Improving SCADA Security using IDS and MikroTIK

Albert Sagala and Rudy Pardosi
Del Institute of Technology, Toba Samosir, North Sumatera, Indonesia.
albert@del.ac.id

Abstract—Industries have realized that SCADA System was built without considering the security aspect. It was believed that there are no attacks to the scada plant. Unfortunately, in this era, SCADA network needs to be connected to the Internet to increase its performance. In this case, the protection of Supervisory Control and Data Acquisition (SCADA) is needed against cyber-attacks. Much research has seen the big lost as cyber-attack happens at critical infrastructure. In this research, we simulated a test bed environment of SCADA system to monitor and mitigate the attack as well as give fast response report to the operator. We used Network Based Intrusion Detection System using SNORT rule, which is integrated with MikroTik for Deep Packet Inspection (DPI). This system inspects all traffic data going through the scada system. Results from the experiment show that the testbed environment was able to detect attacks effectively and efficiently.

Index Terms—DDoS Attack; MikroTik Router; SNORT, SCADA Security.

I. INTRODUCTION

Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) is built in isolated system to secure the plant [1], [2], [8]. However, the system for the next generation of SCADA needs to be accessed from anywhere using the internet connection. This fact can be seen with the emerging of Internet of Things (IoT) technology. Things are connected to and communicate with each other to do the job as provided by the command. SCADA integrated with the office network makes it more susceptible to be attacked by a hacker [10], [14]. We know that the advanced hacking technique is evolving to crack the system and there is a need to anticipate this issue in the SCADA plant.

To enhance the SCADA security, while getting it connected to the Internet, we integrated the technology of MikroTik IDS (Intrusion Detection System) using CALEA Configuration, iptables firewall, and SNORBY interface, which can be used as a new tool to monitor traffic data coming into the controller. For this purpose, we have made some changes to the previous SCADA topology. Researches that use IDS system to enhance the security have already been conducted by many researcher from many universities [4],[6],[13].

Changes in the topology are needed to integrate Network Based IDS (NIDS) and MikroTik. These topology changes are based on the research that has already ben conducted to secure the scada system [9],[11],[12]. Trafr packet sniffing was installed on SNORT server. MikroTik helps the SNORT server, detects or monitors the network traffic passively. We installed SNORBY as a graphical user interface (GUI) for operator’s easy usage.

Our contribution in this paper is to give a solution to improve scada security by integrating SNORT IDS Sensor and Packet Inspection using MikroTik.

The rest of the paper is organized as follows: Section II discusses the related work of our research and the experimental environment. Section III explains the network topology of our system in more detail. Section IV elaborates the result and an analysis, and we conclude in Section V.

II. EXPERIMENTAL

The SCADA security can be improved using many methods. Many researches were conducted to develop the design of a testbed environment to make an easy testing of the scada [9],[11]. In this research, the modbus protocol [15] used for communication between the HMI and the controller is excluded to enhance the security. Our previous research has already proposed a method to enhance the security using the modbus protocol.

On [5], Raspberry PI was used as a gateway to encrypt and decrypt the communication from HMI to the controller. While, in [3], in order to improve cyber-security of SCADA networks, research presented a rule-based Intrusion Detection System (IDS) using a Deep Packet Inspection (DPI) method, which includes signature-based and model-based approaches tailored for SCADA systems. The proposed signature-based rules can accurately detect several known suspicious or malicious attacks.

In our research, the environment needs to be prepared well for anticipating internal or external attacker. These section will explore the environment proposed as a method to increase the SCADA security.

A. Testbed Environment SCADA Security

The experiment was conducted on a SCADA testbed designed as shown in Figure 1. We extended the network using a MikroTik device to increase the plant. In the attack scenario, an adversary may compromise a system on the workstation network typically connected to the internet. From there, the attacker gains access to the MikroTik router, then infects the SCADA Operator, and finally performs reconnaissance, before continuing with the ethical-hacking steps.

As depicted in Figure 2, we put the sensor using Inline mode Sensor [7], where it must be placed in line with the firewall and other network security devices to monitor actual network traffic. Table 1 shows the hardware and software specification for our testbed.
In this part, we make the general DDOS rules of SNORT, which can detect TCP SYN flood attack from any port launched by the attacker. When the SNORT server detects the DDoS attack, it will send a trigger to the operator.

### SNORT Rules

In this part, we make a general DDOS rules of SNORT, which can detect TCP SYN flood attack from any port launched by the attacker. When the SNORT server detects the DDoS attack, it will send a trigger to the operator.

#### Table 1

<table>
<thead>
<tr>
<th>Device Name</th>
<th>IP Address</th>
<th>Operating System</th>
<th>Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCADA Operator</td>
<td>192.168.10.2</td>
<td>Windows XP</td>
<td>Client</td>
</tr>
<tr>
<td>Attacker</td>
<td>192.168.10.106</td>
<td>Kali Linux</td>
<td>Client</td>
</tr>
<tr>
<td>Snort Sensor</td>
<td>169.254.213.6</td>
<td>Ubuntu</td>
<td>Sensor</td>
</tr>
<tr>
<td>Database Snort Server</td>
<td>169.254.213.5</td>
<td>Security Onion</td>
<td>Server</td>
</tr>
<tr>
<td>Water Plant</td>
<td>169.254.213.2</td>
<td>Controller</td>
<td>Plant</td>
</tr>
<tr>
<td>Router Mikrotik</td>
<td>169.254.213.1</td>
<td>RouterOS</td>
<td>Access Point</td>
</tr>
</tbody>
</table>

### D. Packet Filtering on Ubuntu

Next, we set the IPTables packet filter so that it can accept the forwarding packet from MikroTIK on port 37008.

```
root@ubuntu:~# iptables -L INPUT 50 -p udp -dport 37008 -j ACCEPT
```

**“Accept sniffed traffic from ROUTERBOARD”**

### E. CALEA Client Configuration

Communications Assistance for Law Enforcement Act (CALEA) requires the routers in the USA to have the ability to intercept and log the network traffic. Currently, RouterOS provides this facility by means of firewall rules. RouterOS can also function as a data retention server if the additional CALEA package is installed. The first step involves downloading the TRAFR archive file. The program will be used to encapsulate the packet sent by CALEA MikroTIK. After that, we extract the archive file and then, we start the TRAFR program to test the receiving packet from CALEA.

