Author: Dang Hoan Nguyen

This test is conducted after resolving some incompatibilities: (https -> http and wss -> ws)

Pre-testing:

1. Set up connection so that your server can connect to the target server
2. Run 2 servers
3. Run 2 clients (one on each server)

Testing:

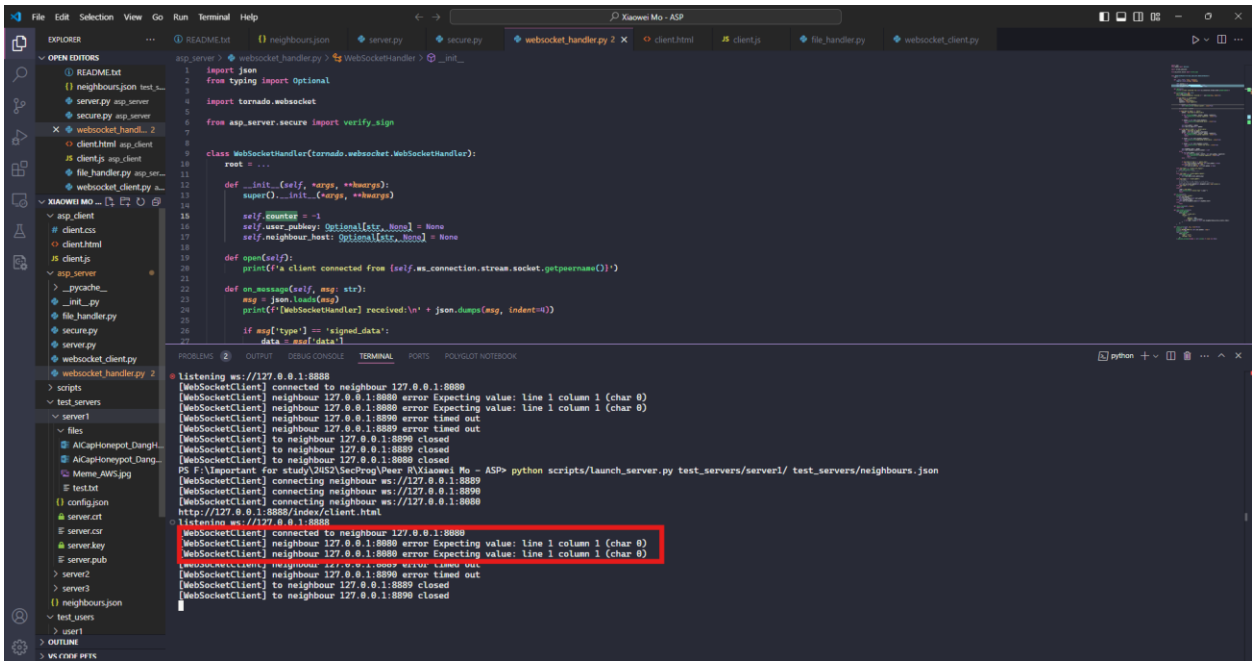
	Process	Expected behavior	Result (Pass / Fail / Unsure)	Comment
1	server_hello	The traffic is captured at the server	Unsure	The traffic is captured but the signature is not verified.
2	client_update_request	A client list is sent back to the server.	Pass	This works on our end, but does not on the other. When a client on the Group 43 connect or disconnect, our online user list is updated.
3	Sending message (chat or public_chat) from clients.	The message successfully appears in the correct format at target client (s).	Fail	The transaction is captured, but the signature is not verified. Public key is not received on Group 43's client, so private chat does not work. Fingerprint, signature techniques differences.
4	Updated online users	When a new user connects or a user disconnect in the distant server, the clients list on left-hand side menu is updated.	Pass	This works on our end, but does not on the other. When a client on the Group 43 connect or disconnect, our online user list is updated.

Conclusion: All unsinged functionalities on our end functions well. There are conflicts in how signature and fingerprints are generated which make signed_data not receivable.

