# Secure Chat Application

## Readme

## Team Details :


| | |
|---|---|
| Patel Heetkumar Dilipbhai | CS23MTECH11029 |
| KR Anuraj | CS23MTECH13002 |
| Vishal Patidar | CS23MTECH14017 |


## Task 2 : Executing Simple Chat Application

- Copy secure_chat_app.cpp file and Certificates folder IntCA and RootCA at both sides i.e. Alice and Bob.
- Copy Alice1 and Bob1 folder of certificates and keys to their respective machine.
- Compile the secure_chat_app.cpp using below command:
  "`g++ -o secure_chat_app secure_chat_app.cpp -w -lssl -lcrypto`".
- Now to start app run "`./secure_chat_app -s`" at Bob's side and "`./secure_chat_app -c bob1`" at Alice's side.
- You will enter into the secure DTLS mode automatically (also you can see what control message are passing while configuring DTLS mode) then you can simple use it as messaging app.
- To close chat app enter "`chat_close`" in terminal at any side.

## Task 3 : Executing Simple Chat Application with Interceptor

- Copy secure_chat_app.cpp file and Certificates folder IntCA and RootCA at both all sides i.e. Alice, Bob and Trudy.
- Assuming Trudy has hacked into IntCA we have Alice and Bob's fake certificate ready, copy it to Trudy
- Copy Alice1 and Bob1 folder of certificates and keys to their respective machine.
- Now to poisoned /etc/hosts of Alice and Bob execute below command in host's machine where this Alice, Bob, Trudy's container are present:
  "`bash ~/poison-dns-alice1-bob1.sh`".

- Compile .cpp files at respective sides using below command: "`g++ -o <output file> <.cpp file> -w -lssl -lcrypto`".
- Now first start the interceptor at Trudy using "`./secure_chat_interceptor -d alice1 bob1`" then Bob using "`./secure_chat_app -s`" and Alice using "`./secure_chat_app -c bob1`".
- You can see the control messages passing through the Trudy and while getting chat_START_SSL Trudy replies chat_START_SSL_NOT_SUPPORTED which results in simple UDP communication which can be Intercepted at Trudy.
- To close chat app enter "`chat_close`" in terminal at any side.
- To unpoisoned the /etc/hosts file execute below command : "`bash ~/unpoison-dns-alice1-bob1.sh`".

## Task 4 : Executing Simple Chat Application with MITM

- Copy secure_chat_app.cpp file and Certificates folder IntCA and RootCA at both all sides i.e. Alice, Bob and Trudy.
- Assuming Trudy has hacked into IntCA we have Alice and Bob's fake certificate ready, copy it to Trudy
- Copy Alice1 and Bob1 folder of certificates and keys to their respective machine.
- Now to poisoned /etc/hosts of Alice and Bob execute below command in host's machine where this Alice, Bob, Trudy's container are present: "`bash ~/poison-dns-alice1-bob1.sh`".
- Compile .cpp files at respective sides using below command: "`g++ -o <output file> <.cpp file> -w -lssl -lcrypto`".
- Now first start the interceptor at Trudy using "`./secure_chat_active_interceptor -m alice1 bob1`" then Bob using "`./secure_chat_app -s`" and Alice using "`./secure_chat_app -c bob1`".
- On completing the DTLS handshake you will get the Typing Interface where you can start chatting.
- To close chat app enter "`chat_close`" in terminal at any side.
- To unpoisoned the /etc/hosts file execute below command : "`bash ~/unpoison-dns-alice1-bob1.sh`".

## Task 5 : ARP Cache Poisoning

- To perform ARP Cache Poisoning copy gratuitous_fake_ARP.cpp file into Trudy.
- Compile that using "`g++ -o gratuitous_fake_ARP gratuitous_fake_ARP.cpp -w -lpcap`" command.
- Now to run execute "`./gratuitous_fake_ARP`" command.
- This will broadcast ARP response packets every 5 seconds.
- To check whether ARP cache poisoning works or not execute "`arp -n`" before and after executing gratuitous fake ARP file and compare the table.