RMIT Computer Science

Security in Computing and Information Technology (COSC2536/2537)

Assignment, Semester 2, 2017

Aims

- To learn how to stay up-to-date with security threats
- To illustrate a practical aspect of security, such as vulnerabilities, threats and attack techniques, incident analysis.
- To familiarise students with some basic security infrastructure, such as software vulnerability and virus databases
- To illustrate the process of encrypting with mechanical devices
- To understand the efficacy of different security mechanisms

Method

This assignment will be attempted by students individually.

Time frame

Time allocated for this assignment: 5 calendar weeks

Due date: Week 12 (Thursday, 12 October, 11:55pm)

Special Consideration

Any extension request must be submitted via Special Consideration (https://www.rmit.edu.au/students/student-essentials/assessment-and-exams/assessment/special-consideration)

Submission

What to submit

- You should submit one file in PDF format, and it should be named *S< Your Student Number >.pdf* (replace <Your Student Number> with your own student number). **Files in any format other than PDF will not be marked.**
- For your answers, you should use the template specified at http://titan.csit.rmit.edu.au/~e51577/SIC/Assign/SICReportTemplate-2017-s2.docx
- You should start each question (1.1, 1.2.1 etc.) on a new page.

Submission method

- Submission is via *Blackboard*. If you are not familiar with submitting assignments via Blackboard, please visit

  http://goo.gl/YEo4U5 or

  https://en-us.help.blackboard.com/Learn/9.1_Older_Versions/9.1_SP_10_and_SP_11/Student/060_Tests_and_Assignments/Submitting_Assignments

Marking

This assignment contributes 35% towards your final mark in the course, and will be marked out of 100.

Students are reminded that cheating, whether by fabrication, falsification of data, or plagiarism, is an offence subject to University disciplinary procedures. In particular, students should acknowledge any material that is not their own work and is submitted as part of an assignment.

Students should be aware of their rights and responsibilities regarding the use of copyright material. If you need help referencing, have a look at RMIT's Referencing Guide.

Part 1

Vulnerabilities and Malware

Background

Your company is re-evaluating its operations. It uses a very large number of applications running on different computers. You are given the task of providing information about vulnerabilities in applications so that IT management can consider which applications should be disabled, disconnected from the network or restricted to special workstations in order to reduce the possibility of attacks.

Your manager thinks the company relies on outdated protection and wants an update on recent malware, and asks you to recommend a new antivirus program for the Windows desktop machines. You need to support your proposal with facts and arguments.

Tasks

Task 1.1 CVSS *(25 marks)*

Using your skills learnt in the week 3 lab, select a recent (not older than two months) vulnerability from the National Vulnerability Database and analyse it from the following aspects:

i. Criticality level (Check Secunia, Screenshot Accepted)
ii. Impact including CVSS Score. (Screenshot Accepted)
iii. Explain the purpose of using CVSS scores. (Two valid bullet points expected.)
iv. Proposed Solution (Screenshot Accepted)
v. Indicate which of the Australian DSD Strategies (https://www.asd.gov.au/infosec/mitigationstrategies.htm) can be applied to mitigate the vulnerability. Include valid explanations for your answer. (At least two if possible, one will suffice only in rare cases.)

Ensure that you also provide a detailed description of the vulnerability.

Task 1.2 Vulnerability analysis *(20 marks)*

1.2.1 Select a recent vulnerability from an antivirus company's database, and analyse it from the same aspects as in task 1.1. (Note: No need to explain the purpose of using CVSS scores again.)

1.2.2 Select three recent, different threats from three different antivirus companies' databases. Describe for each

i. How it spreads (attack strategy)
ii. The target of malicious activity (information, resource etc)
iii. The way of hiding inside the victim's computer.

Task 1.3 Security incident analysis *(20 marks)*

From last year (2016), select a major cyberattack method that affected many victims and describe it by using kill chain analysis (week 9 lab). Describe how each step in the kill chain was executed in the attack.

