Mittuniversitetet
MID SWEDEN UNIVERSITY

Final exam

DT145G Computer Security

Daniel Bosk

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

2016-10-24

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 39

Questions 8

Preliminary grades

The following grading criteria applies: E $\geq$ 50%, D $\geq$ 60%, C $\geq$ 70%, B $\geq$ 80%, A $\geq$ 90%.

Questions

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

1. You are asked to estimate some password policies. The policies are the following:

   basic12 At least 12 characters consisting of upper and lower case, and numbers.

   randswedict4 Randomly choose four words from the Dictionary of the Swedish Language (SAOL). This dictionary contains approximately 125 000 words.

   You should answer the following:

(4p) (a) Estimate the entropy for the passsword policies. (You may rely on the results in certain published research papers discussed in the course for certain estimates.)

(2p) (b) Decide how suitable they are for use in a large organization.

(2p) (c) Decide how suitable they are for use in a web application.

   Note that you will not get any points without a motivation.

(3p) 2. Explain the idea of double-entry book-keeping.

> **Suggested solution** It originates from banks. Every entry is either a credit or a debit. Every credit must have a corresponding debit, i.e. they cancel each other if added together. This means that when all entries are added together, the final balance should be zero. Thus, we keep the constant state of zero balance, and when the final balance is non-zero we know that something is wrong.

3. Describe the terms

(2p) (a) identification and

(2p) (b) authentication.

   Make sure to illustrate your explanations by examples. You must also give an example of a mechanism for each of the terms.

> **Suggested solution** In identification you claim an identity. This can be done using e.g. a username, fingerprint or DNA sequence.
>
> 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).

4. Explain the following terms:

(1p) (a) Confidentiality

(1p) (b) Integrity

(1p) (c) Availability

(1p) (d) Accountability

(1p) (e) Non-Repudiation

> **Suggested solution** See [**Gollmann2011cs**] and [**Anderson2008sea**] for definitions.

(4p) 5. Give an example of a side-channel attack and motivate why it is a side channel.

Suggested solution A side channel is an unintended channel emitting information which is due to physical implementation flaws and not theoretical weaknesses or forcing attempts.

(2 points) Extracting the secret key from a device by measuring energy consumption or electromagnetic emissions while the device performs computations using the secret key.

(1 point) This is a side channel since it relies on a weakness in the hardware implementation. (1 point) It is further an active attack since we might need the device to perform operations on certain ciphertexts (or plaintexts).

6. A user wishes to provide confidentiality to a file.

(3p) (a) She can accomplish this through mechanisms provided in the operating system. Explain how this works and what are the limits.

(3p) (b) She can also accomplish this through purely cryptographic mechanisms. Explain how this works and what are the limits.

Suggested solution The first way she's securing her file is by using access control mechanisms in the operating system (OS).

Assuming we have physical access to the computer, then we can just read the raw data from the disk. This can be accomplished by either booting our own OS on her computer, or by removing the disk.

If we don't have physical access we can always try to bypass the access control mechanisms in other ways, e.g. by gaining privileges in the system or seeing if the OS has failed to protect reading from the raw disk (i.e. not using the file system).

The main point here is that the operating system must be working correctly for its mechanisms to be effective. The *running* operating system will provide confidentiality by not allowing other users' requests to open the file.

The most obvious way to have system independent security for this file is to encrypt it, i.e. using cryptographic mechanisms. This way no one can read it unless they have access to the key, and this is true no matter if you change the environment. (Of course, if the system is untrusted someone can get to the key that way, but that's outside the scope of this question.)

(3p) 7. Can a files such as images (e.g. JPEGs) and other data be dangerous?

Suggested solution Yes, they can contain machine code which can be executed if there is e.g. a buffer overrun vulnerability in the software that reads the data.

8. Human psychology is important in security. It is used in both security usability and social engineering.

(2p) (a) Give an overview of why psychology is important in security.

Suggested solution Då systemen vi är beroende av och som ska upprätthålla vår säkerhet handhas av människor blir psykologin genast viktig. Vi behöver psykologin inom säkerhetsområdet för att kunna ta hänsyn till hur människor fungerar när vi konstruerar säkerhetssystem. Exempelvis, om vi gör ett system för komplext och användaren tycker att komplexiteten är onödig, då kommer denne användare att aktivt försöka att ta sig runt systemet — kanske genom att skriva upp långa lösenord istället för att lära sig dem utantill.

Om vi däremot tar hänsyn till användarnas kognitiva begränsningar, då kan vi konstruera system som både är säkra och enkla att använda.

(4p) (b) Give an example of an attack which exploits weaknesses in human psychology. Also explain why it works.

Suggested solution En psykologibaserad attack utnyttjar svagheter hos användarna för att ta sig runt ett säkerhetssystem, det är alltså inte säkerhetssystemen som angrips.

Ett exempel på en sådan attack kan vara att en användare får ett e-brev som till synes är från banken och som innehåller en länk till en inloggningssida, kallat nätfiske. Brevet kan be användaren att uppdatera någonting hos banken via internet. Ett förfarande beskrivs och sedan läggs till "eller klicka på länken". Med en förfarande som låter som att det kan ta fem till tio klick kommer användaren sannolikt att välja enklicksalternativet. Notera att förfarandet måste vara korrekt för banken medan länken är till en phishingsida. Utformandet kan leda till vad litteraturen [**Anderson2008sea**] kallar *capture errors*, att användaren använder ett invant beteende: i detta fall att användaren klickar på direktlänkar.

Därutöver försöker nätfiskaren att få användaren att tillämpa fel regler i situationen. Exempelvis, användaren kanske (omedvetet) lägger större vikt vid att ett hänglås syns i webbläsaren för säker anslutning än att bankens namn är rätt stavat i URL:en. Även att bankens namn finns med någonstans i URL:en kan vara en tillräckligt stark regel för att användaren ska undvika att detektera den felaktiga fiske-URL:en.