Apr 20th, 1:00 PM - 3:00 PM

Watergate

Aidan Satterwhite

Nick D'Angelo

Watergate - Ethical Hacking PLCs

Aidan Satterwhite & Nick D'Angelo
Dr. Frances Grodzinsky & Professor Sajal Bhatia
Sacred Heart University - Computer Science

Introduction

We believe that running penetration testing on Industrial Control Systems will give us knowledge on the vulnerabilities that exist in resource plants across the globe. We believe that we will be able to attack and compromise a SCADA (Supervisory Control and Data Acquisition) system within minutes and take control over the requests sent and received by the device. We believe that attacking a Programmable Logic Controller using the Ettercap suite will be more successful than using Ettercap in a virtual environment on virtual machines.

Materials

1x Laptop computer
- GTX 1060 6gb
- i7 7700HQ 2.2ghz
- 16GB RAM

3x Debian virtual machines
- Two act as Client/Server
- One acts as attacker

1x Ettercap
- Used to run attacks

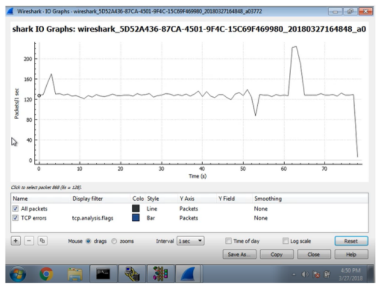
1x Allan-Bradley PLC

1x RSLinx
- Acted as PLC server

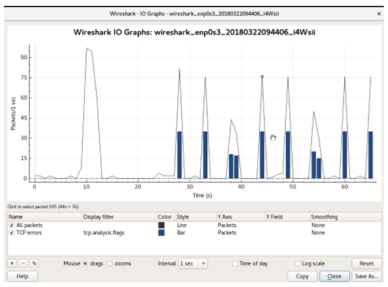
Terminology

DoS - denial of service attack. In this instance, we flooded the server with SYN and ACK packets so that a client/server interaction could not be made.
MiTM - man-in-the-middle attack. Sends falsified ARP messages to link attacker IP to victim IPs. All information will pass through the attacker.
Pulse - pulse attack. DoS attack carried out in timed intervals.
PLC - programmable logic controller. Controls and manages industrial equipment.
SCADA - supervisory control and data acquisition. Systems that monitor and control a process.
VM - virtual machine. Separate operating system running on host machine.

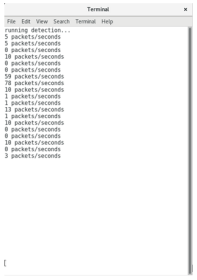
Screenshots



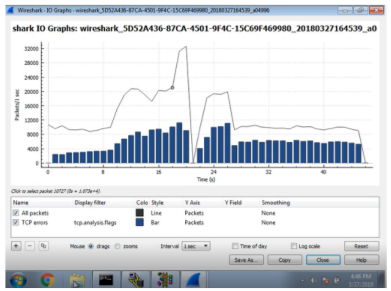
PLC Man-in-the-Middle.



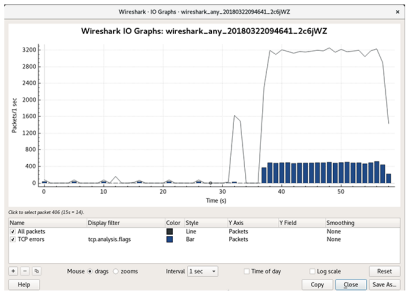
Virtual Man-in-the-Middle



MiTM Detection.

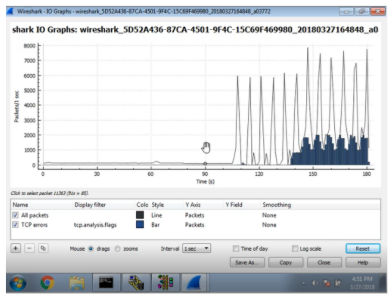


PLC Denial of Service.

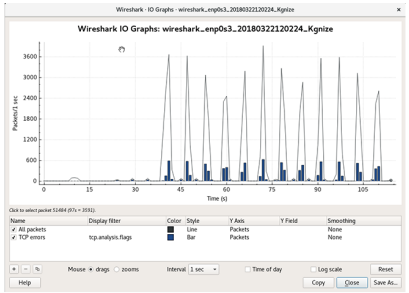


Virtual Denial of Service.

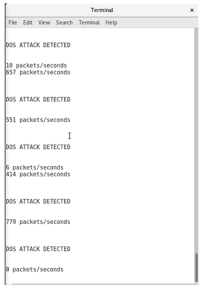
DoS Detection.



PLC Pulse attack.



Virtual Pulse attack.



Pulse Detection.

Conclusion

Our hypothesis is shown to be true through the research and data we were able to analyze while conducting these attacks on a Programmable Logic Controller. Creating the attacks was easier on the virtual machines, however, the effect that our 4 penetration tests had on the machines was quite astounding. When running anyone of our attacks on either system the attacking suite, Ettercap floods the system with acknowledge and Synchronize packets. These packets flood the system to prevent standard requests from being processed. Our hypothesis was correct, we were able to bring down the PLC within a minute and the amount of packets sent during each attack was significantly higher than the amount of packets sent during the virtual lab. (Specifically 13 times the amount of packets) We were able to identify the vulnerabilities present in these SCADA systems such as: no user verification, no filters to prevent SYN and ACK floods, and no prevention or detection for such attacks.

Works Cited

Incapsula.com, www.incapsula.com/web-application-security/man-in-the-middle-mitm.html.
"Man in the Middle (MITM) Attack." Veracode, 2017, www.veracode.com/security/man-middle-attack.
Occupytheweb, et al. "Hack Like a Pro: How to Conduct a Simple Man-in-the-Middle Attack." WonderHowTo, WonderHowTo, 2014, null-byte.wonderhow-to.com/how-to/hack-like-pro-conduct-simple-man-middle-attack-0147291/.
Electric, Schneider. "SCADA Systems." Telemetry & Remote SCADA Solutions, Mar. 2012, pp. 1–13.
Vosough, Sadegh, and Amir Vosough. "PLC and It's Applications." INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY SCIENCES AND ENGINEERING, vol. 2, no. 8, Nov. 2011, pp. 1–6., www.ijmse.org/Volume2/Issue8/paper9.pdf.
"What Is a PLC?" AMCI : Advanced Micro Controls Inc :: What Is a PLC?, www.amci.com/industrial-automation-resources/plc-automation-tutorials/what-plc/.

Published by Aidan Satterwhite and Nick D'Angelo: Watergate - Ethical Hacking PLCs, 2018