Com3501 mock-2016-17

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 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.

All questions carry equal weight. Figures in square brackets indicate the percentage of available marks allocated to each part of a question.

Note that this is a mock exam giving you an idea what *kind* of questions (not the content) might be asked in the actual exam. It is not representative for the topics/content that the final exam might cover. All content discussed in the lecture, the labs, and the homework (as long as not otherwise stated) is relevant for the final exam.

THIS PAGE IS BLANK.

1. **Security Fundamentals & Access Control**

a) Define briefly the concepts Authentication and Authorisation. [10%]

b) For each of the following multi-factor authentication systems, exp0lain briefly if the it is a good or bad multi-factor authentication systems:

(i) A *password* and a *fingerprint*. [5%]

(ii) A *fingerprint* and a *retina scan*. [5%]

(iii) A *password generator* and traditional *password*. [5%]

(iv) A *GPS signal* and a *password*. [5%]

c) In access control enforcement, briefly explain the role of the *policy enforcement point (PEP)* and the *policy decision point (PDP)*. [10%]

d) Given the following RBAC model:

$$\begin{aligned}
\mathit{ROLES} &= \{\texttt{lecturer}, \texttt{demonstrator}, \texttt{student}\}\\
\mathit{USERS} &= \{\texttt{achim}, \texttt{eleni}, \texttt{heidi}, \texttt{alice}, \texttt{bob}\}\\
\mathit{PERMISSION} &= \{\texttt{read\_comx501\_slides}, \texttt{write\_comx501\_slides},\\
&\quad \texttt{read\_comx501\_exam}, \texttt{write\_comx501\_exam},\\
&\quad \texttt{read\_comx501\_solutions}, \texttt{write\_comx501\_solutions}\}\\
\mathit{UA} &= \{(\texttt{achim}, \texttt{lecturer}), (\texttt{eleni}, \texttt{lecturer}),\\
&\quad (\texttt{heidi}, \texttt{demonstrator}), (\texttt{alice}, \texttt{student}),\\
&\quad (\texttt{bob}, \texttt{student})\}\\
\mathit{PA} &= \{(\texttt{lecturer}, \texttt{read\_comx501\_slides}),\\
&\quad (\texttt{lecturer}, \texttt{write\_comx501\_slides}),\\
&\quad (\texttt{lecturer}, \texttt{read\_comx501\_exam}),\\
&\quad (\texttt{lecturer}, \texttt{write\_comx501\_exam}),\\
&\quad (\texttt{lecturer}, \texttt{read\_comx501\_solutions}),\\
&\quad (\texttt{lecturer}, \texttt{write\_comx501\_solutions}),\\
&\quad (\texttt{demonstrator}, \texttt{read\_comx501\_slides}),\\
&\quad (\texttt{demonstrator}, \texttt{write\_comx501\_slides}),\\
&\quad (\texttt{demonstrator}, \texttt{read\_comx501\_exam}),\\
&\quad (\texttt{demonstrator}, \texttt{read\_comx501\_solutions}),\\
&\quad (\texttt{student}, \texttt{read\_comx501\_slides}),\\
&\quad (\texttt{student}, \texttt{read\_comx501\_exam})\}
\end{aligned}$$

QUESTION CONTINUED ON THE NEXT PAGE

(i) Explain briefly how you can compute the permissions of `eleni` and name all permissions of `eleni`. [10%]

(ii) Explain briefly one benefit of hierarchical RBAC. [5%]

(iii) Transform the given RBAC model into a hierarchical RBAC model. [45%]

2. **Cryptography & PKIs**

a) (i) Sketch the "ideal" setup of a X.509 PKI with one global root CA that should serve eight entities (users).
[**Hint:** Recall the concept of intermediate CAs.] [5%]

(ii) Explain briefly two advantages of intermediate CAs. [5%]

(iii) Explain briefly the concept of *self-signed certificates*. [5%]

b) (i) Explain briefly what security guarantee(s) can be established by *encrypting* a message. [5%]

(ii) Assume that n persons want to be able to communicate securely with each other. Compare the necessary number of keys for symmetric and asymmetric cryptography. [15%]

(iii) Can symmetric cryptography be used for providing digital signatures. Explain you answer. [10%]

c) (i) Explain briefly the substitution cipher ROT13. [5%]

(ii) Encrypt the text "`YOUR COMPUTER IS NOT SECURE`" [15%]

