Future Internet Forum
Newsletter
<88호>
2017. 11. 21

SDN 기술을 활용한 DNS 증폭 DDoS 공격 탐지

김형식 (성균관대 소프트웨어학과) / FIF ArchitectureSecurity WG

DNS (Domain Name System) amplification 공격은 대표적인 DDoS 공격 중 하나로, 공격자가 희생자의 IP 주소를 스푸핑(spoofing)하여 DNS 요청을 전송하여 DNS 서버로부터 희생자에게 DNS 응답이 전송되는 공격이다. DNS 응답 패킷의 사이즈는 요청 패킷 사이즈의 약 100배까지 달할 수 있고, 공격자가 쉽게 DNS 요청을 생성할 수 있기에 매우 심각한 공격이라고 할 수 있다. 일반적인 공격 과정은 그림 1과 같이 설명될 수 있다.

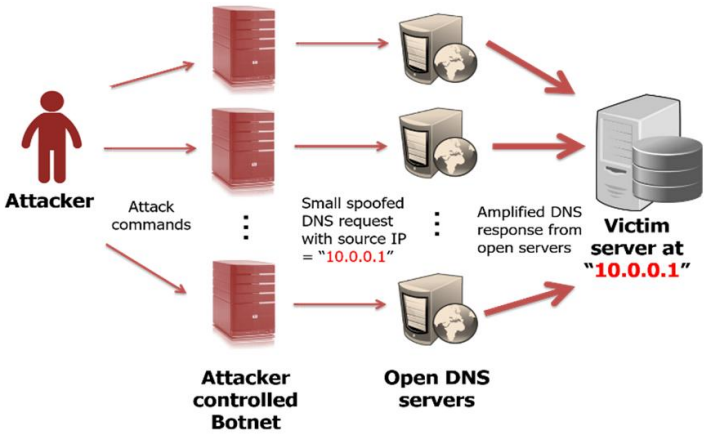

그림 1. DNS 증폭 DDoS 공격의 과정 [1]

학계에서는 이러한 DNS 증폭 DDoS 공격을 막기 위한 다양한 연구가 진행되었는데, (1) DNS 응답 패킷의 수를 제한하여 특정 DNS 응답 패킷수를 제한하는 방법 [1], (2) DNS 요청 메시지 정보를 저장하여 DNS 응답의 유효성을 검사하는 방법 등이 제안된 바 있다. 특히, DNS 요청 메시지를 저장하여 DNS 응답의 유효성을 검사하는 방법이 학계에서는 많이 연구되었는데, 요청 메시지 정보를 효율적으로 확인하고 저장 정보의 공간 복잡도를 낮추기 위하여 블룸 필터(Bloom filter)를 활용하는 방법이 제안되었으나, 거짓 양성(false positives)이 원천적으로 발생한다는 점에서 한계를 가진다 [2]. 이러한 기존 연구의 한계점을 극복하기 위해, SDN (Software Defined Networking) 기술을 이용한 보안 솔루션이 소개된 바 있다 [1]. DNS 요청 정보를 동적으로 유연하게 저장할 수 있는 방법을 제시하여 보다 효과적으로 DNS 증폭 DDoS 공격을 방어할 수 있다 (그림 2 참조).

