Academic Year: Winter Semester 2021/22

6090: Security of Computer and Embedded Systems

Assignment (40%)

1. **(2 points)** Many banks issue hardware tokens for authenticating their e-banking customers. These hardware tokens
    - require the user to enter a code into the hardware token and
    - generate a one-time password that the user enters as password into the e-banking application (website).

    Explain why this is considered a two-factor authentication and explain if this is a good or bad two factor authentication system.

2. **(3 points)** Recall the "STRIDE" mnemonic used in threat modelling.
    In the below table, you are given certain threat/problem examples.
    Fill the "Threat" and "Property Violated" columns in the table with corresponding elements where
    <u>"Threat":</u> STRIDE threats (each letter stands for a threat) and
    <u>"Property Violated":</u> Confidentiality, Integrity, Authentication, Authorization, Availability, Non-repudiation.

Threat	Property Violated	Example
		Allowing someone to read the Windows source code; publishing a list of customers to a website
		Modifying a DLL on disk or DVD, or a packet as it traverses the network
		Allowing a remote internet user to run commands, going from a limited user to admin
		Pretending to be any of Bill Gates, Paypal.com, or ntdll.dll
		"I didn't send that email", "I didn't modify that file", "I certainly didn't visit that website!"
		Crashing Windows or a web site, sending a packet and absorbing seconds of CPU time, or routing packets into a black hole

3. **(6 points)** What is the output of the first round of the DES algorithm [2] when the plaintext and the key are both
    - all zeros?
    - all ones?

   Calculate and give details step by step using paper, pen, and a simple calculator. You may want to write a small program to check the correctness of your answers (or find online tools for verification).

4. **(8 points)** This problem deals with the lightweight cipher PRESENT.

   Calculate the state of PRESENT-80 [2] after the execution of one round. Give details of your calculation step by step. You can solve this problem with paper, pen, and simple calculator. You may want to write a small program to check the correctness of your answers (or find online tools for verification). Your calculation details should include Round key and States after KeyAdd/S-Layer/P-Layer. Use the following values (in hexadecimal notation):
   Plaintext: **0000 0000 00XX XXXX**
   (XX XXXX being your matriculation number. If it is only five digits, then the first X should be 0.)
   Key: **BBBB 5555 5555 EEEE FFFF**

5. **(2 points)** Assume a (small) company with 120 employees. A new security policy demands encrypted message exchange with a symmetric cipher. How many keys are required, if you are to ensure a secret communication for every possible pair of communicating parties?

6. **(6 points)** Alice wants to compute an RSA key-pair. She chooses the “large” prime numbers p = 13 and q = 7. Complete the RSA key generation for Alice, i.e., compute an RSA key pair for her. Describe briefly the intermediate steps of your calculation.
   (Hint: You might want to make use of the following fact: 7^{-1} mod 72 = 31.)

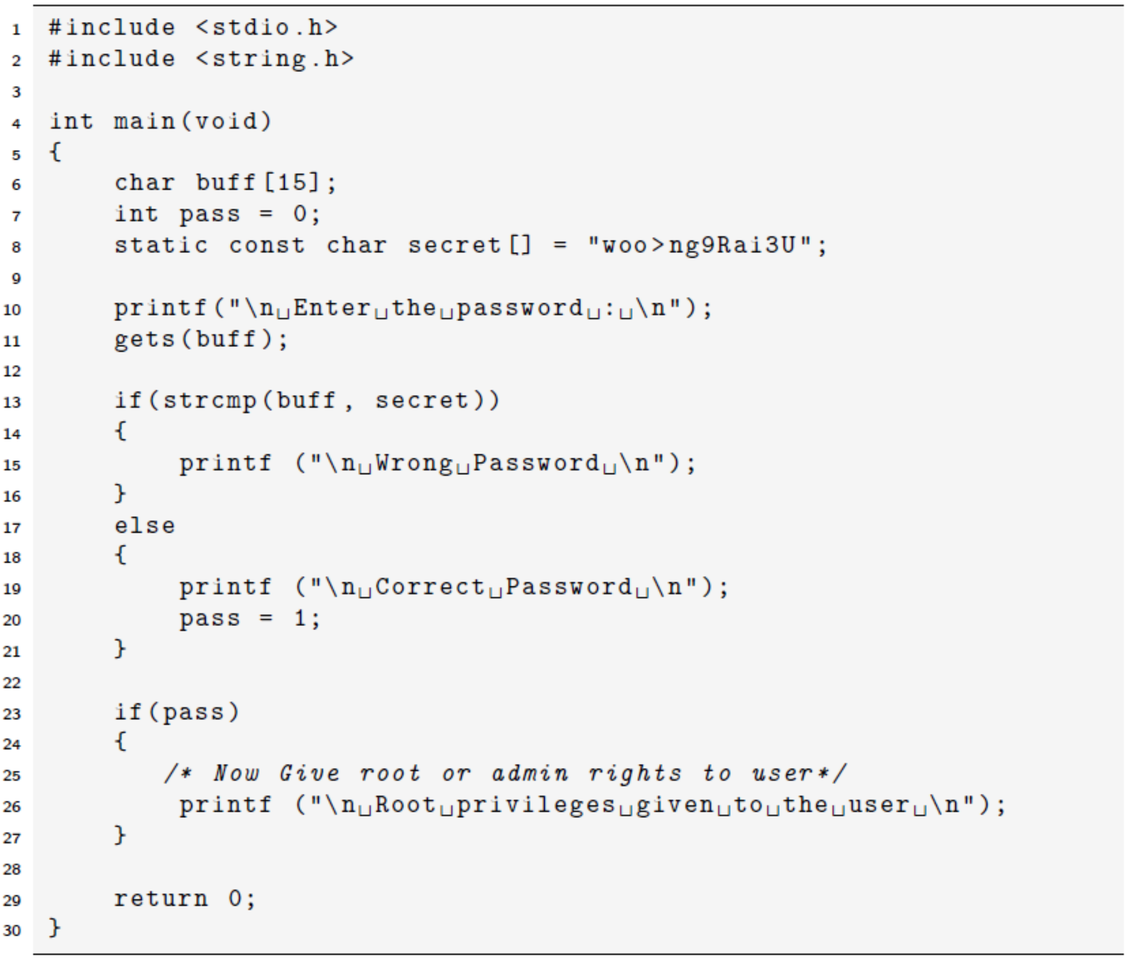
    - Bob wants to send Alice the message “topsecret” as encrypted. Encode the letters by their position in the alphabet (e.g., the letter "a" is represented by the number 1) and compute the ciphertext for each character of the message.
    - Alice wants to send Bob the signed message “signature”. Encode the letters by their position in the alphabet (e.g., the letter "a" is represented by the number 1) and compute the signature for each character of the message (i.e., to simplify the problem, we do not hash the message).

