UNIVERSITY OF EDINBURGH

COLLEGE OF SCIENCE AND ENGINEERING

SCHOOL OF INFORMATICS

INFR10067 COMPUTER SECURITY

Friday 10th May 2019

09:30 to 11:30

INSTRUCTIONS TO CANDIDATES

Answer any TWO of the three questions. If more than two questions are answered, only QUESTION 1 and QUESTION 2 will be marked.

All questions carry equal weight.

CALCULATORS MAY NOT BE USED IN THIS EXAMINATION

Year 3 Courses

Convener: C. Stirling
External Examiners: S.Rogers, S. Kalvala, H.Vandierendonck

THIS EXAMINATION WILL BE MARKED ANONYMOUSLY

1. (a) Alice’s computer has the below firewall policy. Read it and use it to answer the following questions.

```
# Alice’s computer
# Generated by iptables-save v1.6.0
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p udp -m udp --dport 6666 -j DROP
-A INPUT -p udp -m udp --dport 6666 -j ACCEPT
-A INPUT -p tcp -m tcp -s 192.168.1.0/24 --dport 443 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -j DROP

-A OUTPUT -m conntrack -ctstate RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -j DROP
COMMIT
```

i. If Eve (192.168.1.16) were to run a port scan on Alice’s computer using nmap what ports would she see as open? List the numbers of the open ports and explain your reasoning. [*4 marks*]

ii. Imagine Alice were to use her computer to access the Computer Security class website. You use Wireshark and limit the collection of packets to those coming from Alice’s computer headed for ports 80 or 443. In 1-2 sentences, describe the traffic you would expect to see coming from Alice’s computer. You can assume that no other computers are communicating with Alice at the time. [*3 marks*]

iii. There are several different types of firewalls that operate at different layers of the OSI network stack. Name the type of firewall shown above and explain how you know it is of that type. [*3 marks*]

iv. Imagine that Eve decides she really does not like Alice having an internal website on port 443. She decides to launch a SYN Flood attack against Alice. The SYN Flood described here has some disadvantages for Eve. Name one of the problems with this attack and suggest a better approach Eve could use. [*3 marks*]

QUESTION CONTINUES ON NEXT PAGE

(b) For each of the following, assume that the user is correctly using Tor on their computer.

i. Bob logs into a website which uses HTTP, but not HTTPS. Can he be absolutely certain that his password will be safe in transit? Explain. [*2 marks*]

ii. Bob connects his laptop to a local coffee shop's free WIFI. There have been some past reports of the shop recording website traffic and selling it. Is Bob's browsing data safe from the coffee shop? [*2 marks*]

(c) Eve discovers a company website where she can log in using the username "admin" and the password "admin". She uses this information to log onto the website and take a large amount of personal customer data.

i. How could this attack have been prevented. [*2 marks*]

ii. There are three types of authentication which start: "Something you..." Which type of authentication did Eve use? [*1 mark*]

iii. The website administrator would like to add an invisible second authentication mechanism to the website in addition to the password to further improve security. Describe how such an approach might be implemented on the site. [*3 marks*]

iv. There are five properties of security. Name one property which was violated in this attack and describe how it was violated. [*2 marks*]

2. **RSA signatures**

In class we discussed the RSA Signature Scheme. I briefly remind you the details of this cryptoscheme here:

- **Key generation -** Bob generates two large random primes p and q, and computes $n = pq$. He then picks a number v that is relatively prime to $\phi(n)$, and computes s such that $s \cdot v = 1 \mod \phi(n)$. From this point on, he can "throw away" the values p, q, and $\phi(n)$. They are no longer needed. Bob's public verification key is $vk_B := (v, n)$. His private signing key is $sk_B := s$. He keeps sk_B secret, but publishes vk_B to allow others to verify signatures he has issued under his signing key.
- **Signing algorithm -** Bob can sign a message m under his signing key sk_B as follows:

$$\mathsf{Sign}(sk_B, m) := (m, (\mathsf{h}(m))^s \mod n)$$

  where h is a secure cryptographic hash function.
- **Verification algorithm -** Given Bob's verification key vk_B, Alice can verify if a signature (m, σ) is a valid signature from Bob by testing if $h(m) = \sigma^v \mod n$. That is,

$$\mathsf{Verif}(vk_B, m, \sigma) = \begin{cases} \mathsf{True} & \text{if } h(m) = \sigma^v \mod n \\ \mathsf{False} & \text{otherwise} \end{cases}$$

The goal of this exercise is to explore why is hashing the message necessary for computing an RSA signature. We will consider the simplified RSA signature scheme which skips the hashing of message m and just uses m directly. So now to sign a message Bob just computes $\sigma := m^s \mod n$ and sends (m, σ) to Alice.

