NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Computer and Information Sciences

Examination paper for TDT 4237
Software Security

Thursday December 18th 2014, 09:00 - 13:00

This exam has been created by Lillian Røstad. Quality assurance by Guttorm Sindre.

Contact person during the exam is Lillian Røstad (contact: 994 00 628).

Language: English

Category D:

No printed or hand-written materials allowed. Approved calculator allowed.

Results available: Monday January 19th 2015

Read each task carefully. Identify what the task asks for.If you find that information is missing in a task you are free to make the assumptions you consider necessary, but remember to explain and clearly mark your assumptions.

Side

Checked by:

_____

Date Signature

Problem 1 – (30 points)

a. What information are you looking for in the information gathering phase of a security test?
b. What are the main properties of a cryptographic hash function?
c. OpenSAMM defines four Business Functions and for each of these three Security Practices. What security practices are included in the Verification Business Function? Briefly explain how each works.
d. The first two steps of the RMF has a focus on understanding the business context and linking technical risks to business risks. Why is this important?
e. Explain the core properties of the Biba and Bell LaPadula security models. How are they different?
f. What is a buffer overflow vulnerability? How do you test for buffer overflows?

Problem 2 – (30 points)

A university is testing a new system for managing exams digitally. The system allows the exam tasks to be distributes to a dedicated set of computers that the students can use to answer and upload their exam. The computers are set up so they can only communicate with the server of the exam management system. No other communication is allowed. All communication with the exam management server is encrypted. The system is based on web-technology and set up with single sign-on so that the students are using their ordinary username and password issued by the university to log on to the system.

Your task is to perform a security analysis of the model, by using three different types of threat modeling: data flow diagrams, attack trees and misuse cases. For each of the threat models you create, explain the pros and cons of this type of threat model.

Problem 3 – (20 points)

For each of the code snippets listen below, your task is to:

- Identify the security vulnerability.
- Explain why this is a security issue.
- Fix the code. You may use pseudo-code for this. Remember to explain your solution.

Code snippet 1

```
<?php
$email = "abc123@sdsd.com";
$regex = '/^[_a-z0-9-]+(\.[_a-z0-9-]+)*@[a-z0-9-]+(\.[a-z0-9-]+)*(\.[a-z]{2,3})$/';
if (preg_match($regex, $email)) {
echo $email . " is a valid email. We can accept it.";
} else {
echo $email . " is an invalid email. Please try again.";
}
?>
```

Code snippet 2

```
try {
openDbConnection();
}
catch (Exception $e) {
echo 'Caught exception: ', $e->getMessage(), '\n';
echo 'Check credentials in config file at: ', $Mysql_config_location, '\n';
}
```

Code snippet 3

```
$id = $_COOKIE["mid"];
mysql_query("SELECT MessageID, Subject FROM messages WHERE MessageID = '$id'");
```

Code snippet 4

```
<?php
$newEmail = filter_input(INPUT_POST, 'email', FILTER_SANITIZE_EMAIL);
$pdoStatement = $pdoDb->prepare('UPDATE user SET email=:email WHERE ID=:id');
$pdoStatement->execute(array(':email'=>$newEmail, ':id'=>$_SESSION['userId']));
```

Problem 4 – (20 points)

The Risk Management Framework enables you to manage risks in the Software Development Lifecycle (SDL). The output of the RMF depends on where you are in the SDL.
You have been given the task of performing a security review of an existing system for ordering movie tickets. The system allows the users to see information about upcoming movies, see the schedule for the week, book and pay for tickets. Issued tickets are sent to the customer's e-mail address.

The RMF has been used by the team developing this system, so you are lucky. You have a lot of information to base your review on. Below is an excerpt of a spreadsheet that summarizes identified business risks, corresponding technical risks, and implemented mitigation techniques.

	Probability	Consequence	Risk	Mitigation (requirements)
BR1: System unavailable				
TR1: DDoS				
TR1.1: Botnet attack	M	H	H	System shall be able to handle 100 000 reuests per second.
TR2: System crash				
TR2.1: Server hacked	L	H	M	All servers included in the system shall always be up-to-date
BR2: Payment card data stolen				
TR1:System hacked				
TR1.1: SQL-injection to dump data	L	M	M	Input validation shall be performed all on information that is used to communicate with database.
TR1.2: Utilize vulnerability in database server	L	H	M	All servers included in the system shall always be up-to-date
TR1.3: Utilize default account on database server	L	H	M	All servers included in the system shall be properly hardened.
TR2: Insider access to database				
TR2.1: Operations engineer misuse	H	H	H	Only allow personal users for traceability. Review logs
TR2.2: Application admin misuse	M	M	M	Only allow personal users for traceability. Review logs periodically. Extracting data shall be a two-step process

To perform the security review, your first action is to test if the mitigation techniques are in place and works as intended. Using the RMF-excerpt above, your task is to create a risk-based test plan to use in your review.