공업조종체계에서 Snort를 리용한 침입검출의 한가지 방법

손일명, 손현진, 김명일

공업조종체계는 인민경제의 주체화, 현대화, 정보화, 과학화를 실현하는데서 매우 중요한 자리를 차지하고있다.

공업조종망의 보안요구는 전통적인 IT체계의 보안요구보다 훨씬 높으며 공업조종체계의 보안[1]은 여러가지 많은 문제점들을 가지고있다.

최근에 공업조종체계를 하나의 독립적인 체계로 보고 이 체계에 대한 보안체계를 독립적인 보안체계로 발전시켜나가고있다.

이러한 보안체계[1]들은 SCADA체계와 분산형조종체계(DCS : Distributed Control System)를 중요한 안전보호대상으로 취급하고있다.

공업조종체계는 초기에는 하나의 상대적으로 닫긴체계로 등장하였으나 최근에 인터네트기술, 통신기술, 대용량자료기술이 급속히 발전하고 이 기술이 공업조종령역에로 확장되면서 개방적인 체계로 되게 되였다. 그런것으로 하여 공업조종체계에 대한 해킹공격이 더욱 많아지고있으며 공업조종체계에 대한 정보보안을 실현하는 문제는 더욱 중요한 문제로 되고있다.

최근에 세계적범위에서의 공업조종체계에 대한 해킹공격사건들이 자주 발생하여 엄중한 후과를 초래하였다.

Stuxnet비루스공격사건, 여러 나라들의 전력공급망에 대한 해킹공격사건[2]들은 공업조종체계에 대한 보안을 고도로 중시할것을 요구한다.

론문에서는 정보체계들에 전통적으로 리용되던 Snort침입검출모형을 공업조종체계의 특성에 맞게 갱신하여 새로운 공업조종체계의 침입검출모형을 작성하고 갱신된 침입검출모형의 성능을 분석하였다.

1. 공업조종체계의 침입검출모형

침입검출체계(IDS : Intrusion Detection System)는 망 또는 체계보호를 위하여 망에서 악성공격행위를 검출하는 도구이다.

정보체계들에서 Snort를 리용한 침입검출모형의 구조[2]는 그림 1과 같다.

공업조종체계망이 개방적으로 되고있고 또 새로운 해킹공격수단들이 강화되면서 망파케트흐름속에는 막기 힘든 악성침입공격흐름이 들어갈수 있다.

그러나 정보체계의 전통적인 침입검출체계는 여러가지 망통신규약들에 대하여 설계된것이므로 공업조종체계에서 전문적으로 리용하는 통신규약에 대하여서는 효과적이지 못하다.

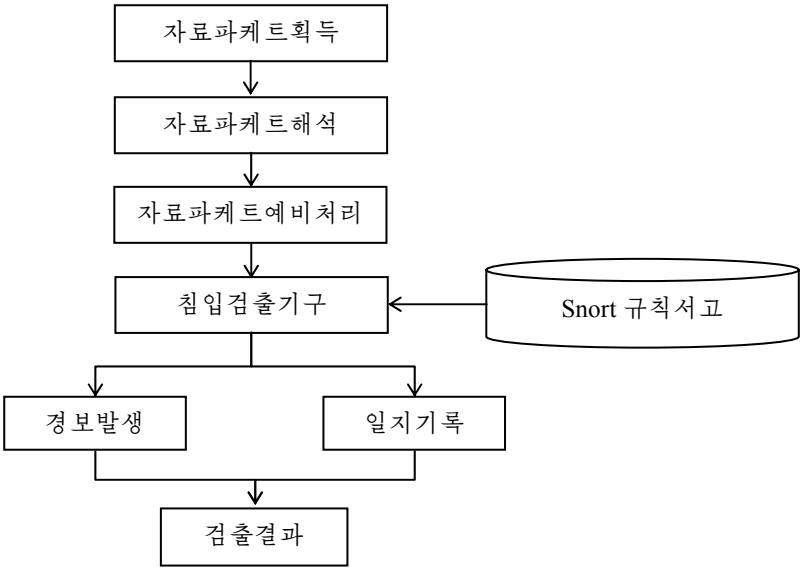

그림 1. 정보체계들에서 Snort를 리용한 침입검출모형의 구조

Snort는 사용에서 매우 유연하고 모듈화된 체계구조를 갖추고있는것으로 하여 침입검출체계를 확장할수 있다. 만일 공격자가 공업조종체계의 전용통신규약을 리용하여 공격하는 경우 Snort의 규칙서고에 이 류형의 자료파케트에 대한 처리를 진행할수 있는 규칙을 추가하여 효과적으로 침입검출을 진행할수 있다.

