14:332:424 Introduction to Information and Network Security Fall 2017

Assignment 4

Due: Friday, December 8th, 11:55pm

Total: 100 points

For each of the protocols below, please answer the following questions

Question 1: What is the flaw of this protocol? How can attackers break the protocol?

Question 2: What are the possible methods to prevent the attack?

You only need to answer the above two questions for protocol 1 and 2. The maximum of 30 extra points will be given if you finish protocol 3.

<u>Protocol 1</u>: Naïve Vote Protocol (50 pts)

Step 1: $\boldsymbol{A \rightarrow S: \{V\}_{K_S}}$

The voter $\boldsymbol{A}$ encrypts his vote $\boldsymbol{V}$with the public key $\boldsymbol{K_S}$ of the vote server $\boldsymbol{S}$. The server decrypts the message with his private key and registers the vote.

<u>Protocol 2</u>: Handshake Protocol (50 pts)

Step 1: $\boldsymbol{A \rightarrow B: \{N_A\}_{K_{AB}}}$

Step 2: $\boldsymbol{B \rightarrow A: \{N_A + 1\}_{K_{AB}}}$

$\boldsymbol{A}$ generates a random number (*nonce*) $\boldsymbol{N_A}$ and sends it to $\boldsymbol{B}$ encrypted with shared key $\boldsymbol{K_{AB}}$, $\boldsymbol{B}$ decrypts the message, computes $\boldsymbol{N_A + 1}$, and returns to $\boldsymbol{A}$ the encrypted result.

Protocol 3: Simple Symmetric Key Exchange Protocol (Extra: 30pts)

Step 1: $\boldsymbol{A \rightarrow S: \{T_A, B, K_{AB}\}_{K_{AS}}}$

Step 2: $\boldsymbol{S \rightarrow B: \{T_S, A, K_{AB}\}_{K_{BS}}}$

$\boldsymbol{A}$ **chooses a session key** $\boldsymbol{K_{AB}}$ **and shares the key with** $\boldsymbol{B}$ **through a trusted server** $\boldsymbol{S}$**.** $\boldsymbol{T_A}$ **and** $\boldsymbol{T_B}$ **are timestamps given by** $\boldsymbol{A}$ **and** $\boldsymbol{S}$ **respectively.** $\boldsymbol{B}$ **will accept** $\boldsymbol{K_{AB}}$ **as fresh if it arrives in a certain window of time.**