are responsible for the implementing security gain more from giving the impression that they are doing something useful rather than actually doing something. There may of course be several reasons for this, but the question is specifically about influences in society, so in the following discussion we can exclude personal motives, such as the criminal (e.g. I will sell you an antivirus software that has trap-doors in it so that I can gain access to your computer without you knowing it) or lack of competence (e.g. I don't know how to secure my bosses computer, but he has told me to do it so I should do something that looks good to keep him happy).

a) The feeling of security clearly has a value to people and may make them act in desirable ways, such as to buy things on the Internet or to fly in aeroplanes, where feelings of insecurity might otherwise hinder them from doing so. However, security is no doubt too complicated a subject for the normal person in the street to understand enough to make judgements on whether security countermeasures actually work. At the same time there is much to suggest that that person in the street in not willing to pay much for security. At a very general level we can therefore identify *ignorance* and *greed* on the part of the consumer, and *commercial gain* for suppliers as contributing factors.

For example, after a number of terrorist attacks on aeroplanes[3], including those of September the 11th 2001, the general public may have an idea that they should seek other means of communicating and travelling. There are not only commercial interest in keeping the public flying, but national interests to do with the economy in general and investment in the infrastructures that allow for

[1] The phrase "security countermeasures" can be a little confusing to foreign speakers of English, and I spent some time addressing this in the exam rooms. You could claim that Schneier has been a little sloppy in his English usage here, as "security measures" or "threat countermeasures" make better literal sense. Nevertheless it is quite natural to read this as meaning "countermeasures for the sake of security" which is surely Schneier's intention.

[2] I use the American spelling since that is what Bruce Schneier naturally used when coining the concept. As an English speaker I am very tempted to alter the concept slightly and call it Security Theatre)

[3] Examples from the field of IT security are normally preferred in exam answers, but this example happens to be one that Schneier himself refers to as an example of Security Theater.

communication and travel. Making security measures obvious to the traveller, such as prohibiting sharp objects on a plane (even though a ballpoint pen can be lethal in the hands of an experienced assassin), or limiting the amount of liquids allowed for each person (even though a colluding group of passengers could carry a dangerous amount of explosives when all their liquids are added together) could be part of a Security Theater that would make us feel that so much is done that we can continue to travel by plane, even suffering the indignity and the inconvenience that such measures might entail.

Note however that these Security Theater measures may have a role in *raising the level of security conciousness* in people, so that one would be extra vigilant. Understanding that security is important and that there are measures all around one, a person might be more inclined to report someone who was trying to set fire to their shoelaces on a plane than on the street. This is one example of when Security Theater might have an indirect real effect.

Another possible real effect is when fake security measures are employed to utilise the fact that attackers might be ignorant of the difference. For example, one can buy a flashing LED light to install in your car window to emulate the kind of light that shows that an advanced car alarm system has been activated. Just the flashing light might discourage some attackers from breaking into the car. But with this example we are getting away from the *influences in society* part of the question again.

Security Theater may be used when there is a real threat, but it is possibly more likely to be used *to counter a perceived threat*. There may be elements in society that have a vested interest in making the general public afraid of a threat, even when the threat is in reality not so great. It is easier for journalists to sell us stories that tell us that we should be scared of something, so in general we might expect the media to provide us with a picture of our society that is more scary and dangerous than the truth. Politicians, especially those in opposition to those that are in power, can gain from promoting a picture of insecurity which might make us believe their policies are sound. We might vote for a party that will promise to invest in law and order if we perceive that there is a growing crime problem. We might even give an elected government extended powers over us if we perceive that there exists a threat that the state can solve when they have such powers. For example, we might normally expect that our privacy rights would prohibit anyone from monitoring our network traffic. If, however, we believe that there is an imminent danger of terrorist attacks in our society we might be more complaisant when laws are introduced that allow government wire-tapping. Security Theater could therefore be used to implement a hidden agenda.

This is a discussion that can be held on several levels, and this example answer is only one of them. Whatever the level of discussion good answers are expected to show an understanding of the holistic nature of the subject of IT Security.

