네트워크 보안 기능 인터페이스 내의 보안 정책 번역

양진혁, 정재훈
성균관대학교

{jin.hyuk, pauljeong}@skku.edu

Policy Translation within Interface to Network Security Functions

Jinhyuk Yang and Jaehoon (Paul) Jeong
Sungkyunkwan Univ.

요 약

본 논문은 네트워크 보안 기능 인터페이스(Interface to Network Security Functions, I2NSF) 프레임워크에서의 보안 정책 번역 구조를 소개한다. I2NSF 프레임워크는 다양한 제조사에서 개발된 네트워크 보안 기능(Network Security Function, NSF)을 호환 및 제공하기 위해 국제인터넷표준화기구(Internet Engineering Task Force, IETF)에서 제안한 표준 인터페이스이다. 본 논문은 I2NSF 프레임워크에서 보안 정책 전달을 위한 정책 번역의 필요성과 동작 과정을 설명한다.

Ⅰ. 서론

오늘날에는 APT(Advanced Persistent Threats, 지능적 지속 위협) 공격과 DDoS 공격(Distributed Denial of Service attack, 분산 서비스 거부 공격) 등 특정 기관 및 기업의 시스템을 공격하는 다양한 기법이 연구되었다. 보안 시스템을 공격하는 방법이 점점 치밀하고 강력해지고 있으며, 피해 사례 또한 지속적으로 발생하고 있다. 보안업체 넷스카웃 아버의 보고서에 의하면, 업체 390 곳을 조사한 결과, 기업의 10%는 디도스 공격 때문에 2017 년 한 해 동안 작년보다 5 배 높아진 10 만 달러 이상의 피해를 입었다고 한다[1].

이처럼 치밀하고 강력해진 공격에 대응하기 위해 보안 회사들은 네트워크 보안 기능들(Network Security Functions, NSFs)을 개발하고 있다. NSF 의 예시로는 방화벽(Firewall), 웹 필터(Web filter), DDoS 공격 완화(DDoS attack mitigation) 등이 있다.

하지만 시스템 구성 요소들이 개별적으로 보안을 유지하는 방법은 치밀해진 공격에 대한 대응책이 될 수 없다. 기업 및 기관의 시스템 규모가 커지고 복잡해짐에 따라 보안 정책의 관리 및 적용이 중요해지기 때문이다. 또한, NSF 는 다양한 제조사에서 개발이 진행되므로 인터페이스와 설정 방법이 제조사마다 달라진다. 이는 호환성 문제를 유발하여 NSF 들의 관리를 어렵게 만든다.

이를 해결하기 위해 국제인터넷표준화기구(Internet Engineering Task Force, IETF)에서는 시스템 관리자가 유연하게 NSF 를 관리할 수 있도록 네트워크 보안 기능 인터페이스(Interface to Network Security Functions, I2NSF) 프레임워크를 설계하고 있다[2].

본 논문에서는 I2NSF 프레임워크에서의 보안 정책 전달을 위한 정책 번역의 동작 과정을 자세히 설명한다. 또한, 번역 과정을 DFA(Deterministic Finite Automata, 결정적 유한 오토마타)와 문맥자유 문법(Context-free Grammar)으로 구조화하여, 프레임워크의 효율적인 NSF 관리 방법을 소개한다.

Ⅱ. 본론

본론에서는 I2NSF 프레임워크와 정책 번역 구조에 대해 설명한다. 또한 번역 과정을 구조화할 때의 이점을 제시한다.

1) I2NSF 프레임워크

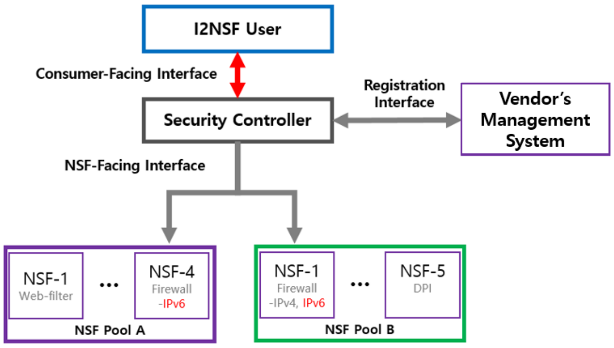

Figure 1. I2NSF 프레임워크.

