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

2019-06-05

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.

Questions 5

Preliminary grades

Each question can be awarded up to three points: one point for E, two points for C and three points for A. To get an E, you must get at least one point on each question — i.e. no question must be awarded zero points. For a C, you must get two points on at least half of the questions. For an A, you must get three points on at least half of the questions.

Questions

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

(3p) 1. Game consoles is a good example of a class of devices where part of the security is to lock the user out from the highest privileges. The classic example is the Sony PlayStation where users at first could choose to run Linux instead, but Sony later changed their mind and disallowed that. However, users found ways around that, namely buffer overruns (*e.g.*, stack overflows).

Explain, on a conceptual level, how one could exploit a buffer overrun (*e.g.*, stack overflow) in the PlayStation operating system to install and run Linux instead.

> **Suggested solution** The case from reality happened like this:
>
> Someone found a stack overflow vulnerability in a Zelda game (Twilight princess?). One could change the name of the pony in a game save (can be done on another system!) to something very long. The system would not check the length of this name since it was "not changeable". This would cause a stack overflow. In the name one could include executable code which would launch the Linux installer.

(3p) 2. Alice and Bob wants to communicate securely, *i.e.*, through an end-to-end encrypted and authenticated channel (*e.g.*, Signal, Telegram, WhatsApp, PGP/Protonmail). What do they have to do to make this happen?

> **Suggested solution** They would have to create secure keys and store them securely in some devices. They would have to verify each other's public key: either they verify it themselves or they must trust someone. *E.g.*, they can trust that Signal's verification of phone numbers work and if they previously verified the phone numbers, then it should work now too.

(3p) 3. You are asked to analyse two password policies. The policies are the following:

basic12 Let *the user choose* at least 12 characters consisting of: upper and lower case, numbers.

randswedict4 *Generate a password for the user* by randomly choosing four words from the Dictionary of the Swedish Language (SAOL). This dictionary contains approximately 125 000 words.

Analyse the two policies: what are the advantages and disadvantages of each, how do they compare to each other.

(3p) 4. What is attribute-based access control (ABAC) and what are its advantages?

> **Suggested solution** It's an access control model.
>
> It uses attributes in the security policy: e.g. identities, age limits, times. This requires authenticated attributes.
>
> This is the most general access control model.

(3p) 5. 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.