A few student discussions suggested that Security Theatre would not cost anything and is therefore better than doing nothing. Note that security theatre costs. Perhaps it costs less that real security, but it is a waste in real security terms, i.e. it could well be worse than doing nothing.

b) The problem here is that the security measures are presumably not having an effect on the security of a situation that is proportional to the cost of those measures. The quick and simple answer to this question is therefore to apply *cost benefit analyses* (though exam answers should of course also give an indication that the examinee understands the idea behind and what such an analysis involves). For a short explanation of what this involves you can refer to the course book [Bishop05, pp14-15]. Whether a cost benefit analysis is tractable in the situations where security theater can be found is a debatable matter, but the “hopefully” in the exam question allows us to stick our necks out a bit and assume that it could.

Some answers suggested that *risk analyses* would be required. Risk analysis can be seen as a counterpart to cost benefit analysis, and as such these answers were judged to be on the right track and an indication of an insight into the holistic nature of the subject.

On a more general level we could say that both cost benefit and risk analyses are reliant on good *security metrics*. This is an active field of research, and a tough subject. It is not a subject that figured greatly during the course though, so understandably answers that discussed the area of security metrics were few and far between.

A number of answers proposed the Common Criteria as a relevant security measure. As an approach to avoid Security Theater the CC is very limited, but it is certainly methodical. One could even claim that a method that certifies certain operating systems as secure, but the small print explains that this is only when computers are not connected to any peripherals, is helping to contribute to Security Theater! Answers that tied in the CC were given some credit, but were not judged as showing the same degree of the holistic insight of answers such as cost benefit analysis.

One answer suggested that the area of ethics could help against Security Theater. The argument was interesting and relevant, but it is hard to claim that it is methodical, as in the problem text.

Whatever actual method was chosen for the answer, points were awarded for convincing arguments, so long as they kept to the problem text.

Problem 2

> Having knowledge of which language is used in a clear text can assist a cryptanalyst in deciphering the corresponding ciphertext. This is true whether the cipher is based on substitutional or on transpositional methods (or a mixture of both). Explain in outline (i.e. you need not go deeply into cryptanalytical techniques) how.

Frequency analysis on natural language texts can for example ascertain how often a particular letter is likely to occur. In English, the most frequent letter is 'e', occurring 13.1% of the time [Davies&Price89]. In a simple substitutional method where each letter of the clear text has a direct mapping to a symbol[4] of the ciphertext, if we find a symbol occurring 13.1% of the time and if we know the language to be English, then we can surmise that that symbol was most likely mapped from an 'e'.

Patterns in language are not limited to frequencies of single letters. We find that certain combinations of letters are also language dependent. In English the letters 't' and 'h' occur together in a *digram* far more often than they do in, for example, Swedish. This also applies to *trigrams* such as 'the' and 'nce'. Imagine then a simple transpositional encryption method that has changed the order of the letters of a text. If we know that the text is English then if we can find a key and algorithm that would cause a large proportion of the letters 't' and 'h' to occur together then we have efficiently limited the space of possible algorithms and keys.

Note that the above explanation assumes that the encrypted text is long and non specific enough to exhibit close to the normal frequencies of a natural language. If a message is very short knowing the language help us in the specific way described here.

The above is just two examples of the kinds of patterns that could be utilised. Several student answers had other good examples, such as the fact that letters in English might contain the word “Dear” followed by the name of the recipient.

A number of students confused the cracking of cryptographic ciphers with the cracking of passwords, and therefore gave answers involving *dictionary attacks*. There is a vague connection in that dictionary attacks could possibly be used to crack the key used in an encryption under the assumption that the key itself can be set by a user, and that the user then chooses a work unwisely. However, this is a very big assumption, and it only helps if you already know which encryption method has been used. The problem text is specific that it is about you knowing the language that

[4] Several answers assumed that substitutional methods only substitute letters with other letters. This is not necessarily true. You could use any symbol set in substitutions. A number of answers even confused substitutional methods with alphabet shift methods such as the Caesar Cipher. That is just one very simple example of substitution.

the encrypted message was in, not the language of the key. What is more, dictionary attacks are not based specific language dictionaries so much as lists of likely words (including the kind that you would not find in any dictionary, such as 'London' or 'alan99') and as such are largely language independent. 'Dictionary attacks' is therefore a very wrong answer that signifies that the examinee we very confused at the exam, and mixed the subject matter from separate parts of the course and subject matter. I only mention it here because there were several such answers, and students should understand that their answers are based on quite a serious misunderstanding of the course subject matter.

