Dynamic ACL 모델을 사용한 SCADA 시스템 내 FTP 서비스의 화이트리스트 표현에 관한 연구

Study on the Whitelist Representation of FTP Service in SCADA System by using Dynamic ACL Model

정우석, 김성민, 구영훈, 김명섭

고려대학교 컴퓨터정보학과

{ hary5832, gogumiking, gyh0808, tmskim }@korea.ac.kr

요 약

SCADA 시스템은 최근 비즈니스 시스템과의 통합으로 인해 개방형 시스템으로 전환됨에 따라 보안상 취약점들이 증가하고 있다. SCADA 시스템의 보안문제 해결을 위해 화이트리스트를 기반으로 한 제어시스템의 보안 기법이 각광받고 있다. 현재 대부분의 화이트리스트 보안 기법에서 사용하는 Static ACL 모델의 경우 표현의 한계점을 지니고 있다. 본 논문에서는 FTP 서비스의 특징을 추출하여 Dynamic ACL 모델로 표현하는 방법을 제안한다.

Keywords : Industrial Control System, SCADA, Whitelist, Dynamic ACL, FTP

1. 서론

제어 시스템은 특정 산업현장 전체 또는 산업 단지를 전반적으로 감시하고 제어하기 위하여 다양한 기간 시설과 산업에서 사용되고 있는 컴퓨터 기반의 시스템이다. 미국 ICS-CERT 는 미국내 기반시설에 대한 사이버공격 2015 년 한해 동안 공식 보고된 침해사고 수만 294 개에 달한다고 발표했다. 안전이 증명된 것만을 허용하는 화이트리스트 보안 기법은 제어시스템 환경에서 보안을 담보할 수 있는 효율적 방안으로 주목 받고 있다.

현재의 화이트리스트를 사용한 제어시스템의 보안 기법은 Static ACL 모델을 사용하고 있다. 하지만 Static ACL 모델은 표현상의 한계점을 지닌다.

본 논문에서는 기존 Static ACL 모델이 가지는 한계를 극복하기 위해 FTP 서비스를 대상으로 정의 된 순서를 가지는 ACL 의 집합인 Dynamic ACL 모델을 사용하여 표현하는 방법을 제시한다.

2 장에서는 Static ACL 모델이 가지는 한계점을 서술하고, 3 장에서는 제안하는 FTP Dynamic ACL 모델에 대해 서술한다. 4 장에서는 결론 및 향후 연구에 대해 서술한다.

이 논문은 2015 년도 정부(교육부)의 재원으로 한국연구재단(No.2015R1D1A3A01018057) 및 한국과학기술정보연구원의 "첨단연구망기반 협업플랫폼 서비스 및 글로벌 연동"과제(K-16-L01-C02-S03)의 지원을 받았음.

2. Static ACL 의 한계점

SCADA 시스템에서 FTP 나 OPC 와 같이 Dynamic 서버 포트를 사용하는 통신을 Static ACL 모델로 표현하는 방법은 ANY-ANY 규칙을 사용하는 것이 유일하다. 하지만 ANY-ANY 규칙을 허용하게 되면 해당 IP 간의 모든 연결에 대하여 모든 포트를 오픈을 해야한다. 이는 기존 해당 IP 간에 생성된 다른 ACL 규칙들이 무의미 해지게 되는 것을 의미하며, 특히 FTP 를 사용하는 서버는 해당 서버에 접근하는 모두에게 오픈 될 가능성이 있다.

두번째는 빈도에 상관 없이 Static ACL 모델로 작성된 모든 규칙은 항시 오픈 된다는 점이다. 1 년에 몇 회 사용되지 않는 규칙도 불필요하게 항시 열어두어야한다.

3. 제안하는 Dynamic ACL 모델

ACL(Access Control List)은 사용자들이 특정 시스템에 접근할 수 있는 권한을 설정해 놓은 리스트이다. ACL 은 표현 할 수 있는 범위에 따라 Static ACL 모델과 Dynamic ACL 모델로 나누어진다. Static ACL 모델이 단순한 네트워크 및 시스템에 대한 접근 권한 리스트라면, Dynamic ACL 모델은 ‘A 가 접근한 이후에 B 가 접근 가능하다.’ 또는 ‘C 는 월요일에만 접근 가능하다.’ 라는 ACL 의 순서나 조건까지 표현이 가능한 모델이다.

Figure 1 은 Passive FTP 를 사용할 때, ANY-ANY 규

칙이 생성되는 과정을 도식화 한 것이다. 서버의 21 번 포트를 사용하여 세션이 유지되는 사이 서버와 클라이언트에서 랜덤 포트로 데이터를 교환한다. 데이터 전송을 위해 서버와 클라이언트 모두 랜덤 포트를 사용하기 때문에 ANY-ANY 이 생성된다.

