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

2015-08-27

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 44

Questions 9

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 [Gol11] and [And08] for definitions.

2. 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).

3. You have implemented a Mandatory Access Control (MAC) system in the organization you work for.

(4p) (a) Explain what properties you might have wanted which made you do this.

(2p) (b) Some employees use laptops. If you only rely upon the operating system to enforce the policy through MAC, then those employees with laptops might be able to break your policy. Give an example of how a user can break your security policy in this situation. Make clear what part of your policy is violated and why it can be done.

> **Suggested solution** The most obvious property is confidentiality. If we add MAC, then we lower the risk of accidentally exposing confidential data since the system would automatically assign the correct classification to the result. (This prevents data in high from going to low.)
>
> Another property which is plausible is integrity. This way the system ensures that we don't trust data more than its source. E.g. if we download a file from the network, then we shouldn't trust it more than we trust the network. This means that the system can e.g. disallow executing such a file. (We only allow execution of trusted data.)
>
> A user with a laptop has access to the hardware. This means that the user can bypass the operating system. By doing that the user can read and write arbitrary data from and to the hard-disk.

4. The company you work for want to implement extra features as in-app purchases for the company's main product. You are currently in a meeting about that particular topic, the chairperson of the meeting points at you and asks: "How would you design this system? The customers must pay for the features, for every installation, we cannot allow them to just buy once and copy later. Give us an overview. "

(2p) (a) Outline the main points in your strategy.

(2p) (b) There are some things you simply cannot protect against. Explain the limits of systems such as these, so that everyone present understands the limits.

> **Suggested solution** If possible, put the features on a server and execute them remotely. This requires proper authentication. Ensure this authentication cannot be broken, so that two devices can use the same credentials. Try to use a platform where a user must "root" their phones to violate this.
>
> The limitations of these systems are that they try to protect code running in a hostile environment. If the user has total control of the hardware, then the user can simply copy the software to another device. The user can even make arbitrary changes to the running code. This means that any keys can be copied from one device to another. Even if the app is programmed to transmit the device ID, the app can be reprogrammed to transmit a hard-coded static device ID.

(5p) 5. Your boss is finally convinced that the company needs an Information Security Management System (ISMS, Swe. 'ledningssystem för informationssäkerhet'). He comes to ask you how an ISMS is best implemented, explain how that is done.

6. 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 [And08, s. 23] 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.

(4p) 7. Describe the main differences between Mandatory Access Control (MAC) and Discretionary Access Control (DAC).

Suggested solution In MAC the access control policy for new material is derived from the subject and objects it is based on. One example is Bell-LaPadula (BLP): where information only flows upward, a document produced by someone with clearance A will also require clearance A to be read—clearance $B < A$ will not suffice. The system sets the access policy for objects.

In DAC this is under the control of the owner of an object. The owner sets the access policy. An example is the UNIX file system.

8. Define the following terms:

(1p) (a) Trusted

(1p) (b) Trustworthy

(1p) (c) Secrecy

(1p) (d) Confidentiality

(1p) (e) Privacy

(1p) (f) Integrity

(1p) (g) Authenticity

Suggested solution Anderson [And08, ss. 13–14] 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'" [And08, s. 13].

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**].

9. Separation of duties is a core concept for security.

(2p) (a) Describe the two types of separation of duties.

(1p) (b) What is the main reason for separation of duties?

Suggested solution There are two types of separation of duties: dual control and functional separation. Dual control means that two or more subjects must act together (at the same time) to authorize a transaction. Functional separation means that several functions are needed to authorize a transaction—e.g. create a transaction and verify it—and one subject is not allowed to do both functions.

The reason for separation of duties to make it impossible for one malicious subject to compromise a system. With separation of duties the malicious subject must persuade one or more other subjects to collude.

References

[And08] Ross J. Anderson. *Security Engineering. A guide to building dependable distributed systems.* 2nd ed. Indianapolis, IN: Wiley, 2008. ISBN: 978-0-470-06852-6 (hbk.) URL: `http://www.cl.cam.ac.uk/~rja14/book.html`.

[Gol11] Dieter Gollmann. *Computer Security.* 3rd ed. Chichester, West Sussex, U.K.: Wiley, 2011. ISBN: 9780470741153 (pbk.)