CERIAS
The Center for Education and Research in Information Assurance and Security

# TCP Stream Splitting Moving Target Defense

Siddharth Gupta[1], Sahithya Kodam[2]
[1]Purdue University, gupta287@purdue.edu ; [2]Purdue University, kodam@purdue.edu
Michael L Thompson, Nate J. Evans from Argonne National Laboratory

## Motivation

•Communication channels are one of the significant contributors to the attack surface.
•Static networks provide access to complete data in transit over the communication channel from a single point.

## Research Question

Using traditional TCP, how can you devise a stream splitting Moving target defense mechanism at Application Layer to make the network system secure and uncertain for the attacker?

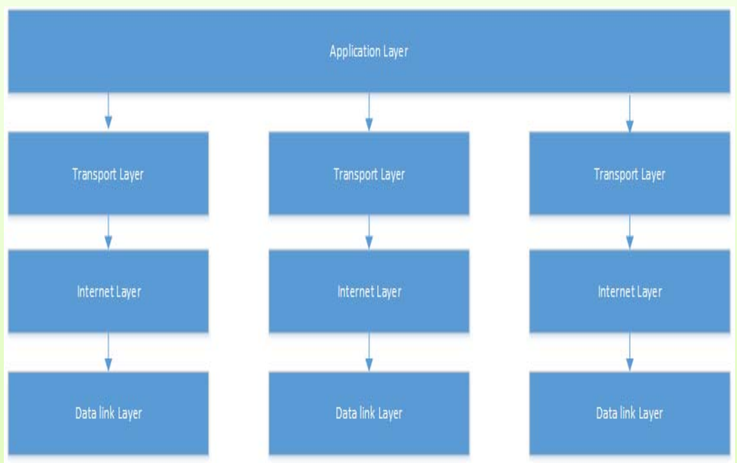
## Research Plan

•Study TCP and current stream splitting techniques.
•Design the technique.
•Identify attack scenarios mitigated from the design
•Simulate and test the design

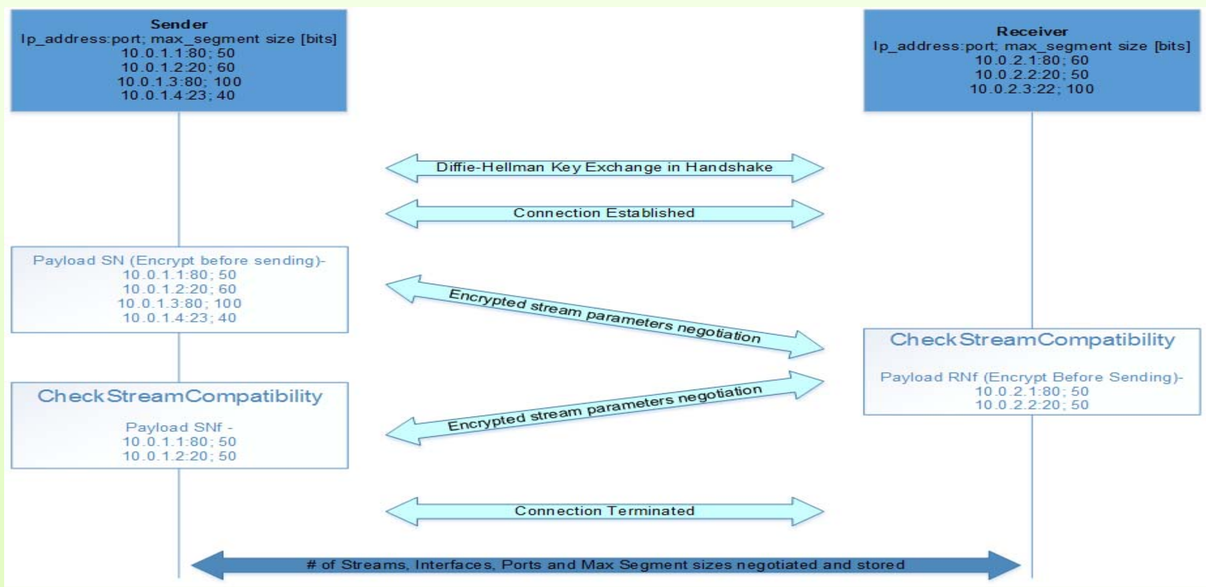
## Progress till date

1.High Level TCP/IP design.
2.Secure stream negotiation design.
3.Initiating connections and data transfer design
4.Attack Scenarios mitigated
5.Retransmission data design