Screenshot:

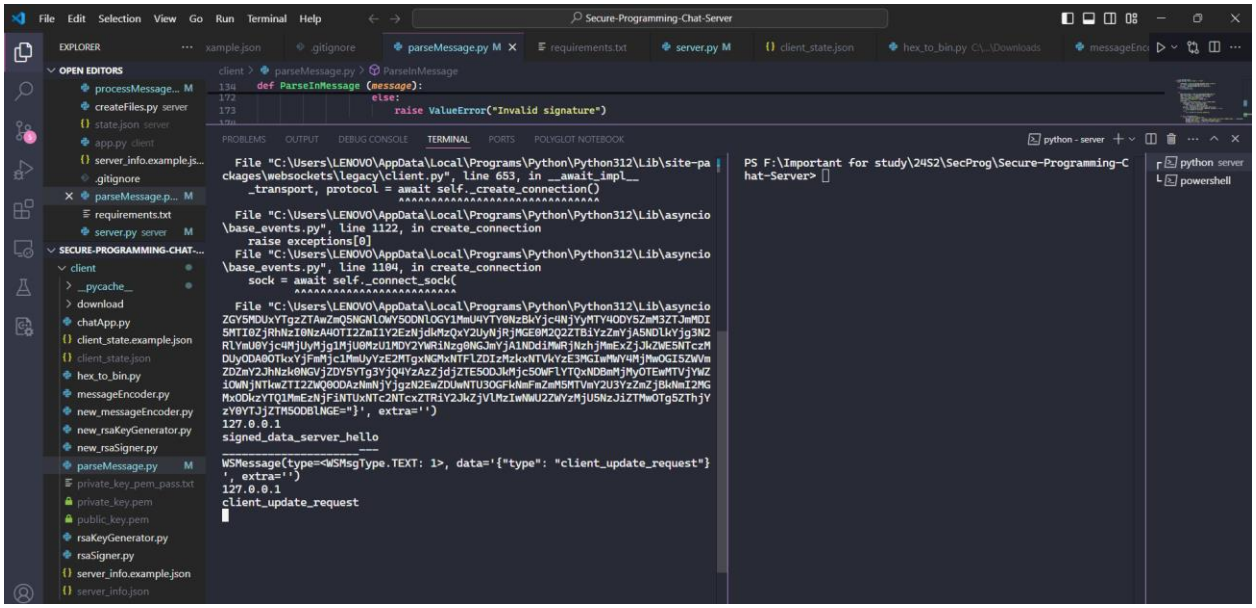
1. Server hello.

   Group 43's server:

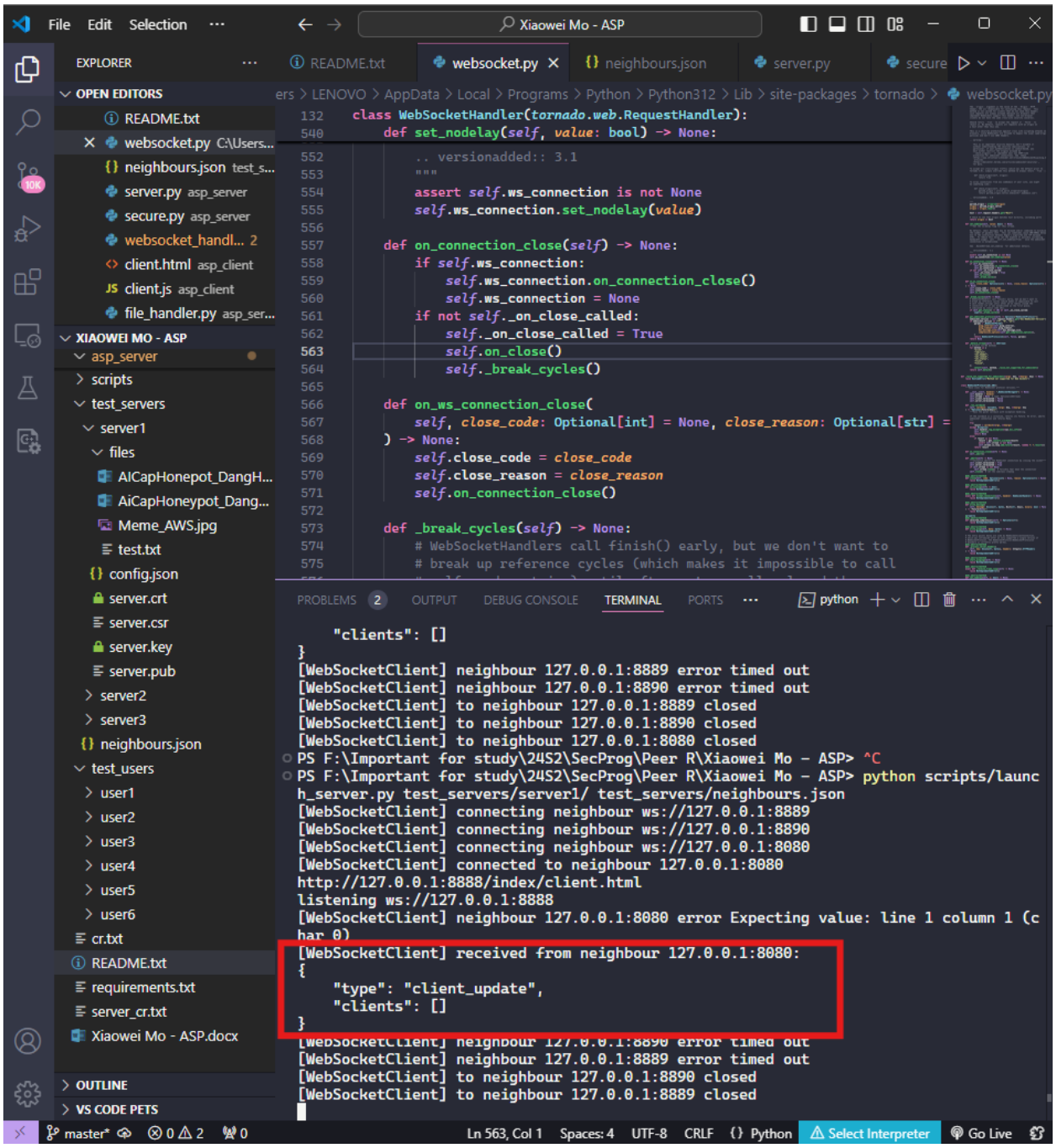


The connection is kept open.

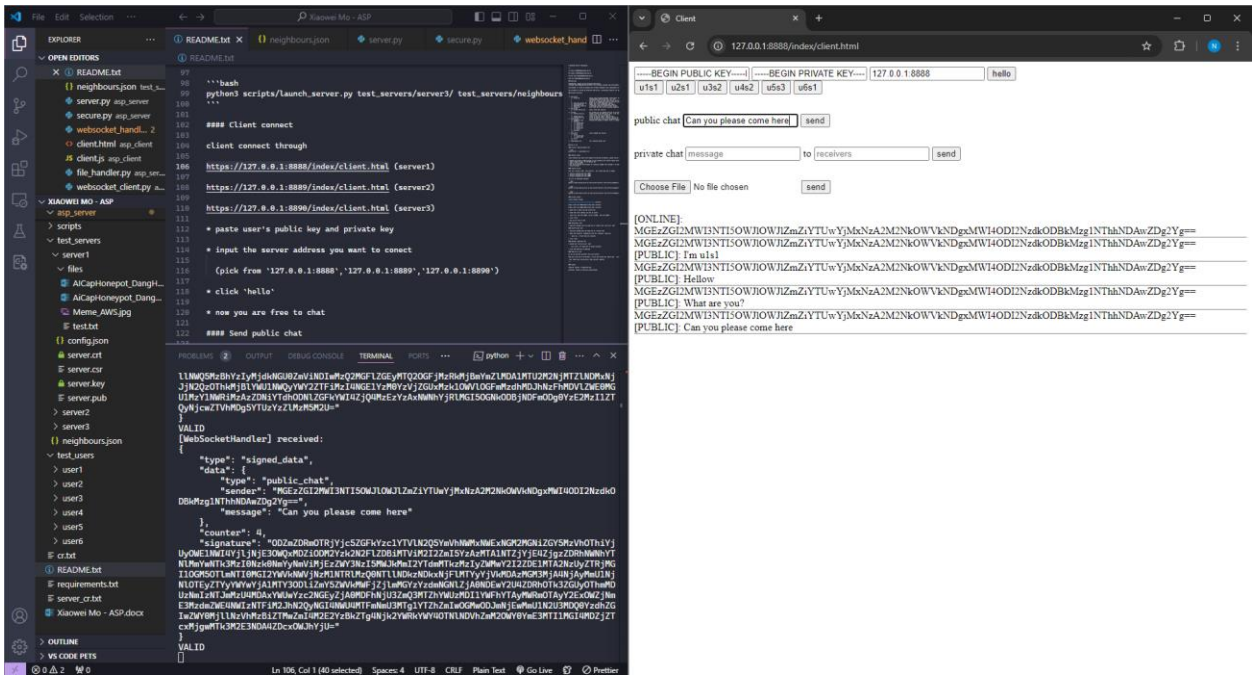
On our side:

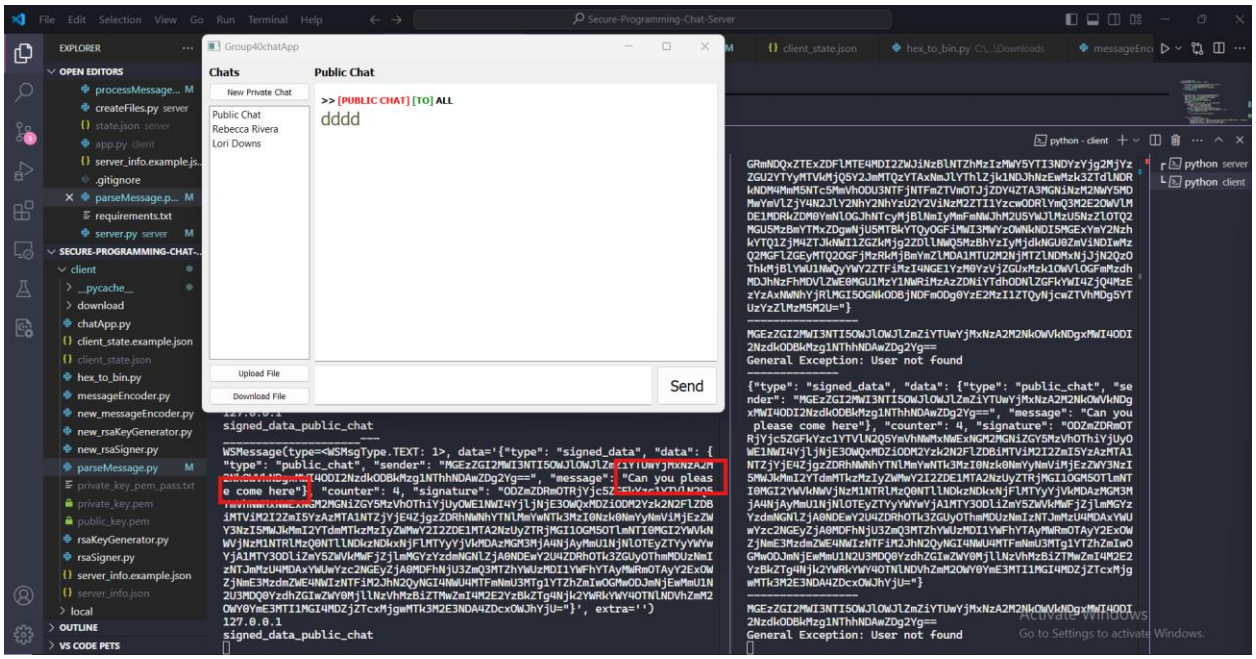


2. After server Group 43 send server_hello.


File Edit Selection
Xiaowei Mo - ASP
EXPLORER
README.txt
websocket.py
neighbours.json
server.py
OPEN EDITORS
XIAOWEI MO - ASP
asp_server
scripts
test_servers
server1
files
test_users
class WebSocketHandler(tornado.web.RequestHandler):
def set_nodelay(self, value: bool) -> None:
PROBLEMS 2
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
"clients": []
}
[WebSocketClient] neighbour 127.0.0.1:8889 error timed out
[WebSocketClient] neighbour 127.0.0.1:8890 error timed out
[WebSocketClient] to neighbour 127.0.0.1:8889 closed
[WebSocketClient] to neighbour 127.0.0.1:8890 closed
[WebSocketClient] to neighbour 127.0.0.1:8080 closed
PS F:\Important for study\24S2\SecProg\Peer R\Xiaowei Mo - ASP> ^C
PS F:\Important for study\24S2\SecProg\Peer R\Xiaowei Mo - ASP> python scripts/launch_server.py test_servers/server1/ test_servers/neighbours.json
[WebSocketClient] connecting neighbour ws://127.0.0.1:8889
[WebSocketClient] connecting neighbour ws://127.0.0.1:8890