Problem 3

> Suggest and describe two alternative methods that could be used to authenticate that a server that I access on the network is not an imposter. Discuss your methods' respective strengths and weaknesses.

There was naturally a wide spectrum of possible answers to this question, and as usual good marks were given for well structured and well motivated discussions. The problem text includes the term 'alternative' which in such a problem is assumed to be a relative term, i.e. some pairs of answers are more alternative than others, so the more the two answers are different from each other, the better.

One way to structure this answer is by reference to the four basic classes of authentication classes that we have studied during the course. Of course, naming these classes is not a useful part of an answer unless it is used to reason about the methods described.

The following is a selection of the kinds of answers given and comments on these answers.

Something the entity knows

A number of answers suggested that passwords would be a possible way to the server to authenticate itself. This is possible, but not a very practically feasible method. It would require that a server 'knew' a distinct password to each user that wanted to connect to it. It could not share a single password as that would mean that anyone who knew that password could masquerade as the server. So the amount of work involved to create, share and transfer specific passwords for each possible user makes this a very cumbersome method. Only answers that described the inherent awkwardness of this method would gain good marks. Since most who suggested passwords did not enter into any such discussions I was more inclined to suspect that this answer came from a misunderstanding either of the question, or else of how passwords work. It is of course far more common for users to authenticate themselves to a server with a password than vice versa.

There were a few answers that instead required the user to first id themselves so that the server could return individual info that could be recognised by the user. This suffers from some of the same problems as passwords though. There would have to be some phase when the user provides the server with the personal knowledge required, so how is the server trusted in the first instance when that information is provided. There is also a question of how the information should be sent so as to avoid it being eavesdropped and later replayed in a masquerade attack.

Something the entity has

Certificates and private keys - If the server has a private key and can keep that key well protected, then it could prove that it has possession of that key through cryptographic means. The user could encrypt a short, unique message with the public key that corresponds to the server's private key, and send that encrypted message to the server. The server is the only holder of the private key that can decrypt that message, so if the server can return the message unencrypted then that is proof of possession of the key. The SSL protocol uses similar mechanisms for authentication, and also to secure the session traffic.

The public key used to encrypt the message must be trusted as being the proper counterpart to the server's private key. This is normally achieved through a Public Key Infrastructure. The public key is part of a certificate that is signed by another trusted party. Trust in that signature may in turn be ascertained by verification through another party's public key. The intricacies of possible PKI schemes is outside of the scope of this question.

One of the main weaknesses of this scheme is in the trust of the certificates that contain public keys. It may be possible to fool a user into accepting a false certificate, in which case masquerading and MITM attacks will be possible.

Answers on the private key theme were varying in depth and detail. Writing that the server could send a certificate to authenticate itself was not sufficient to show an understanding of the mechanism of authentication. Some answers confused the idea of having a certificate and having a private key. A private key can be kept within a certificate, though when it comes to private keys the distinction between the two is minor. A certificate just contains some useful information about that key, such as the algorithm used to create it and its period of validity. The distinction is far more important where it comes to public keys since a certificate also embodies the means to trust the public key that it contains. The certificate is a cryptographically signed data structure.

There are other methods that can be used to prove possession of the private key apart from the one described above. Some of the schemes as described in exam answers were weaker and vulnerable to replay attacks.

Something the entity is

This class of authentication methods is the most difficult to apply to a server. It seems more relevant to apply this class to people than to machines. Some exam answers did go into the subject of biometrics, but I could only assume that these came from misunderstanding the question.

Perhaps the closest we can come to an identifying attribute is the machine's ethernet MAC address, or rather the MAC address for the machine's network interface hardware. This address should be unique, and therefore could be seen as an identifier. However, the address is not made unique for the purpose of identification, but to avoid addressing conflicts in networks. This can explain why it is simple to falsify mac address numbers. Since such addresses can be falsified, they are not very trustworthy at all.

Where the entity is

IP address could be viewed as an indication of where a machine is, or at least which network it belongs to. Different number series are assigned to different countries and different organisations. Falsification of such number series is possible, but not entirely trivial. For two way communication to work with a false number series an attacker would have to assume some amount of control of network routers and gateways. We can therefore have some trust in IP addresses, though by no means complete trust.

