A Burst-based Whitelist Model for DNP3 Communication in the SCADA System

Jeong-Han Yun[1], Sung-Ho Jeon[1], Kyoung-Ho Kim[1], and Woo-Nyon Kim[1]

[1]The Attached Institute of ETRI,
P.O.Box 1, Yuseong, Daejeon, 305-600, Korea
{dolgam,sdeva,lovekgh,wnkim}@ensec.re.kr

Abstract. The Distributed Network Protocol Version 3 (DNP3) protocol is widely used in SCADA systems as a means of communicating observed sensor state information back to a control center. In general, utilities that use the DNP3 protocol repeat their own limited operations, so a whitelist-based approach is clearly suitable for network intrusion detection. In this paper, we propose a burst-based whitelist model for utilities using the DNP3 protocol. A *burst* is a group of consecutive packets with shorter inter-arriving time than packets arriving before or after the burst of packets. When utilities communicate on the DNP3 protocol, one transaction at the application-level is mapped to one burst. We applied our whitelist model to DNP3 network traffic of a real-world SCADA system, and we analyzed how whitelist rules based on the model can be used to detect cyber-attacks.

Keywords: DNP3, SCADA, network anomaly detection, whitelist, burst

1 Introduction

The cyber-attack is a new and essential weapon of modern warfare. Control systems are targets of the highest priority for cyber terrorists, leading many countries to reinforce their investment in the area of cyber security.

The control system is managed by the Supervisory Control and Data Acquisition (SCADA) system,which is used to monitor and control plant or equipment in the telecommunications, water and waste control, and energy industries among others. Distributed Network Protocol Version 3 (DNP3) is used by SCADA systems to communicate between the master host and the outstation units.

A *burst* is a group of consecutive packets whose inter-packet arrival time is shorter than the threshold of inter-packet arrival time[1].When utilities communicate on the DNP3 protocol, one transaction at the application-level is mapped to one burst. In this paper, we are proposing a new whitelist model for utilities using the DNP3 protocol. The major difference of our whitelist model from previous research[2–4] is burst-based approach. Using this approach, we can use application-level characteristics without such deep packet inspection (DPI) as packet recombination. To confirm the validity of the model proposed herein, we extracted whitelist rules for the collected network traffic based on the model and analyzed how the whitelist rules can be used to detect cyber-attacks.

2 A Burst-based Whitelist Model

When a transaction such as status monitoring using a `read-response` is executed on the DNP3 protocol, the transaction consists of several packets including 'data packets' and 'acknowledge packets'. Each packet's size is determined by the DNP3 objects and the frame fragmentation rule of the DNP3 protocol. In general, the time interval between two transactions is greater than the time interval between two packets in a transaction. Therefore, the packets caused by one transaction constitute a burst.

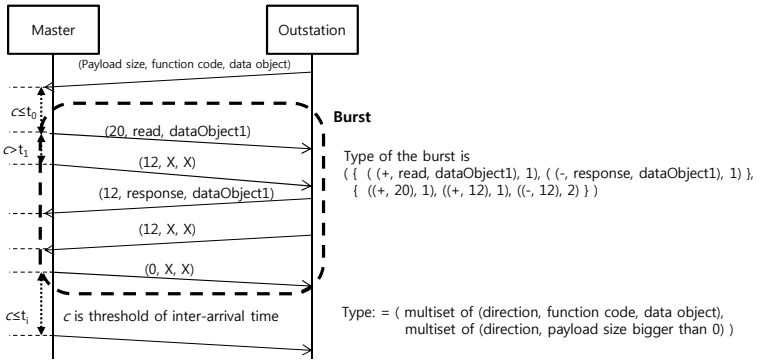

Fig. 1. An example of a burst and its type

We can extract several characteristics of a burst. In this paper, we define the type of burst as a 2-tuple (multiset[1] of (direction, function code, data object)) and (multiset of (direction, payload size bigger than 0)). The direction is + if a packet is sent from a master to an outstation, and the direction is - otherwise. Figure 1 shows an example of a burst and its type.

```
          Whitelist   :=   Set of Rule
               Rule   :=   (Master, Outstation, Bursts)
             Master   :=   (IP, Port)
         Outstation   :=   IP
         BurstTypes   :=   Set of BurstType
          BurstType   :=   (MControls, MPayload1)
          MControls   :=   Multiset of Control
          MPayload1   :=   Multiset of (Direction, pay1)
            Control   :=   (Direction, function_code, data_object)
          Direction   :=   + | -
ThresholdInterval     :=   time
```

Fig. 2. Whitelist model

[1] The number of times an element belongs to the multiset is the multiplicity of that member. For example, a set {a, a, b} is represented by {(a, 2), (b, 1)} in the multiset.

