README

May 2020

1 Introduction

We develop the Dolev-Yao attacker model. It is a formal model used to prove properties of interactive cryptographic protocols.
We develop our model base on the resource from UCSD:
`https://cseweb.ucsd.edu/classes/sp05/cse208/lec-dolevyao.html`
We are going to determine whether the different authentication protocols has potential vulnerability with Dolev-Yao attacker model.
In our model, it will have three user (sender, receiver, attacker). Sender will send different message to receiver. The receiver will get the message from sender and send back the message. Attacker will try to intercept the message from sender or receiver. What we try to prove is that attacker could intercept the message and decode it.
For the attacker, we made it could intercept all message from both sides(sender and receiver), it also could store all the message that it intercept, it also could send the intercept message and its own constructed message. And Attacker will be valid in the system and not been exposed.
For the sender, it will have public key and private key to encode its message so that it could protect its message.
For the receiver, it will have also have public key and private key to decode sender's message and encode its responds.
Then we import the NSPK protocol and try to use our Dolev-Yao attacker model to attack it and see if there is any leak. For the NSPK protocol, it will have three states:
A→B : $K_B\{N_A, A\}$
B→A : $K_A\{N_B, B\}$
A→B : $K_B\{N_B\}$
for this protocol, the N is the message and K will be the public key. We just try to see if the attacker could get the N.