No calculator allowed in this examination

UNIVERSITY OF BIRMINGHAM

School of Computer Science

Introduction to Computer Security

Exam including model answers!

Main Summer Examinations 2019

Time allowed: 1:30

[Answer all questions]

Question 1

(a) Assume a webserver is accessible only via TLS with Forward Secrecy. The operator of the webserver wants to enable a webfilter which checks all incoming traffic to the webserver for malware before it reaches the webserver.

(i) Why is this not possible if the webfilter only gets the private key of the webserver and a feed of the incoming traffic? **[4 marks]**

(ii) Which changes are necessary to make these checks possible? Justify your answer. **[4 marks]**

(b) Assume a webserver uses AES in counter mode. Furthermore assume the attacker has managed to install malware on the webserver which sets the nonce used in the counter mode to a value specified by the attacker. If the malware can in addition cause the webserver to encrypt data of the attacker's choice, can the attacker decrypt all traffic to the website? Justify your answer. **[7 marks]**

Model answer / LOs / Creativity:

(a) (i) Because of forward secrecy, passive attacks (like this) do not work.

(ii) The traffic needs to be decrypted first and then sent to the webfilter, or the session keys need to be sent to the webfilter as well. Either of these solutions is fine.

(b) Always use the same nonce for all encryptions and decryptions, and ask for the encryption of a long sequences of 0's with this nonce. Now you can xor all encrypted traffic with this data.

Question 2

(a) Is it safe to replace nonces by timestamps in a security protocol? Justify your answer. **[5 marks]**

(b) Consider the following protocol:

$$\begin{array}{rcl} A & \rightarrow & B : N_A, B \\ B & \rightarrow & A : E_A(N_A), E_A(Sign_B(\text{Pay Elvis } £5), \text{Pay Elvis } £5) \end{array}$$

Assume different protocol runs produce different payment messages. Is this protocol secure? If yes, explain why. If not, give an attack in Alice-Bob notation. **[5 marks]**

(c) Consider the following protocol:

$$\begin{array}{rcl} A & \rightarrow & B : E_B(N_A, A) \\ B & \rightarrow & A : E_A(N_B, B) \\ A & \rightarrow & B : E_B(N_B) \end{array}$$

where N_A and N_B are nonces, and $\#(N_A, N_B)$ is a symmetric key based on the hash of N_A and N_B. By giving an attack in Alice-Bob notation, show that this protocol does not satisfy key agreement. **[5 marks]**

Model answer / LOs / Creativity:

(a) In general no. As an example, if in the Needham-Schroder protocol the nonces are replaced by timestamps, the key is guessable.

(b) Because there are two separate encryptions in the second message, a replay attack will work. A trace is given below, where Pay_E is the message

$$E_A(Sign_B(\text{Pay Elvis } £5), \text{Pay Elvis } £5)$$

and Pay_C is the message

$$E_A(Sign_B(\text{Pay Charlie } £5), \text{Pay Charlie } £5)$$

.

$$\begin{array}{rcl} A & \rightarrow & B : N_A, B \\ B & \rightarrow & E(A) : E_A(N_A), Pay_E \\ E(B) & \rightarrow & A : E_A(N_A), Pay_C \end{array} \qquad \begin{array}{rcl} A & \rightarrow & B : N'_A, B \\ B & \rightarrow & E(A) : E_A(N'_A), Pay_C \\ E(B) & \rightarrow & A : E_A(N'_A), Pay_C \end{array}$$

(c) This is the Needham-Schroder protocol without the nonce N_A in the second message, which is vulnerable to an attack when there are two runs of this protocol and the

attacker exchanges the messages $E_A(N_B)$ and $E_A(N'_B)$ which Alice cannot detect, as N_A is not part of this message. A trace for the two sessions is given below:

$$\begin{array}{rcl} A & \rightarrow & B : E_B(N_A, A) \\ B & \rightarrow & E(A) : E_B(N_B) \\ E(B) & \rightarrow & A : E_B(N'_B) \end{array} \qquad \begin{array}{rcl} A & \rightarrow & B : E_B(N'_A, A) \\ B & \rightarrow & E(A) : E_B(N'_B) \\ E(B) & \rightarrow & A : E_B(N_B) \end{array}$$

Now A calculates the two keys as $\#(N_A, N'_B)$ and $\#(N'_A, N_B)$, whereas B calculates the two keys as $\#(N_A, N_B)$ and $\#(N'_A, N'_B)$.

Question 3

(a) Browsers allow access to cookies only if the domain of the cookie is the same as the domain for the website. Describe an attack which is prevented by this restriction. **[4 marks]**

(b) A website uses https for authentication but the link to the general conditions of use on the same domain uses only http. How could an attacker get access to this website without authentication? **[4 marks]**

(c) Consider the following php-code running on a web server:

```
1  <?php
2  $filename = $_REQUEST["filename"];
3  $command = "ls -l /var/www/img/" . "$filename";
4
5  system("$command". $result);
6  if ($res <> 0) {
7      echo File "$filename" already uploaded;
8  }
9  else {
10     mysqli_multi_query($con,"INSERT INTO pictures (username, filename)
11                 VALUES (" . get_current_user() ", " . "$filename)");
12 }
13 ?>
```

Describe three security weaknesses in this website, how they might be exploited and explain why these weaknesses are serious. **[9 marks]**

Model answer / LOs / Creativity:

(a) Website A could obtain session cookies for website B and use them to connect directly to website B.

(b) The cookies are automatically sent to the website, hence packet sniffing on the unencrypted connection will give the session cookie to the attacker.

(c) The weaknesses are arbitrary command execution, cross-site scripting attacks and SQL injection. Arbitrary command execution give you control over the server, the SQL injection gives you access to the underlying database, and the cross site scripting makes it possible to execute javascript provided by the attacker on the browser of the client, thereby possibly granting remote attackers access to the current session by stealing the session cookies.