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

2016-08-22

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 32

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.

(2p) 1. What is the purpose of logging?

> **Suggested solution** The purpose of logging is to be able to follow how the system has transitioned between states. We want to do this to be able to find vulnerabilities that might have been exploited during a breach. Also to verify or reject possible breaches.

2. Explain how information theory can be used to estimate the strength of passwords chosen under a given password composition policy:

(2p) (a) How can you estimate the upper bound, i.e. the maximum possible entropy?

(2p) (b) Why can't you estimate any (useful) lower bound, i.e. the minimum possible entropy?

(2p) (c) How can you estimate the average case, i.e. what is usually the case when users choose the passwords?

> **Suggested solution** You assume that every part of the password is chosen uniformly randomly. This gives the maximum entropy, i.e. it is an upper bound. You have to account for all choices the password composition policy allows. Or rather, all choices the policy removes.
>
> This is hard because a user can choose a very easy to guess password, which has almost no entropy. Similarly, if all users choose the same password, then the entropy would be zero.
>
> The average case can be estimated as in [**Komanduri2011opa**]. You have to *sample a lot of user-generated passwords*, then you can perform a frequency analysis to find the probabilities and compute the entropy. The users are the stochastic variable (random output) and you must get a large enough sample to estimate the probability distribution.

(3p) 3. Describe the requirements for a process to be able to assess the integrity of itself and its execution environment.

> **Suggested solution** If the process can trust its environment (i.e. the operating system), then it can rely on the environment to assess its own integrity. Thus the process relies on the integrity of the operating system. The oerating system in turn relies on the integrity of the hardware and must rely on the hardware to assess its own integrity. Hence the process needs hardware that will not allow a modified version of the operating system to run.

4. 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).

5. 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.

(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.

7. 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.

(3p) 8. Given an example of an active side-channel attack.

Suggested solution Extracting the secret key from a device by measuring energy consumption or electromagnetic emissions while the device performs computations using the secret key. It is an active attack since we might need the device to perform operations on certain ciphertexts (or plaintexts).