Comp5631: Cryptography and Security
2024 Spring – Written Assignment Number 4
Sample Solutions

Q1. A distributed system has a service-ticket server S whose duty is to issue service tickets to clients and a certificate authority (CA) who issues a digital certificate to each party in the distributed system. Assume that the following hold:

- Each party's digital certificate containing the RSA public key is available in a public directory of the CA's server.
- Each party's ID is available in a public directory of the CA's server.
- A hash function h is in the public domain and fixed in the system.
- The RSA public key cipher is computationally secure.
- The hash function h has the one-way property and weak-collision resistance property.

The server S has just issued the following email ticket Ticket_V to a client C:

$\text{Ticket}_V := ID_S||ID_C||ID_V||\text{period validity}||D_{k_d^{(S)}}(h(ID_S||ID_C||ID_V||\text{period validity}))$

where ID_S, ID_C, ID_V are the ID of S, C and the email server V, respectively; $k_d^{(S)}$ is the RSA private key of S.

To request for the email service from V, Client C sends the following text to the email server V:

$$ID_C||ID_V||TS||\text{Ticket}_V||D_{k_d^{(C)}}(h(ID_C||ID_V||TS||\text{Ticket}_V))$$

where TS is the current time plus date and $k_d^{(C)}$ is the RSA private key of C.

Please answer the following questions:

1. What should the email server do after receiving a text from Client C? $\boxed{\text{16 marks}}$

   Answer: The email server V will carry out the following step by step:

   - Check if the first part is the ID of C or not. If the answer is no, ignore the received message. Otherwise, go to the next step.
   - Verify if the digital signature in the received text was created by Client C or not with the public key of C. If the answer is no, reject the request for email service. Otherwise, go to the next step.
   - Check if the TS is about the current time and date. If the answer is no, the text is viewed as a replayed earlier message and the server V rejects the request for email service. Otherwise, go to the next step.
   - Check if the ID_V is in the second field or not. If the answer is no, reject the request for email service. Otherwise, go to the next step.
   - Verify if the Ticket_V was issued by S or not. Specifically, the email server verifies if the signature in the Ticket_V was created by S or not with the public key of S. If the answer is no, reject the request for email service. Otherwise, go to the next step.

- Check if the first four fields in the Ticket$_V$ are consistent with the format of the ticket. If any field is not correct, reject the request for email service. Otherwise, provide the email service to C.

2. Is it hard to forge the email service ticket Ticket$_V$? Justify your answer briefly. $\boxed{\text{7 marks}}$

   Answer: Yes. Forging the email service ticket Ticket$_V$ is to forge the digital signature of S on a given message $ID_S||ID_C||ID_V||$period validity. This is computationally hard as the RSA public key cipher is assumed to be computationally secure and the hash function h is assumed to have the one-way property and weak-collision resistance property.

3. Can any modification of the email service ticket Ticket$_V$ be detected with high probability? Justify your answer briefly. $\boxed{\text{7 marks}}$

   Answer: Yes. If any part in Ticket$_V$ is modified, then the signature verification in the modified ticket will fail with high probability, as the RSA public key cipher is assumed to be computationally secure and the hash function h is assumed to have the one-way property and weak-collision resistance property.

Q2. Suppose that the PGP key policy is modified into that each PGP user is allowed to have only one pair of public key and private key. In this case, is it necessary to include the public key ID in the transmitted message? $\boxed{\text{10 marks}}$

Answer: No. This is unnecessary.

Q3. Suppose you and I have just bought our workstations and just installed an IPSec software into our workstations. Assume our IPSec softwares use IKEv2 for key management. Please answer the following questions. You should use the format on Slide No. 19 of Lecture 20 without using "[]".

- Now it is the first time that our IPSec modules run IKEv2. What are the formats of the two messages in Phase 2? $\boxed{\text{5 marks}}$

  Answer: They are

  ```
  HDR, SK{Ni}  -->
  ```

  and

  ```
  <-- HDR, SK{Nr}
  ```

  The two nonces exchanged and the key SK_d will then be used to compute KEYMAT, which will be cut into pieces as AH/ESP keys. IPSec algorithms and traffic selectors were already negotiated in Phase 1.2.

  Grading guideline: If a student's answer is different, please give 1.5 mark.

- One week later suppose the current pair of IPSec SAs expires but the lifetime of IKE SAs is valid. The IPSec modules would like to negotiate new IPSec SA keys without stronger PFS, but would keep the current IPSec algorithms and the current traffic selectors TSi and TSr. To this end, they need to exchange the two messages in Phase 2. What are the formats of the two messages in Phase 2 in this case? $\boxed{\text{5 marks}}$

  Answer: They are

  ```
  HDR, SK{N, Ni}  -->
  ```

and

```
<-- HDR, SK{Nr}
```

This is re-keying.
Grading guideline: If a student's answer is different, please give 1.5 mark.

- One week later suppose the current pair of IPSec SAs expires but the lifetime of IKE SAs is valid. The IPSec modules would like to negotiate new IPSec SA keys with stronger PFS, but would keep the current IPSec algorithms and the current traffic selectors TSi and TSr. To this end, they need to exchange the two messages in Phase 2. What are the formats of the two messages in Phase 2 in this case? $\boxed{\text{5 marks}}$
  Answer: They are

  ```
  HDR, SK{N, Ni, KEi}  -->
  ```

  and

  ```
  <-- HDR, SK{Nr, KEr}
  ```

  This is re-keying.
  Grading guideline: If a student's answer is different, please give 1.5 mark.

- One week later suppose the current pair of IPSec SAs expires but the lifetime of IKE SAs is valid. The IPSec modules would like to negotiate new IPSec SA keys without stronger PFS and new IPSec algorithms, but would keep the current traffic selectors TSi and TSr. To this end, they need to exchange the two messages in Phase 2. What are the formats of the two messages in Phase 2 in this case? $\boxed{\text{5 marks}}$
  Answer: They are

  ```
  HDR, SK{N, SAi, Ni}  -->
  ```

  and

  ```
  <-- HDR, SK{SAr, Nr}
  ```

  Grading guideline: If a student's answer is different, please give 1.5 mark.

Q4. Explain why SSL needs an alert protocol, while IPSec does not need such a protocol? $\boxed{\text{20 marks}}$

Solution: In IPsec it is compulsory to support a specified cipher and hash function etc., while in SSL there is no such requirement. Hence, in IPSec two IPSec modules will be able to choose a cipher and one hash function supported by both parties, while this may not be true in SSL. In addition, during SSL handshaking a number of other errors may occur (e.g., server authentication may fail). This is why SSL needs an alter protocol, while IPSec does not.

Q5. I use everyday the SSH in my laptop to access my Unix account. The client authentication is password-based. Assume that I used the SSH in my laptop to connect my Unix account two times yesterday and sent the Unix command "ls -a" from my laptop to the Unix server two times in the two separated SSH connections. Was the command "ls -a" encrypted using the same set of security parameters by the SSH in my laptop? Justify your answer briefly. $\boxed{\text{20 marks}}$

Solution: No. The Unix command "ls -a" is encrypted using a different secret key each time, as whenever SSH is invoked a set of new security parameters is negotiated.