DSV SU

SEC:I/IV2024
Information and Computer Security
Autumn Term 2010

Alan Davidson

Suggested Solutions to the Exam 2010-10-22 and Comments on the Marking (version 1.0)

The answers suggested here may contain more aspects or discussion than would normally be expected from students to achieve the highest grade. The intention is to give students not only explanations of why their answers were graded as they were, but also to give students plenty of food for thought (if applicable, for future exam sittings).

Problem 1

> One practical security measure might be to encrypt a computer's hard drive so that only after correct authentication would the content be decrypted. Based and structured on the CIA triad, discuss and explain how this measure can be said to effect system security, both positively and negatively.

Confidentiality.

Even if someone should manage to bypass the authentication mechanisms that protect the computer's hard drive (such as by removing the hard-drive and inspecting it under another system) the data will not readable. The effect on confidentiality can therefore be said to be positive.

Integrity

The integrity of the data on the hard drive could be said to be lessened since all the data is transformed and will only be retrievable in its correct form if the correct decryption process is applied. Care should also be exercised in choice of the encryption algorithm used. It would be unfortunate if methods such as Cipher Block Chaining were used, which might mean that if an error occurred in the data the error would propagate in the decryption process, thus making more data than just the original error unretrievable.

On the other hand the encryption/decryption process can be seen as an integrity check. If anything were to be changed on the encrypted hard drive, the decryption mechanism would most likely make the error all the more detectable. It is possible that the decryption mechanisms used could signal the error. That is not as good as being able to reconstruct the lost data, but it is better than nothing.

As with confidentiality, there is an extra mechanisms to ensure that authentication cannot be bypassed. Only authorised users can change the unencrypted data, so assuming that those users are trusted, only trusted users can change the data. This is therefore also a measure to ensure that untrusted users are not able to manipulate the unencrypted data.

Availability

The availability of the data on an encrypted disk will be dependent on some kind of cryptographic key. For confidentiality the key must be kept separate from the disk until such time as the decryption is called for. The availability is now dependent on two factors, the disk and the key, instead of just one in the case of an unencrypted disk. If either one of the disk and key pair are lost, then the availability will be lost.

There will be a process of constant encryption and decryption of data to the and from the disk. This will take computing resources that could otherwise be used for other processing. This means that it will take some extra resource, such as time, to use an encrypted hard drive as compared to an unencrypted drive. Availability is therefore adversely affected.

One novel answer suggested that the encryption gave the possibility to safely carry the hard drive

around in the knowledge that if it were lost or stolen the data would still be safe. This portability factor could be seen as improving availability.

A few strange answers seemed to suggest that the encrypted disk had lesser availability than an unencrypted disk because unauthenticated users could (presumably illicitly) have access to data in the unencrypted disk. Availability is of course only about ensuring access to those who are authorised, not everybody.

Problem 2

> Suggest diverse possible ways in which a computer might be authenticated within a network, and discuss your methods' relative strengths and weaknesses. Good answers will cover a breadth of possible methods.

Categories of authentication methods are presented during the course, and these can by all means be used to present an answer to this question that has the breadth that the question asks for. However, it becomes clear that these categories are more easily applied to humans than to computers. Whether one categorises, for example, an IP address as something a computer knows, has, is, or where it is is of less importance. I will use those headings to give the following examples some structure, though they are by no means assumed to be necessary for good answers.

Something the entity knows (Though of course whether a computer really know anything is a matter for interpretation)

An entity can hold onto a secret data token – one form of which we often call a password – that is shared with the system that the entity needs to be authenticated with. The authenticating entity presents the secret token to the system, or else (for added confidentiality) shows that the entity 'knows' the secret without actually presenting it, with the aid of particular protocols designed for that purpose. Under the assumption that no other entities know that same secret then that entity can be uniquely authenticated.

