This question paper consists of 4 printed pages, each of which is identified by the Code Number COMP391101.

This is an open book examination. Any written or printed material is permitted.

School of Computing

January 2019

COMP3911

Secure Computing

Answer all three questions

Time allowed: 2 hours

TURN OVER FOR QUESTIONS

Question 1

This question concerns a hypothetical new social media site, Witter.

(a) Witter's marketing material boasts that "our unique symmetric encryption algorithms, designed specially by our programmers, use uncrackable 128-bit keys to protect your valuable content!"

Discuss the merits of the claims made in this quote. **[4 marks]**

(b) Witter's server has been implemented in Java. A security analyst performing a source code review comes across the following lines of code, intended to create the 128-bit encryption key:

```
Random rng = new Random(seed);
byte[] key = new byte[16];
rng.nextBytes(key);
```

The class `Random` is part of the standard Java API and "uses a 48-bit seed, which is modified using a linear congruential formula", according to the documentation. This documentation also notes that the `nextBytes` method of the class fills the provided array with random bytes.

Discuss the suitability of this code for key generation, stating any assumptions you have made about other code not shown here. **[4 marks]**

(c) Witter's 'specially designed' symmetric cipher uses 64-bit blocks. An analyst studying the content of an encrypted post stored on Witter's servers notices that a particular pattern of 64 bits occurs at three distinct locations in the encrypted file.

What weaknesses does this highlight in Witter's approach to protecting users' posts, and how should they be fixed? **[4 marks]**

(d) Witter suffers a data breach. One of the files stolen in the breach is named `users.csv`. The first few lines of this file are as follows:

```
USERNAME,PASSWORD
joe@foo.com,mypassword
mary@marysmith.net,friday
dave777@hotmail.com,x
```

On the basis of this evidence, identify two different problems in Witter's approach to user authentication. In each case, give a detailed explanation of a good solution to the problem. **[8 marks]**

[Question 1 total: 20 marks]

Question 2

(a) CVE-2018-14883 is a recent vulnerability in PHP's image handling—specifically, in the function `exif_thumbnail_extract`. This function extracts thumbnail image data contained within the EXIF header of an image file. The following C code is part of its implementation:

```
if ((img->Thumbnail.offset + img->Thumbnail.size) > length) {
  EXIF_ERRLOG_THUMBEOF(img);
  return;
}
```

In this code, `img` points to a C struct containing information about the image and `Thumbnail` is another struct containing details of the image's thumbnail. `Thumbnail` has a member `offset` that stores the position of the thumbnail within the image file header and a member `size` that stores how many bytes of the header are thumbnail data. Both of these members are unsigned 32-bit integers.

(i) The vulnerability report refers to a problem with the `if` statement in the code above. Explain the likely nature of this problem. Identify the conditions necessary for the problem to occur. **[5 marks]**

(ii) What are the possible consequences of this problem for a PHP application that displays thumbnails of uploaded images? **[3 marks]**

(b) A Java web application contains the following code fragment:

```
if (url.contains("../")) {
  String message = "Bad URL\n" + getServerDetails();
  throw new WebException(message);
}
```

(i) Explain carefully what the programmer is attempting to prevent here. **[3 marks]**

(ii) How could an attacker try to defeat this input validation attempt? **[3 marks]**

(iii) Even if this code performs its intended function, there is still a security issue. What is the nature of the problem? **[2 marks]**

(c) A security researcher informs a software vendor about a vulnerability and states that they have 30 days to fix the problem before the researcher publishes their findings. The vendor accuses the researcher of 'blackmailing' them. Is the vendor justified in their complaint? Explain your reasoning. **[4 marks]**

[Question 2 total: 20 marks]

Question 3

An audit of the PCs in a small company's offices identifies a machine with a piece of malware running on it. Analysis indicates that the malware has recruited the machine to be part of a botnet. Machines in this botnet can be commanded remotely by the attacker.

(a) Discuss two different ways in which the malware could have ended up on the PC. Give a plausible explanation why the malware might have been able to avoid detection by anti-virus software running on the PC. **[6 marks]**

(b) The malware shows up in process listings as a process that you would normally expect to see running on this OS. The corresponding executable file has the same name as a legitimate tool available for that OS. Given these facts, discuss two different ways in which the malware may have aroused the analyst's suspicions. **[6 marks]**

(c) The analyst suggests that providing digital signatures for all executable files on the PC would be a good way of defending against malware-based attacks. Explain briefly how this would work. In your explanation, identify the conditions necessary for this technique to protect the system successfully. **[4 marks]**

(d) Discuss how the attacker responsible for the malware might use their botnet to conduct a DDoS attack on a victim. Include in your discussion an explanation of why firewalls on the company's network or the malware-infected PC itself might be unable to prevent the PC from being commanded to participate in the DDoS. **[4 marks]**

[Question 3 total: 20 marks]

[Grand total: 60 marks]

END