

# 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

```

root@kali:~/Desktop# ./generated$ sudo ./Bob
-----STATE__init
-----STATE__Bob_State_1
Receive message
ethernet frame received
length received
id received :0
data received: hexre0000J0J0ve:000[00B000%
ethernet frame received end
endloop data:hexre0000J0J0ve:000[00B000%
Receive message end
decryption: bbbbbb00000000000000
encrypted received:hexre0000J0J0ve:000[00B000%
DecKey: bbbbbb00000000000000
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: aaaaaaaaaaaaaaaaaa
0i0010009000 End: 000J00Y;0E040
send Broadcast
here
lookup
lookup end
getDevice
getDevice end
sendEtherPacket
Send ether packet: length = 32, from = 0x7fff883f2af4, to = 0x7fff883f
Send ether packet end
send Broadcast end
-----STATE__Bob_State_3
ethernet frame received
length received
id received :0
data received: S\D|000T
9V-70d\,0mx*0R
ethernet frame received end
endloop data:S\D|000T
9V-70d\,0mx*0R00
encrypted received:S\D|000T
9V-70d\,0mx*0R00
DecKey: bbbbbb00000000000000
decrypted: 0,4321,0,0,default
0,4321,0,0,default
0,4321,0,0,default
-----STATE__Verify_State2
-----STATE__final
FINISHED!!!

```

```

1 lexmag@lexma-ThinPad-P52s:~/Desktop/generated$ sudo ./Alice
-----STATE__init
-----STATE__Alice_State_1
serialized data: 0,1234,0,0,default
EncKey: bbbbbbbbbbbbbbbb
Alice Encryption End: hexr+++0+J+Jev:+++[0+0+0%
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
0i0010009000: 000J00Y;0E040
ethernet frame received end
Receive message end
decryption: aaaaaaaaaaaaaaaaaa
0i00100090000evd:000J00Y;0E040
DecKey: aaaaaaaaaaaaaaaaaa
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 = 0x7fff133114b4, 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.
- ▶ Iteration based on implementation.
- ▶ More functionalities?