A few exam answers suggested that one could test where a machine is on the network by executing a *traceroute* to the desired server. Traceroute reports back to the requester how traffic to a given machine is routed through the network, i.e. through which machines it passes. This is not a method discussed during the course, but I assume that anyone who has studied computer networks would be familiar with this service. This might not be a kind of authentication that one could expect the average user to employ. Note that an attacker who has control of a router could falsify the traceroute.

Other answers

A *domain name* could be an identifying attribute, but as we have seen during the first assignment, one that is easy to falsify. Some students proposed that with DNSSEC we can be assured that domain names are correct and not falsifiable. DNSSEC is a scheme that utilises digital signatures so that servers verify themselves to DNS servers, and so that information from such servers can be trusted. This is another subject that has not been covered during the course (beyond possibly a mention) but that is unarguably a good suggestion. The current downside of this scheme is that it must be deployed in all relevant nodes and DNS servers before it can be used. Though Sweden is relatively well advanced in the deployment of DNSSEC, the scheme is by no means in common use as yet.

Some answers mentioned the possibility for authentication through a trusted third party. This could presumably be by means of PKI as described above, or schemes like Kerberos. Most of these answers were very vague on exactly what third party trust implied, and were not judged good evidence of understanding.

A number of answers cited challenge-response as a good method to authenticate the server. Discussions on how this worked varied in quality. Several seemed to miss the point that challenge-response does not necessarily authenticate both parties. I have a key-calculator from my bank. They send a key to me, that I transform with my calculator as proof that I possess that specific calculator. I am only authenticating myself to the bank. If an imposter posing as my bank sends me a false code I will enter it into my calculator and return the result to the imposter. The imposter just has to accept that code. At no point in this am I guaranteed that I would discover that I am communicating with an imposter. If I were to enter a different number from the one given and return the calculated code, and if the receiver accepts that code then I could understand that it is not the real bank. No student answers went so far as to suggest this action though.

Some students gave more than two alternative methods. Some students believe that more answers must be better. This is not the case; in fact it is the opposite. If the question asks for two answers and you give three than that must be taken as an indication that you are not able to distinguish which of the two are the best answers. You are therefore leaving it up to the examiner to decide for you, and in that situation the only objective alternative is to choose the worst two answers of the three. Giving more answers than asked for will therefore very often mean lower, rather than higher, marks.

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. Structure each of your answers with headings *description*, *related concept*, and *example.*
>
> - The *append* privilege
> - DMZ
> - The Principle of Separation of Duty
> - The Common Criteria

The append privilege

Description

The append privilege is one that allows a subject to write to an object, but only to the end of its contents. It does not allow the subject to alter or delete any of the existing contents. It is one of the kinds of privileges that define the access rights subjects can have over objects. We are used to seeing such privileges listed in access control matrices.

Related concept

The *write privilege* will normally allow the subject to put anything at any position in the object, and even remove existing content even to the point of deleting the object. The write privilege can therefore be viewed as more powerful and even more potentially destructive than append.

Example

Accounting systems can usefully use the append privilege. When logging on to a system the login process will early on in the process use an append privilege to write an entry to a log file over all logins. Even if the login can be subverted later on it its process, assuming that no privilege escalation is possible, the fact that a person logged on cannot be altered and may be useful information to discover an attack.

Several answers stated that append is a privilege in Unix systems. This is not the case. Several thought that the game high-score list that we used as an example in a lecture was a good example of the use of append. However, even during the same lecture we discussed that append would not stop you from cheating by writing a false high-score to the file. It just means that the previous values could not be changed.

DMZ

Description

DMZ stands for Demilitarized Zone, and in an IT context refers to an area of an organisations network that separates the local network from the external network, and includes protective mechanisms. The DMZ (which Alan has claimed is a bad name for the concept, but the misnomer has unfortunately stuck) normally comprises an area between and including an internal and an external firewall. Between them can be a number of servers, such as web servers and mail servers that necessarily should be given connection to the network outside of the organisation's. They are thus protected from the outside network by the outer firewall, while the organisations local network is protected from possible security breaches of the security of the DMZ servers by the inner firewall. Both firewalls are often hosted by a single computer in order to simplify the administration and running of the DMZ.