Your analysis should be brief, in the range of 200-300 words, and properly indicate the source of information.

Notes

- Description of attacks methods and attack tools are described by security software vendors (Cisco, Sophos, Symantec, Trendmicro etc) in threat reports, blogs etc. They usually refer to attacks as threats, in particular when they do not identify victims. You can base your report on such a threat description, but you need to identify at least one victim.
- Automated attacks, such as virus/Tojan/worm-based attacks usually have many victims.

Guidelines

The Task 1 report should be concise, normally not longer than 900 words altogether (excluding pictures). You must start each task/subtask on a new page.

To support your arguments

- Provide screen-dumps for each question (Maximum four screen dumps per question; each screen dump must be large enough to read the text). Feel free to format the page to accommodate larger screenshots.
- Provide references (URLs) when you use information from different sources.
- For referencing help, please see the RMIT web site (http://www1.rmit.edu.au/library/referencing) .

Part 2

Symmetric and asymmetric ciphers

In this part you will practice encrypting and digitally signing documents.

Task

(15 marks)

The Enigma machine was a piece of encryption hardware used by the Germans to protect commercial, diplomatic and military communication before and during World War Two. Although it had some cryptographic weaknesses, it was procedural flaws, operator mistakes and the capture of key tables and hardware by the Allies that enabled the successful breaking of messages encrypted by Enigma machines.

For this assignment you are required to use the following Enigma Machine Simulator [http://enigma.louisedade.co.uk/enigma.html] using the parameters specified below:

```
Enigma Type: M3
Reflector Wheel (Umkehrwalze): C
Wheel Order (Walzenlage): IV III II
Ring Setting (Ringstellung): DGA
Ground Setting (Grundstellung): YPW
Plugs: AV CN FG IY WJ ME
```

The task is to encrypt the following with the Enigma emulator: your family name followed by ten letters of 'L'.

In your answer you must state explicitly:

- The plain text
- The three letters for the operator's machine setting (as described in the Help section of the emulator)
- The final message as described in step 9 in the Emulator Help
- The final ground setting after encryption

You have to write down your answer, a screenshot alone is not sufficient.

Part 3

Defence Mechanisms

For this task you will first practice modulo operation that is the basis for most encryption methods. A brief video about it was shown in the lecture when discussing encryption. You can also find many explanations on the web. Then you will have to answer the question that the result of the operation points to.

Task

(20 marks)

You have to calculate *xxxxxxx* mod 3 (where *xxxxxxx* is your seven-digit student number), and show the result in your report. Then, if the result is 0 you need to answer question 3.0, if the result is 1 you need to answer question 3.1 and if the result is 2 your question is 3.2.

Below is a list of security mechanisms and threats. For each security mechanism, indicate whether it is very effective, partially effective or not effective against the listed threats. Provide a brief explanation for each answer.

Question 3.0

> Security mechanisms: Packet filter, X.509 certificates , sandboxing, RAID
>
> Threats: Key loggers, spyware, CPU/resource stealing, poisoned search results, clickjacking, phishing, password cracking, statistical inference attack, ransomware.

Question 3.1

> Security mechanisms: Multifactor authentication, digital signature, same-origin policy, anomaly-based intrusion detection
>
> Threats: Key loggers, spyware, CPU/resource stealing, poisoned search results, clickjacking, phishing, password cracking, statistical inference attack, ransomware.

Question 3.2

> Security mechanisms: Proxy server, IPsec, exponential backoff, query-size restriction
>
> Threats: Key loggers, spyware, CPU/resource stealing, poisoned search results, clickjacking, phishing, password cracking, statistical inference attack, ransomware.

You should organize your answer in a table, the rows representing the threats and the columns representing the methods.

E.g.

	Mechanism 1	Mechanism 2	Mechanism 3	Mechanism 4
Threat 1	Not effective, because …	Very effective, because it can eliminate the threat by …	Partially effective, as it can address … but cannot address …	Very effective, because …

The End