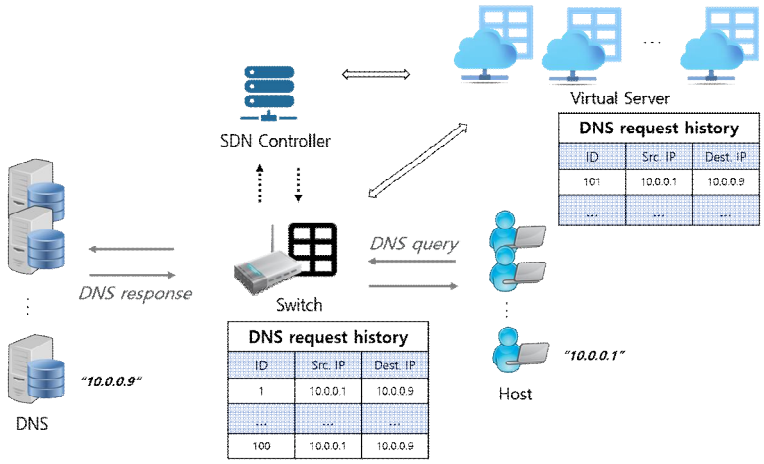

그림 2. SDN 기반의 DNS DDoS 증폭 공격 방어 시스템

DNS 요청 정보에 대한 저장소를 동적으로 유연하게 선택하여 저장함으로써 기존 방어 방법에서 발생하였던 거짓 양성 문제를 효과적으로 해결할 수 있다. SDN 가상 프레임워크 환경인 미니넷(mininet)에서 Open vSwitch와 POX controller의 코드를 수정하여 실험해 본 결과, DNS 증폭 공격이 일어나더라도 제안 환경에서는 통신이 정상적으로 수행되는 것을 확인할 수 있는 반면에, 일반 통신에서는 패킷 전달률이 30% 이하로 감소하는 문제점을 발견할 수 있었다 (그림 3 참조). 더욱이, 기존 연구에서 발생하던 거짓 양성 패킷이 발생하지 않는 특성을 보였다.

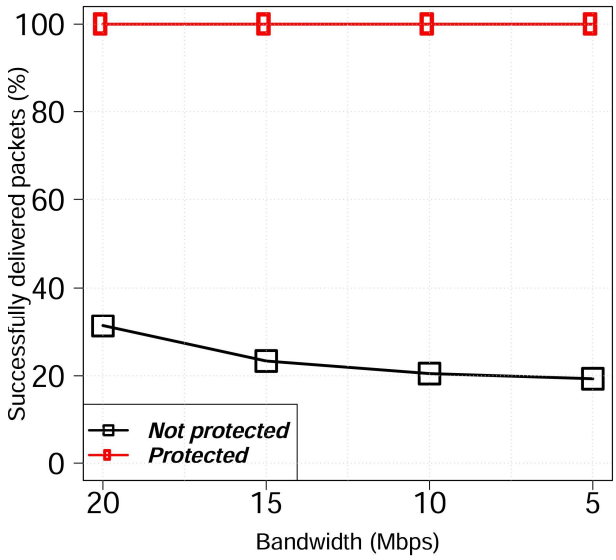

그림 3. 통신 성공 비율 (SDN vs 일반 통신 환경)

DNS 요청 정보를 저장, 관리할 때, 저장소 서버의 성능 및 통신 오버헤드를 고려하여 저장소 서버를 선택한다면 제안 시스템의 성능을 보다 효과적으로 개선할 수 있으로 기대하고 있다. 종래의 기술로 해결하기 어려웠던 네트워크 보안 문제들을 새로운 SDN 및 NFV 환경에서는 보다 효과적으로 대처할 수 있을 것으로 기대되기 때문에, 종래의 고전적인 보안 문제들에 대한 솔루션을 제고하는 것이 중요한 연구의 한 방향이 될 것으로 예상된다.

참고문헌

[1] S. Kim, S. Lee, G. Cho, M. E. Ahmed, J. P. Jeong, and H. Kim.: Preventing DNS Amplification Attacks Using the History of DNS Queries with SDN. In: Proceeding of the 22th Conference on European Symposium on Research in Computer Security (2017)

[2] Sun, C., Liu, B., Shi, L.: Efficient and low-cost hardware defense against DNS amplification attacks. In: Proceedings of the 24th IEEE Global Communications Conference (2008)

