Pseudo-System Protocol for Information Transfer

Akshay, Amogh, Prajwal, Rohan & Prof. Pushpa
Department Of Computer Science and Engineering, PES University

Problem Statement

To design and implement a networking protocol that achieves complete host security by implementing pseudo-systems, thereby ensuring host isolation in a network.
This protocol secures the data being transferred and masks the host so that a third party cannot gain access to the hosts. The protocol sequences the transfer of data such that the hosts always remain disconnected from the internet while using the internet as the primary medium for the transfer

Background

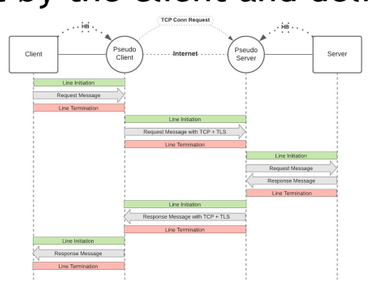
1. Historically, networking protocols have focused primarily on data-security and not so much on host-security.
2. Host-security is traditionally achieved by means of conventional mechanisms like firewalls and antivirus applications.
3. TCP's TLS-SSL encryption handles data-security well and necessitates no reinvention of the wheel.
4. Conventional computer networks are prone to an array of active, passive and advanced attacks.

Product Features

1. Maximum host-isolation: The host can communicate through the internet without ever connecting to it.
2. Industry-standard reliability and congestion-control: PSPIT comes with these features built in as it uses TCP under the surface.

Design Approaches / Methods

The client starts the session by sending the request to the pseudo-client. The pseudo-client isolates the client from itself before forwarding the request to the pseudo-server. The pseudo-server establishes a connection with the server and forwards this request after isolating itself from the public internet. The server after processing the request, sends it to the pseudo-server. The pseudo-server approves the connection request and forwards the response to the pseudo-client. The pseudo-client responds to the heartbeats sent by the client and delivers the response.



Results and Discussion

1. Real-time logs of the protocol executing were fed into a simulation system and the results were examined for bottlenecks and loops.
2. The multi-system test was successfully carried out

Summary of Project Outcome

This objectives of this research were successfully achieved. In order to ensure complete host isolation, we made the use of heartbeats in our protocol. At no point during the communication session was the real identity of the host systems exposed to the public internet.

Conclusions and Future Work

The future work for the protocol involves working on further safeguards localized in the pseudo-systems like sandbox testing.

References

26-34. 10.1145/1128817.1128826
539-556. 10.1109/SP.2017.17.