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

2015-10-30

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 44

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.

1. Explain the following terms:

   (1p) (a) Confidentiality

   (1p) (b) Integrity

   (1p) (c) Availability

   (1p) (d) Accountability

   (1p) (e) Non-Repudiation

2. The apps in the Google Play store or Apple's AppStore are provided with some DRM, e.g. you cannot copy a paid-for app from one phone to another etc. There are also other things you are not allowed to do with these smartphones, e.g. installing whatever software you like, modifying the software in any way you like, etc. (However, many know of the terms "jail-breaking" or "rooting" their phones, which bypasses these mechanisms on the phones.)

   (3p) (a) Explain how this type of protection system works, including the fundamental assumptions needed for it to fulfil its purpose.

   (3p) (b) Explain how the above system can be broken and whether it could be fully solved or not.

3. 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

4. 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.

   (4p) (b) Give an example of an attack which exploits weaknesses in human psychology. Also explain why it works.

5. 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?

6. You have implemented a Mandatory Access Control (MAC) system in the organization you work for. Your goal was to achieve stronger confidentiality for data.

   (2p) (a) In one sense this is true, explain why.

   (2p) (b) Some violations of confidentiality simply cannot be protected against, give an example and explain why this is so.

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.)

(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. Look at the C code in Listing 1 on the next page.

(3p) (a) Identify all vulnerabilities in that code and motivate by stating how they can be exploited.

(3p) (b) Suggest improvements to remedy these vulnerabilities, you must motivate why they work.

```c
#include <stdio.h>

int
get_some_input( void )
{
  char buffer[128];

  printf( "Please enter the key: " );
  scanf( "%s", buffer );

  /* process input */

  return 0;
}

void
make_full_name( char *dst, int dstlen,
                const char *src, int srclen,
                int maxsize )
{
  if ( dstlen + srclen + 1 >= maxsize )
    return -1;

  strncat( dst, " ", 1 );
  return strncat( dst, src, srclen );
}

int
main( int argc, char **argv )
{
  char first[256];
  char last[256];

  printf( "Please enter your first name: " );
  scanf( "%s", first );
  printf( "Please enter you last name: " );
  scanf( "%s", last );

  make_full_name( first, strlen( first ),
                  last, strlen( last ), 256 );

  if ( get_some_input() < 0 )
    return -1;

  return 0;
}
```

Listing 1: Some vulnerable C code.