Figure 1 은 I2NSF 프레임워크를 보여주고 있다. 보안 서비스(예, 방화벽, 웹 필터)를 제공하는 NSF 는 VMS(벤더 관리 시스템, Vendor Management System)에서 등록 인터페이스(Registration Interface)를 통해 등록한다. 등록된 NSF 의 능력(Capability)는 보안 제어기(Security Controller)에 저장된다.

I2NSF 유저(I2NSF User)는 사용자가 이해하고 관리하기 편한 고수준 보안 정책을 생성 및 관리한다. 소비자-직면 인터페이스(Consumer-Facing Interface)는 생성된 고수준 보안 정책을 보안 제어기에 전달한다[3]. 보안 제어기는 I2NSF 유저로부터 전달받은 고수준 정책을 NSF-직면 인터페이스(NSF-Facing Interface)에 적합한 저수준 보안 정책으로 번역한다. 번역된 저수준 보안 정책은 NSF-직면 인터페이스를 통해 프레임워크에 등록된 NSF 를 관리한다.

2) 고수준 정책 해독을 위한 DFA 설계

고수준 정책은 웹사이트, 안드로이드 어플리케이션 등 다양한 인터페이스를 통해 생성이 가능하다. 정책 전달은 일반적으로 XML 처럼 태그 형식의 문법이 사용된다. Figure 2 는 웹 필터 NSF 의 정책 설정을 위한 XML 파일이다.

```
<I2NSF>
  <Policy_web>
    <Rule_name>google_block</Rule_name>
    <Rule_id>7</Rule_id>
    <Action>reject</Action>
    <Position>Staff</Position>
    <Web>google</Web>
    <Time_range>
      <Start_time>09:00</Start_time>
      <End_time>13:00</End_time>
    </Time_range>
  </Policy_web>
</I2NSF>
```

Figure 2. XML 형식의 고수준 보안 정책 – 웹 필터.

본 논문에서는 태그 형식의 문법으로 정책이 전달되었을 때 문법 적합성 에러 감지와 데이터 추출을 편리하게 제공할 수 있는 DFA 구조를 제안한다.

DFA 는 특정 이벤트가 발생할 때마다 상태를 전이시키며 동작하는 추상적 기계이다.

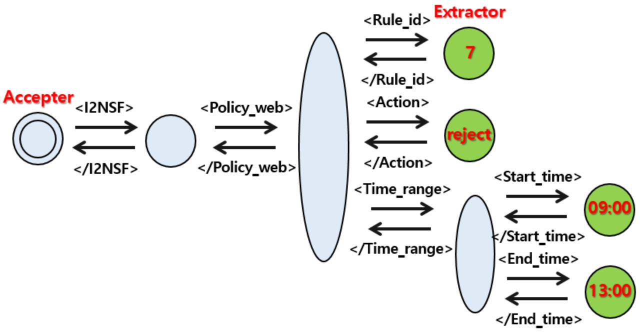

Figure 3. 고수준 정책의 데이터 추출 DFA.

Figure 3 은 Figure 2 의 고수준 정책 파일의 데이터를 추출하는 DFA 이다. 고수준 정책 파일이 데이터 모델의 계층을 충족하기만 한다면 DFA 로부터 수락되며 데이터 추출이 가능하다. 만약 문법에 위배된 형태로 DFA 에 전달될 경우 수락이 되지 않는다. 문법 적합성까지 테스트할 수 있어 정책 관리에 큰 이점을 가져온다. 또한, DFA 사용 시 자유도가 높은 번역기를 만들 수 있어 정책 관리에 유리하다.

