University of Glasgow

Thursday 3 May 2018
2.00 pm – 4.00 pm
(Duration: 2 hours)

DEGREES OF MSc, MSci, MEng, BEng, BSc,MA and MA (Social Sciences)

Cyber Security Fundamentals (M)

(Answer All Questions)

This examination paper is worth a total of 60 marks

The use of a calculator is not permitted in this examination

INSTRUCTIONS TO INVIGILATORS

Please collect all exam question papers and exam answer scripts and retain for school to collect. Candidates must not remove exam question papers.

1. (a) Describe how the RSA public key system is able to provide both security and authentication.

[2]

(b) Describe the man-in-the-middle attack on a public key system, explaining the privileges an attacker would need to carry it out.

[2]

(c) Explain how a public key certificate system can prevent a man-in-the-middle attack. What details must a certificate contain? How can public key certificates be attacked?

[3]

(d) A university has decided to record attendance at classes by requiring all students to carry a smart student card that contains a chip. Readers at the entrance of a classroom can communicate with the chip at a range of 4 meters. Explain how you would organise this system. Describe how a smart computing science student might try to bypass the systems and how you prevent this type of attack.

[6]

(e) Explain why a robust random number generator is needed by the RSA public key system.

[2]

2. Read the following scenario:

The School of Informatics at Faber College have recently migrated their entire Desktop IT infrastructure to using ChromeBooks and Google's Accounts infrastructure. Upon joining the School staff are provisioned with a ChromeBook and a Staff Google Account. For compute needs the School also provides a private cloud infrastructure that provisions staff with a publically accessible (via SSH) hosted Virtual Machine images that run Debian Stable. These images are provisioned after the staff member has joined the department. Staff are expected to self administer the machines. When staff leave their user accounts and virtual machines are disabled in the week after their last day by the School's System Team. ChromeBooks are handed in on their last day of work.

(a) Identify four technical assets from the above scenario, and four non-technical assets.

[4]

(b) Select one non-technical and one technical asset from the previous question. For each asset identify two distinct vulnerabilities, and two threats that utilise the identified vulnerability. Make sure you identify for each identified vulnerability its origin, and for each threat its ISO 27K threat type.

[4]

(c) For each of the four identified risks from the previous question, discuss the likelihood of the risk occurring, and the appropriate form of treatment.

[4]

(d) Select two risks from the previous question, and discuss what recommendation you would make to address the identified risk.

[2]

(e) What is Information Assurance?

[1]

3. Alex and Mark have been a team of Ethical Hackers for the last 7 years; they acquired their knowledge by a self-taught procedure and now they are thinking of opening their own security consultancy firm. They will offer different types of penetration testing for companies who wish to undergo through this process.

(a) Describe and explain what the difference is between a hacker and an ethical hacker? Are there any other known terms or types of hackers? Explain.

[2]

(b) Describe and compare different types of penetration testing that a client might ask Alex and Mark to complete, considering how much available information and access will be originally acquired.

[3]

(c) Alex and Mark will provide full penetration testing which means that they will need to have skills and tools, to complete the five steps of Penetration testing. Give a brief overview of the "five steps of Penetration testing"; for the first two steps a bit more in depth analysis will be needed including description of tools that can be used and providing examples

[10].

4. You are assigned to test the web application of a NHS surgery for vulnerabilities. The web application is written in php and uses a SQL based database backend.

(a) Take a look at the following code snippet. It is part of the login procedure. Name the vulnerability, describe the basic concept behind the vulnerability and describe how it can be exploited.

[2]

```
    $user = $_GET['user'];
    $pass = $_GET['password'];
    $query = "select * from userlist where user_name = '".$user."' and pas
sword = '".$pass."';";
```

(b) How could the above vulnerability be avoided? (You do not have to provide code)

[1]

(c) Still working on the login procedure your attention is drawn by the following code. You assume you found a Cross-Site Scripting (XSS) vulnerability. What input could you use to validate your assumption? How could it be avoided?

[2]

```
// $login_failed is a boolean variable indicating an unsuccessful login
if($login_failed){
    echo $user." not found or wrong password";
    include("login_form.html");
}
```

(d) How could an attacker use this in order to gather patient credentials? (Describe the necessary steps)

[2]

(e) Still working on the login page, you realise it is possible to try a lot of username and password combinations. What category of vulnerability might this be? How could a malicious attacker use it and how can you fix it?

[2]

(f) You progress to the internal area for patients. It provides the possibility to arrange appointments online and free appointments for a provided period of time, which are shown in a list. After clicking around your attention is drawn to the URL `http://www.bestsurgery.co.uk/internal/appointment.php?free&from=22012018&till=250118`. You replace the till variable as follows `till=25012018 and (SELECT 1 FROM users) = 1`, which results in an error message. What vulnerability is indicated by this? Describe the basic concept behind it.

[3]

(g) After further testing you manage to find a table named “patients”. You remember the “UNION SELECT” statement and this enables you to display the contents of the “patients” table. This table includes information like patients name, age, address, reoccurring prescription, national insurance number and the full patients health record. What kind of flaw/vulnerability have you found (besides injection)? What is the possible impact for the surgery and/or for the patient (name 3 total)?

[3]