네트워크 기능 가상화 환경에서의 해시 체인 기반의 네트워크 보안 기능 경로 인증 기법

정재홍, 정재훈*
성균관대학교 전자전기컴퓨터공학과
{darkhong, pauljeong}@skku.edu

A Hash-Chain-Based Path Authentication Scheme of Network Security Functions in Network Functions Virtualization Environment

Chaehong Chung, Jaehoon (Paul) Jeong*
Electronic, Electrical and Computer Engineering, Sungkyunkwan University

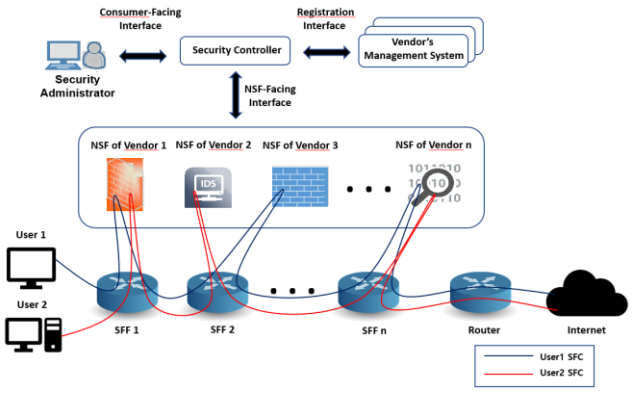
요 약

네트워크 기능 가상화(Network Functions Virtualization, NFV) 기술의 발전으로 소프트웨어 기반의 다양한 네트워크 보안 기능(Network Security Function, NSF)을 제공하는 시스템이 개발되고 있다. 국제인터넷표준화기구(Internet Engineering Task Force, IETF)는 네트워크 보안 기능 인터페이스인 I2NSF(Interface to Network Security Functions)의 프레임워크 및 표준 인터페이스를 표준화하고 있다. 본 논문에서는 I2NSF 의 여러 네트워크 보안 기능들이 서비스 기능 체이닝(Service Function Chaining, SFC) 순서로 실행되었는지를 확인하기 위해 Hash-based Message Authentication Code(HMAC) 기반 SFC 경로 인증 기법을 제안한다.

Ⅰ. 서 론

최근 네트워크 기능 가상화(Network Functions Virtualization, NFV) 기술의 도래로 다양한 네트워크 환경에서 네트워크 기반 서비스 수행에 있어서의 비용 절감과 자원의 효율적 활용이 가능하게 되었다. 하지만 여러 장점의 이면에는 보안 취약성이 따랐다. 특히 NFV 기술의 외부 클라우드 영역에서 보안 기능들의 상호 연동과 인증 등의 보안적 이슈가 있다[1]. 이에 국제표준화기구(Internet Engineering Task Force, IETF)의 네트워크 보안 기능 인터페이스(Interface to Network Security Functions, I2NSF) 워킹그룹(Working Group, WG)은 여러 벤더(Vendor)의 네트워크 보안 기능(Network Security Function, NSF)을 클라우드에서 효과적으로 사용할 수 있는 프레임워크와 인터페이스를 표준화하고 있다[2]. 다양한 NSF 들은 보안 정책에 맞게 수행 순서를 정해 서비스 기능 체이닝(Service Function Chaining, SFC)을 통해 NFV 시스템에서 보안 기능을 제공할 수 있다[3]. (그림 1)은 I2NSF 의 프레임워크에서 사용자 패킷들에 대해 보안 서비스를 하기 위해 다수의 NSF 로 구성된 SFC 서비스 경로를 보여주고 있다.

