Computer Networks Lab – Technical Description

Team members: Reuben John, Soorya Annadurai

Project Description:

The project involves a proposed improvement to the current SSH mechanism. In the current scenario, key-exchange mechanisms like the Diffie-Hellman Algorithm are used to transmit security variables across an insecure connection to agree upon a shared secret. SSH consists of three stages, namely, SSH-TRANS, SSH-AUTH, and SSH-CONN. The key exchange mechanism takes place in the SSH-TRANS stage, and the shared secret is hence used in symmetric encryption algorithms to secure all forthcoming data transfers. Typically, algorithms like AES (128 bit) are used to secure the data transfer.

However, for a given session, the shared secret remains constant. This means that, if an SSH session is not closed, or the system maintains the connection for too long, attacks can be implemented on the sniffed data traffic to crack the symmetric encryption algorithm’s key. This attack can become more effective with a weaker data encryption algorithm.

One way to mitigate this type of attack is by implementing the proposed mechanism, wherein the key exchange is done and repeated in regular intervals. The newly generated shared secret can depend on several factors, such as random system variables, previous data traffic, and improved key exchange mechanisms.

This is the high-level description of the aims for the Computer Networks project.