To activate TRAFR with SNORT, this command is entered:

```
root@ubuntu:~# /trafr -s | snort -r
```

If the output messages that confirm the settings and rules are loaded successfully, the operator needs to wait few minutes before stopping the process with Control + C. If the statistics show a number different from 0, it means that Snort works well with Trafr. Snort must start as a process that cannot be demonized because of Trafr data injection. This means that the operator needs to run it directly on a console or use a tool like "screen" and then run Snort with Trafr. The last line instructs Snort to use a specified configuration and log path. All of the traffic that go through the router for a specified source/destination addresses was intercepted and sent to CALEA Server (sniff-target).

```
[admin@Mikrotik] > ip firewall calea print
Flags: X – disabled , I – invalid , D – dynamic

[admin@Mikrotik] > ip firewall calea add action=sniff chain=forward sniff-target=169.254.213.6 sniff-target-port=37008 sniff-id=100.
```

Set up the Streaming Configuration for MikroTIK to accept the entire data stream on Packet Sniffer Settings.
III. RESULTS AND DISCUSSION

We conducted testing on the environment that we prepared. The HMI can monitor and control the plant. We added the Intruder to assess the topology proposed.

![MikroTik Settings for Packet Sniffer](image1.png)

**Figure 3: MikroTik Settings for Packet Sniffer**

The steps taken for the implementation are in the configuration of SNORT and MikroTIK configuration, and setting the Network Topology. We used TRAFR for tcpdump translate from the MikroTIK to SNORT server. Installation and configuration were done using Ubuntu 12.04 TLS operating system server. DDoS attack was trained using HPING3 tools, in which the traffic was sniffed by SNORT server to forward to MikroTIK.

### A. Testing DDoS Attack on SCADA

The attack was conducted by sending a TCP SYN flood packet with a header size with 120 bytes of data on its protocol_header. Data will be sent up to 10000 of data in windows 64 bit ID. Protocol attacked is an active port of SCADA controller, in this case is the port 80. If the intrusion that goes across the MikroTIk is detected, then it will send the message to the server monitoring which gives alert message to the operator.

### B. Graphical User Interface BASE and ACID

Analyzing the traffic that comes from another system is used by BASE (Basic Analysis and Security Engine) and ACID (Analysis Console for Intrusion Databases). They have a web interface to see the graphical statistic of the traffic. We can set and install the application on the sensor server in Ubuntu 10.04 Lucid environment. The interface is as shown in Figure 5 and 6.

![IDS Phase Snort on SCADA System](image2.png)

**Figure 4: IDS Phase Snort on SCADA System**

![Figure 5: BASE Interface that access from the browser](image3.png)

**Figure 5: BASE Interface that access from the browser**

![Figure 6: BASE Interface that access from the browser](image4.png)

**Figure 6: BASE Interface that access from the browser**

### C. Alert to Operator From SNORBY

SNORBY has event report and history for the traffic analyzer. SNORBY can separate three severity events of the event data traffic on the network. The report will be shown on the dashboard as can be seen in Figure 7.

![Graphical User Interface (GUI) On Attack Detection Using SNORBY](image5.png)

**Figure 7: Graphical User Interface (GUI) On Attack Detection Using SNORBY**

If we want to see the detail of the event, we click the Severity Interface, and the detail of the event will be shown as presented in Figure 8.

![Medium Thread for Alert on Event Log](image6.png)

**Figure 8: Medium Thread for Alert on Event Log**
The most important event was High Severity event, as shown in Figure 9, these categories must be highly concerned because it is categorized for a high risk attack.

Figure 9: High Thread for Alert on Event Log

For every detail event, it has more specific information as shown in Figure 10.

Figure 10: Event Detail on SNORBY Detection Log

The proposed integrated method will give rich information to the operator, so the anomaly traffic can be detected early and the data have more detailed information from the MikroTik or SNORT Server. In MikroTik, MRTG was activated to see live traffic.

Figure 11: MikroTik Graph For Data Traffic in SCADA Network

Figure 11 shows the graphic when DDoS attack was executed. In a short period of time, the traffic increased very fast and slower after the DDoS stopped. The attack was used by hping3 tools. As shown in Figure 12, the alert was sent to the operator.

IV. CONCLUSION

A DDoS-like attack was simulated on SCADA system and the effects of attacks were observed by implementing the IDS and MikroTik. While the effects of the total communication disruption might have been estimated and mitigated by using IDS SNORT, DDoS attack can be detected if the router in sniffing mode and SNORT can classify the packet that came in. In such a case, a simulation is the best way to estimate the detection of these IDS. The difference of this method with another method is that the IDS is combined with MikroTik. The iptables only allows the traffic from MikroTik, and IDS effectively detects the traffic to SCADA system.

In our simulation, we used a general rule attack, which is DDoS. Hacker can modify the technique and attack to avoid the firewall or Intrusion Detection System; hence it still needs further research to enrich the rule tested.

ACKNOWLEDGMENT

We are grateful for the support from Lab Cyber Security Research Centre of Del Institute of Technology for using SCADA plant to make this experiment feasible.

REFERENCES


