CS5321 Network Security, National University of Singapore
- Semester 2: AY2022/2023 -
Due: 11:59 PM (Singapore Time) on 3 March 2023 (Friday)

Take-home Exam 1

Answer to all of the following questions. The answers must be **typed** and uploaded in **PDF** format to "Take Home Exam 1" in Assignment on CANVAS before the deadline. (**Late submission is subject to 20% penalty.**) Make sure to include your name and Student ID number on the **FIRST** page of the PDF and name your submission file **"[ID]_[NAME].pdf"**. **Open book. No collaboration is allowed.**

Question 1 [5pt]

In Week 2 and 3, we studied Diffie–Hellman (DH) key agreement protocol and Station-to-station (STS) protocol. What is the additional security guarantee that STS protocol has, compared to DH protocol. Please explain in 2-3 sentences.

Question 2 [5pt]

In the commitment scheme discussed in Week 2, if we implement the commitment for message m (e.g., bid price for an auction) using a secure hash function H as follows instead, does it provide the same security guarantees as the one discussed in Week 2 slide? Please also explain why (in 1-2 sentences). Note that XOR is the bit-wise exclusive OR operator. Recall that r (random number) and m are kept secret until they are revealed to open the commitment.

$$C(m) = H(r\ XOR\ m)$$

Question 3 [5pt]

Let us consider the following unilateral authentication protocol between A (client) and B (server) to establish a session key K_s. A and B shares a long-term shared secret key k in advance. Both R and K_s are 128-bit long.

$$A \rightarrow B : \text{“I am A”}\ || R$$
$$B \rightarrow A : E(k, R || K_s)$$

Here, A rejects the response from B if R is not decrypted correctly. E is AES-CBC encryption using key k. Does this protocol satisfies perfect forward secrecy? Please also briefly explain why.

Question 4 [5pt]

In Week 3, we studied Kerberos authentication protocol. However, we only discussed until the session key ($K_{C,V}$) establishment between C and V. Assuming V is a printer and C wants to securely send some data to be printed (print job p). Please design a protocol using $K_{C,V}$ that offers both confidentiality and authenticity/integrity protection for p. Please also briefly justify your design.

Question 5 [10pt]

Alice takes a role of maintaining the personal information entries (say, a set of name, phone number, and mailing address) of all the registered employees (1000 employees) of a company. Let us label the identification (or ID) numbers (e.g., NRIC) as $ID_1, ID_2, \ldots, ID_{1000}$. As the data size is big, she decided to upload all data to the cloud (and delete local copy of entries) and retrieve only some entries when needed. When downloading from the cloud, Alice wants to make sure the downloaded employee's entry is authentic and not tampered after upload. Please briefly explain the mechanism using Merkle Hash Tree to realize the features described above, including the following points:

- How Alice can construct a Merkle hash tree for this dataset
- What Alice should maintain locally for later verification
- How the data authenticity can be checked. Please show example using the hash tree constructed above.

Question 6 [10pt]

Recall Needham-Schroeder protocol we studied in Week 3. Let us consider Eve, an eavesdropper who has been logging all messages sent and received by Alice. Since Eve does not know $K_{a,kdc}$, she cannot learn any useful information at this point. Later time, she is successful to somehow learn (or steal) $K_{a,kdc}$. Fortunately, shortly after that, Alice noticed that her key has been compromised and then contacted KDC to update her key to $K'_{a,kdc}$. Please answer to the following questions.

1. The key update does not completely prevent Eve from impersonating Alice against Bob. Please explain how Eve can benefit from knowledge of $K_{a,kdc}$ and recorded messages (to/from Alice) to achieve it?
2. Please discuss a possible countermeasure in 2-3 sentences.

Question 7 [10pt]

Alice and Bob share a secret key k. In order to periodically inform Bob of her up-to-date IP address so that Alice can get push message from Bob (e.g., paid subscription service). To do so, Alice sends her ID and her IP address along with timestamp for freshness checking.

$$Alice \rightarrow Bob : E\{k, \text{``}Alice\text{''} || IP\ address || timestamp\}$$

ID, IP address, and timestamp are all represented as bitstring of fixed (and known) length. For instance, each character in the ID is represented with 1 Byte, and ID has fixed 16-character size (with some padding if necessary). IP address is represented with 32 bits, and timestamp is represented as a standard Unix format (32 bits). Let us assume that AES (128-bit block size) is used for encryption.

Now Eve, who can sniff message from Alice to Bob, wants to impersonate Alice to receive future messages from Bob (by sending Eve's IP address along with Alice's ID).

1. When CBC mode encryption is used in an appropriate way, is the attack possible? Please also explain why.
2. When CTR mode encryption is used in an appropriate way, is the attack possible? Please also explain why.
3. Please discuss a possible countermeasure in 2-3 sentences.

