ABSTRACT

Multipath Transmission Control Protocol (MPTCP), a state-of-the-art rising transport layer protocol, has been standardized to eliminate the restriction of Transmission Control Protocol (TCP) by enabling numerous disjoint routes for communication over a single connection. According to the current networking scenario, most computing devices, like servers, mobile phones, etc., are connected to multiple networks (multi-homed) and have multiple network cards (multi-addressed). Moreover, Datacentres have redundant links among nodes for offering reliable communication. However, the current computing devices are multi-homed and multi-addressed, and TCP doesn't allow using more than one network card for single communication.

For the unified transmission of application data across numerous interconnected TCP flows, referred to as sub-flows, MPTCP enhances TCP through a novel range of signalling possibilities. The primary goal of MPTCP was to allow for the simultaneous usage of numerous network interfaces over a single network connection to fulfill the demand of various information technology fields. Several routes can be used to increase the overall throughput. With backup connections, MPTCP can quickly resume operation once a connection loss occurs. MPTPC is also backward compatible with the application level as it uses a TCP header and option field (like MP_CAPABLE, MP_JOIN, etc.) to communicate the required details. Moreover, MPTCP also uses 3-way handshake procedure like TCP in order to bypass the middleboxes and exchanges the security keys at the time of connection establishment. It uses the same keys in future to authenticate subsequent sub-flows established by host over same connection. In this case, the keys are just plain text.

Although the benefits of MPTCP are obvious, studies have revealed various security risks associated with MPTCP connections, including denial-of-service, flooding, connection hijacking, and others that can target the connections. As MPTCP supoorts use of multiple routes, it opens many doors for attackers compared to TCP. A security breach on one of the routes could significantly affect the throughput, resiliency, durability, and quality of service (QoS) of the connection.

This thesis examines vaulnerabilities of MPTCP header options which can be used to initiate several attacks that threaten the various security goals. Various experiments have been performed to demonstrate the attack scenarios like session hijacking and MitM attack.

Moreover, the likely security methods for safeguarding MPTCP connections are studied thoroughly to understand the current security levels, and the Secure Key Exchange Model for

MPTCP (SKEXMTCP) using Identity Based Encryption (IBE) is proposed and analysed to overcome some of the issues. IBE encrypts the session keys exchanged during the 3-way handshake to offer security against various attacks by eliminating the need for exchanging the keys in prior and permitting using random strings as the public key for encryption. The experimental evaluation demonstrates that key generation is not required at the time of encrypting the message with the IBE which makes the encryption process less complex as compared to Elliptic Curve Cryptography (ECC). The experimental evaluation of the security and performance of SKEXMTCP is conducted and compared to existing solutions.