SNMP 대상 퍼징기술 개발

김수훈⁰, 강병훈^{*}

^OKAIST 정보보호대학원,

*KAIST 정보보호대학원
e-mail: soohunkim@kaist.ac.kr⁰, brentkang@kaist.ac.kr^{*}

Fuzzer for Private MIB in SNMP

Soohun Kim^o, Brent ByungHoon Kang*

^oGraduate School of Information Security, KAIST,

*Graduate School of Information Security, KAIST

요 약 ●

일반적으로 네트워크 장비는 원활한 장비 관리를 위해 SNMP라는 프로토콜을 활용한다. SNMP를 활용함에 있어, 각 장비 제조사에서는 고유 기능을 정의하여 사용하기도 하는데 이를 Private MIB이라고 한다. 본 연구에서는 이러한 Private MIB을 대상으로 하는 퍼장(Fuzzing) 기술을 고인하였다. 본 논문에서는 특정제조사의 Private MIB에 대해 페이로드를 만드는 전략과 실제 페이로드의 생성을 보인다. 이는 수많은 소프트웨어 혹은 장비들의 초기 안전성 평가를 수행하는 데 응용될 수 있을 것으로 기대한다.

키워드: 간이 망 관리 프로토콜(SNMP), 퍼징(Fuzzing)

I. Introduction

소프트웨어의 안전성을 검증하기 위한 방법 중 하나로 퍼정 (Fuzzing)이 있다. 퍼징은 대상 소프트웨어에 임의의 다양한 입력 값을 전달하여 프로그램이 내재한 오류를 검출하는 기법으로, 블랙박스 퍼징, 화이트박스 퍼징, 그레이박스 퍼징으로 분류할 수 있다. 이 중 블랙박스 퍼징의 경우 대상 소프트웨어에 대한 정보가 제한적일 경우 즉, 내부 상태정보를 활용하지 못하는 경우 사용하며, 초기단계의 안전성 및 취약점 분석에 활용된다. 본 연구에서는 네트워크 장비를 대상으로 안전성을 검증하는데 있어 사용한 블랙박스 퍼저 중 일부인 SNMP 대상 퍼저를 소개한다. 퍼징 전략을 세우는 데 있어 고려한 프로토콜의 특성을 기술하며, 해당 특성을 활용한 기초적인 임의 값 생성 및 전달기능을 보인다.

II. Background

1. SNMP

SNMP 는 'Simple Network Management Protocol'로 UDP 기반 통신을 통해 네트워크 상 다양한 리소스 간의 여러 상호작용에 사용되는 프로토콜이다. SNMP는 특히 네트워크 장비들을 대상으로 각 장비들의 일부 기능을 설정하거나 상태정보를 획득하기 위해 사용되며, 주로 MIB(Management Information Base)을 통해 상호

작용한다. MIB은 트리형식의 구조를 가지는 일종의 정보 객체로, 대부분의 제조사에서 공통적으로 사용하는 Enterprise MIB과 각 제조사에서 독립적으로 사용하는 Private MIB으로 구분할 수 있다.

III. The Proposed Scheme

1. 퍼징 전략

본 연구에서는 A사의 Private MIB에 대해 퍼징을 수행하였다. 약 6,000개의 제조사 Priavte MIB을 식별하였으며, 그 중 가변 길이 값을 입력으로 받는 MIB을 식별하였다. 기변길이 MIB은 아래 표와 같은 형식을 가진다.

Table 1. 가변길이 MIB 상세 구성요소

ENTERPRISE	PRIVATE	OID	Length	
1.3.6.1.4.1		*	N	Val₁Val _n

가변길이를 사용하는 MIB 구조를 살펴보면 OID의 나열 이후 길이 값(Length)을 정의하는데, 이어 길이 값과 같은 개수의 데이터가 나타남을 알 수 있다. Table 2. A사 고유의 가변길이 MIB 예제

1.3.6.1.4.1.*.<u>8</u>.108.105.110.107.68.111.119.110 ("linkDown")

예를 들어 위 예제 OID의 경우 밑줄 친 8이 뒤이어 나오는 데이터의 개수이며 8개의 10잔수 형태의 ASCII값이 나타남을 관찰할 수 있다. A사의 경우 위와 같은 형태의 가변길이 MIB을 정의하여 사용하며, 본 연구에서는 이러한 특징을 활용하는 퍼저를 고인하였다. 가변길이 정보를 다루는 OID 리스트를 관리하고 각각의 OID에 대해 임의의 길이 값과 임의 개수의 데이터를 무작위로 생성하는 퍼저를 개발하였다.

2. 퍼저 구현

보다 자유로운 PDU(Protocol Data Unit)를 생성하기 위해, snmpget 등의 기존 도구가 아닌 직접 구현한 도구를 사용하여 임의의 페이로드를 만들고 송수신하였다. 개발은 파이썬을 이용하여 수행하였으며, 본 퍼저는 가장 초기단계의 퍼저로 퍼정 대상 장비로부터수신한 유의미한 피드백들을 지속적으로 코드에 반영하였다.

\$ python3 ./my_fuzz.py
Usage: ./my_fuzz.py <target_address> <community_name>

Fig. 1. SNMP Fuzzer

위 Fig. 1과 같이 퍼정 대상 장비의 IP 주소와 SNMP설정 시 적용한 Community name을 입력으로 받아 퍼정을 수행한다. 퍼정은 아래 Fig. 2와 같이 임의의 더미 OID들을 생성하여 get request 패킷을 구성하고 대상 장비에 송신한다.

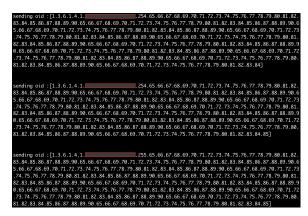


Fig. 2. Dummy OID

임의의 OID를 구성할 때 각 SNMP 요청에 대해 사전에 정의한 특정 길이를 넘기지 않도록 구현하였으며 Length 필드에 임의의 큰 값, 이어 나오는 데이터 개수에 임의의 큰 값, 두 영역 모두에 임의의 큰 값을 생성하는 세 가지 경우를 고려하여 송신하도록 구현하였다.

IV Conclusions

임베디드 장비에 대한 안전성 검증에 있어 초기에 흔히 사용되는 기법중 하나로 퍼장이 있다. 본 연구에서는 스위치, 라우터 등 네트워크 장비에 흔히 사용되는 SNMP에 대하여 해당 프로토콜의 특성을 활용한 퍼장 방법을 제안하고 구현하였다. 본 연구가 취약점 점검 및 안전성 검증 초기단계에서 다양한 특성의 소프트웨어에 특화된 퍼저를 설계 및 구현하는데 도움이 될 것으로 기대한다.

REFERENCES

- [1] H. Liang, X. Pei, X. Jia, W. Shen and J. Zhang, "Fuzzing: State of the Art," in IEEE Transactions on Reliability, vol. 67, no. 3, pp. 1199-1218, Sept. 2018,
- [2] V. J. M. Manès et al., "The Art, Science, and Engineering of Fuzzing: A Survey," in IEEE Transactions on Software Engineering, vol. 47, no. 11, pp. 2312-2331, 1 Nov. 2021.
- [3] Presuhn, R., Ed., "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3416, Dec 2002, https://www.rfc-editor.org/info/rfc3416.