[WebSocketClient] connecting neighbour ws://127.0.0.1:8080
[WebSocketClient] connected to neighbour 127.0.0.1:8080
http://127.0.0.1:8888/index/client.html
listening ws://127.0.0.1:8888
[WebSocketClient] neighbour 127.0.0.1:8080 error Expecting value: line 1 column 1 (char 0)
[WebSocketClient] received from neighbour 127.0.0.1:8080:
{
"type": "client_update",
"clients": []
}
[WebSocketClient] neighbour 127.0.0.1:8889 error timed out
[WebSocketClient] to neighbour 127.0.0.1:8890 closed
[WebSocketClient] to neighbour 127.0.0.1:8889 closed
master*
Ln 563, Col 1
Spaces: 4
UTF-8
CRLF
Python
Select Interpreter
Go Live

3.



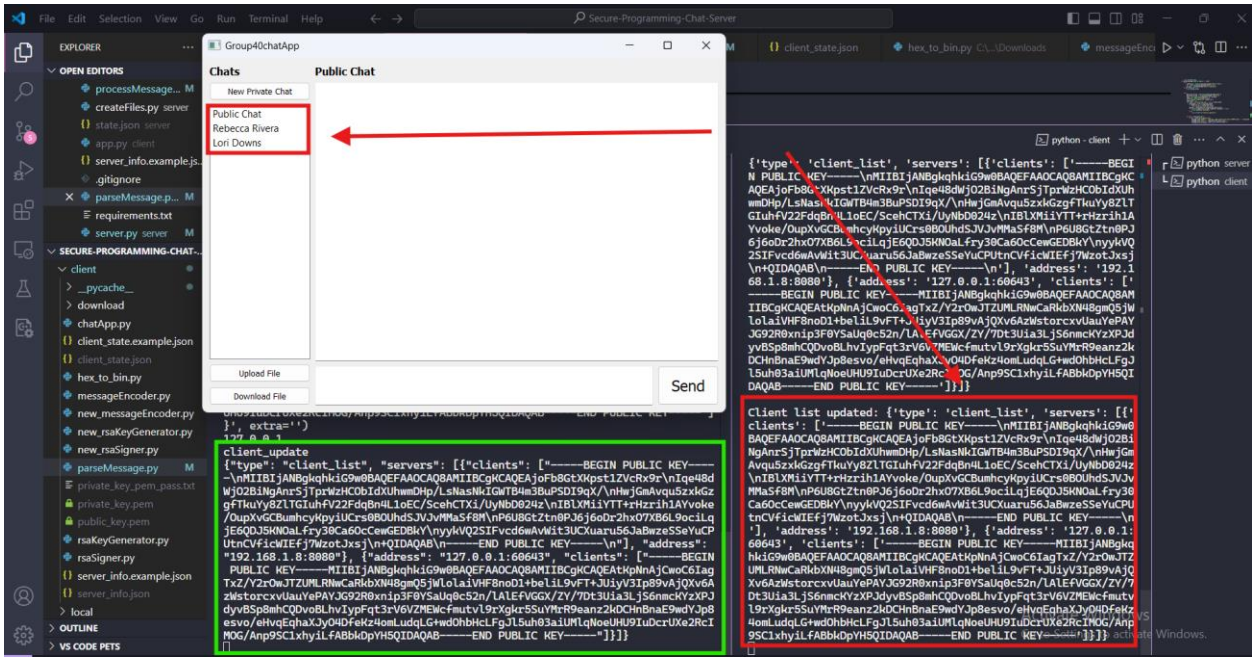


The message is received at our server, but signature is not verified.

4. When a client on server Group 43 send hello.

Red: Updated client list at client

Green: Received client_update from Group 43's server.


Group40chatApp
Chats
Public Chat
New Private Chat
Public Chat
Rebecca Rivera
Lori Downs
Upload File
Download File
Send
client_update
Client list updated:
EXPLORER
OPEN EDITORS
SECURE-PROGRAMMING-CHAT-...
OUTLINE
VS CODE PETS