론문에서는 Snort침입검출체계를 공업조종체계에 적용할 때 여기에 공업조종체계의 전용통신규약에 대한 검출규칙생성부분을 추가하여 침입검출체계를 공업조종체계의 전문적인 침입검출체계로 만들었다.

그림 2에 공업조종체계의 특성에 맞게 갱신한 침입검출모형을 보여주었다.

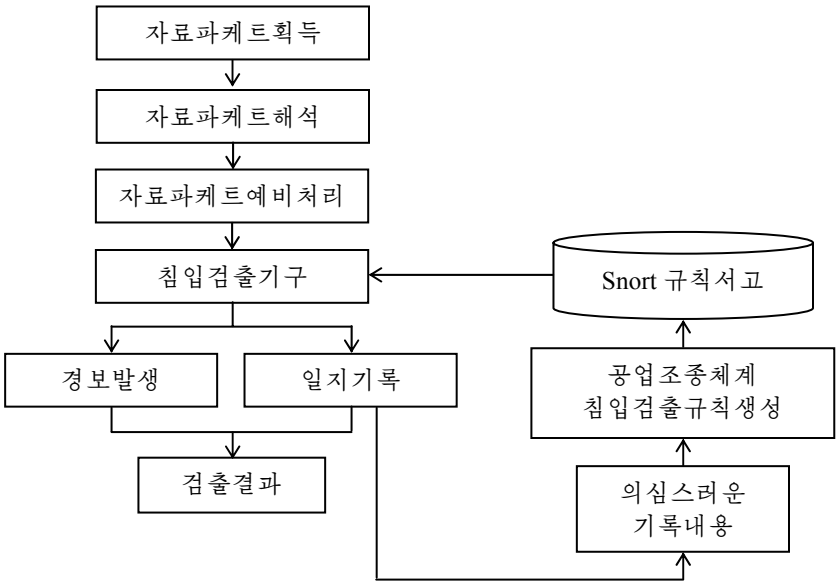

그림 2. 갱신한 침입검출모형

침입검출규칙생성부분은 일지에 기록된 내용에서 의심스러운 내용들에 의하여 검출규칙을 새롭게 생성하는 부분이다. 이 부분에서는 공업조종체계의 전용통신규약인 Modbus TCP규약[3]에 따르는 자료파케트에 대한 Snort검출규칙머리부와 검출규칙본체를 생성하여 규칙서고에 추가한다.

2. ModbusTCP통신규약에 대한 침입검출방법

우리는 ModbusTCP통신에서 침입파케트를 검출하기 위하여 SVM을 리용하였다.

공업조종체계에서 ModbusTCP통신파케트들의 다차원공간에서의 분포특성을 분석하면 편기가 많은것으로 하여 편기점들이 검출결과에 영향을 준다.

이 문제를 해결하기 위하여 SVM판별조건에 편기변수 $\xi_i > 0, i = 1, \cdots, n$ 을 도입하고 통신파케트패턴이 일정한 정도로 편기된 초평면상에 놓이는것을 허용하여 새로운 판별조건을 세웠다.

$$y_i(w^{\mathrm{T}} x_i + b) \geq 1 - \xi_i,\ i = 1, \cdots, n \tag{1}$$

편기량을 조종하기 위한 목적함수는 식 (2)와 같다.

$$\min \frac{1}{2}\|w\|^2 + C\left(\sum_{i=1}^{n} \xi_i\right)^k \tag{2}$$

여기서 C는 벌칙결수, $\sum_{i=1}^{n} \xi_i$ 는 총편기량이다.

임의의 정의 실수 k에 대하여 식 (2)는 불룩계획문제로 되며 $k = 1$ 또는 $k = 2$일 때 2차계획문제로 된다.

특히 $k = 1$일 때 식 (2)에 ξ_i가 없어진다.

라그랑쥬승수 μ_i를 ξ_i가 정수가 되도록 하기 위하여 도입한다.

