Security
30 June 2014

- This exam consists of three parts: (1) six short questions, every one counts for 5 points, (2) eight true/false questions, for each of them, a correct answer scores 2.5 points, an incorrect answer **-1** point, and (3) four problems, every one counts for 12.5 points. In order to get the maximum amount of points,
  - answer the Short Questions, and
  - answer the True or False Questions, and
  - solve **all** Problems from the third part.
- Mark every page with name and student number.
- Use of books, additional course material, mobile phones, tablets, etc is prohibited.
- Use of calculators is allowed.
- Do not use pencil or red ink.
- Give your answers on the exam paper (if needed, you may request additional paper.)
- Answer in English.

Please do not write below this line.

Question	**Scored points**
Short Questions	
True or False Questions	
Problem 1: Cryptography	
Problem 2: Buffer Overflows	
Problem 3: Network Security	
Problem 4: The Base-Rate Fallacy	

---

1 Short Questions (30 points: 6 × 5 points)

1. (5 points) What is the Kerckhoffs's principle?

2. (5 points) Is it easier to passively eavesdrop on UDP traffic than on TCP traffic, or does it not matter?

3. (5 points) What is the role of a Certificate Authority? Where on your computer can you find a list of Certificate Authorities?

4. (5 points) An access control system could give a process created by executing a file the same permissions as the owner of the file. What feature of Unix achieves this?

5. (5 points) Describe SYN flooding attacks.

6. (5 points) What is a drive-by-download and how does it differ from a worm?

2 True or False (20 points: 8 × 2.5/-1 points)

Circle TRUE or FALSE. Optionally you can add one line to justify your answer. A correct answer scores 2.5 points, an incorrect answer scores **-1** point, a lack of answer scores 0 points.

7. (2.5/-1 points) TRUE or FALSE: Properly used, a MAC provides both confidentiality and integrity.

8. (2.5/-1 points) TRUE or FALSE: If Alice has a message to send to Bob and she wants to encrypt the message using asymmetric cryptography so that no one other than Bob can read it, she does so by using Bob's public key.

9. (2.5/-1 points) TRUE or FALSE: An attraction of public key cryptography is that, if implemented properly, the algorithms generally run much faster than those for symmetric key cryptography.

10. (2.5/-1 points) TRUE or FALSE: Depending on the application, user authentication on a biometric system involves either verification or identification.

11. (2.5/-1 points) TRUE or FALSE: Intrusion detection is based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified.

12. (2.5/-1 points) TRUE or FALSE: Signature-based approaches attempt to define normal, or expected, behavior, whereas anomaly approaches attempt to define proper behavior.

13. (2.5/-1 points) TRUE or FALSE: The attacker needs access to a high-volume network connection for a SYN spoof attack.

14. (2.5/-1 points) TRUE or FALSE: Buffer overflow attacks result from careless programming in applications.

3 Problems (50 points: 4 × 12.5 points)

15. (12.5 points) **Problem 1: Cryptography**

Let's consider the following statement:

If PA is the public key of A, SB is the secret key of B, and $E(K, X)$ denotes encryption of X with the key K, then we can safely say that for practical purposes

$$E(PA, E(SB, M)) = E(SB, E(PA, M)) \tag{1}$$

Note that the equality sign should be read as equality in the mathematical sense, i.e., stating that the message on the left-hand-side of the equation is *exactly the same* as the message on the right-hand-side of the equation.

(a) (2.5 points) Is this statement true or false?

(b) (10 points) If the statement is true, explain why. If it is false, give a complete counterexample using the RSA algorithm. If the latter,

1. provide the values you selected for key generation,
2. compute the keys,
3. provide the message you selected,
4. perform the encryption as specified in formula (1), and show that the equation does not hold.

In all the above steps, if the algorithm makes assumptions about the selected values, state them, and show that your example satisfies them.

16. (12.5 points) **Problem 2: Buffer Overflows**

Consider the following code snippet coming from a server that accepts a network connection from a client, and then expects the client to specify which file the client request. If this file can be read by a regular user, i.e., a non-root user, the server sends it back to the client. Finally, the server exits.

```
int main(int argc, char *argv[]) {
    char requested_filename[256];
    int uid; /* user id */
    int i;

    uid = 1002;

    /* Accept a connection from client */

    /* Read and store the filename requested by client */
    i = 0;
    while(true) {
        requested_filename[i] = read_next_byte_from_socket();
        if (requested_filename[i] == ' ') {
            break;  /* exit the while loop */
        }
        i++;
    }

    if (user with uid has the rights to read requested_filename) {
        /* Open the requested_filename, send its contents back to the client,
         * and close the network connection. */
    } else {
        /* Send an ACCESS DENIED message back to the client,
         * and close the network connection. */
    }

    return 0;
}
```

For the sake of simplicity, the `while` loop above exits when the server reads a white space character `' '`. For example, if a client sends `'\foo \bar'`, the while loop exits once it has read `' '`, so the `requested_filename` ends up being `'\foo '`.

