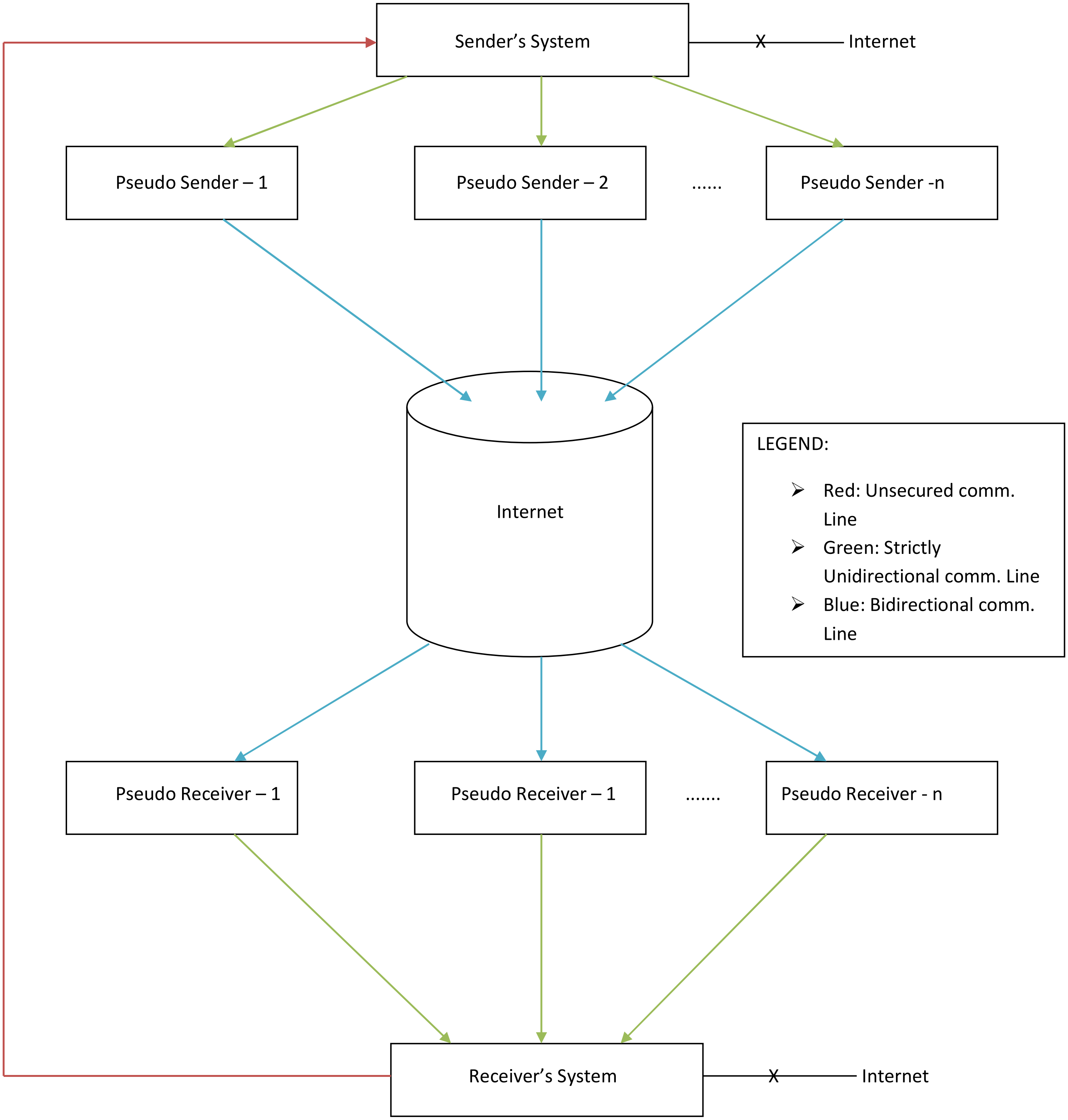
PSEUDO-SYSTEM PROTOCOL FOR INFORMATION TRANSFER

-Akshay Vasudeva Rao

ARCHITECTURE



PROTOCOL

1. The sender's and receiver's system must be isolated from the internet.
2. (a) The communication framework between the sender's system and the pseudo-senders must allow only unidirectional transfer of packets, i.e. from the sender's system to the pseudo-system.