Secret data token mechanisms can be relatively cheap to implement. Since computers do not have the same kinds of problems in remembering tokens as humans do in remembering passwords, many of the problems that humans have in the choice of passwords need not be a problem here. The method is nevertheless dependent on the secrecy of the token, which might in practice be difficult to achieve and maintain. To use this method to authenticate a single computer in a network is not as simple as its common use in authenticating users to single computers. If the computer is to be able to authenticate itself to every node in that network then it must presumably share individual secrets with each of those nodes; a situation that would surely require considerable effort to install and manage.

A number of answers suggested that passwords would be one method for authentication of a computer in a network. A majority of such answers were confused, and seemed to lose track of whether it was a computer or a user that was the subject of authentication. Without clarity on this point answers were not given high marks.

Something the entity has

MAC address. Each network interface that a computer has is given a supposedly unique MAC address number. Presenting that number on request is a possible method of authentication. MAC addresses are readily available on all networked computers. However, the uniqueness of such numbers can be questioned since the routines that are used to ensue that duplicates do not occur are not entirely trustworthy. What is more, MAC addresses can easily be simulated in software, so they can be impersonated by malicious parties that have administrator privileges.

Cryptographic keys. If the computer holds its own private key from an asymmetric key pair, and the remaining nodes in the network have access to the corresponding public key, then there are simple protocols by which the computer can show that it is the holder of that private key. For example, a network node could send a once off, original string as a authentication challenge to the computer. The computer then creates a digital signature on that sting and sends it back. If the

digital signature can be verified with the public key then the computer is authenticated as the holder of that private key. This is a strong and simple authentication method, but it is dependent on

1. The private key must be kept secure. This can be difficult in practice.
2. Some method of instilling trust in the authenticity of the public key is necessary, such as Public Key Infrastrucutres. This can be complex to implement and run in practice.

Something the entity is (or does)

We normally associate this category with the field of biometrics, and it is therefore questionable if this category should be applied to inorganic computers at all. In some situations we might be able to authenticate with the essence of a computer:

Chip manufacturers can create tamper-proof versions of individualised chips. In principle they implement the same idea as the private key solution above, but the private key is built into hardware in a manner that does not allow it to be directly accessed.

Inasmuch as computers have their own individuality, it may be possible to authenticate them from collections of their individual characteristics. What operating system is being run, what network services, normal response times, etc might all be factors that together could give an indication that we recognise a certain computer. This seems to be a possible impromptu method, i.e. that I might be able to run such checks on a machine that I was suspicious of, but as a primary method of authentication it does not seem to trustworthy since machine profiles will be subject to change and impersonation as soon as it is known that the method is being used.

Where the entity is

To some degree we can view the IP address of a computer to be a representation of where it is in a network. For example, local networks will often have their own IP address space, which means that if all local routers, switches and bridges are functioning reliably, we can view a machine with local IP address as being authenticated as coming from that local network. This is a simple and ubiquitous method, but since network equipment may not be trustworthy, and since we know that IP addresses can be spoofed, one can understand that it has not proved to be a strong method.

Another way to test where a computer is in a network is to check the route that data packets take through the network on their way to the given computer, and thereby authenticate them a being in 'the right place'. The program *traceroute* is one example of a method to do this. This is another convenient impromptu method that requires some technical understanding to run the check, and it is not foolproof as the results returned by the routing network to the requesting program could be spoofed.

Some answers to this problem made statements of the kind that certificates or challenge response protocols can be used for authentication. This is indeed true, but many such answers were so vague as to give no idea as to how the authentication is actually achieved. Only answers where it is made clear that the student understands the methods involved could achieve high marks.

A few answers made reference to clients and servers as if there was an obvious relationship between the two in this problem scenario. Since these roles are not significant for the problem I found such answers confusing and difficult to understand. The problem is of one computer that should be authenticated in a network of other machines.

The suggested solutions I have given above are relatively low level. Other solutions, such as discussing Kerberos and its pros and cons, were also quite acceptable.

Problem 3

> One of the important rights that you might expect to find represented in an access control matrix is *own*. What this right actually entails can depend on what type of access control is applied. Explain and exemplify how the *own* right will have different practical implications depending on whether DAC, MAC, or ORCON is applied.

