UNIVERSITY OF EDINBURGH

COLLEGE OF SCIENCE AND ENGINEERING

SCHOOL OF INFORMATICS

INFR10067 COMPUTER SECURITY

Monday 2nd May 2022

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.

This is an OPEN BOOK examination.

Year 3 Courses

Convener: D.Armstrong
External Examiners: J.Bowles, A. Pocklington, H.Vandierendonck

THIS EXAMINATION WILL BE MARKED ANONYMOUSLY

1. (a) 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, but not identify them with certainty. As long as at least two of the cryptographers are honest and do not collude with any other then this is secure. For this question, we add one more party for 4DC (A, B, C, and D) in this protocol. 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:0, D:1.

   The completion of the protocol yields a result of 1.

   i) Using the information given in this question, is it possible to work out who paid for the meal; was it A, B, C, D, or the NSA? Show your work. [*4 marks*]

   ii) Consider now that we change the protocol. Instead of each party flipping coins with every other party at the table, they now only flip coins with their neighbours on either side of them. Is 4DC still secure, using the same assumption as before that at least two non-colluding cryptographers are present? Explain your reasoning for your answer. [*6 marks*]

   (b) Tor is useful as a tool to allow users to anonymously communicate with each other and with online services.

   i) Explain how it allows users in regions with censorship to connect to censored websites hosted outside the region. Assume that the adversary is external to the communication channel (i.e. not one of the end-points) and observing the network but is not able to manipulate any traffic. [*3 marks*]

   ii) Imagine that two users are communicating over Tor from within the same region where an adversary has complete observability of network traffic. Are these users linkable? Explain your reasoning with details of how. Recall what kind of adversary Tor is secure against and what kind of adversary it is not secure against. [*6 marks*]

   (c) Distributed denial of service (DDoS) attacks often use the bandwidth of unsuspecting computers on the Internet to drive traffic to victim machines on the Internet. Imagine you are such an adversary and want to deploy a DDoS attack against some victim machine.

   i) Explain how and why you would use network broadcast addresses in your attack. [*3 marks*]

   ii) Explain how and why you would use address spoofing for your attack. [*3 marks*]

2. **TLS protocol.** In class, we discussed the Diffie-Hellman TLS (DH-TLS) handshake protocol, that we briefly recall here:

   (1) The handshake starts with client C sending to server S a random 256-bits nonce N_C, and the list of supported cipher suits.

   (2) S selects one of the cipher suit Algs in the list and sends it to C along a server-chosen random 256-bit nonce N_S.

   (3) S then sends its digital certificate $Cert_S$. Remember, the certificate contains the server name, the trusted certificate authority (CA) that issued it, and the server's public verification key vk_S. The certificate is signed under CA's signing key.

   (4) S sends the DH parameters g and p and its contribution to the DH key signed under its signing key sk_S.

   (5) C checks the validity of the certificate (chain) before proceeding (recall that CA's verification key is installed on the client's browser). The client replies with it contribution to the DH key.

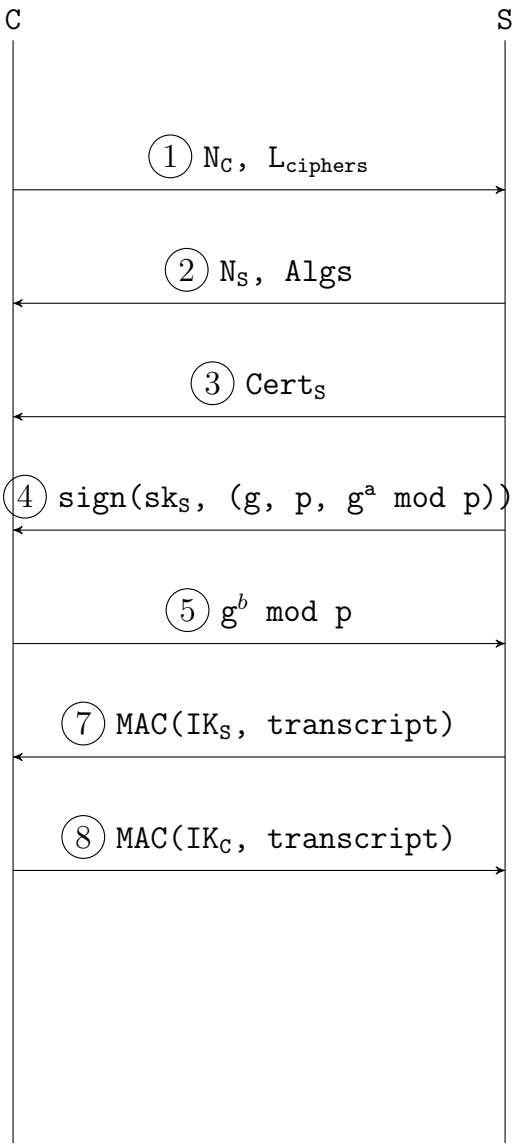
   (6) Both parties use g^{ab} mod p, N_C, and N_S to generate unique encryption and integrity keys for subsequent data exchange:

   $$(CK_C, CK_S, IK_C, IK_S) \leftarrow \text{HKDF}(g^{ab} \bmod p, N_C, N_S)$$

   (7) S sends the MAC of the transcript of the above dialogue (messages sent in steps 1-5).