   (b) The communication framework between the pseudo-receivers and the receiver's system must allow only unidirectional transfer of packets, i.e. from the pseudo-receivers to the receiver's system.

   (c) The communication framework between the pseudo-senders and pseudo-receivers must allow bidirectional communication.

   (d) 2(a) and 2(b) must be implemented by a "fire and forget" protocol like UDP.

   (e) 2(c) must be implemented by an internet standard such as TCP.

3. The sender's system must split the information randomly into packets with the following criteria in place:
   (a) The receiver must have a mathematically related public and private splitting/regrouping (S/R) key.
   (b) The receiver must share his public S/R key with the sender. This may happen by means of an unsecure communication line.
   (c) The sender must use the receiver's public S/R key in a mutually acceptable algorithm (may be publically known) used to split the data.
4. The packets must travel through the internet to reach the designated pseudo-receivers.
5. The pseudo-receivers must not be capable of regrouping the packets of data to get any meaningful piece of unified data.
6. The receiver's system must be capable of terminating its connections with the pseudo-receivers upon need.
7. The receiver's system must use the receiver's private S/R key to regroup the packets in order to get a unified piece of meaningful data.

NETWORK ANALYSIS

Step-1: Receiver sends his public S/R key to the sender via an unsecured line.

Step-2: The isolated sender’s system splits the data into packets using the receiver’s public key by virtue of a mutually agreeable algorithm.

Step-3: The split data is sent to the pseudo-senders though a one-way communication line.

Step-4: The said pseudo-senders send the packets across the internet using standard TCP to their corresponding pseudo-receivers.

Step-5: The pseudo-receivers then send the packets to the receiver’s system.

Step-6: The receiver’s system terminates its connections with the pseudo receivers.

Step-7: The receiver’s system uses the receiver’s private S/R key to regroup the packets into a unified meaningful piece of data.

COMPONENT DEFINITIONS

1. Sender’s System:
   (a) Functionality: Storage of data, splitting of data.
   (b) Connections: Unidirectional to pseudo-senders.
   (c) NOTE: Must be isolated from the internet.
2. Receiver’s system:
   (a) Functionality: Storage of data, regrouping of data.
   (b) Connections: Unidirectional from pseudo-receivers.
   (c) NOTE: Must be isolated from the internet.
3. Pseudo-sender:
   (a) Functionality: Reception of packets, shooting of packets.
   (b) Connections: Unidirectional from the sender’s system, bidirectional to the internet.
4. Pseudo-receiver:
   (a) Functionality: Reception of packets.
   (b) Connections: Unidirectional to the receiver’s system, bidirectional from the internet.

DISSERTATION

The strength of the Pseudo – System Protocol for Information Transfer lies in the fact that the sender's and receiver's systems are completely immune to data theft or corruption due to the fact that these systems are virtually isolated from the internet despite the fact that the internet is the medium that the protocol uses to transfer data.

This isolation is further strengthened by the unidirectional connections involved. These make sure that the pseudo senders involved do not have the capability to ping the sender's system for information on the chance that they are being accessed by Eves through the internet.

Another key feature of the PSPIT is the fact that a pseudo-sender has no direct link with any other pseudo-sender on the network. The one way connection between the sender's system and the pseudo sender ensures that no Eves can identify the other pseudo-senders on the network. This way, even if an unauthorised entity gains access to a pseudo-sender, the said entity only has access to a meaningless set of packets. The same logic applies to pseudo-receivers.

A key step in PSPIT is the termination of the connection between the receiver's system and the pseudo-receivers the second that last packet arrives at the receiver's system. This guarantees inaccessibility of the receiver's system from the internet once the jumbled, but complete data has reached the receiver's system. Thus, the PSPIT ensures that the entire set of information is never available to Eves at any point in time throughout the entire process of data transfer!