I2NSF 프레임워크에서 SFC 서비스를 수행함에 있어 보안 이슈가 존재한다. 현재 표준화가 진행중인 IETF SFC WG 의 “Proof of Transit” 기고서는 SFC 보안 고려사항을 기술하고 있고, SFC 경로를 거쳐왔는지를 확인하는 기법을 제안한다[4]. 하지만 이 기고서는 SFC 경로 순서대로 패킷이 처리되었는지를 확인할 수 없는 제약점이 있다. 본 논문에서는 보안 이슈 중 공격자의 패킷 탈취를 통한 재전송 공격(Replay Attack)과 중간자 공격(Man-in-the-middle Attack)을 완화하기 위해 SFC 의 네트워크 서비스 헤더(Network Service Header, NSH)[5]에 Hash-based Message Authentication Code(HMAC)을 적용하였다. 이를 위해 경로 인증 값을 정의하여 NSH 의 옵션에 추가하였다. 이 값은 SFC 에서 노드의 순서를 고려하지 않는 점을 해결하기 위해 해시 체인(Hash Chain) 기법을 적용하여 순서를 고려하였다.

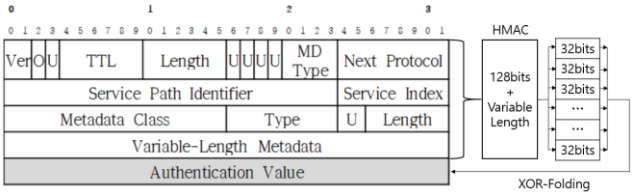


(그림 1) I2NSF 프레임워크와 SFC

Ⅱ. 본론

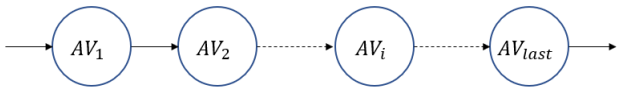
본 논문은 다양한 NSF 의 사용에 있어서 SFC 경로 인증 기법을 기술한다. 기존의 SFC 에서는 재전송 공격과 중간자 공격에 취약한데, 이러한 공격을 방어하기

위해 NSH 에 HMAC 을 적용한 값인 Authentication Value(AV)를 통해 검사하는 기능을 제안한다. (그림 1)의 보안 관리자(Security Administrator)가 사용자 패킷에 보안 정책을 적용하기 위해 검사 패킷(Probe Packet)을 이용하여 보안 제어기(Security Controller, SC)에게 SFC 경로에 해당되는 NSF 의 경유 정보를 포함한 AV 를 전달한다. 검사 패킷은 다수의 사용자의 패킷에 SFC 를 적용하기 전에 SFC 의 경로를 사전에 경유하여 경로를 파악할 수 있다. SC 는 검사 패킷을 통해 각각의 AV 를 NSF 순서에 맞게 해시 체인(Hash Chain)으로 구성하고, 마지막 NSF 를 경유하고 생긴 AV 를 사용자의 패킷에 적용하여 경로 인증 값으로 사용한다.



(그림 2) Authentication Value 를 추가한 NSH

(그림 2)는 HMAC 을 적용하여 Authentication Value 를 추가한 NSH 의 구조이다. NSH 는 Variable-Length Metadata 를 갖는 NSH MD Type2 의 Option 에 NSF 의 SFC 정보를 추가하고, NSH 전체를 NSF 등록에 사용한 그룹키를 이용하여 HMAC 으로 해싱(Hashing)한다. 생성된 해시 값은 32bits 단위로 나누어 XOR-Folding 연산을 하여 32bits 크기의 AV 를 만들어 헤더에 추가한다. AV 는 각 NSF 를 경유할 때마다 갱신되는 인증 값이다.