Related concept

Proxy servers are intermediary servers that relay requests from clients to other servers. Proxy servers can also act as a kind of firewall that mediates traffic to and from those servers. A DMZ typically protects a proxy server on the outer perimeter of an organisation's network.

Example

If an organisation has a website that is important for its operation and also needs email connection with the outside network, the outer firewall of a DMZ could ensure that only http and smtp requests are allowed to pass into the DMZ. The web server within the DMZ might need to access database information from within the organisation, while users within the organisation may access their incoming emails that are on the email server in the DMZ. In this case the inner firewall would only permit database accesses from the web server and IMAP and POP session instigated from within the organisation's network to the email server. It could disallow other kinds of traffic.

The Principle of Separation of Duty

Description

The principle of *separation of duty* says that if more than one operation is required to complete a task then those operations should be executed by more than one person. This assures the integrity of the task in that it would take two parties in collusion to improperly complete the task.

Related concept

Saltzer and Schroeder's design principles for security systems include the *principle of separation of privilege* which states that a privilege should not be granted on a single condition. This is based on a similar idea as the separation of duty, in that it provides a similar kind of defence in depth. Whereas separation of duty requires that two people execute separated operations within a task, separation of privilege can involve a single person but several factors. I must present both my bank card and my PIN code to and ATM machine to gain access to my account. That is separation of privilege, but not separation of duty.

Example

In the economy department of a company many invoices are paid. The task of paying an invoice can be divided into two operations: check the veracity of the invoice, and pay the invoice. If one person checks that the invoice is correct and another pays the invoice, then the system is protected from any one of these people presenting the company with a false invoice that gives their own bank account as the receiving account. If the invoice checker tries to fool the company then the invoice payer will notice that the receiving account is not that of a legitimate company. It the invoice payer tries to cheat the company then the invoice checker will notice that the invoice itself is false.

The Common Criteria

Description

The Common Criteria (CC) is an internationally standardised scheme to provide assurance in security software. Its two main sections define standardised means of describing functional requirements and assurance requirements. A specific product's security requirements are described in a standardised Security Target document. Generalised security requirements for a type of product can be described in a Protection Profile. A product can be certified as fulfilling its Security Target. There are different levels of assurance requirements which means that when a product is certified it is certified as meeting one of the CCs seven Evaluation Assurance Levels (EALs), where EAL1 provides the least assurance, EAL7 the greatest.

Related concept

TCSEC, also known as *The Orange Book*, was an earlier standard designed by the USA Department of Defence. This standard was designed primarily to measure the assurance of the security mechanisms of operating systems. In contrast, the CC is more generally applicable to all kinds of software systems. TCSEC is no longer in current usage and has been superseded by the CC.

Example

A government organisation may have a need for firewall software. They therefore create a Protection Profile (PP) where they describe their requirements according to the CC documentation standard. A company intends to compete for orders for firewalls from this government organisation and therefore designs a firewall that fulfils the requirements in the PP. They describe the firewall's security related aspects in a Security Target, and a CC certified third party organisation verifies that the Security Target and the product that it describes meet a certain EAL.

Problem 5

> In practice an individual's need for privacy can be
>
> - Culturally dependent
> - Situation/Scope dependent
> - Time dependent
>
> Describe example situations that clearly illustrate how the need for privacy can vary according to these factors.

The 'clearly' of the problem text is an important aspect. One should consider in what ways this can be made clear since clarity in answers will be a deciding factor for the grade.

Privacy needs may be individual, but society nevertheless makes general assumptions about them, in laws, in how far it applies surveillance methods, etc. If we can find situations that highlight how the assumptions made in society can have drastically different effects dependent on the given factors, that should make it clear.

For extra clarity, answers can also relate to both the kinds of privacy that we have defined in the course, i.e. *spacial privacy* and *informational self determination.*

Cases closer to reality are more convincing than supposition based on fictitious scenarios.