Future Internet Forum
Newsletter
<88호>
2017. 11. 21

I2NSF 표준화 동향

정재훈 (성균관대 소프트웨어학과) / FIF ArchitectureSecurity WG

국제인터넷표준화기구인 IETF(Internet Engineering Task Force)의 I2NSF(Interface to Network Security Functions) 워킹그룹(Working Group, WG)은 네트워크 기능 가상화 (Network Functions Virtualization, NSF) 환경에서 클라우드 기반 네트워크 보안 함수(Network Security Function, NSF)를 제공하기 위한 프레임워크(Framework)와 주요 콤포넌트 간 인터페이스(Interface)를 표준화하고 있다. I2NSF WG은 각 인터페이스의 정의를 위해 정보 모델(Information Model) 및 데이터 모델(Data Model) 표준 기고서를 작성하고 있다. I2NSF의 목표는 클라우드 기반 보안 서비스를 제공하기 위해 다양한 벤터들의 네트워크 보안 함수(NSF)를 NFV의 가상 기능 함수(Virtual Network Function, VNF)로 동작시키고자 한다. I2NSF 프레임워크에서는 네트워크 관리 시스템인 I2NSF 유저(User)가 관리하에 있는 네트워크의 고수준 보안 정책(High-level Security Policy)을 정의하여 네트워크에 적용을 요청하면, 자동으로 네트워크에 수행될 저수준 보안 정책(Low-level Security Policy)에 대한 규칙(Rule)으로 변환하여 해당 NSF에 보안 설정을 수행한다.