[*Comment:* In reality, strings in C are null-terminated characters, and `'\'` is an escape character (to encode a backslash, one would need to use `'\\'`). However, there is absolutely no need for you to worry about it. You can safely assume that if a client sends `'\home\makai\file.txt '`, the `requested_filename` buffer will contain `'\home\makai\file.txt '`, and the server will open the `\home\makai\file.txt` file.]

Make the following assumptions:

- the server process is executed by the root user,
- a user with `uid = 1002` is a regular user, with restricted privileges,
- each call to `read_next_byte_from_socket()` returns one subsequent byte read from the network socket,
- the process executes on a 32bit machine, which means that the size of an `int` is 4 bytes, the size of an address (such as e.g., the return address) is 4 bytes, and the size of a `char` is 1 byte,
- the compiler placed the `requested_filename` buffer just underneath the `uid` and `i` variables, i.e., the buffer starts at a lower address in memory,
- no stack protection mechanisms have been implemented.

(a) (2.5 points) Sketch a diagram illustrating the memory layout in the function frame of `main()`. Indicate all local variables, their sizes, and relative distances. Show where the return address is located.

(b) (5 points) Identify a buffer overflow vulnerability. Can you exploit it to execute your own shellcode of the length of 199 bytes? If not, why? If yes, propose a request you would need to send. Include the length of the request, its exact layout, and contents.

(c) (1 point) What reply would you receive from the server if you send the following request: '`\etc\shadow` '?

(d) (4 points) Can you exploit the vulnerability so that the server sends you back the contents of the `\etc\shadow` file? If not, why? If yes, propose a request you would need to send. Include the length of the request, its exact layout, and contents.

17. (12.5 points) **Problem 3: Network Security**

(a) (6.25 points) **Firewalls**

Can a stateless firewall (such as a packet filter) enforce the following policy?

Policy: Block TCP connection initiation requests from any external host to any internal host. Allow TCP connection initation requests from any internal host to any external host, and also allow returning traffic on these connections initiated by internal hosts.

You may assume that the internal hosts (those on the inside of the firewall) all have IP addresses of the form `145.108.123.x`, where the `x` can be anything in the range 0-255, and no external host has an IP address of this form. You may assume that the TCP/IP stack on every internal host operates correctly.

i. (1.25 points) Circle TRUE or FALSE, depending on whether you think a stateless firewall (such as a packet filter) can enforce the policy above or not.

ii. (5 points) Justify your answer.

(b) (6.25 points) **DNS**

Today, DNS servers accept queries via the UDP protocol. But imagine that DNS had been designed differently, so that DNS used only TCP (not UDP) and DNS servers accepted queries only via TCP (ignoring all UDP packets). Would this make the DNS cache poisoning attack easier, harder, or have no effect?

i. (1.25 points) Circle one answer:
   1. The attack would be easier.
   2. No effect.
   3. The attack would be harder.

ii. (5 points) Justify your answer.

18. (12.5 points) **Problem 4: The Base-Rate Fallacy**

Suppose that an Intrusion Detection System (IDS) performs a check that is 99% accurate, i.e. when the test is performed on network connections all of which are malicious, 99% of the checks indicate an attack, and likewise, when the network connections were known to be 100% benign, 99% of the test results were negative. In general, attacks are rare. On average, only 1 in 10000 network connections is malicious.

When solving the problem, assume the following notation:

- I denotes intrusion, i.e., an attack; $\neg I$ denotes non-intrusion, i.e., a benign connection,
- A denotes an alert raised by the IDS; $\neg A$ denotes the lack of an alert raised by the IDS.

(a) (5 points) A network administrator notices that the IDS raises an alert on a particular network connection. What, given the above information, is the probability of the connection being malicious?

(b) (1.5 points) Explain the Base-Rate Fallacy phenomenon.

(c) (3 points) **False Positive rate**

i. (1 point) Define *False Positive* (FP) rate.

ii. (2 points) Compute the FP rate of the above IDS.

(d) (3 points) **False Negative rate**

i. (1 point) Define *False Negative* (FN) rate.

ii. (2 points) Compute the FN rate of the above IDS.