

Diateam: SCAD@COPS

A Hybrid Network Intrusion Detection System

Lisa MALIPHOL

July 2015

- 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
- Tools
 - Wireshark

- TShark
- UNIX utilities - sed, awk, bash, etc.
- R
- C++
- SQLite3/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

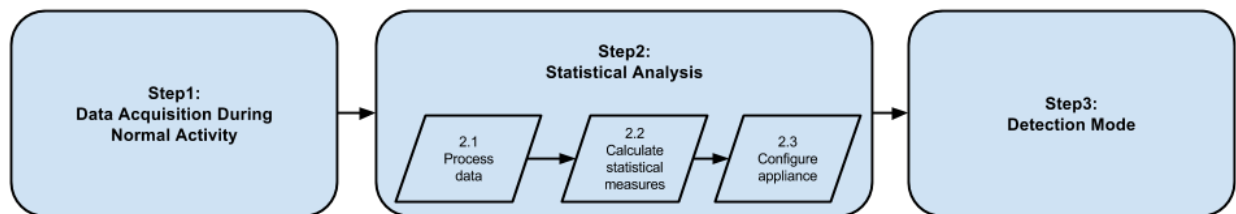
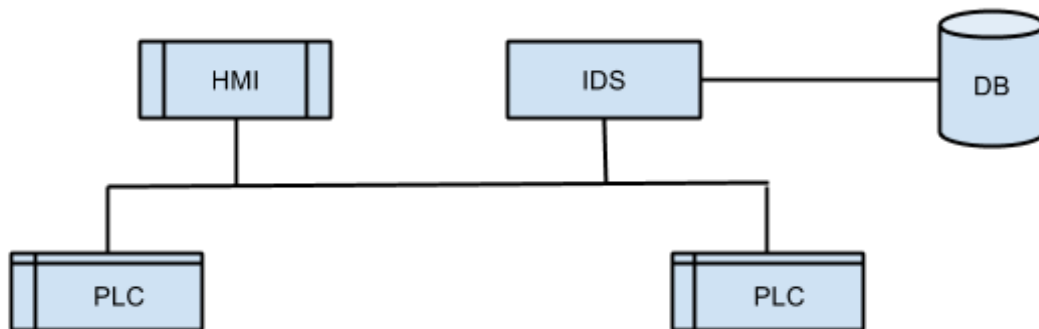


Figure 2 - Technical Architecture



- Implementation
- Testing/Evaluation
- Conclusion/Future Work
- Bibliography
- Appendices