   (8) C checks the received MAC. If it fails to verify then C aborts the session, otherwise C sends a MAC over the transcript of the above dialogue (messages sent in steps 1-6).

   (9) The session is now established.



   (a) Can a passive adversary that has managed to steal the server's TLS private signing key decrypt intercepted subsequent communications? If yes describe the attack,

otherwise explain your answer. [*2 marks*]

(b) Can an active adversary that has managed to steal the server's TLS private signing key decrypt intercepted subsequent communications? If yes describe the attack, otherwise explain your answer. [*2 marks*]

(c) Does TLS protect against censorship whereby the Censor tries to identify and prevent connections to specific websites and only these connections? Explain your answer. [*2 marks*]

(d) Can a certificate authority that issues a TLS certificate for `acmeebook.com` decrypt TLS traffic to `acmebook.com`? Explain your answer. [*2 marks*]

(e) It is common for companies to deploy TLS decrypting proxies in an effort to better protect their assets from attacks. TLS decrypting proxies are devices that act as man-in-the-middle (MitM) to decrypt encrypted TLS traffic travelling across WAN. This requires the administrator `A` to generate a signing and verification key, and install a self-signed root certificate for that verification key on all employees' computers. Now, all employees' browsers will trust any certificate signed with `A`'s signing key. Explain how the administrator can now decrypt all HTTPS connections established by any of the employees' browser, to an external HTTPS website. Explain this man-in-the-middle attack at each step of the protocol. [*6 marks*]

(f) Assume that a company uses a TLS decrypting proxy and one of its employees connects to `acmebook.com`. Can Acmebook's server detect this attack? Explain your answer. [*3 marks*]

(g) Assume that a company uses a TLS decrypting proxy and one of its employees connects to `acmebook.com`. Can the employee detect this attack? Explain your answer. [*3 marks*]

(h) In order to act as a man-in-the-middle, the TLS decrypting proxy needs to issue and sign a certificate under `A`'s signing key for the visited external domain (for example for `acmebook.com`). Imagine that the TLS decrypting proxy does not do any checks on the certificate sent by `acmebook.com` server. Explain how an attacker outside the company can now mount man-in-the-middle attacks on the company's employees. Describe your attack at each step of the protocol. [*5 marks*]

3. **Memory safety.** Consider the following C code. Unfortunately whoever wrote this code had clearly fallen asleep during the lectures on memory safety!

```
 1.  int main(int argc, char **argv){
 2.      char entered_pwd[128];
 3.      char pwd[128];
 4.
 5.      strcpy(pwd,"123456");
 6.
 7.      printf("Enter password: ");
 8.      fgets(entered_pwd, sizeof(entered_pwd), stdin); // no buffer overflow !
 9.
10.     if(strcmp(entered_pwd, pwd)){
11.       printf("Incorrect password:");
12.       printf(entered_pwd);
13.     }
14.     else{
15.       printf("Correct password!");
16.     }
17. }
```

(a) What line contains a memory vulnerability? What is this vulnerability called? [*2 marks*]

(b) Explain how an attacker can exploit this vulnerability and learn the password `pwd`. Provide details including what happens in memory that allows this attack.
[**Hint:** Since the array is allocated on the stack, use `%x` and not `%s`. [*5 marks*]

(c) How would you fix this code? [*3 marks*]

(d) A friend of the sleepy programmer who was awake for the memory safety lectures tells them that instead they should enable stack canaries to make the code memory safe. Do you agree that enabling stack canaries indeed prevents this code from being exploited and leaking the password `pwd`? Explain what stack canaries are, and why you think they can or cannot thwart the attack from question 3b. [*5 marks*]

(e) What about enabling `W^X` (also known as non-executable pages, DEP, or the NX bit)? Would that thwart the attack from question 3b? Explain what is the effect of enabling `W^X`, and why you think this would or would not prevent the password `pwd` being leaked. [*5 marks*]

(f) What about enabling ASLR? Would that thwart the attack from question 3b? Explain what is the effect of enabling ASLR, and why you think this would or would not prevent the password `pwd` being leaked. [*5 marks*]