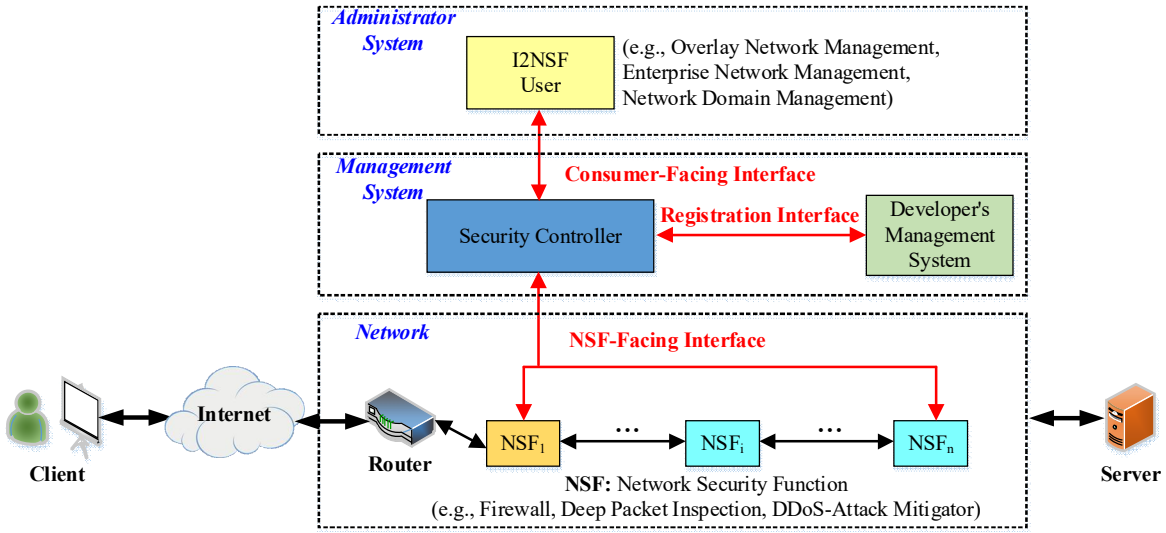

그림 1. I2NSF Framework 기반 클라우드 보안 서비스

그림 1은 I2NSF의 프레임워크를 이용한 클라우드 보안 서비스를 보여주고 있다. 이러한 I2NSF 프레임워크는 I2NSF 유저(I2NSF User), 보안 콘트롤러(Security Controller), 개발자 관리 시스템(Developer's Management System) 및 네트워크 보안 함수(NSF)로 구성되어 있다. I2NSF 유저는 네트워크에 대한 고수준 보안 정책을 설정하는 관리자 시스템(Administrator System)으로서 고수준 보안 정책을 Consumer-Facing Interface를 통해 보안 콘트롤러에게 전달한다. 보안 콘트롤러는 전달받은 고수준 보안 정책을 NSF에서 수행될 수 있는 저수준 보안 정책(Low-level Security Policy)에 대한 규칙(Rule)으로 변환하고, 이를 수행할 NSF를 선택하여 보안 정책의 규칙을 NSF-Facing Interface를 통해 설정한다. 개발자 관리 시스템은 I2NSF 프레임워크에서 사용될 NSF의 능력(Capacity)을 Registration Interface를 통해 보안 콘트롤러에게 등록하고, 보안 서비스를 위한 NSF 생성 및 소멸 등의 생명주기관리(Life Cycle Management)를 수행한다. 그림 1과 같이 I2NSF 프레임워크에서 보안 정책에 따른 보안 서비스가 설정이 되면 원격에 있는 Client(예, VOD Client)는 클라우드에 있는 Server(예, VOD Server)로부터 설정된 보안 정책에 따라 안전하게 클라우드 데이터 서비스를 제공받을 수 있다.

I2NSF WG은 현재까지 Problem Statement 및 Use Case를 표준문서인 RFC 8192[2]로 등록했고, I2NSF Framework WG문서[3]는 현재 RFC로 승인되기 위한 IESG(Internet Engineering Steering Group) 심사를 받고 있다. I2NSF WG문서로는 I2NSF를 적용하기 위한 프레임워크 및 유스케이스 문서, NSF Capability 정보 모델 문서, Consumer-Facing Interface에 대한 요구사항분석 문서, SDN 기반 IPsec 플로우 보호 문서, I2NSF Terminology 문서가 있다.

IETF 100 차 정기회의에서 I2NSF WG는 현재 Consumer-Facing Interface에 대한 정보 모델 및 데이터 모델 기고서, NSF-Facing Interface에 대한 데이터 모델 기고서, I2NSF Capability에 대한 데이터 모델 기고서를 WG문서로 채택하기 위한 논의를 하였다. IETF 100차 해카톤(Hackathon)에서 성균관대팀은 I2NSF Project로 참가하여 Best Student Project Award를 수상하였다. 이번 해카톤을 통해 Capability 데이터 모델 기반의 Registration Interface를 NETCONF/YANG으로 구현했고, Consumer-Facing Interface를 RESTCONF/YANG으로 구현했다. 또한 Time-Dependent Firewall 서비스를 위해 방화벽과 웹필터를 서비스 기능 체이닝(Service Function Chaining, SFC)으로 구현하여, I2NSF 프레임워크와 데이터 지향(Data-Driven)의 인터페이스를 통한 효과적인 보안 서비스에 대한 POC(Proof of Concept)를 수행하였다. 또한 성균관대는 이번 I2NSF 워킹그룹 회의에서 다음의 4건의 기고서를 발표하였다.

- I2NSF Applicability
- I2NSF Capability Data Model
- I2NSF NSF-Facing Interface Data Model
- I2NSF Consumer-Facing Interface Data Model

특히 I2NSF Applicability 문서[4]에서 I2NSF 프레임워크가 SDN Network를 포함할 때, 보안 서비스의 이원화를 통해 효과적인 보안 서비스를 할 수 있음을 제안했다. 즉 패킷 헤드 기반의 단순한 필터링 같은 방화벽(Firewall) 서비스를 SDN Switch에서 수행하고, 플로우와 패킷 페이로드의 콘텐츠 기반의 복잡한 보안 서비스인 DPI(Deep Packet Inspection)는 VNF로 동작하는 NSF에서 수행하는 것이다. 그림 2는 이러한 SDN과 I2NSF를 결합한 네트워크 시스템에서의 이원화된 보안 서비스를 보여주고 있다.

