Real-Time Detection of Stepping-Stones Using Neural Networks

Brian White Jr
Computer Science and Electrical Engineering
University of Maryland, Baltimore County

What is a Stepping-Stone?

A stepping-stone is an intermediary host in a connection chain

•Are used to hide the identity of a network intruder

•Connection chains are created using SSH, Telnet , or Rlogin

Detection of Stepping-Stones

Analyzing TCP/IP packets

•The contents of the packets are not important

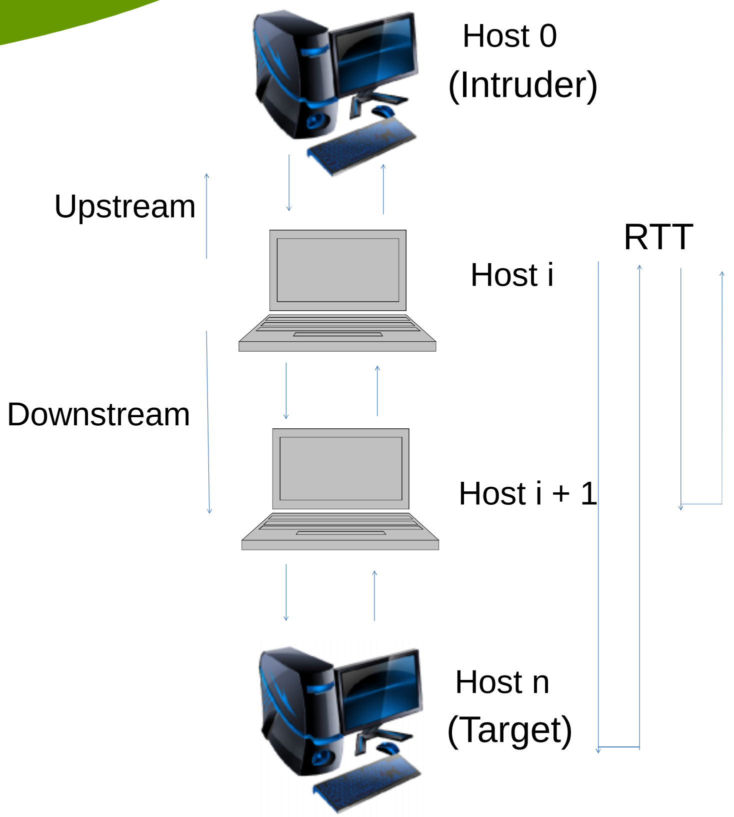
•Packet length and size

•Round-trip time (RTT)

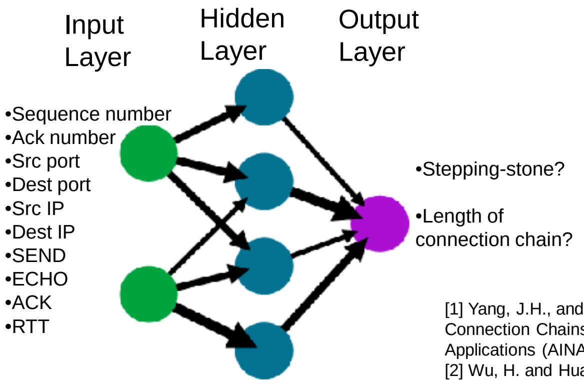
TCP Packet Matching

```
Initialize a SendQ queue;
while (there are more packets) {
   Capture the next packet P;
       if P is a Send packet {
      Compute Time Gap TG;
       If (TG > Threshold){ Reset the SendQ;}
       else add {P to SendQ;}
    } else if P is an Ack packet{
      // Ignore it
  } else if P is an Echo packet{
      Q = dequeue (SendQ);
      if ((Q.ack# = P.seq#) and (Q.seq# < P.ack#)){
         Packets P and Q are matched;
      Compute round-trip time between P and Q;
  } else if(((Q.ack# =< P.seq#)
             and (Q.seq# < P.ack#)){
         Packets P and Q are matched;
        Compute RTT between P and Q;
      } else {//No match;}
   } else {Return;}
}
```

Connection Chain



Feed Forward Neural Network



Neural Network

•Are fast and flexible in their analysis of data

•Once the neural network is trained with the testing data the only data collected is the new incoming data, not the whole connection session

Methods

1. Collect network data for neural network training

   (Sequence number, Acknowledgement number, size, source and destination port and IP, SEND, ECHO, RTT, ect)

2. Setup connection chain with computers on a local network

3. Collect TCP packet data

4. Run the newly collected data through a feed-forward network, trained using the data from step1

5. Results should determine if the computer is part of a connection chain

Next Step

•Move some of the computers in the connection chain off-site

•Introduce inter-packet delay and chaff to training and test cases.

Future Work

Analyze the upstream connection to determine the origin of the intruder

[1] Yang, J.H., and Huang, S-H.S., "Matching TCP Packets and Its Application to the Detection of Long Connection Chains," Proceedings of International Conference on Advanced Information Networking and Applications (AINA2005), Taipei,Taiwan,pp1005-1010,March 2005.

[2] Wu, H. and Huang, S. S. 2010. Neural networks-based detection of stepping-stone intrusion. *Expert Syst. Appl.* 37, 2 (Mar. 2010), 1431-1437.