(a) What is the verification algorithm for the simplified RSA signatures? In other words, what equation should Alice check, to confirm whether (m, σ) is a valid signature from Bob? *[2 marks]*

(b) Mallory knows that Alice and Bob are both using the simplified RSA signature scheme, and wants to trick Alice. Assume that Mallory has captured over the network two signed messages from Bob (m_1, σ_1) and (m_2, σ_2). How (using these two messages) is Mallory able to forge a valid signature under Bob's signing key, of a message different than m_1 and m_2? Justify your answer. *[3 marks]*

QUESTION CONTINUES ON NEXT PAGE

(c) Alice and Bob are still using the simplified RSA scheme, but suppose now that Mallory has not previously seen any valid signature issued by Bob. Explain how only knowing Bob's verification key vk_B, Mallory is still able to forge a valid signature under Bob's signing key. In other words Mallory can find m and σ such that $\mathsf{Verif}(vk_B, m, \sigma) = \mathsf{True}$. Justify your answer. [Hint: m and σ can be chosen freely.] [*8 marks*]

(d) For standard RSA signatures, we typically set v to a small prime value such as 3. For this question, let Bob's signing key be $sk_B = 3$.

Charlie is holding an auction. The protocol is simple. Bidders just submit signed bids (using the simplified RSA signature scheme) to Charlie. The message m is their bid (in pounds). Charlie will accept the highest bid and will expect that person to pay the amount they bid. Mallory wants to mess with Bob's bidding. So, when Bob forms his bid m and sends to Charlie his signed bid (m, σ) where $\sigma = m^s \mod n$, Mallory intercepts it. Mallory would like to tamper with m and σ to form a new signature $(64m, \sigma')$ that corresponds to a bid for 64 times Bob's original bid. This will force Bob to win the auction and pay much more for it. More precisely, she'd like to find a value σ' such that σ' is a valid signature on $64m$, so she can replace (m, σ) with $(64m, \sigma')$ and forward the result onto Charlie. Help Mallory out: explain to Mallory how she can compute such a σ'. You will assume that m is small enough so that $64m < n$, so that $64m$ does not wrap around modulo n. Justify your answer. [*6 marks*]

(e) Are your attacks from questions 2b, 2c and 2d possible against the real RSA signature scheme (the one that includes the cryptographic hash function)? Explain your answer. [*6 marks*]

3. **Web security**

Answer each question, and do not forget to justify or explain your answer.

(a) Consider this piece of pseudo PHP code

```
$query = "SELECT name FROM users WHERE uid = $UID";
// Then execute the query
```

where $UID represents a URL parameter named UID supplied in the `HTTP GET` request.

i. There is a security issue with this code. Explain what it is and how you would exploit it to delete all tables in the database. [*3 marks*]

ii. How does blacklisting work as a defence? What are some difficulties with blacklisting? [*2 marks*]

iii. What is the best way to fix the security issue from question 3(a)i? Justify your answer. [*2 marks*]

(b) Is setting the `Secure` flag on a cookie enough to defend from all CSRF attacks? Justify your answer. [*3 marks*]

(c) Is setting the `Secure` flag on a cookie enough to defend against all XSS cookie-stealing? Justify your answer. [*3 marks*]

(d) Is setting the `HTTPOnly` flag on a cookie enough to defend against all XSS cookie-stealing? Justify your answer. [*3 marks*]

(e) Is switching all application requests to `HTTP Post` enough to stop all CSRF attacks? Justify your answer. [*3 marks*]

(f) Is the Same Origin Policy enough to prevents all XSS attacks? Justify your answer. [*3 marks*]

(g) Can two Javascript scripts embedded in pages running in two different tabs on a user's browser access the resources (such as cookies) of each other? Justify your answer. [*3 marks*]