3) 저수준 정책 생성을 위한 문맥자유 문법

저수준 정책 또한 일반적으로 XML 문법 형식을 갖추어 전달한다. 따라서 Equation 1 과 같이 문법을 문맥자유 형식으로 일반화할 수 있다. 데이터가 포함된 태그의 경우는 Equation 2 와 같이 표현이 가능하다. 관리자는 두 번째 줄의 데이터 삽입 부분만 조정하여 사용한다. 중복을 허용하는 태그의 경우는 Equation 3 을 추가하는 것으로 구현할 수 있다.

Equation 1. 일반적인 태그 구조의 문맥자유 문법.

$$[pol] \rightarrow <tag>\ [pol']\ </tag>$$

Equation 2. 태그 구조에서의 데이터 삽입.

$$[pol] \rightarrow <tag>\ [data]\ </tag>$$
$$[data] \rightarrow data\ 1 \mid data\ 2 \mid \cdots \mid data\ n$$

Equation 3. 태그의 중복 허용.

$$[pol] \rightarrow [pol][pol]$$

저수준 정책에 대한 문법을 문맥 자유 문법으로 정의하면 정책 관리를 효율적으로 진행할 수 있으며, CYK 알고리즘을 사용하면 문법 적합성도 판단 가능하다.

DFA 로 데이터를 추출한 뒤 Equation 2 를 이용하여 문법을 조정하면 저수준 보안 정책을 생성할 수 있다.

```
<pol:policy>
  <pol:policy-id>2</pol:policy-id>
  <pol:policy-name>i2nsf-web-filter</pol:policy-name>
  <pol:rules nc:operation="create">
    <pol:condition>
      <pol:packet-security-condition>
        <pol:packet-security-ipv4-condition>
          <pol:ipv4-src>10.0.0.2</pol:ipv4-src>
          <pol:ipv4-src>10.0.0.4</pol:ipv4-src>
        </pol:packet-security-ipv4-condition>
      </pol:packet-security-condition>
    </pol:condition>
    <pol:payload-content>google</pol:payload-content>
    <pol:schedule>
      <pol:start-time>09:00:00Z</pol:start-time>
      <pol:end-time>13:00:00Z</pol:end-time>
    </pol:schedule>
    <pol:action>
      <pol:action-type>reject</pol:action-type>
    </pol:action>
  </pol:rules>
</pol:policy>
```

Figure 4. 저수준 보안 정책.

Figure 4 는 Figure 2 의 고수준 보안 정책을 DFA 와 문맥자유 문법으로 번역한 저수준 보안 정책이다. 패킷을 차단할 IP 주소는 Figure 2 의 Position 태그의 정보를 기반으로 보안 제어기의 데이터베이스에서 가져올 수 있다. 여러 개의 IP 주소가 입력될 수 있으므로 <ipv4-src> 태그는 Equation 3 으로 중복을 허용한다.

Ⅲ. 결론

본 논문에서는 I2NSF 프레임워크에서의 보안 정책 번역 구조를 제시하였으며, 번역 구조의 동작 과정과 필요성을 설명하였다. 번역 과정을 오토마타 이론을 이용하여 구조화하여 관리의 효용성을 높이는 것을 초점으로 연구를 진행했다. 이는 복잡해진 네트워크 시스템을 효율적으로 관리할 수 있는 보안 시스템의 방향이 될 것이라고 전망한다.

ACKNOWLEDGMENT

본 논문은 2018 년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구(2016-0-00078, 맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발)이다. 또한 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었다.

참 고 문 헌

[1] P. Alcoy et al., "13th Annual Worldwide Infrastructure Security Report", NETSCOUT Arbor, 2018.

[2] R. Lopez et al., "Framework for Interface to Network Security Functions", IETF, RFC 8329, Feb. 2018.

[3] R. Kumar et al., " Information Model for Consumer-Facing Interface to Security Controller", IETF, draft-kumar-i2nsf-client-facing-interface-im-05 Mar. 2018.