Assignment 2 - Konrad Wisniewski - 10135143

Question 2: Kerberos Forward Secrecy (20 points)

**1. What are the long-term secrets in Kerberos?**

The **Client Key** () is a long-term key of client C that is derived from the user's password. It is usually hashed and salted.

The **Ticket Granting Service** **Key** () is a long-term key of the TGS that is known by Authentication Service and Ticket Granting Service.

The **Key for Service S** () is a long-term key of network service S. This service could be a something like a printer. is known to the the service S and the Ticket Granting Service. Each service has its own key.

**2. What are the short-term secrets in Kerberos?**

**():** This is a short-term session key between the Client and the Ticket Granting Service. It is created by Key distribution service and used by the Client and Ticket Granting Service.

**():** This is a short-term session key between the Client and the Service S. It is created by Ticket Granting Services and known to the Client and Ticket Granting Service.

**3. For each secret (long-term and short-term), assume that the secret is leaked to a passive adversary who has previously recorded all network traffic. What new information does this adversary learn that was not already known?**

1. **Leaked**

The adversary will be able to decrypt the communication between the Client and the authentication service. They will be able to learn since it is encrypted with .

1. **Leaked**

The adversary will be able to read the ticket for the Ticket Granting Service. This grants them all the information inside the ticket including .

1. **Leaked**

The adversary will be able to read the ticket sent from the Ticket Granting Service to access the Service S. This grants them all the information inside the ticket including .

1. **Leaked**

The adversary will be able to decrypt the communication between the Client and the Ticket Granting Service. They will be able to learn since it is encrypted with .

1. **()Leaked**

The adversary will be able to decrypt the communication between the Client and the Service he is trying to reach (ie a printer). They will learn the data that they are sharing for that particular session. This could be a confidential document that the user wants to print.

For the short term secrets, the adversary will only get data sent between the client and the service for the particular session that the short term key was used. Knowing a higher level secret reveals information about lower level secrets and knowing lets you reveal all other secrets for past sessions. This means that Kerberos does not have forward secrecy.

**4. Explain why Kerberos does not have forward secrecy. Be specific about what data**

**needs to be compromised and what the consequences of it are.**

Forward secrecy means that if all the data is recorded, past sessions are not revealed by future compromises of keys. Forward secrecy can be achieved by generating a unique session key for every user session. This means that the compromise of a single session key should not reveal any data unrelated to the data exchanged in the specific session protected by that particular key.

Kerberos is built for speed and therefore does not implement forward secrecy. Ifis leaked, all past interactions would be at risk of decryption.

From question 3, you can see that knowing reveals . If the adversary knows, he can use it to decrypt data that contains. The adversary can that use to decrypt the confidential data that the client sends the printer. Since never changes, the adversary can decrypt all data that he has recorded. This means that Kerberos does not have forward secrecy.

**5. Augment Kerberos to have forward secrecy for the actual communication between Alice and Bob. You only need to specify the message sequences for the parts of the Kerberos protocol that you change (i.e., if Alice’s communication with the TGS is unchanged then you do not need to specify it).**

Adding forward secrecy to Kerberos is as simple as integrating a Diffie Hellman key exchange during the initial communication between the user and the Authentication Server. The first two steps of Kerberos are modified while the rest stay the same.

1. Client -> Authentication Server:

2. Authentication Server -> Client:

…

[Rest of Kerberos protocol here]

Both parties now know and use it as . These two steps are repeated each time there is a new communication between the two parties. Kerberos now has forward secrecy since one leak of won't reveal all previous communications.

**Legend:**

TGS: The ticket granting service the client wants to reach

TGT: The ticket for the ticket granting service,