In this paper, we defined our whitelist mode for the master-outstations, as shown in Figure 2. Each rule represents the allowed types of bursts between a master and an outstation. A `Master` is distinguished by IP and service port, while an `Outstation` is distinguished by IP. `ThresholdTime` is the threshold of the inter-packet arrival time. (direction, function code, data object) is an authorized function between a master and an outstation. The multiset of (direction, function code, data object) shows the executed functions in a transaction. The multiset of (direction, payload size bigger than 0) shows the packet fragmentation of a transaction. We do not consider packets without a payload because packets without a payload are generated by the TCP/IP protocol rather than the DNP3 protocol. We use multiset of the information instead of a sequence because the time order of packets may often be changed by trivial causes, such as the switch port mirroring condition.

3 Security Analysis based on Attack Models

During ten-day period, we collected the network traffic in a real-world SCADA system. It includes one master and 42 outstation using the DNP3 protocol. The DNP3 network traffic volume in that ten-day period amounted to 887MB.

We introduce how to detect three attack models which can occur in SCADA system and which cannot be detected using the previous research.

3.1 Applying Our Whitelist Model to Real Network Traffic

In our experiment we chose *0.2 seconds* for the `ThresholdTime` of the collected network traffic. In applying this whitelist model to the network traffic collected in seven days, a pair of a master and an outstation used eleven different types of bursts and four different (direction, function code, data object) on average. Each master-outstation pair has its own types of bursts.

To check the coverage the extracted rules, we extracted whitelist rules from last three days of network traffic. The extracted whitelist rules from seven days of network traffic include all the whitelist rules extracted from last three days of network traffic.

3.2 Abnormal Data Transfer

When a malware is propagated through network, a malware causes abnormal type of bursts. If a malware is attached to normal data, it causes bigger bursts than usual. Therefore, type of bursts can detect abnormal data transfer.

Cyber-attack using vulnerability is also a kind of abnormal data transfer such as buffer overflow and vulnerable commands. Digital Bond[2] provides attack traffic using twelve DNP3 vulnerabilities. In our experiment, our extracted whitelist rules detected all the attacks because the attack traffics make bursts that their types are not included in the whitelist rules.

3.3 Traffic Flooding Attack

This attack causes to the sending of too many packets to a victim, and it causes that many packets are arrived in a short time. It is the most typical DoS attack but threatening attack. The dense packet interval time causes bigger bursts than usual, and this attack can be detected using our whitelist model.

In our experiment, we succeeded to detect two methods of traffic flooding attack. One is to try many meaningless operations; e.g., SYN flooding attack. We generated the attack traffic by an attack simulation system[2]. The other is to try many allowed operations such as monitoring data requests. To simulate this attack, we modified packet interval times of the collected network traffic shorter than usual[3].

3.4 Man-in-the-Middle Attack

Previous work does not reflect the time interval aspect. but our whitelist model strictly specifies the interval time limit of packets so as to divide bursts. A 'Man-in-the-Middle (MITM) attack' slows down packet delivery time due to the relay of attacker between victims. Delayed packet arrival time makes unusual type of bursts, such as consisting of fewer packets compared with the bursts of the whitelist rules. Thus, our whitelist model, which considers the time interval, can detect MITM attacks.

4 Conclusion

We have proposed a burst-based whitelist model for DNP3 network traffic between a master and an outstation. Our burst-based approach can represent the characteristics of application-level operations and inter-packet arrival time. To confirm the validity of our whitelist model, we extracted the whitelist rules of 42 working master-outstation pairs and analyzed how the rules can be used to detect cyber-attacks in a SCADA system.

References

1. Shakkottai, S., Brownlee, N. and Claffy, KC: A study of burstiness in tcp flows. Passive and Active Network Measurement, pp. 13–26, Springer, (2005)
2. Quickdraw SCADA IDS, `http://www.digitalbond.com/tools/quickdraw/`
3. Mander, T., Cheung, R., and Nabhani, F.: Power system DNP3 data object security using data sets. Computers and Security. vol. 29, no. 4, pp. 487–500. Springer, (2010)
4. Fovino, I.N., Carcano, A., De Lacheze Murel, T., Trombetta, A. and Masera, M.: Modbus/DNP3 state-based intrusion detection system. Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, pp. 729–736, IEEE, (2010)

[2] `http://www.breakingpointsystems.com/`

[3] Previous work based on authorization[3] cannot detect this attack because all the function codes and data objects are authorized.