

Security report

The application which I presented as a solution for COSC540 Assignment 2 was a simple application which demonstrated socket communication and threading between a client and server.

Security was not considered as a requirement and therefore the system was inherently insecure.

Here are the issues identified with my solution and how they could be remedied

Communication not encrypted:

Communication should be encrypted. An extra layer should be added and socket wrapped with TLS. A certificate should be installed at the client and signed by a trusted authority, which is registered and accepted on the server.

User not authenticated:

Currently anyone who has the client code can connect to the server and optimise their codons. The user should be authenticated by a public key.

IP whitelist:

If the client side is compromised and the password and program stolen, the server is vulnerable to unauthorised use. By whitelisting the appropriate IP address, the server can limit connections to a physical location and provide another layer of security

Activity log:

The server should create logs of connections and traffic. At present there is no way of monitoring traffic or connections other than watching what is logged on the terminal. Based on monitoring of traffic, users could be authorised for a certain amount of traffic