Mittuniversitetet
MID SWEDEN UNIVERSITY

Final exam

DT145G Computer Security

Daniel Bosk

Department of Information Systems and Technology,
Mid Sweden University, SE-851 70 Sundsvall
Email: daniel.bosk@miun.se
Phone: 010-142 8709

2017-08-30

Instructions

Carefully read the questions before you start answering them. Note the time limit of the exam and plan your answers accordingly. Only answer the question, do not write about subjects remotely related to the question.

Write your answers on separate sheets, not on the exam paper. Only write on one side of the sheets. Start each question on a new sheet. Do not forget to *motivate your answers.*

Make sure you write your answers clearly, if I cannot read an answer the answer will be awarded no points—even if the answer is correct. The questions are *not* sorted by difficulty.

Time 5 hours.

Aids Dictionary.

Maximum points 24

Questions 8

Preliminary grades

Each question can be awarded up to three points: one point for E, two points for C and three points for A. To get an E, you must get at least one point on each question — i.e. no question must be awarded zero points. For a C, you must get two points on at least half of the questions. For an A, you must get three points on at least half of the questions.

Questions

The questions are given below. They are not given in any particular order.

(3p) 1. Describe the terms identification and authentication and how they relate to each other. Make sure to illustrate your explanations with examples.

> **Suggested solution** In identification you claim an identity. This can be done using e.g. a username, fingerprint or DNA sequence. Anyone can do this.
>
> In authentication you prove you are who you claim you are. This can be done using e.g. *who* you are (biometric), *where* you are (location) or what you *do* (biometric), something you *have* (e.g. BankID), or something you *know* (password). One important part of authentication is freshness.

(3p) 2. Discuss the relation between the following pairs of terms:

(a) Trusted and trustworthy

(b) Confidentiality and privacy

(c) Integrity and authenticity

> **Suggested solution** **Anderson2008sea** definierar begreppen enligt följande:
>
> **Pålitlighet** Ett system eller principal som innehar pålitlighet (is trusted) är ett system eller principal som kan bryta din säkerhetspolicy.
>
> **Pålitlig** Ett system eller principal som är pålitlig (is trustworthy) är ett system eller principal som inte kommer att misslyckas. (Den kommer alltså inte att bryta din säkerhetspolicy.)
>
> Ett exempel för att illustrera skillnaden ges av följande citat: "if an NSA employee is observed in a toilet stall at Baltimore Washington airport selling key material to a Chinese diplomat, then (assuming his operation was not authorized) we can describe him as 'trusted but not trustworthy'" [**Anderson2008sea**].
>
> **Sekretess** Sekretess är en teknisk term för effekten av en mekanism som begränsar antalet principals som kan ta del av information.
>
> **Konfidentialitet** Konfidentialitet syftar till att tillhandahålla sekretess för andra principals hemliga information.
>
> **Personlig integritet** Detta är förmågan eller rätten att kunna skydda sin personliga information. Det gäller alltså bara individer, exempelvis företag har ingen personlig integritet.
>
> **Integritet** Detta är en teknisk term för egenskapen att data förblir oförändrat, eller, om förändring sker ska den inte förbli obemärkt.
>
> **Autenticitet** Detta begrepp innefattar integritet och fräshhet. Om kommunikation spelas in och sedan spelas upp vid ett annat tillfälle, då kommer integriteten att ha bevarats men inte fräshheten — alltså är en återuppspelning inte autentisk.
>
> Dessa definitioner stämmer även överens med RFC 4949 [**rfc4949**].

(3p) 3. Describe an attack scenario where a side-channel is of central interest.

> **Suggested solution** The adversary is interested in learning classified information. They set up a device which records electromagnetic emissions to reconstruct the image on a screen, thus when a target works with the classified data on the computer the adversary sees the same image. This is a passive attack.

(3p) 4. Explain why it is not possible to *securely* embedd a cryptographic key in a program (e.g. a smartphone app), i.e. why the adversary can steal the key. Also describe the requirements for a solution and possibly some example.

> **Suggested solution** Since the software might run in a hostile environment, the adversary can extract the key.
>
> The only way to prevent an adversary from extracting the key is to store it in special-purpose hardware. If you can ensure the integrity of the operating system, then sandboxing the applications will protect the key from other (malicious) applications who tries to steal the key.

(3p) 5. What is the purpose of separation of duty? Explain and illustrate your explanation with an example.

> **Suggested solution** The purpose of separation of duty is to make it more difficult for a malicious entity to subvert the system. E.g. a systems developer at the bank should not be able to add a back-door for himself so that he later can steal money without anyone noticing. If he is only allowed to write the code, but not to certify its correct function — then there is a higher chance that he is caught before the system is launched. So to subvert the system a malicious actor must act together with others.

(3p) 6. Give an example where "data" can be mistaken for "code".

> **Suggested solution** Shell scripting is an easy example. Here you can store part of the code in variables, the simply substitute them. Consider the following `/bin/echo -e ${1}`. The variable `${1}` will be substituted and the result will be interpreted as code.
>
> A more general example: any time a program interacts with a database using SQL. The database cannot differentiate which parts of the SQL-query comes from the program code the programmer wrote and the input provided to that program by the user.

(3p) 7. Bell-LaPadula (BLP) is a mandatory access-control (MAC) model for confidentiality. Biba is also a MAC model, but for integrity. (It is sometimes called "BLP upside-down".)

Explain how you can use MAC (e.g. Biba) to ensure the integrity of a system, e.g. to prevent malware from infecting a system. (Microsoft actually introduced such a technique in Windows Vista.)

> **Suggested solution** We assign different objects to different levels of integrity. E.g. system files have a high level of integrity, the users documents have lower, but still higher than temporary files.
>
> When we download files from untrusted sources they will get the lowest level of integrity. Thus if we download executable files they will execute with the lowest level of integrity. As such they can not modify system files, since those are on a higher level. Possibly they cannot modify user-generated files either, since output from local programs (which do not communicate with the outside world) might have a higher level of integrity.

(3p) 8. The National Institute of Standards and Technology (NIST) updated their recommendations on password policies in June 2017. Among the changes are:

- Forced password changes should only happen when a breach has occurred.
- Long passphrases are favoured over complex passwords, i.e. a mix of special characters, upper- and lowercase letters is no longer a requirement.

Explain why this is a better recommendation. Illustrate your explanation with examples.

Suggested solution The increased security can easily be demonstrated. E.g. a password of four randomly chosen words forming a passphrase will have $4 \log_2 125\,000 \approx 4 \cdot 16.9 \approx 67.7$ bits of entropy. (We assume a word list of 125 000 words, e.g. the standard Swedish dictionary.) A completely randomly generated password consisting of eight upper- and lowercase letters, numbers and special characters will yield $8 \log_2(26 \cdot 2 + 10 \cdot 2) \approx 8 \cdot 6.2 \approx 49.3$ bits of entropy.

User will not choose entirely randomly. There are studies on how well users choose passwords under these two policies. The results favour passphrases. In the same study, the conclusion is that passphrases also provide better usability.

Removing the requirement to periodically change the password further improves usability. The periodic change of passwords simply forced users to adapt easy-to-guess systems for their password choices.