이러한 조건을 추가하면 풀어야 할 문제는 다음과 같은 라그랑쥬함수로 얻어진다.

$$\begin{aligned} L(w, a, b, \xi, \mu) = \frac{1}{2}\|w\|^2 + C\left(\sum_{i=1}^{n} \xi_i\right) - \\ - \sum_{i=1} a_i(y_i(w^{\mathrm{T}} x_i + b) - 1 + \xi_i) - \sum_{i=1}^{n} \mu_i \xi_i \end{aligned} \tag{3}$$

라그랑쥬함수 L을 w, b, ξ_i에 대하여 편미분을 취하면

$$\frac{\partial L}{\partial w} = 0 \rightarrow w = \sum_{i}^{n} a_i y_i x_i \tag{4}$$

$$\frac{\partial L}{\partial b} = 0 \rightarrow \sum_{i}^{n} a_i y_i = 0 \tag{5}$$

$$\frac{\partial L}{\partial \xi_i} = 0 \rightarrow C - a_i - \mu_i = 0 \tag{6}$$

이다.

식 (4)와 (5)를 L에 대입하면

$$\mu_i \geq 0$$

이므로 $a_i < C$ 이다.

이때 쌍대문제는 다음과 같다.

$$\max \sum_{i=1}^{n} a_i - \frac{1}{2} \sum_{i,j=1}^{n} a_i a_j y_i y_j < x_i,\ x_j >$$
$$C \geq a_i \geq 0,\ i = 1, \cdots, n \tag{7}$$
$$\sum_{i=1}^{n} a_i y_i = 0$$

침입검출판별식은 다음과 같다.

$$y = \mathrm{sign}\left[\sum_{i=1}^{n} a_i y_i < x_i,\ x > + b \right] \tag{8}$$

3. 실험 및 결과분석

공업조종체계의 현장층과 감시조종층사이에서 침입검출정형을 분석하였다.

실험에서는 공업조종체계의 전용통신규약인 Modbus TCP규약으로 되여있는 4 326개의 공격자료파케트들을 가지고 파케트송신도구인 IDSInformer를 리용하여 공격과정을 실현하였다.

검출률과 오검출률을 가지고 침입검출모형의 성능을 평가하였다.

검출률 = 검출한 공격회수 / 총공격회수

오검출률 = 검출하지 못한 공격회수 / 총공격회수

표 1에 전통적인 침입검출모형에 대한 공격실험결과를, 표 2에 갱신된 침입검출모형에 대한 공격실험결과를 보여주었다.

표 1. 전통적인 침입검출모형공격실험결과

번호	공격류형	공격회수	검출회수	검출률%	오검출회수	오검출률%
1	Nmap	215	198	92.09	17	7.91
2	Imap	44	44	100.00	0	0
3	Backdoor	1 021	982	96.18	39	3.82
4	Portsweep	113	104	92.04	9	7.96
5	Dos	78	74	94.88	4	5.12
6	Buffer	34	34	100.00	0	0
7	Flood	2 812	2 704	96.16	108	3.84
8	Tamper	9	9	100.00	0	0
	계	4 326	4 149	95.91	173	4.09

표 1과 2의 실험결과로부터 알수 있는것처럼 검출된 공격류형에 관계없이 최종적인 검출률은 올라갔으며 갱신된 침입검출모형은 전통적인 침입검출모형보다 높은 성능을 가지고있다. 갱신된 침입검출모형은 검출률이 98.17%로서 전통적인 침입검출모형의 검출률보다 2.26% 더 높아졌다.

표 2. 갱신된 침입검출모형공격실험결과

번호	공격류형	공격회수	검출회수	검출률%	오검출회수	오검출률%
1	Nmap	215	215	100.00	0	0
2	Imap	44	44	100.00	0	0
3	Backdoor	1 021	997	97.65	24	2.35
4	Portsweep	113	106	93.81	7	6.19
5	Dos	78	74	94.88	4	5.12
6	Buffer	34	34	100.00	0	0
7	Flood	2 812	2 768	98.44	44	1.56
8	Tamper	9	9	100.00	0	0
	계	4 326	4 247	98.17	79	1.83

참 고 문 헌

[1] J. Brown et al.; IEEE Computer Society, 283, 2016.

[2] 王喆; 微计算机信息, 27, 2, 156, 2011.

[3] 张盛山 等; 计算机工程与设计, 35, 11, 3701, 2014.

주체108(2019)년 5월 5일 원고접수

Intrusion Detection System for Industrial Control System by Using Snort

Son Il Myong, *Son Hyon Jin* and *Kim Myong Il*

In this paper, we proposed a new intrusion detection model by updating Snort model which was used originally in information system and then evaluated its performance.

Key words: IDS, SVM, ICS