Progress Report 1: Code Generation

Xie Li

September 4, 2020

Overview of the Progress

- Finish the refinement of the generated code and able to communicate once between alice and bob.
- Begin to change the implementation of the code generation module based on the implementation.

Modeling

Running Result

clexma@clexma-ThinkPad-P52s:~/Desktop/generated$ sudo ./Bob
-------------------STATE___init
-------------------STATE__Bob_State_1
Receive message
ethernet frame received
length received
id received :0
data received: h◆xr◆◆◆0◆J◆J◆v◆:◆◆◆[0◆B◆◆%◆
ethernet frame received end
endloop data:h◆xr◆◆◆0◆J◆J◆v◆:◆◆◆[0◆B◆◆%
Receive message end
decryption: bbbbbbbbbbbbbbbb
encrypted received:h◆xr◆◆◆0◆J◆J◆v◆:◆◆◆[0◆B◆◆%
DecKey: bbbbbbbbbbbbbbbb
decrypted: 0,1234,0,0,default
0,1234,0,0,default
0,1234,0,0,default
decryption end
-------------------STATE__Bob_State_2
serialized data: 1,0,1234,4321,default
Enckey: aaaaaaaaaaaaaaaa
◆li◆◆1◆◆◆9◆◆◆n End: ◆◆◆J◆◆Y;◆E◆4◆
send Broadcast
here
lookup
lookup end
getDevice
getDevice end
sendEtherPacket
Send ether packet: length = 32, from = 0x7fff883f2af4, to = 0x7fff883F
sendEtherPacket end
send Broadcast end
-------------------STATE__Bob_State_3
ethernet frame received
length received
id received :0
data received: S\D|l◆◆T
9v~?◆d\,◆mx`◆R◆◆
ethernet frame received end
endloop data:S\D|l◆◆T
9v~?◆d\,◆mx`◆R◆◆
encrypted received:S\D|l◆◆T
9v~?◆d\,◆mx`◆R◆◆
DecKey: bbbbbbbbbbbbbbbb
decrypted: 0,4321,0,0,default
0,4321,0,0,default
0,4321,0,0,default
-------------------STATE__Verify_State2
-------------------STATE___final
FINISHED!!!

clexma@clexma-ThinkPad-P52s:~/Desktop/generated$ sudo ./Alice
1
-------------------STATE___init
-------------------STATE__Alice_State_1
serialized data: 0,1234,0,0,default
Enckey: bbbbbbbbbbbbbbbb
Alice Encryption End: h◆xr◆◆◆0◆J◆J◆v◆:◆◆◆[0◆B◆◆%
send Broadcast
here
lookup
lookup end
getDevice
getDevice end
sendEtherPacket
Send ether packet: length = 32, from = 0x7fff133114b4, to = 0x7fff13311344
sendEtherPacket end
send Broadcast End
-------------------STATE__Alice_State_2
Receive message
ethernet frame received
◆li◆◆1◆◆◆9◆◆◆:◆E◆4◆
ethernet frame received end
Receive message end
decryption: aaaaaaaaaaaaaaaa
◆li◆◆1◆◆◆9◆◆◆eived:◆◆◆J◆◆Y;◆E◆4◆
DecKey: aaaaaaaaaaaaaaaa
decrypted: 1,0,1234,4321,default
1,0,1234,4321,default
decryption end
-------------------STATE__Verify_State
-------------------STATE__Alice_State_3
serialized data: 0,4321,0,0,default
Enckey: bbbbbbbbbbbbbbbb
send Broadcast
here
lookup
lookup end
getDevice
getDevice end
sendEtherPacket
Send ether packet: length = 32, from = 0x7fff133114b0, to = 0x7fff13311344
sendEtherPacket end
send Broadcast End
-------------------STATE___final
FINISHED!!!

Problems

- Serialization → Encryption → Decryption → Deserialization(ERROR)
- Identification of the package: currently the package are identified with the id and ethernet protocol number 0x888f.
- Length of the array when receiving.

Questions

- How "automatic" should we be?

Later Work

- ▶ An overall test combining different modules.
  - ▶ UDP communication.
  - ▶ Other en/decryption algorithms.(Currently is AES).
  - ▶ Find new serialization library.(JSON based e.g.)
- ▶ Refactor of the code generation module.
  - ▶ Add the generation of compile code.
  - ▶ Refine the code related to cryptor and communicatio based on the refined generated code.
  - ▶ More functionalities?