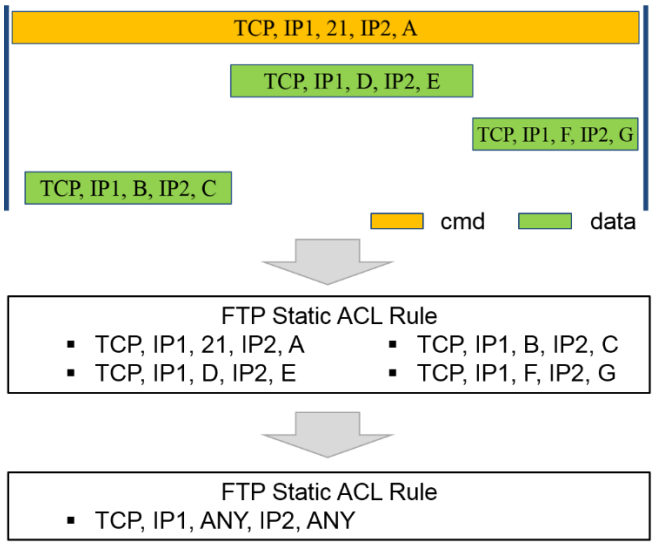

Figure 1. ANY-ANY 규칙이 생성되는 과정

Figure 2 는 일반적으로 Static ACL 모델을 사용하여 화이트리스트를 표현한 예시이다. 5-tuple 정보를 포함하고 있지만 ACL 간의 순서나 조건을 표현 하지 못한다는 한계점을 가지고 있다.

{TCP, (IP1, ANY <-> IP2, ANY)}

Figure 2. 일반적인 Static ACL 모델

Figure 3 은 FTP 를 본 논문에서 제안하는 Dynamic ACL 모델을 통해 표현한 것이다. IP1 과 IP2 사이에 서버 21 번 포트를 사용한 세션이 열려 있는 경우 ANY-ANY 규칙을 각각 n 시간만큼 오픈한다는 의미를 내포하고있다. 또한 "<<"를 사용하여 서버를 구분함으로서 더 확실한 제어가 가능하다.

{TCP, (IP1, 21 <<-> IP2, ANY),
+, ((IP1, ANY <<-> ((IP2, ANY), n)}

Figure 3. 제안하는 Dynamic ACL 모델

Algorithm 1 은 FTP 를 Dynamic ACL 모델로 표현하기 위한 규칙 생성 알고리즘이다. 알고리즘의 입력은 플로우의 5-tuple 정보와 플로우의 지속 시간인 duration 이고, 알고리즘의 결과물은 FTP 규칙이다.

Input : Flows
Output : FTPRules

```
1:  For each Flow in Flows do
2:      makeFTPList(protocol, dIP, dPort,
                    sIP, sPort, duration)
3:  end for
4:
5:  For each Flow in Flows do
6:      FTPRuleGeneration(protocol, dIP, dPort,
                          sIP, sPort, duration)
7:  End for
8:
9:  makeFTPList:
10:     if dPort == 21
11:         addFTPList(sIP, dIP)
12:
13: FTPRuleGeneration:
14:     if sIP and dIP ∈ FTPList
15:         AddFTPDurationDic(sIP+dIP: duration)
16:
17:     For sIP+dIP in FTPDurationDic
18:         Limittime(sIP+dIP) = MAX(duration)
19:
20:     For dIP in FTPList
21:         AddFTPRule(protocol, dIP, ANY,
                       sIP, ANY, Limittime+ α )r
22:     End for
```

Algorithm 1. FTP Rule 추출

4. 결론 및 향후 연구

본 논문에서는 SCADA 시스템의 보안에 사용되는 화이트리스트 보안 기법의 표현을 위해 사용하는 static ACL 모델이 가지는 한계점을 서술하고, 이를 극복하기 위한 방법으로 FTP 서비스를 Dynamic ACL 모델로 표현 할 수 있는 방법을 제안하였다. 제안한 모델은 Static ACL 모델로는 표현하기 어려운 Passive FTP 의 통신 특성과 순서를 반영하여 Dynamic ACL 모델로 표현하였다.

향후 연구에서는 FTP 뿐만 아닌 Static ACL 모델로 표현하기 어려웠던 Dynamic 서버 포트를 사용하는 모든 프로토콜에 대하여 Dynamic ACL 모델로 표현하고 이를 실제 환경에 적용하는 방법에 대해 연구할 계획이다.

[1] Yun, Jeong-Han, et al. "Burst-based anomaly detection on the DNP3 protocol." International Journal of Control and Automation 6.2 (2013): 313-324.

[2] Choi, Seungoh, et al. "Traffic-Locality-Based Creation of Flow Whitelists for SCADA Networks." Critical Infrastructure Protection IX. Springer International Publishing, 2015. 87-102.

[3] 유형욱, 윤정한, 손태식. "제어시스템 보안을 위한 whitelist 기반 이상징후 탐지 기법." 한국통신학회논문지 38.8 (2013): 641-653

[4] Schneider, Johannes, Sebastian Obermeier, and Roman Schlegel. "Cyber security maintenance for SCADA systems." Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research. British Computer Society, 2015.