7. **(3 points)** As you have seen in the lectures, public-key cryptography can be used for encryption and key exchange. Furthermore, it has some properties (such as non-repudiation) which are not offered by secret key cryptography. So why do we still use symmetric cryptography in current applications?

8. **(4 points)** One of the most attractive applications of public-key algorithms is the establishment of a secure session key for a private-key algorithm such as AES over an insecure channel.

Assume Bob has a pair of public/private keys for the RSA cryptosystem. Develop a simple protocol using RSA which allows the two parties Alice and Bob to agree on a shared secret key. Who determines the key in this protocol, Alice, Bob, or both?

9. **(4 points)** Consider the C program for which we assume that in the block starting at line 24, code with administrative privileges is executed.
The program has two different vulnerabilities. Name the vulnerabilities and explain them briefly.



```
1  #include <stdio.h>
2  #include <string.h>
3
4  int main(void)
5  {
6      char buff[15];
7      int pass = 0;
8      static const char secret[] = "woo>ng9Rai3U";
9
10     printf("\n␣Enter␣the␣password␣:␣\n");
11     gets(buff);
12
13     if(strcmp(buff, secret))
14     {
15         printf ("\n␣Wrong␣Password␣\n");
16     }
17     else
18     {
19         printf ("\n␣Correct␣Password␣\n");
20         pass = 1;
21     }
22
23     if(pass)
24     {
25        /* Now Give root or admin rights to user*/
26         printf ("\n␣Root␣privileges␣given␣to␣the␣user␣\n");
27     }
28
29     return 0;
30 }
```

10. **(2 points)** You have two security testing tools with the following false positive and negative rates:

Tool A	**Tool A**
False Positive Rate 20%	False Positive Rate 40%
False Negative Rate 70%	False Negative Rate 40%

Assume you want to minimize the risk of delivering insecure software to customers. Would you use Tool A or Tool B? Why?

You can of course work on the assignment together with your peer colleagues (because I anyways cannot control this), but the same or very similar submissions will be considered as copying. So, you can work together with other, but prepare your assignment submission just by yourself using your own words. You are expected to submit your *handwritten&scanned and/or computer-typed* answers to the assignment (file to be named as **NameSurname.pdf**; pay attention to upper/lowercase while naming, submissions not following the naming and file requirements will not be accepted) via Stud.IP (6090 Course [Lecture] -> Files -> **Assignment Submission**) latest on **28.01.2022 at 17:00 CET**.

References

1. NIST, FIPS 46-3: The official document describing the DES standard, 1999 (https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf).
2. Bogdanov, A. et al.; PRESENT: An Ultra-Lightweight Block Cipher. Lecture Notes in Computer Science. 4727 (Cryptographic Hardware and Embedded Systems - CHES'07), pages 450–466, 2007. (https://www.iacr.org/archive/ches2007/47270450/47270450.pdf)