Mittuniversitetet
MID SWEDEN UNIVERSITY

Final exam

DV026G Information 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

2016-06-01

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, course material and notes.

Maximum points 41

Questions 8

Preliminary grades

The following grading criteria applies: E $\geq$ 50%, D $\geq$ 60%, C $\geq$ 70%, B $\geq$ 80%, A $\geq$ 90%. No question must be awarded zero points.

Questions

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

1. 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.

2. 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.

(2p) 3. 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.

(3p) 4. 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.

(4p) 5. (a) Give an example of a covert channel and

> **Suggested solution** A server is anonymous (e.g. a Tor hidden service), i.e. you may access the server but not know its location. Part of the server's service is giving the time. It has been shown that the variations in the system clock depend on the ambient temperature. This means that by studying how the time on the server varies over day and night and over the seasons, we can eventually figure out the ambient temperature. From the ambient temperature we can later deduce the geographical location of the server.

(3p) (b) how we can prevent (or at least limit) it.

> **Suggested solution** We can lower the resolution in the time-stamps the server gives, e.g. by not giving seconds. This lowers the bandwidth of the covert channel, perhaps so that the attack is infeasible. We could also sync the servers clock more often, e.g. by using the Network Time Protocol. However, the only way to prevent it is by not revealing the time of the server's system clock.

(4p) 6. Give an example of a DRM system, the idea behind it and why it works or not.

> **Suggested solution** Hardware dongles: You have a hardware dongle attached to the computer, the software can then communicate with the dongle. The idea is that the software can be copied easily, but the dongle cannot. Thus the software can only run in as many instances as there are hardware dongles.
>
> The hardware dongle can be simulated by other software in many cases. For the software to be able to tell the dongle and the simulated dongle apart, it must be able to trust the operating system — thus it needs to verify the integrity of the operating system, which in turn requires special hardware. The alternative approach is that the dongle is more sophisticated, e.g. that it uses unforgeable digital signatures as output. In this case we instead modify the software itself, so that it simply skips the checks with the dongle (e.g. the signature verification always returns true).

7. 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.)

> **Suggested solution** Basic12 requires at least 12 characters. We can use upper and lower case, as well as numbers. This yields an *upper bound* of $\log(26 + 26 + 10) \cdot 12 \approx 71$ bits of entropy.
>
> Randswedict4 requires at least four words from the Swedish dictionary. This yield an *upper bound* of $\log(125000) \cdot 4 \approx 68$ bits of entropy.

> To achieve these upper bounds we must choose uniformly randomly. Most likely passwords under basic12 will yield an entropy somewhere between that of basic8 and basic16 in [**Komanduri2011opa**].

(2p) (b) Decide how suitable they are for use in the home environment.

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

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

8. Explain the following terms:

(1p) (a) Brute force

(1p) (b) Dictionary attack

(1p) (c) Hash table

(1p) (d) Social engineering

(1p) (e) Two-factor authentication

(1p) (f) Phishing