Exam 2017, questions

Computer Security and Forensics (University of Sheffield)

The University Of Sheffield.

Data Provided:
None

DEPARTMENT OF COMPUTER SCIENCE Spring Semester 2016-2017

COMPUTER SECURITY AND FORENSICS 2.5 hours

Answer ALL FOUR QUESTIONS. Write clearly in the sense of logic, language, and readability. The clarity of your arguments and explanations affects your grade.

Questions 1 and 2 carry a weight of 20%, questions 3 and 4 carry a weight of 30%. Figures in square brackets indicate the percentage of available marks allocated to each part of a question.

THIS PAGE IS BLANK.

1. Security Fundamentals & Access Control

a) List and define the three concepts of the CIA triad. [10%]

b) Consider the concept of multi-factor authentication.

(i) Give a brief definition of multi-factor authentication and explain what property a good multi-factor authentication system should satisfy. [10%]

(ii) Name
- an example of a good multi-factor authentication system and
- an example of a bad multi-factor authentication system.

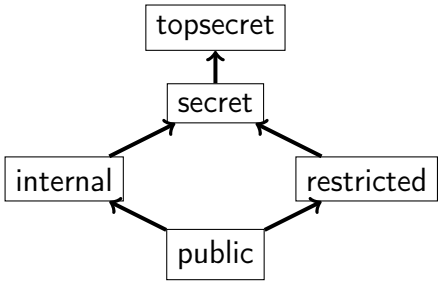
Give a brief justification of why your examples are good/bad multi-factor authentication systems. [10%]

c) Recall the concept of multi-level security where data labels are organised in a hierarchy.

Now consider the following multi-level security setting in which all data is labelled with one label out of the following set of labels: {topsecret, secret, internal, restricted, public}.

Access by a user to a (labelled) file is granted if the user has a sufficiently high clearance level.

The labels are ordered in the following hierarchy.



Note that labels in the upper part of the figure are more confidential than labels at the lower part of the figure:

Assume that data labels are applied at file granularity, i.e., a label is always assigned to the whole content of a file.

Answer the following questions. For each of the questions, your answer should be a subset of {topsecret, secret, internal, restricted, public}.

(i) Write down the user clearance level(s) required to read files that are labelled "restricted". [5%]

(ii) Write down the user clearance level(s) required to read files that are created from the content of two files, one with the label "restricted" and one with the label "internal". [10%]

QUESTION CONTINUED ON THE NEXT PAGE

d) Consider a company with the the following organisational roles and tasks:

- Members of *staff* can *request* business *travel*.
- *Managers* can *approve* business *travel*.

The company has the following employees: Alice, Bob, Eve, and Charlie.

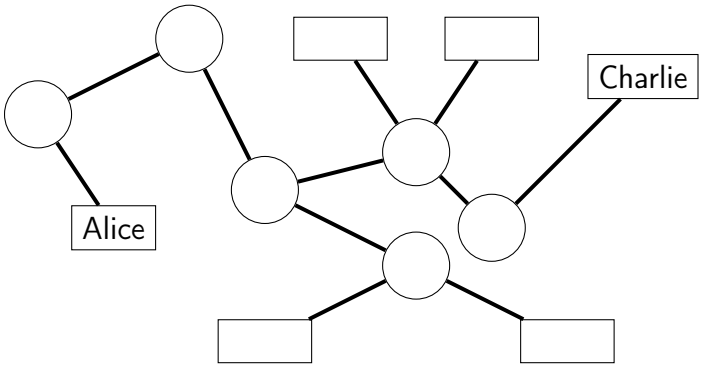
Alice and Charlie are managers.

(i) Define a *hierarchical* role-based access control (RBAC) policy for this company and explain how the set of permissions of Alice can be computed using the defined RBAC policy. [45%]

(ii) Briefly explain either one limitation of RBAC in the context of the company scenario of this exercise or describe a generic weakness of RBAC. [10%]

2. Cryptography & PKIs

a) The following figure shows a chain of X.509 certification authorities and users. The lines indicate the hierarchical relationship among the certificate authorities. Circles indicate certificate authorities and boxes indicate end users.



