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

2015-06-05

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 42

Questions 7

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) Brute force

(1p) (b) Dictionary attack

(1p) (c) Hash table

(1p) (d) Social engineering

(1p) (e) Two-factor authentication

(1p) (f) Phishing

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

   comprehensive8 At least 8 characters consisting of upper and lower case, numbers and special characters (assume the ones common with the numbers on a keyboard).

   randswedict3 Randomly choose three 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 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.

(5p) 3. When you start in the company you realize that there is no Information Security Management System (ISMS, Swe. 'ledningssystem för informationssäkerhet'). You go into your boss's office: persuade him and the management that you need an ISMS.

(5p) 4. 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.

5. 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**].

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.

(5p) 7. Describe what problems can arise when using biometrical systems. Explain why they still can be used if employed properly.

Suggested solution Anderson [And08] anger några problem med biometriska system, sammanfattningsvis är de

- att systemen fungerar dåligt eller inte alls för personer med kroppskador, då systemen är anpassade för mycket begränsad naturlig variation;
- att många system går att lura med hjälp av inspelningsattacker, exempelvis att ett gammalt fingeravtryck visas upp för fingeravtrycksläsaren eller att en inspelning spelas upp för ett röstigenkänningsystem;
- att det är svårt för en mänsklig operatör att verifiera eller falsifiera biometriska data;
- att precisionen i det biometriska systemet är för dålig för att kunna skilja en användare från en annan.

En anledning till att de ändå kan användas är för att de kan ha en avskräckande effekt, alltså en ren psykologisk effekt hos angripare (och hos användare generellt). De kan även användas i kombination med en annan säkerhetsmekanism, exempelvis ett lösenord, för att åstadkomma tvåfaktorautentisering.

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`.