In DAC it is at the owner's discretion to set the rights of the object to whatever they deem appropriate. E.g. if I was the owner of my own diary object, DAC would allow me to choose what kind of access other should have to it. I could presumably keep access to it from my mother but choose to allow read access to my best friend.

In MAC there are system defined rules that stipulate and enforce what rights an owner of an object may set for other subjects in the systems (and themselves for that matter). An accountant within a company may own files that have details of what upper management earn, but that does not mean to say that the accountant can choose to allow for other workers in the company to read or to set such figures.

In ORCON the rights that an owner may set and for an object can be decided by the originator of that object. E.g. A recording company is the originator of a music CD. I pay money for a copy of this CD and become its owner. I may choose to let a friend listen to the CD, but the originator does not give me the right to allow that friend to make a copy from my copy. Indeed, there may be technical support methods that practically hinder me from doing so.

A number of answers only discussed the right to transfer ownership and how that is affected by the different policies. The other kinds of rights are of course relevant too.

There was some confusion over whether owner means (or usually means) creator. The very idea of ORCON surely implies that they are not necessarily the same (if we assume the originator to be the creator). Otherwise, I do not think the distinction is especially relevant for a discussion on MAC or DAC. I suspect that very many of the files that I am the owner of on my computers have been copied from other sources so that I would not regard myself as the creator of, say, a recorded television program or of photographs that my family have passed on to me.

There was occasionally some confusion over the problem's connection to the rights of the special role of administrator. As Bishop points out [Bishop05, p241] the *root* or *administrator* role in popular operating systems is only relates to ACLs in a limited manner, i.e. these are pragmatic constructions to allow for the proper setup and running of the systems themselves. As such we normally view them as separated from such principles and mechanisms as those discussed in this problem

Given the above description of MAC one might be tempted to call the system the owner of the object, in which case there does not seem to be much difference between DAC and MAC, just whether the owner of the object is the system or the subjects within the system. I suggest that this is an erroneous view that leads to confusion. One point that should dispel this misconception was given in one exceptionally enlightened exam answer: Who the owner of an object is can effect what MAC rules should be applied. For example, if a military general owns an object there may be system-wide specific MAC rules that allow that general to lower the object's security classification to allow all to read it. The same rule does not apply to object owners who are military personnel of a lower rank.

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 *description*, *relationship to [your chosen related concept]*, and *example:*

- Certification Authority
- Kerberos
- SQL Injection
- Evaluation Assurance Levels (EALs)

Certification Authority

Description

Certification Authorities (CAs) are normally associated with Public Key Infrastructure schemes. Such authorities are trusted parties that issue digital certificates. Certificates bind a public key to an identity and thereby provide a means for trust in a public key. Trust in a public key implies trust that the corresponding private key is in the ownership of the individual that is identified in the certificate, and these are necessary requirements for asymmetric cryptosystems to be practical.

Relationship to PGP certificate signatories

The early versions of PGP used a *web of trust* model to provide similar trust in keys as is achieved by Certification Authorities in Public Key Infrastructures. Certification Authorities have hierarchical relationships to each other and to the entities whose keys they sign. At the top of such hierarchies there will be a Certification Authority whose certificate is not signed by another but is a so called *self-signed certificate*, i.e. signed by the CA itself. In the original PGP scheme, certificates were signed by any party that could verify that the certificate was trustworthy. There would therefore not necessarily be any such top node, by a web of signed certificates. A PGP signatory is therefore similar to a CA in the function of signing a certificate, but different in terms of the trust relationship between signatories.

Example

When Internet browsers are distributed and installed they normally come with top node CA certificates that implies that the CAs that are represented in those certificates are implicitly trusted. Well known examples of CAs whose certificates are included with browsers are Thawte, Verisign and RSA Security.

Kerberos

Description

Kerberos is a system that implements Single Sign-On authentication, i.e. it allows a user to authenticate themselves once and thereby be given access to services throughout a network. Kerberos has similarities to capability based access control systems in the way that once the use is authenticated it distributes limited lifetime tickets to the user that grant access to services.

