Enhancing Visibility in Industrial Control Networks using Bro IDS

Aya Khalafalla, Jeffery Wang, John Barberis, Ola Jamalallail, Roaa Mahdi

Sponsor: Bechtel, Inc.

Subject Matter Experts: Andrew Hunt, Tom Wallis

BACKGROUND

Problem Statement:

- **Industrial control system (ICS)** infrastructures are increasingly vulnerable to cyber security attacks
- Can we adapt technologies successful in the IT world to ICS networks?
- Enhancing visibility will help detect and prevent **cyber security threats** in ICS networks

Project Objective:

- Build a protocol parser in **Bro IDS** to capture and parse **OPC DA** traffic
- Generate log files that contains important aspects of said traffic
- Feed log files to **ELK stack** and visualize them using **Kibana**

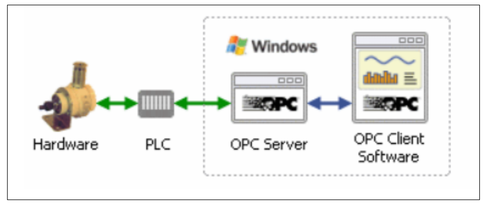

Figure 1: Communication in OPC Environment
Image Source: https://opcdatahub.com/WhatIsOPC.html

TOOLS & CONCEPTS

- An **intrusion detection system (IDS)** is a piece of software that can monitor network traffic and alert users if any malicious activity has occurred
- **Bro IDS** is an open source network traffic analyzer. It allows users to develop scripts to parse custom network protocols. Our group is utilizing Bro's scripting engine to parse OPC DA network traffic
- **OPC Data Access (OPC DA)** is a group of client-server standards that provide specifications for communicating real-time data from data acquisition devices such as Programmable Logic Controllers (PLCs) to display and interface devices like Human-Machine Interfaces (HMI)
- The **ELK stack** is a package of open source tools that can utilized for visual analysis
  - Elasticsearch is a search and analytics engine
  - Logstash ingests data from Bro and sends it to Elasticsearch
  - Kibana lets users visualize data with charts and graphs in Elasticsearch

METHOD

1. Install and configure **Bro and ELK** per best practices
2. Create a **data pipeline** from Bro to ELK
3. Install the new **Bro module** and test for functionality
4. Configure visualization dashboard per SMEs' suggestion
5. Use an **agile software development process** to modify the parser and dashboard as necessary to meet ongoing requirements

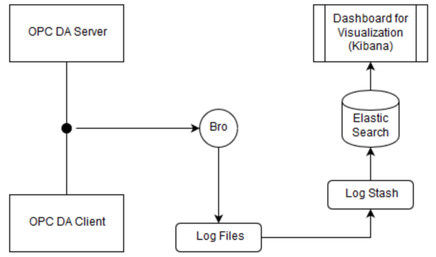

Figure 2: Implementation

RESULTS

- The system successfully parses the following pieces of OPC DA network traffic using Bro IDS and displays it in a dashboard utilizing the ELK stack:
  - Source and destination IP address
  - Session duration
  - Session number
  - Number of bytes within the sent and received packets
  - Ongoing connections between devices on the network
  - Network users mapped to network nodes

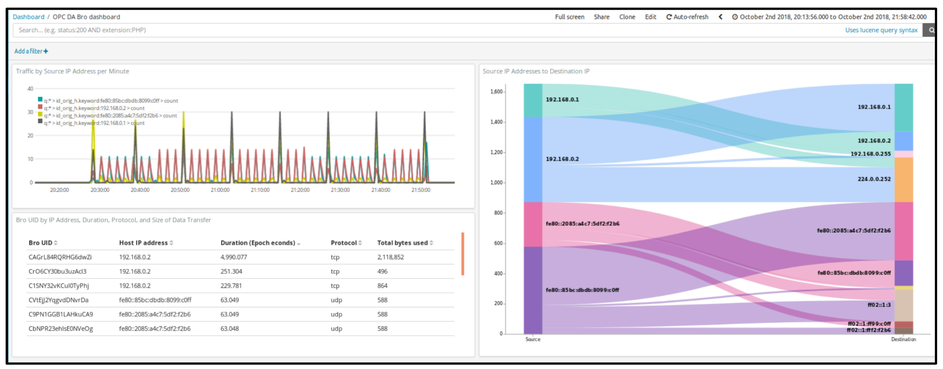

Figure 3: Kibana Dashboard

From left to right: A line graph showing network activity by host ip address, a table showing the address, duration, protocol, and size associated with each UID, and a Sankey diagram showing the distribution of traffic across the network

RESULTS – CONT.

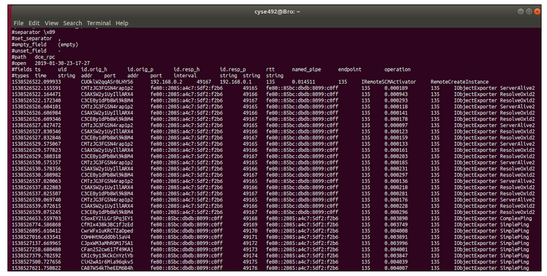

Figure 4: Bro's raw output of OPC DA network traffic

The parser is capturing an important aspect of OPC DA traffic (e.g. IPs, ports, protocols, operations, users, etc.) and creates log files which will be used for creating dashboards

CONCLUSION

- Presented a viable solution to **enhance visibility in ICS networks**
- Created a **custom module** for the open source **Bro IDS** to operate within critical infrastructure network environments
- **Highly customizable** module that can be modified to fit the needs of systems
- The **visualization dashboard** can used to establish traffic baselines and detect anomalies
- Future work includes developing a **machine learning** agent with **Apache Spark** to enhance network monitoring using the custom Bro module and ELK visualizations

ACKNOWLEDGEMENTS

We are indebted to our sponsor Bechtel and their SMEs Mr. Andrew Hunt, Tom Wallis, Ovi Hossain, Nikolas Upanavage, Amand Benjamin for their guidance and unfailing encouragement during this project. We our also indebted to our mentor Rock Sabetto and our professor Gino Manzo of George Mason University for their help, guidance, and feedback which helped shape this project. Finally, we owe thanks to George Mason University for providing access to journals and publications and Matrikon and the OPC Foundation for their published documentation and research on OPC technologies.

REFERENCES

[1]R. Sommin, "Bro: An Open Source Network Intrusion Detection System," tech.

[2] The Zeek Project Revision, "Bro Plugins DCE_RPC," base/bif/plugins/Bro_DCE_RPC.events.bif.bro - Zeek User Manual v2.6.1. unpublished.

[3] OPC Foundation, "Data Access Automation Interface Standard Version 2.02," February 1999.

[4] J. Weber and W. Worrall, "A Beginner's Guide to OPC," unpublished.

[5] "DCE/RPC," DCE/RPC - The Wireshark Wiki. unpublished

May 2nd, 2019