Time is unfortunately too short for me to provide a proper discussion in this version of this document. As a guideline to what kinds of answers where judged as good I have summarised below examples that illustrate differences in both types of privacy for each of the three factors. Note that such brief notations as sometimes occur below are not sufficient for your exam answers, but here they will hopefully give you clues to what examples your discussion could be based upon to achieve good marks.

Culturally dependent,

- spacial privacy
    - Nakedness and public displays of affection will offend people in some cultures where you would expect laws and law enforcement to protect you from having to experience them. In other cultures e.g. nudity may be the norm.
- informational self determination
    - in some cultures a picture is regarded as containing the essence of one's soul and therefore not something that anyone should take and have control over. For others an id photo (as opposed to photographs of me in any number of other situations) is a common and undisturbing means of proving my identity.
Several answers quoted this same situation as an example of violation of spacial privacy, but it seems to me that it must be the picture that is the problem more than the taking of the picture...?
    - You wages in Sweden is part of public record whereas in other countries it is considered secret information
    - Asking someone's age in USA or England is commonly considered an invasion of privacy, but not so in Sweden or China

Situation/Scope dependent

- spacial privacy
    - Imagine that you are in a field, listening to birdsong. You may well consider it a public nuisance if someone came walking by playing loud music from a portable stereo. The very same field might be used for an outdoor rock concert where I would expect to hear loud music.
    - In an avant guard theatre production I might expect actors to accost members of the audience, and even purposefully embarrass them. If I were similarly accosted by the same person while minding my own business in the street I would see it as an affront to may personal privacy.
    - Calling a person for a chat at any time vs when that person is bereaved.
    - Calling your systems administrator at home when there is a crisis situation at work, counter calling them because you cannot get a game to install properly on your home computer. (This could also be situation dependency of self determination if we are talking about the use of the telephone number)
    - To illustrate the aspect of scope: If I am disturbed by someone talking loudly in their mobile phone, the problem is not so great if I feel that I can move a few steps away to avoid the nuisance. If there are people talking loudly in mobile phones wherever I go then the problem is serious.

- informational self determination.
    - Helping to solve a crime, you may offer up all sorts of information on where you were, what you saw etc. Were a person to ask the same kind of information without a given purpose, it could even be harassment.
    - I may be want to let people know my political affiliation if I am campaigning for office, but in the voting booth your political affiliation is nobody's business but your own.
    - Data that would clearly not be sensitive for most of us, such as our name and address, could be very sensitive for someone who has moved to escape from domestic violence.
    - In a confessional...
    - Police looking up data on you for a) an investigation, b) out of curiosity.

Time dependent

For extra clarity in this factor we can try to specify different kinds of time dependency. Privacy could depend on what time it is we are living in, the lifetime of information, the time of day, or the duration of exposure.

- spacial privacy
    - 40 years ago having television cameras follow you around would have been unthinkable. Today people seek positions in reality programs such as Big Brother.
    - 4am in the morning phone calls from a sales person might be illegal, whereas at 4pm they might at worst be a nuisance
    - I can stand a smoker for three minutes, but not three months.
- informational self determination,
    - The last 3 numbers on the reverse side of your credit card used to be regarded as less important, whereas today we know that it is safer to scratch them off for my privacy. (not a good example though – more about security than privacy).
    - before an auction ends my bids are private, afterwards a part of the verification of the correctness of the auctioning process
    - inventions up to the time the patent is granted.
    - Your boss asks what are you doing during work time vs. during your free time.
    - For the duration of a job application an agent may spread your information, but not afterwards.

In marking I try first try to understand the description, and first ascertain as to whether it pertains to privacy or confuses it with other concepts. Then the answer is assessed according to whether it actually addresses the varying need for privacy according to the given factors. Then the clarity of the answer is judged. Good arguments will therefore show clear distinctions between the influence of the factors, and make universally applicable arguments. If the examiner can find holes and interpretations that would make the answer less than clear then the answer will be awarded less marks.

Several answers mentioned the concepts of *spacial privacy* and *informational self determination*, but without applying it to their answers. I found that strange and a little confusing.

References

Bishop05 Matt Bishop, *Introduction to Computer Security*, Addison Wesley, 2005.

Davies&Price89
Davies, D.W. & Price, W.L., "*Security for Computer Networks*", Wiley, 1989

Schneier03 Schneier, Bruce. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World.* Copernicus Books. 2003