Question 8 [10pt]

In Week 4, we have seen a recent proposal called Certificate Transparency (CT). In order for CT to be effective to counter threats related to PKI, the ecosystem is essential.

To offer better incentive for monitors, a (hypothetical) insurance company InsuredCert starts a new certificate insurance business. When issuing a legitimate certificate $Cert_{CD}$ for a domain D, a CA C purchases an insurance policy P from InsuredCert, say at the insurance premium of S$1,000. The policy P clearly states the incentives and penalties regarding any misissued certificates. i.e., any certificate for D issued by C that is different from $Cert_{CD}$. The policy P specifies that InsuredCert shall refund most of the insurance premium (e.g., S$900) paid by C, if no misissued certificates are detected for a stated period of time, say 1 year. If any misissued certificates are found in CT and reported by any monitor during this period, InsuredCert shall pay $1500 as a reward to the monitor that first reports misisued certificate.

The rationale behind this insurance product is as follows:

- CA C is incentivized to do its best to prevent the issuance of unauthorized certificates for the domain D as it wishes to get the refund.
- Domain owner of D would likely choose CA C for issuing new certificates over other CAs because C is incentivized to protect its certificate signing key (to prevent misissuance). Other CAs with no such insurance may loose their signing keys and result in misissued certificates without any economic loss, albeit some damage to their reputation.
- Third party monitors are economically incentivized to actively monitor CT and report any misissued certificate to InsuredCert before others do so.

For the purpose of this exam, we assume that InsuredCert is trustworthy. This insurance policy, however, has a security concern. Describe one security concern when C itself is malicious. (Hint: show an attack that allows C to intentionally "misissue" a certificate without monetary penalty.)

Question 9 [15pt]

Guessing or knowing the initial TCP sequence number (ISN) that a server will choose enables an attacker to establish a TCP connection.

Please discuss if the following solutions are secure (to prevent hijacking etc.) against off-path attackers and why. $[x]_{32}$ denotes truncation of x to the 32 least significant bits. K is a (permanent) secret key stored locally and only known to the server. H represents a secure hash function (e.g., SHA256) and its algorithm is publicly known. Also note that || means concatenation and current timestamp is represented as UNIX timestamp.

(1) Server selects ISN as $ISN = [\mathrm{H(K)}]_{32}$.

(2) Server computes ISN as follows: $ISN =$ [H(source IP address XOR destination IP address XOR current timestamp XOR K)]$_{32}$.

(3) Server computes ISN as $ISN =$ [H(source IP address || destination IP address || source port number || destination port number || current timestamp)]$_{32}$.

(4) Server selects ISN using a standard (i.e., publicly-known) pseudo random generator with K as a seed.

(5) Server selects ISN as $ISN =$ [AES_ECB(K, counter)]$_{32}$, where the counter is continuous from the previous communication session.

Question 10 [15pt]

Recall that AIP enables a secure shut-off protocol to counter against Denial-of-Service (DoS) attacks, wherein the victim can send a shut-off message to the attacker to have him stop sending packets. The format of the shut-off message that a victim can send to the source is: Victim's public key, Hash of packet received from the source, and TTL, which are all signed with Victim's private key.

Assume that AIP has been deployed worldwide in a way described in the lecture. In this scenario, are the following DoS attacks possible? Please also justify your answer.

(a) Consider an attacker M who is on the path of the connection between A and B, and wants to disrupt their communication.

1. M sends a shut-off message to B, by impersonating A, to prevent B from sending legitimate traffic to A.
2. M eavesdrops a packet from B to A, and then sends the same packet to A, by impersonating B, large enough number of times until A sends a shut-off message to B, then preventing B from sending legitimate traffic to A.

(b) Next, let us consider an attacker M who wants to launch a DoS attack against a server S.

1. M launches a DDoS by instructing a number of bots to send sufficient number of fake shut-off messages to S such that S is fully occupied for validating the large number of shut-off messages.

2. M creates a number of fake EIDs and launches a DoS on S using each of them.
3. M colludes with another attacker M' such that they share a link between them which S uses to connect to the Internet. Both of them then congest that link, thus disconnecting S from the Internet.

Question 11 [10pt]

An NUS researcher has decided to deploy an SSH honeypot to collect threat intelligence (regarding scanning and attack against NUS network). The honeypot is implemented with Cowrie, an widely-used open-source honeypot, and deployed with an unused public IP address that belongs to NUS network. However, after a few days, the researcher found that the honeypot was not attracting much traffic. Please discuss up to 3 potential ways (in bullet list) to attract more access attempts. Please also briefly explain why it helps (in 1-2 sentences for each).