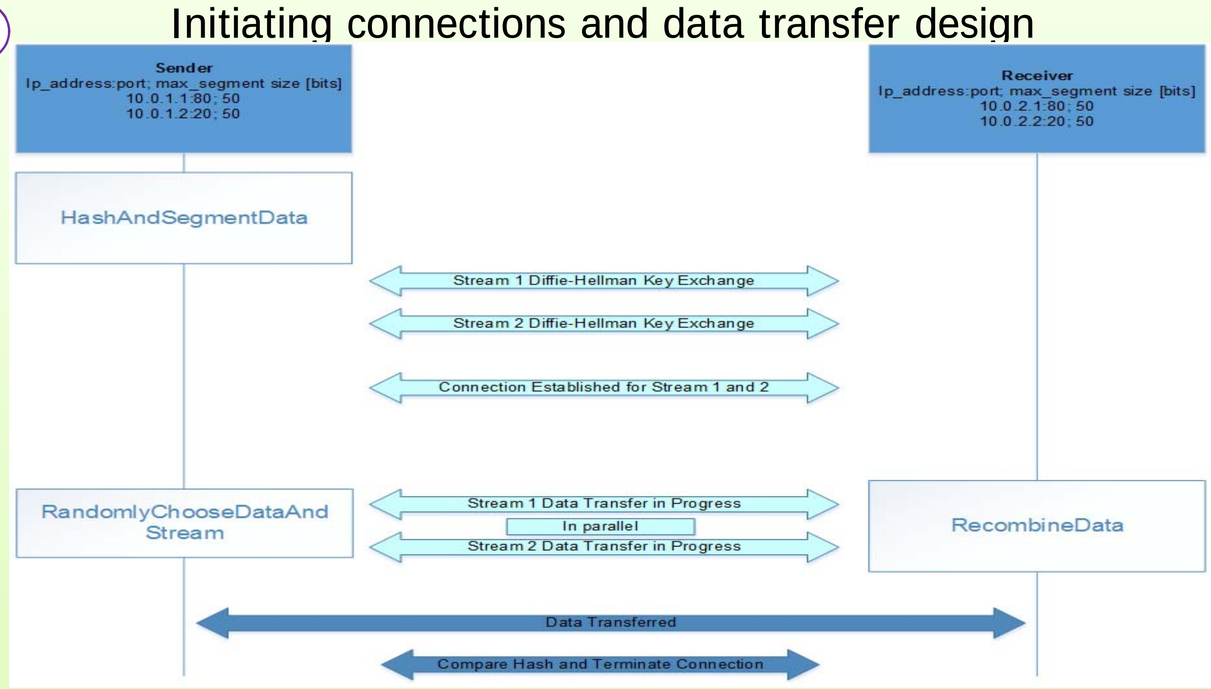
## 1 High Level TCP/IP design




## 2 Secure stream negotiation design.



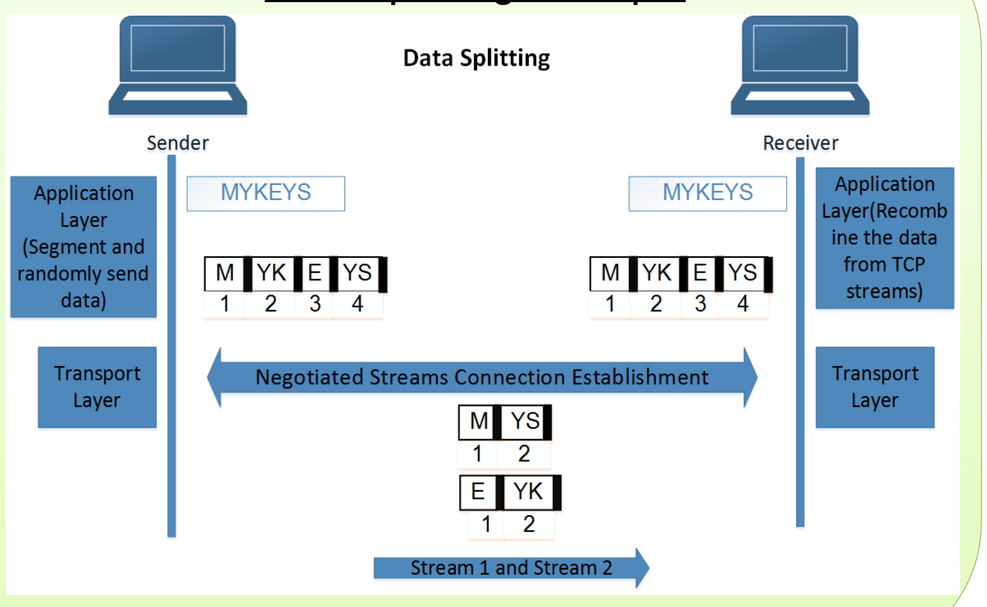

## 3 Initiating connections and data transfer design




## Future Work

•Simulate the technique.
•Capture results

## Data Splitting Example




## 4 Attack Scenarios Mitigated

•Dos Attack – Multiple links to continue communication
•Sniffing/ Eavesdropping – Data sent in no particular order.
•Man-in-the-middle – Hashing used for message integrity.
•Replay Attack – Sequence numbers used.

## 5 Retransmission data design

•Original data will be divided into multiple zones.
•Whole data will be segmented.
•Sender will be randomly select segments following zonal sequence.
•Receiver will request retransmission if previous zone's segments are missing.

CERIAS

PURDUE UNIVERSITY