We know that

- Alice can obtain the public key of Randy using the following chain path: Q«S», S«U», U«T»,T«Randy»
- Charlie can obtain the public key of Eve using the following chain path: W«T», T«Eve»
- Isabelle can obtain the public key of Bob using the following chain path: R«Bob»

Copy the graph to your answer book and write the names of the certification authorities and subjects in their appropriate circles/boxes. [10%]

b) Consider the RSA crypto scheme with the following configuration:

- Alice's public key is $(n_a, e_a) = (33, 7)$, her private key is $d_a = 3$
- Bob's public key is $(n_b, e_b) = (65, 7)$, his private key is $d_b = 7$

Recall that we encode the letters by their position in the alphabet (e.g., the letter "a" is represented by the number 1, spaces are not encoded).

(i) Bob wants to send the message "`meet at noon`" to Alice. What is the ciphertext of the message that Bob sends to Alice. [25%]

(ii) Bob receives the message: "9 1, 52 38, 1, 45, 60". Decrypt and decode the message that Bob received. [25%]

c) Consider the following DES-inspired encryption scheme *without* an initial permutation that is based on

- a block length of 8
- four rounds
- $f_i(x, K) = (i \cdot x)^K \mod 16$ (for $i = 1, \ldots, 4$)

(i) Draw a diagram of the overall structure of the encryption scheme illustrating the four rounds. [15%]

(ii) Encrypt 00000101_2 using the key $K = 1101_2$ $(= 13_{10})$ [25%]

3. **Security Protocols**

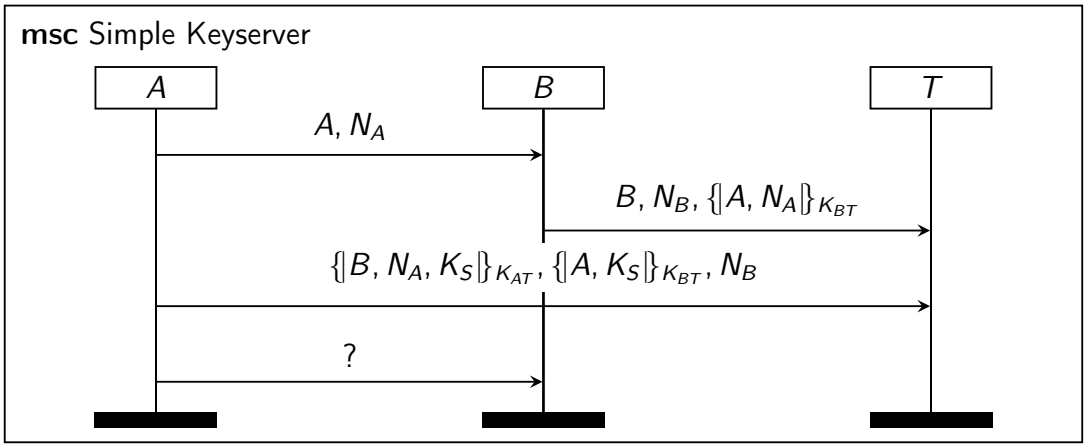
a) Recall the Needham-Schroeder (NSPK) protocol. The following is the Alice & Bob specification of NSPK:

$$A \longrightarrow B: \ \{N_A, A\}_{\mathsf{pk}(B)}$$
$$B \longrightarrow A: \ \{N_A, N_B\}_{\mathsf{pk}(A)}$$
$$A \longrightarrow B: \ \{N_B\}_{\mathsf{pk}(B)}$$

(i) Explain the well-known attack on NPSK (e.g., by drawing a message sequence chart) and explain for each participant
- to whom they believe they are speaking to
- to whom they are actually speaking to [15%]

(ii) Describe a technique that protects NSPK from this well-known attack? [15%]

b) Consider the following protocol in which A and B use a trusted third party T to perform mutual authentication and establish a session key K_S . Assume that initially A and T share the symmetric key K_{AT} and B and T share the symmetric key K_{BT} . A and B generate nonces N_A and N_B, respectively. There are four steps in the protocol, the first three of which are given in the following message sequence chart:



(i) What message should A send to B in step 4 to complete the protocol? [15%]

(ii) State whether or not the protocol is still secure if the message in step 2 is changed to

$$B, N_B, N_A, \{|A|\}_{K_{BT}}$$

Explain your answer.
[**Hint:** Your answer does not depend on your answer to 3(b)(i)]. [10%]