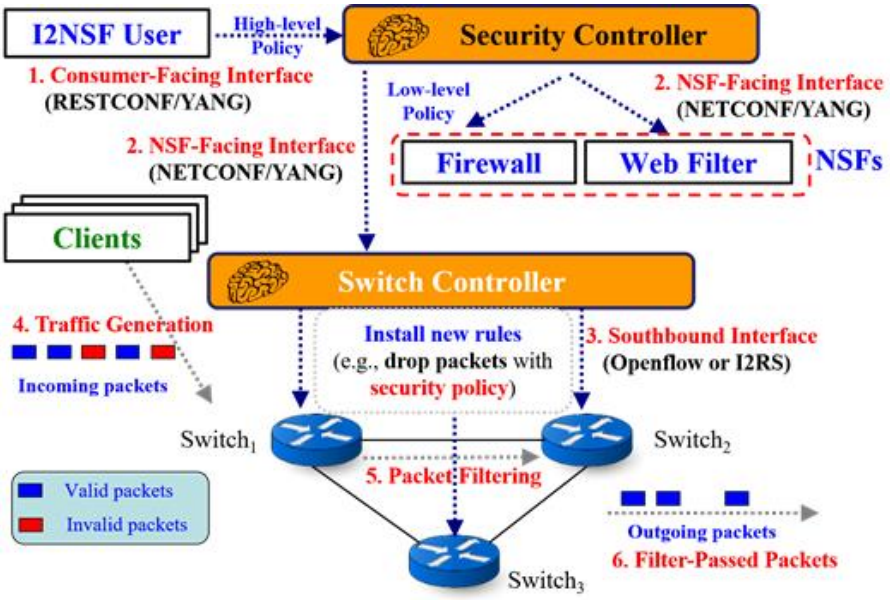

그림 2. SDN 네트워크를 가진 I2NSF Framework에서의 보안 서비스

가까운 미래에 인터넷은 SDN/NFV 중심으로 개편될 예정이다. 이러한 환경에서 다양한 보안 서비스 벤더의 솔루션을 효과적으로 사용하는 클라우드 기반의 보안 서비스가 보편화될 예정이다. 이러한 추세에 맞추어 국내 보안 소프트웨어 기업들 및 ISP는 I2NSF 표준기술을 조기에 도입하여 실제 네트워크에 구현 및 운영함으로써 향후 네트워크 보안 시장에서 큰 경쟁력을 갖출 수 있을 것이다. 성균관대는 ETRI 및 KT와 계속 협력하여 I2NSF 기반 클라우드 보안 서비스 시스템 관련 표준화 아이템을 발굴하고, 효과적인 표준화를 위해 오픈스택(OpenStack) 기반으로 NFV 시스템을 구축하고 이를 바탕으로 I2NSF Framework과 Interface들을 개발 및 검증하여 I2NSF 표준화를 선도해 나갈 예정이다.

참고문헌

[1] I2NSF Working Group, https://datatracker.ietf.org/wg/i2nsf/about/
[2] S. Hares, D. Lopez, M. Zarny, C. Jacquenet, R. Kumar, and J. Jeong, “Interface to Network Security Functions (I2NSF): Problem Statement and Use Cases”, RFC 8192, July 2017.
[3] D. Lopez, E. Lopez, L. Dunbar, J. Strassner, and R. Kumar, “Framework for Interface to Network Security Functions”, draft-ietf-i2nsf-framework-08 (work in progress), October 2017.
[4] J. Jeong, S. Hyun, T. Ahn, S. Hares, and D. Lopez, “Applicability of Interfaces to Network Security Functions to Network-Based Security Services”, draft-ietf-i2nsf-applicability-01 (work in progress), November 2017.

본 뉴스레터는 한국인터넷진흥원 연구지원사업의 일환으로 발간된 자료입니다