Effect of DDOS attacks on simple plant-controller networks

Ricardo Estrada – CSU Monterey Bay

Graduate Mentor: Saurabh Amin, Blaine Nelson and Suzanna Schmeelk, Faculty Mentor: Prof. Shankar Sastry, PhD.

Introduction

This project focuses on the usage of DETER to emulate routing and traffic associated with the Abilene network topology (Internet2) in order to determine the effects of an inside DDoS attack on SCADA systems. The Abilene architecture is simulated at a smaller scale without massive traffic actually being observed. Our critical infrastructure component in this research consists of a power plant and controller infrastructure that will be sending data back and forth across the network. This project was divided across several groups, each responsible for one of the following areas: infrastructure or software development and attack generation. Goal is to conduct a DDoS attack on the Abilene network and measure the effectiveness of the DDoS attacks.

Method

DDoS attack exhausts a victims resources to make it unavailable to its intended users. A common method is to saturate the victims machine with large volumes of traffic, traffic is generated from previously infected machines, such that it cannot respond to legitimate traffic. The methods used to create our DDoS attack on the Abilene network consisted of a series of steps (below). Each step required research and understanding of how to utilize that tool. Each tool played a role in developing a component that attributed to the goal of the project.

Figure 1: DETER is used to create an NS file with a basic topology layout.

Figure 2: Modifications are made to the NS file with TCL scripting.
Modifications range from:
- Addition of nodes & their O.S.
- Set links for nodes
- Execution of scripts
- Automation of events
- Setting of routing protocol

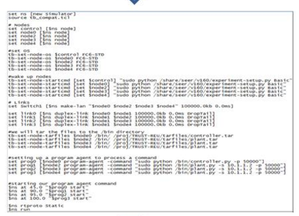


Figure 3: The NS file, which holds our experiment, is swapped in (emulated) to the DETER network.

Figure 4: Tools used to conduct the experiments.
- SSH secure shell (left image)
- TCPDump – Capture traffic (Also seen in the SSH secure shell screen).
- SEER – Used to conduct experiments via GUI (Right image).

Results

The purpose of our experiment was to conduct DDoS attacks on the Abilene network. Our attacks were designed to cause instability in the communication link between the plant and controller, ultimately leading to the failure of the plant. Below are the end results of our cut link script, TCP rampup and flood link attacks.

Figure 6: SEER displaying our swapped in experiment with normal traffic
- Upper Left corner: Controller returning values to plant
- Upper Right corner: Plant sending values to controller
- Bottom half: Other plants sending data across the network

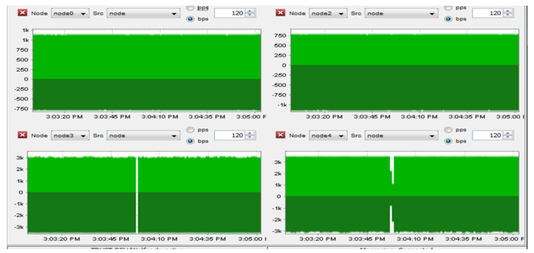


Figure 7: Cut link attack
- **Cut link attack immediately severs the link between controller and plant.**
- **The plant can no longer receive values to maintain stability.**
- **Plant crashes immediately when the link is cut.**

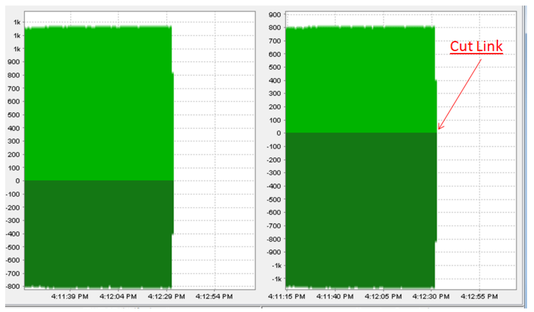


Figure 8: Flood link attack
- **Both attackers send 80Mb each of data to plant (victim).**
- **Link between plant and controller can only handle 100MB.**
- **Router buffer overflows and starts dropping packets**
- **Controller no longer receives the values from plant.**
- **The plants packets are dropped and plant becomes unstable.**
- **Plant crashes within 11 seconds (average) from the time that the attack commences.**

