Diateam: SCAD@COPS
A Hybrid Network Intrusion Detection System

Lisa MALIPHOL

July 2015

Contents

Introduction

Project background

Problem definition

Paper organization

SCADA Systems

Terms

ICS

SCADA

PLC

RTU

HMI

Traffic characterization

Protocols

TCP

MODBUS/TCP

Common Attacks on SCADA

Command Injection

Response Injection

Denial of Service

Intrusion Detection Systems

Host IDS

Network IDS

Signature-based

Anomaly-based

Techniques of Network Intrusion Detection

Statistical

Machine Learning

Data Mining

Captured network packets are saved in the pcap file format and can be dissected and parsed by Wireshark in order to analyze its contents. An important aspect of Wireshark is that of its passive/monitoring nature and so does not send, manipulate, or modify the data passing over the network.

An initial packet capture file was created over simulated network traffic using Wireshark. Using its export facilities, various files were created for further analysis, with information such as TCP endpoints, conversations, etc.

TShark[2]

Another tool from the Wireshark suite is the command-line tool similar to tcpdump is tshark, a network protocol analyzer. In addition to capturing packet data over a live network, it is also capable of analyzing packets from an existing capture file. TShark was used to parse out various pertinent variables pertaining to the Modbus/TCP application protocol enclosed in the packet data.

UNIX Utilities

In order to further parse and transform the data, the UNIX utility tool sed, which supports the use of regular expressions, was also used.

R - Statistical Tool[3]

R is an Open Source programming language and environment used for statistical computing and graphics. Initially developed by John Chambers at Bell Labs as the S language in 1993, R was created as a freely available version under the GNU project by Ross Ihaka and Robert Gentleman at the University of Auckland, New Zealand.

Maintained by the R Development Core Team and with an active and growing community, it provides various statistical and graphical creation capabilities available under most operating systems, and is extensible with numerous packages available.

[2] https://www.wireshark.org/docs/man-pages/tshark.html

[3] http://www.r-project.org/

C++

SQLite3

MongoDB/MySQL

Data Source

Exploratory Data Analysis

Statistical Measures/Features

Architecture

Process (Figure 1)

- Step 1: Data Acquisition During Normal Activity - From the IDS appliance, sniff the network traffic, extract and store data in a database.
- Step 2: Statistical Analysis
  - 2.1 - Process data - Perform any transformation, filtering and data cleansing necessary.
  - 2.2 - Calculate and determine statistical measures.
  - 2.3 - Configure appliance with statistical parameters.
- Step 3: Detection Mode - Appliance is set to detection mode.

Technical Architecture (Figure 2)

Figure 1 - Process

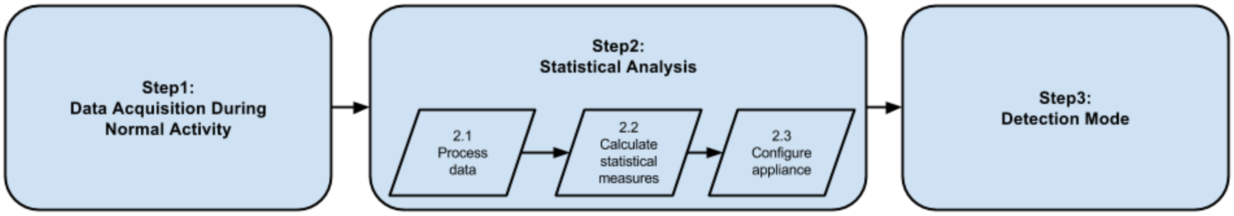
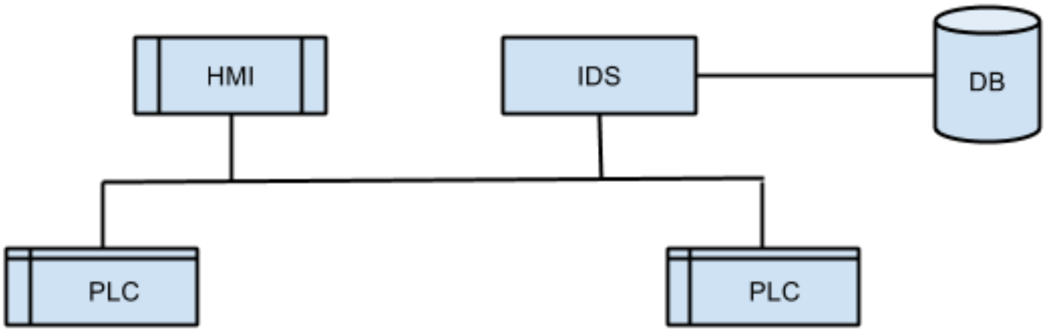


Figure 2 - Technical Architecture



Implementation

Testing/Evaluation

Conclusion/Future Work

Glossary

Bibliography

Appendices