Plant-Controller Attacks via Cut-Link and Flooding

[1]Katherine R. Gabales – [2]Mentors: Saurabh Amin, Blaine Nelson, Dr. Suzanna Schmeelk

[1]California State University, Chico; [2]University of California, Berkeley

Introduction

In an emulated environment of Abilene Network [Figure 8], learning the basic interaction and strategies for attack and defense of control systems and detection systems are vital in building a stronger infrastructure for it can minimize possible number of intrusion. Emulating routing and traffic between **Plant and Controller nodes** will provide insights of possible effects caused by created sample attacks placed within the system. Two **Distributed Denial-of-Service (DDoS)** attacks**,** Cut-link and Flooding attack, were implemented to test the Plant and Controller nodes. **Cut-link Attack** cuts the connection between nodes, and **Flooding Attack** overwhelms Plant nodes by sending overloading packets. The DETER research was divided into three phases: build infrastructure of the network, deploy the learning based DoS detection algorithm and test for attacks, and explore defenses that will allow for the learning system to be more resilient to attacks. The main purpose of the attacks is to record the amount of time when a Plant [or victim node] losses connection.

Methodology

Below are the enumerated approaches in accomplishing the project.

1. Created simple topology [Figures 1-6] on DETER testbed
   a. Topologies are composed of three to twenty-four nodes.
   b. Nodes were either linked via duplex-link or switch
   c. Each topology have at least a Plant node and a Controller node – though most have attacker nodes
2. Examined normal traffic via SEER [Figures 1-6] and ping on SSH [Figure 7]. Communication between the Controller and Plant are on Figure 7.
3. DDoS attacks created on simple topology via Tcl on DETER testbed
4. Examined ratio of normal traffic and attack traffic [Figures 3-6]

Implementation of Experiments

In the experiment, there are 3 nodes: controller, plant, and attacker. Figure 2 illustrates a symmetrical graph of traffic indicating that there is no interruption of any kind. Figure 1 shows the active connection between the plant and the controller without interruption from the attacker. Activating the attacker node, via sending flood attack traffic, attempts to flood the plant displaying a red graph on the incoming traffic of plant node on Figure 4, which is the graph of the attacker in which attacks are only outgoing traffics. Moreover, Figure 6 merely shows that plant's incoming traffic is jammed [flooded] and by looking at Figure 6, the connection between the plant and controller demonstrated that no traffic exist.

Plant-Controller Traffic Observation

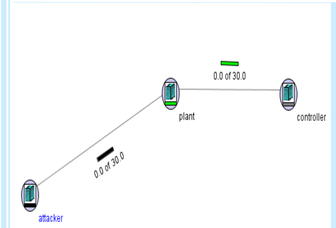

Figure 1. Topology of normal traffic between Controller node and Plant node

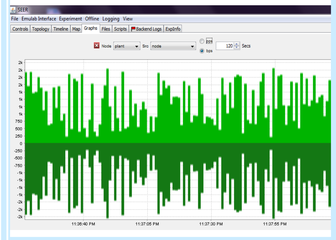

Figure 2. Graph of a normal traffic between the Controller node and the Plant node

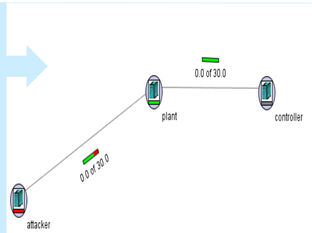

Figure 3. Topology of Attacker node attacking Plant node while is communicating with the Controller node

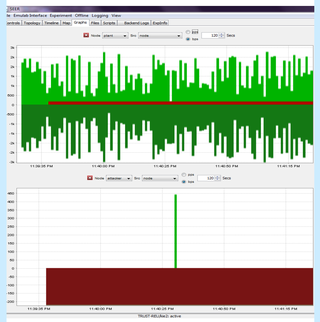

Figure 4. Graph of Attacker node attacking Plant node while communicating with the Controller node.