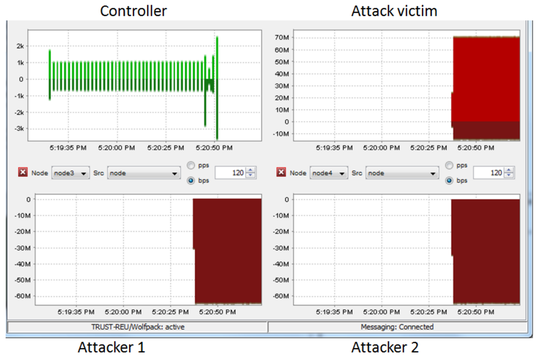
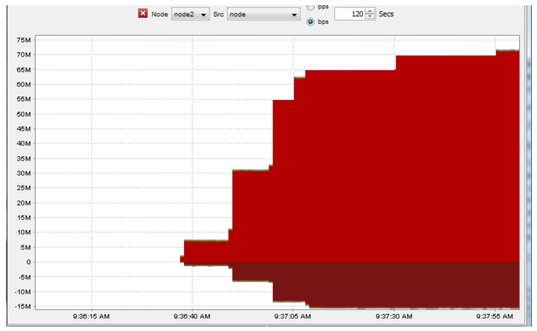


Figure 9: TCP rampup attack
- **This attack consists of a steady increase in attack traffic to our victim over time.**
- **The attack traffic begins to fill up the bandwidth slowly cutting off the plant communication from the controller.**
- **The link bandwidth (over time) will not be able to handle the increase of traffic.**
- **Overflow will occur and packet loss soon after.**
- **The plant will lose connection to the server and crash.**



Conclusion

The goal of a distributed denial of service attack is to exhaust the victim's resources. A successful DDoS attack can deny a service to the victim and its hosts by consuming the network bandwidth or exhausting the computing power. We achieved our DDoS attack by exhausting the link bandwidth and overflowing the buffer, thus leading to the failure of the plant. Below are some key notes learned during this research experience.

- A successful DDoS attack can cause serious damage to critical infrastructure components.
- The Abilene topology we used did not have any forms of security.
- There are far more sophisticated methods designed to penetrate the network and find weaknesses in SCADA systems that have security features implemented.
- Further research should be addressed to ensure that these systems are secure and able to deal with these types of threats.

Future research

My recommendation for future research would be to conduct a DDoS attack from outside the network. This would require further research in finding methods to accomplish the following goals:

- A method for scanning for vulnerable nodes.
- Method for propagating the malicious code to those nodes.
- Selecting the right DDoS attack on the network.

The goal of this approach is to give the researcher a better understanding of how much technical understanding goes into carrying out a sophisticated attack. This will allow the researcher to have a security approach when implementing security on the Abilene network. The researcher can then implement security features on the Abilene network and test his DDoS techniques to find vulnerabilities on those security features.

Acknowledgements

This work is supported by the National Science Foundation Under Award number CFF-0424422, via the Department of Electrical Engineering and Computer Sciences, College of Engineering located in Cory Hall at the University of California Berkeley. I would like to thank the Team for Research in Ubiquitous Secure Technology (TRUST), Dr. Kristen Gates, Larry Rohrbough, Ted Faber, Jelena Mirkovic, the DETERlab team. Additionally, I would like to thank my mentors: Suzanna Schmeelk, Blaine Nelson, and Saurabh Amin. Special thanks also to my groupmates: Katherine Gabales – Chico State University and Kyle Marlin – Youngstown State University.