Relationship to passwords saved in "key rings"

Another method that allows users to authenticate once is the principle of key rings. Here a user's passwords are kept securely encrypted on a local computer. When a key or primary password is provided the system can use that key to access the key ring passwords. The key ring will be integrated with the local system so that that authentication with the individual passwords is automatic from the perspective of the user. Key rings are like Kerberos in that they implement a kind of single sign-on, but different in many ways, such as key ring mechanisms are implemented on a local trusted machine, whereas Kerberos is implemented within a network, and user authentication can be executed from a number of client machines.

Example

DSV and KTH use a Kerberos system that allows students to authenticate themselves once and then have access to file servers, the wiki server, to the video server, etc.

SQL Injection

Description

SQL Injection is the name of a common software vulnerability. It is normally associated with web applications. Such applications have a database back-end and web content is created on the fly using data from that database. Furthermore, what data is used is dependent on the some of the user input at the web client side. If the client side input is used by the web server application to construct an SQL query (without careful input validation), it may be possible for the user to construct the input so that it interferes with the server's construction of SQL queries in such a way as to create new queries that the system designer had not anticipated. Such queries may implement a malicious attack on the web application.

Relationship to script injection,

Whenever user input is used to construct code that is subsequently interpreted, if it is not carefully checked to ensure that the input is of a form that is expected and therefore safe, there is a possibility that a malicious user could utilise such script injection vulnerabilities to create and run code that the system designers did not intend. We can therefore view SQL as only one kind of the more general threat script injection. Script injection also covers similar situations with languages such as php, ruby, sh, etc,

Example

If a server side SQL statement were constructed from the template:

```
'SELECT * FROM foo WHERE in = ' . <user-input> . ';'
```

Then entering the user input

```
1; DROP TABLE users
```

might cause two SQL queries to be executed where only one was originally intended, and the second statement may create considerable damage.

(N.B. This is a good example, but it is not assumed that all students will be able to give such concise examples, especially those who have not studies SQL.)

EALs

Description

EALs are the Evaluation Assurance Levels of the Common Criteria (CC). They are the seven basic levels (1-7) that define ascending levels of trust. When a software system is evaluated it is done with a specific target level in mind. The higher the level the more trust can be invested in the system, but on the other hand the more time and investment must be spent on the evaluation.

Relationship to the evaluation classes of TCSEC

The (now obsolete) TCSEC assurance evaluation scheme also defined a number of levels in its evaluation classes. TCSEC, also known as “The Orange Book”, has CC EALs only 6 levels, though they roughly correspond to the top six CC EALs. The CC EALs are applicable to all kinds of software, whereas TCSEC and its classes are intended for evaluation of operating systems.

Example

Microsoft Vista has been CC evaluated at CC EAL 4+, which means that it has been certified at level 4 but with some additional evaluation factors included.

An extraordinary proportion of answers did not follow the problem instructions with regard to the headings. The headers are intended to on the one hand encourage the answers to be more directed (i.e. the *relationship to [chosen concept]* heading incites examinees to write about a relationship, and not just name a concept) but also to make the discussions more directed and structured so as to make the marking of the answers possible. It there are no headings then the examiner has to make extra effort in interpreting the text to find the required parts. If the heading does not specify the concept that the examinee has chosen, the examiner has to interpret from the text which is the

concept. Though the writer of the exam answer might think that it is easy to understand these things from the context, it very seldom is for the reader. The result is that the answers cannot reasonably be marked within the the limited time allotted for the task. The examiner's only recourse is cut short the reading of such answers, saying that if the parts of the answer are not clear then the examinees marks must suffer, even when a deeper reading might show that the student has indeed understood and covered the subject well. All this goes to emphasise the importance of reading and following exam instructions exactly. It is unnecessary to fail the exam on technicalities.

Choice of the concept and the example is an important part of the answer to these problems, as well as the way they are then described. They should both provide further insight into the given concept. For this exam the choices made were generally substandard.

Problem 5

> There exists legislation (both Swedish laws and European directives) that uphold the privacy rights of individuals. Describe an example of a realistic situation where computer users might either regularly transgress against such legislation, or suffer the consequences of others who transgress against them. Indicate the essence of the legislation that is being transgressed (i.e., even though you may not know the name or designation of a law you should be able to characterise it).