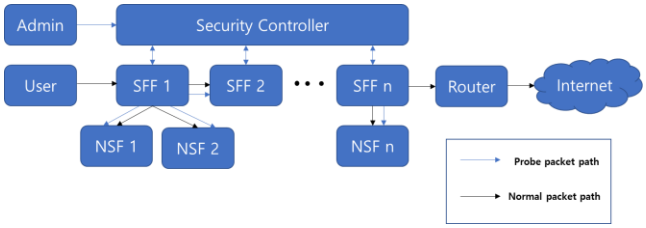


$$AV_i = Hash(AV_{i-1} \oplus HMAC(NSH(NSF_i)))$$

AV_{last} : The last Authentication Value of SFC

(그림 3) 해시 체인 기반의 Authentication Value

(그림 3)은 Authentication Value 의 갱신을 보여준다. 패킷이 SFC 에 해당되는 NSF 를 경유할 때, 각 NSF 등록에 사용한 그룹키를 이용하여 HMAC 을 적용시킨 후 이전의 AV 값과 XOR 연산을 한 값을 해싱하여 새로운 AV 로 갱신한다. 초기의 AV 는 0x00 으로 채워진 값을 디폴트(Default)로 사용하였다. 마지막 NSF 의 AV 를 갱신한 값(AV_{last})는 경로 인증에 사용된다.



(그림 4) Probe & Normal 패킷 경로

보안 관리자가 보안 정책을 내린 후 SC 는 검사 패킷을 이용하여 해당하는 SFC 의 NSF 정보를 습득한다. (그림 4)에서 검사 패킷은 SFF(Service Function Forwarder)를 통하여 해당되는 NSF 를 경유할 때 마다 SC 를 거쳐 AV 를 전달한다. SFC 의 마지막 NSF 를 경유하면 SC 는 각 AV 를 순서에 맞게 해시 체인하여 생성한 값을 최종 Authentication Value 로 사용한다. 정책이 적용된 사용자의 정상 패킷은 해당되는 각 NSF 를 경유할 때마다 같은 방식으로 AV 를 해시 체인하여 갱신한다. 최종적으로 생성된 AV 는 패킷이 라우터 등을 통하여 외부 네트워크로 가기 전에 "Validation Node" 혹은 SC 를 통하여 경로 인증을 수행한다. SC 에서 검사 패킷을 통해 생성한 AV_{last} 와 사용자의 정상 패킷이 최종 NSF 를 경유하고 생성한 AV 값과 일치하면, SFC 경로 순서에 맞게 처리된 것으로 경로 인증이 완료된다. 만약 인증 값이 서로 다르면, 불필요한 NSF 를 경유하거나 필요한 NSF 를 경유하지 않거나 혹은 NSF 경유 순서가 잘못된 경우이므로 패킷 드랍(Drop)을 한다.

Ⅲ. 결론

본 논문은 I2NSF 프레임워크에서 사용자 패킷이 보안 정책을 처리하는 NSF 들의 SFC 경로에 맞게 처리된 것을 인증 기법으로 제안하였다. 이를 위해 SFC 패킷의 NSH 에 HMAC 을 적용하여 연산한 인증 값을 만들고 해시 체인 기법을 이용하여 NSF 의 순서를 고려한 경로 인증을 하였다. 이 방법은 정확한 NSF 의 경로 순서를 보장하지만, 로드 밸런스를 위해 동일한 기능을 가진 NSF 들의 풀(Pool)에서의 경로 인증에서는 비효율적일 수 있다. 따라서 향후 연구로 NSF 종류를 고려한 SFC 경로 인증 기법을 연구할 계획이다.

ACKNOWLEDGMENT

본 논문은 2018 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구 (No.2016-0-00078, 맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발)이고, 또한 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터지원사업의 연구결과로 수행되었음 (IITP-2019-2017-0-01633).

참 고 문 헌

[1] 한국전자통신연구원, "SDN/NFV 보안 표준화 현황", CEO 표준기술-2015-3 호, 10. 2015

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

[3] J. Halpern and C. Pignataro, "Service Function Chaining (SFC) Architecture", RFC 7665. Oct. 2015.

[4] F. Brockners et al., "Proof of Transit", Internet Draft, draft-ietf-sfc-proof-of-transit-02, Mar. 2019.

[5] P. Quinn et al., "Network Service Header (NSH)", RFC 8300, Jan. 2018.

[6] R. Eichelberger et al., "SFC Path Tracer: A Troubleshooting Tool for Service Function Chaining", IFIP, May. 2017.