DSV SU/KTH

IntroSec
Introduction to Information Security
Autumn Term 2015

Alan Davidson

Exam Re-sit 2016-03-22
Hints and comments on the Marking

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

Problem 1

a) Describe what cryptographic elements are involved in the creation and verification of a *digital signature*.

b) Explain digital signatures' role in the certificates that are part of a Public Key Infrastructure (PKI).

a) The answer should show an understanding of how a cryptographic hash and encryption with a private key make a digital signature.

b) Answers should put over the idea that a certificate is a data structure that contains the owner's id and their public key, and that it is signed with a trusted party's digital signature as a means of acknowledging the signers belief that this public key does indeed belong to the signified owner.

Problem

Describe and discuss three weaknesses that biometric methods in general can be said to suffer from that might make them less than suitable as a general authentication method for IT systems. Good answers will show three separate and diverse aspects of the problem.

See Pfleeger et al (2015) p55 onwards for the arguments from the course book. Note that we have had a critical discussion on this subject matter in class, so it is legitimate to question e.g. whether the single point of failure argument is applicable to this problem. Students who could properly cite Pfleeger et al's arguments were of course given marks for their answers. A number of students cited only the examples given in the book without making the same arguments as Pfleeger et al. Such answers could not be given high marks. As an example:

As carefully stated during the course, it is very difficult to claim that a general problem in biometrics is that they do not work when some biological attribute changes. Examples often cited are “fingerprint authentication will not work if I cut my finger” or “voice recognition will not work if I get a cold”. This may (or may not) be true, but one must surely relate this problem to similar ways that other authentication methods fail on occasion, e.g. forgetting one's password. This is far more common, and yet there are usually easy ways to recover or reset the authentication data. So surely we can simply go to the system administrator and register another finger? When Pfleeger et al cite these kinds of examples it is to illustrate that biometrics “can become a single point of failure”, and note how the authors are careful to include the word *can* in this statement.

Some further general arguments include:

Once biometric data has been discovered and a method to masquerade is implemented, there is no given method by which to recover the authentication method. In contrast, if a password is discovered one can recover simply by changing the password.

Biometric data is unavoidably linked to the individual. Not all authentication situations need to uniquely identify individuals in order to give them the rights needed for the situation. E.g. a system that checks if I am someone who has legitimately paid for the right to see a movie only needs to check that, not to know exactly who I am. Biometrics can therefore be seen to introduce problems

associated with privacy.

Biometric data are subject to exposure, even outside of their use for authentication. Fingerprints are one example, where one could expect to find fingerprints on many kinds of surfaces that a person normally touches. If the biometric method is possible to falsify, as fingerprints are, then this kind of exposure will make a targeted attack difficult to avoid.

There are indications that biometrics in general do not meet widely held preconceptions that they are necessarily good.

Answers that made categorical claims for all biometric methods could not be given high marks. Good answers are more balanced and considered. For example, “biometrics are easily falsified” is not something that I would dare claim of biometric methods in general. During the course we have not claimed this, but rather said that some methods have been seen to be possible to fool with relatively small resources. Insofar as there is a general impression that biometric methods are “good”, we can therefore argue that this is not necessarily true.

A tip for such exam discussions as these – do not use words like “very”, “easily” etc to qualify your arguments. They are meaningless in an objective presentation of facts and arguments and probably more likely to be an indication of sloppy arguments.

Problem 3

> The common strategies that antivirus software (or what we have termed *anti-malware* during the course) use to detect malware can mean that they are not as effective as one might hope. Describe and motivate two important and separate aspects of malware that can reasonably be assumed to make it difficult for such antiviral systems to discover their presence.

Possible aspects where one can make convincing arguments for this problem are:

- polymorphic malware
- stealth malware, including rootkits. See section in Pfleeger et al on stealth, pp189-191
- directed malware, i.e., designed for a specific target, with little spread “in the wild”, and therefore less chance of being discovered
- fast and self propagating, so that the malware infects before the time window of detection and protection measures are implemented and disseminated.

N.B. the above would not be sufficient as an answer, but a guide to help understand the grading. The problem text calls to “describe and motivate”.

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:
>
> - Bell LaPadula
> - Denial of Service
> - Mandatory Access Control
> - DMZ

Suggested solutions for problem 4 are not complete in this version of the document. Please see the

course book and other relevant sources in the reading notes as well as the course video material for definitions and examples.

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

- Bell LaPadula – Biba
- Denial of Service – Ransomware, DDos, Availability
- Mandatory Access Control – Discretionary Access Control
- DMZ – Proxy server, Firewall, Defence in Depth

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

Problem 5

a) Give concise arguments for why one can expect that personal privacy issues are likely to become an increasing concern in the future.

b) Describe IT tools that can on the one hand afford an Internet user pseudo-anonymity, and on the other, anonymity, explaining the mechanisms that these tools use in order to achieve these levels of anonymity.:

a)

The following are summaries of arguments that have been made during the course:

In the information age, all the more detailed information on individuals is valuable for society in general (e.g. in predicting trends among a populace, such as the spread of infection) but also valuable for those who can profit from that information (e.g. manipulating information flow to make an individual more prone to choose one product before another).

All the more personal information is being registered by digital devices (mobile phones, watches, fridges, etc.) and they are becoming all the more connected.

Digital technology, with the tools to collect and process information, are becoming increasingly cost effective, allowing greater detail in the collected information, as well as greater opportunity to predict and also manipulate individuals. Such advances include the inclusion of diverse sensors , such as GPS devices, physiological sensors like heart rate, sleep phase sensors, etc., but also advances in data processing such as effective data-mining techniques.

Increasing complexity of the systems that individuals will want to, and be required to, use in common interaction in society means that it becomes increasingly difficult to have insight into the mechanisms and protocols that are used as well as the rights that might be infringed. One is all the more inclined to use things without understanding them or their possible adverse effects.

A prevalent culture of fear as propagated by anti-social elements of society, public media, and within politics may make individuals less likely to protect their privacy rights if they believe it will improve their personal safety.

Examinees often choose emotive language and subjective arguments in this discussion. It should be clear that in an academic context the more objective the argument the more weight it carries. Many discussions only attempted to discuss aspects of current practices, whereas the problem asks for indicators of increasing concern.

b)

Pseudo-anonymity implies the use of pseudonyms, thereby removing the direct reference to an individual, but not removing the possibility to trace the pseudonym back to the original identity

(example case – the Penet remailer penet.fi). This contrast to systems such as TOR which take reasonable measures to ensure that no one single party, or eavesdropper thereof, has enough information about the originating party to ever be able to reveal the connection. The idea of mixnets, including mechanisms of encryption and padding making eavesdropping to discover connections between forwarding agents is an important principle for anonymity. Pseudo-anonymity based systems presume trust in a single anonymising agent to do the anonymization and not reveal information. Anonymity systems presume trust in the principles of the systems themselves, but not any single actor within the system.

N.B. this is not sufficient as an answer, but a guide to help understand the grading.

References

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

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