(iii) State whether or not the protocol is still secure if the message in step 2 is changed to

$$B, \{|A, N_A, N_B, |\}_{K_{BT}}$$

Explain your answer.
[**Hint:** Your answer does not depend on your answer to 3(b)(i)]. [10%]

QUESTION CONTINUED ON THE NEXT PAGE

c) The Dolev-Yao closure $\mathcal{DY}(M)$ consists of *seven* deductive rules. Three of them are:

$$\frac{}{m \in \mathcal{DY}(M)}\ \text{Axiom}\ (m \in M) \qquad \frac{s \in \mathcal{DY}(M)}{t \in \mathcal{DY}(M)}\ \text{Algebra}\ (s \approx t)$$

$$\frac{\langle m_1, m_2 \rangle \in \mathcal{DY}(M)}{m_i \in \mathcal{DY}(M)}\ \text{Proj}_i$$

(i) Define the missing *four* rules of the Dolev-Yao closure *formally* and give a brief informal description what action of the intruder they formalise.
[**Hint:** if you cannot describe the rules formally explain informally the different actions a Dolev-Yao intruder can use for inferring new messages from an initial set of messages precisely (this might need two or three short sentences per rule).] [15%]

(ii) Consider the following intruder knowledge:

$$M = \{\{\!|k|\!\}_{h(n_2)}, \{n_1\}_{\mathsf{pk}(i)}, \{n_2\}_{\mathsf{inv}(\mathsf{pk}(a))}, \mathsf{pk}(a), \mathsf{pk}(i), \mathsf{inv}(\mathsf{pk}(i)), \{\!|secret|\!\}_k\}$$

where h is a public function (i.e., $h \in \Sigma_P$).
Prove formally that the intruder can learn the message "*secret*".
[**Hint:** if you cannot recall the formal proof notation, give a detailed informal argument.] [20%]

4. Application Security

a) The recommendation for preventing injection attacks is to *sanitise* (filter) user input. In general, there are two approaches for filtering input: *black listing* and *white listing*.

(i) Briefly explain the concepts *black listing* and *white listing*. [6%]

(ii) Which approach is usually recommended? Briefly explain your answer. [6%]

b) Consider the following vulnerability in the database system MySQL (CVE-2013-0375):

> A vulnerability in the MySQL Server database could allow a remote, authenticated user to inject SQL code that MySQL replication functionality would run with high privileges. A successful attack could allow any data in a remote MySQL database to be read or modified.

What CVSS v2 Base Vector (AV:?/AC:?/Au:?/C:?/I:?/A:?) would you assign to this vulnerability? Explain your decision. In your answer, you will need to replace the '?' in the CVSS v2 Base Vector. [20%]

c) Suppose you know that a particular web site uses a backend database to implement authentication. Given a login page with username and password fields, what would you type into these fields to try to perform SQL injection to bypass proper authentication? Briefly explain why your approach would work. [14%]

d) Let us assume you have two security testing tools with the following false positive and false negative rates:

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

(i) Briefly define the terms
- false positive (FP)
- true positive (TP)
- false negative (FN)

in the context of application security testing tools. [6%]

(ii) Assume you want to minimise the risk of delivering insecure software to customers. Would you use Tool A or Tool B? Briefly explain your choice. [6%]

(iii) Assume you want to minimise the impact (effort) of introducing a security testing tool. As a developer, would you prefer Tool A or Tool B? Briefly explain your choice. [6%]

QUESTION CONTINUED ON THE NEXT PAGE

e) Consider the following C program for which we assume that in the block starting at line 24, code with administrative privileges is executed.

```
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 }
```

(i) This program has two different vulnerabilities. Name the vulnerabilities and explain them briefly. [20%]

(ii) There are two fundamentally different classes of security testing tools: static (source) code analysis tools and dynamic testing tools (e.g., fuzzers).
Using

- one vulnerability that is easy to detect using a dynamic security testing tool and
- one vulnerability that is easy to detect using a static source code analysis tool

briefly explain the advantages and disadvantages of both security testing approaches.
You can either use the vulnerabilities from the example C program provided above or use your own example. [16%]

END OF QUESTION PAPER