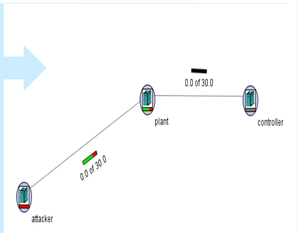

Figure 5. Topology of Controller node not reporting any traffic and Plant node in attacked traffic,

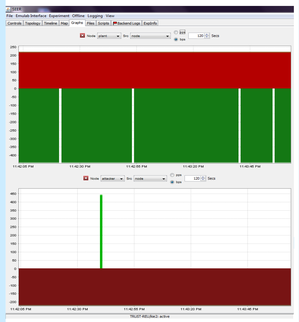

Figure 6. Graph of Attacker node with no traffic and Plant node in attacked traffic

The keys to colored bar for the topology Figures 1, 3, and 5 are as follow:

- **Green bar**-normal traffic
- **Green and Red bar**-ratio of normal to attack traffic
- **Grey bar**-is not reporting counter information to us
- **Black bar**-no traffic present

Packets Captured

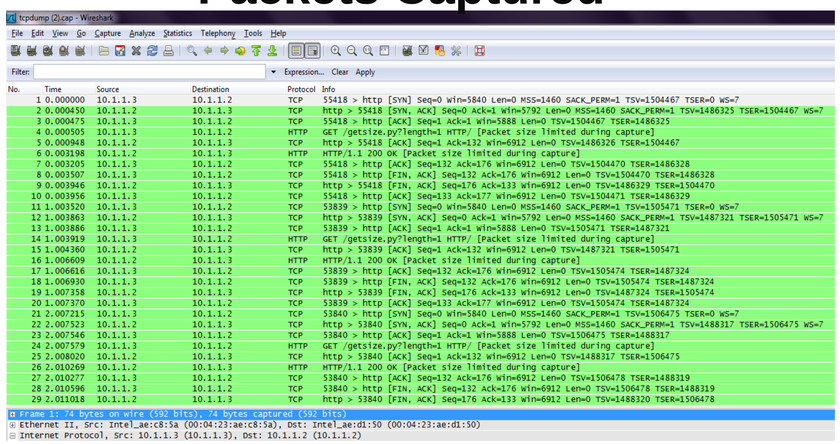

Figure 7. Packets captured by Plant node while Controller node is pinging the Plant node via Wireshark

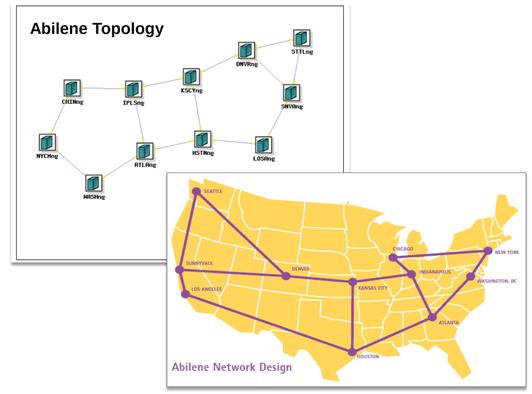

Figure 8. [FRONT] Abilene Network; [BACK] Abilene Topology via DETER testbed. cyber-DEfense Technology Experimental Research network (DETER network) provides necessary infrastructure network, tools, and supporting processes—to support national-scale experimentation on merging security research and advance development technologies

Result

Cut-link and Flood attack scripts function efficiently via manual testing. The Controller node and Plant nodes were able to communicate with via Ping [Figures 2 & 7]; also, packets were captured as Figure 7 illustrates. After creating an attack [Figure 4], the traffic was interrupted and the connection between plants slowly diminished.

Conclusion

Automation of the Plant-Controller is critical. To increase complexity use of the Abilene network, modification of the Tcl file and the Flooding attack is necessary. An example is an individual creation of each Abilene node. This is a tough challenge since a careful study of how each are connected must be taken seriously.

Acknowledgement

This work is supported in part by the National Science Foundation under Award Number CCF-0424422, via the Department of Electrical Engineering and Computer Sciences, College of Engineering located in Cory Hall at the University of California, Berkeley. Thank you to TRUST-REU staff, Dr. Kristen Gates, Dr. Larry Rohrbough, Ted Faber, Jelena Mirkovic, Dr. Suzanna Schmeelk, Blaine Nelson, Saurabh Amin, the DETER cohort, University of California, Berkeley, TRUST 2010 REU interns, especially to Ricardo Estrada of California State University, Monterey Bay and Kyle Marlin of Youngstown State University, Ohio.

This work was supported by the TRUST Center (NSF award number CCF-0424422)