(iii) Explain briefly a cipher-text attack that allows attack substitution ciphers such as ROT13. [10%]

d) Recall the RSA algorithm discussed in the lecture. Furthermore,

- Alice's public key is $(n_a, e_a) = (55, 33)$, her private key is $d_a = 17$
- Bob's public key is $(n_b, e_b) = (39, 5)$, his private key is $d_b = 5$

Bob wants to send the message "`das ist geheim`" to Alice. Encode the letters by their position in the alphabet (e.g., the letter "a" is represented by the number 1) and compute the cipher text. [25%]

3. **Security Protocols**

a) (i) Explain briefly the concept of a *replay* attack. [5%]

(ii) Explain briefly one technique that can be used for protecting protocols against *replay* attacks. [5%]

b) Consider the following voting protocol:

1. $A \longrightarrow S: \ A$
2. $S \longrightarrow A: \ \{Q, N_S\}_{\mathsf{pk}(A)}$
3. $A \longrightarrow S: \ \{Ans_Q, N_S\}_{\mathsf{pk}(S)}$

where A is a voter, S is the voting server, N_S is a nonce sent by the server to ensure freshness, Q is a referendum question, and Ans_Q is A's answer to the questions Q. Assume that A and S share their public keys in advance.

(i) Does this protocol provide anonymity? Can an attacker tell who has voted? [15%]

(ii) Does it provide confidentiality? Can an attacker find out, for a given A, how he or she voted? [15%]

c) Consider the following the key-establishment protocols that we designed in the lecture, which is based on an honest key-server S who has a shared key $\mathsf{sk}(A, S)$ with every agent A. The protocol consists out of four steps, where the first three steps are as follows:

$B \longrightarrow A: \ B, N_B$
$A \longrightarrow S: \ A, B, N_A, N_B$
$S \longrightarrow A: \ \{\!|K_{AB}, B, N_A|\!\}_{\mathsf{sk}(A,S)}, \{\!|K_{AB}, A, N_B|\!\}_{\mathsf{sk}(B,S)}$
$A \longrightarrow B: \ ?$

(i) What message should A send to B in step 4 to complete the protocol? [20%]

(ii) State whether or not the protocol is still secure if the message in step 3 is changed to

$S \longrightarrow A: \ \{\!|K_{AB}, B|\!\}_{\mathsf{sk}(A,S)}, \{\!|K_{AB}, A, N_B|\!\}_{\mathsf{sk}(B,S)}$

Explain your answer.
[**Hint:** Your answer does not depend on your answer to 3(b)(i)]. [20%]

(iii) State whether or not the protocol is still secure if the message in step 3 is changed to

$S \longrightarrow A: \ \{\!|K_{AB}, B, N_A, \{\!|K_{AB}, A, N_B|\!\}_{\mathsf{sk}(B,S)}|\!\}_{\mathsf{sk}(A,S)}$

Explain your answer.
[**Hint:** Your answer does not depend on your answer to 3(b)(i)]. [20%]

4. **Application Security**

a) The website `www.myvideos.com` provides a way to search for videos using an URL parameter. For example, given the request

```
https://www.myvideos.com/search.php?search=cat%20videos
```

the server will return an HTML page with the search results that contains the following part:

```
You searched for: <b>cat videos</b>.
```

In particular, the search phrase from the URL parameter is always included, without changes, in the result page.

(i) Explain briefly the vulnerability that this web site has. [5%]

(ii) Alice is a user of `www.myvideos.com`. Describe how an attacker might be able to use this vulnerability to steal the cookies that Alice's browser has for `www.myvideos.com`. [15%]

(iii) The developer of `www.myvideos.com` is informed about the vulnerability. For protecting their users, they implement a black-listing approach that strips of all occurrences of "<" and ">" from the input. Does this fix the vulnerability? Explain why. [15%]

b) For preventing SQL injections a web application developers implements a *client-side* white-listing in JavaScript. You can assume that the white-listing is strict, e.g., only allowing lower-case and upper-case characters to be passed to the backend.

Does this approach prevent SQL injection. Explain briefly your answer. [15%]

c) Consider the following vulnerability in the program iWork (CVE-2015-1098):

> The program iWork in Apple iOS before 8.3 and Apple OS X before 10.10.3 allows remote attackers to execute arbitrary code or cause a denial of service (memory cor- ruption) via a crafted iWork file.

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. [30%]

d) Suppose you want to develop a security testing tool that helps *security experts* to find as many security problems as possible in a given software application.

(i) Briefly explain what false/true positives/negatives are. [10%]

(ii) For the use case of supporting security experts in finding potential vulnerabilities, what compromise wrt false positives and false negatives would you suggest. Explain briefly your answer. [10%]

END OF QUESTION PAPER