Note that this is not a course where you are expected to study details of legislation, but some relevant laws were discussed during the lecture on privacy, so to gain marks for this problem students should show that they can put such laws into context and show their relationship to current privacy issues. I did allow some degree of deviation from the problem text where good examples were related to other international legislation, but since I cannot check all such answers and since we looked a Swedish and European laws during the course such answers were not awarded as high marks.

Laws and directives that were touched upon during the lecture on privacy were:

EU Data Protection Directive 95/46/EC, including informed consent, purpose specification and purpose binding, Data minimization, no processing of “special categories of data”, transparency, requirement of security mechanisms, and supervision.

EU Directive 2002/58/EC on Privacy and Electronic Communications.

EU Retention Directive 2006/24/EC

The Swedish law of free public access to information (“Offentlighetsprincipen”)

The Swedish law of privacy of personal information (“Personuppgiftslagen (PUL)”)

The Swedish law on electronic communication (“LEK”)

Swedish PUL as well as European directives on data protection make it illegal to publish or export peoples' personal information without their prior consent. Modern social media trends mean that it is easy to forget such laws when publishing information or photographs that include friends. If I were to upload a photograph of a clearly identifiable friend depicted in a situation that clearly is not publicly available, and even tag them as being in that photograph, then even in the process of uploading to, say, Facebook, I am exporting sensitive personal information. Given that web sites and communication channels often cross international borders without our knowledge, it is very easy to accidentally export personal information.

According to Swedish and European law one may not send unsolicited advertising via email. Nevertheless we surely regularly suffer from such spam that is a clear breach of not only laws but also the principle of spacial privacy. The legal issues may not be clear though, since many times it will not be clear what country the spam comes from and therefore what laws apply. Furthermore, the issue of what is solicited seems to have become clouded. I myself regularly receive email advertising from companies I do not recognise where at the end it is stated that I have requested such emails, even though I have no recollection of ever having done so. The Swedish anti-spam law

does in fact come from one that is not included in the lists that Albin gave; it is part of the Marketing Control Act (2004:103, if I understand correctly). I do recall Albin describing American spam laws as being “opt-out” whereas Europeans went with “opt-in”.

I do not recall if Albin spoke of this at the privacy lecture, but a couple of exam answers brought up the issue of cookies. Cookies are collections of data that web sites can request be saved to client's local memory and read on request. Not only that but they are one common method used to track users' surfing habits. Swedish law requires that whenever a Swedish web server makes use of cookies the client must be informed that cookies are being used, what the purpose of the cookies are, and how they can be avoided. These days many Swedish sites do not follow this law. A possible explanation for this is that modern web management tools make it easy for non programmers to create web sites without them understanding that cookies are included in the underlying mechanisms.

A current case in the media is how Google has got themselves into hot water on several occasions by transgressing against local data protection laws. For example, they have operatives that travel around collecting information on among other things the locations of wireless networks. It has lately been revealed that in the process they have saved data traffic that was detected on those wireless networks. This has occurred in many countries, including in Europe. One might question whether such cases meet the requirement set in the problem text of being regular transgression, but it certainly was high profile.

A number of student answers brought up the issue of Copyright. Note however that copyright is not the same thing as privacy rights. Privacy is about protection of individuals, whereas copyright is about protection of property. I marked good discussions on copyright fairly generously even though it could be claimed that they showed a lack of understanding of privacy issues.

Another fairly common mistake was to write of regular transgressions by malware and intrusion attacks. These may be relatively regularly occurring problems, but here to the discussion shows a confusion with privacy issues and other problems. Intrusions are more to do with property rights. If someone broke into your home and stole your belongings I suggest that you would not try to prosecute them for invasion of privacy, and the same applied to computer intrusion.

Some answers were wrote of the privacy principles of *spacial privacy* and i*nformational self determination* as if they were laws, but they are of course not. They are merely one way to classify the subject to assist us in communicating about it.

Reference

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