

SNMP 대상 퍼징기술 개발

김수훈^o, 강병훈^{*}

^oKAIST 정보보호대학원,

^{*}KAIST 정보보호대학원

e-mail: soohunkim@kaist.ac.kr^o, 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

● 요약 ●

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 퍼징(Fuzzing) 기술을 고안하였다. 본 논문에서는 특정 제조사의 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 퍼징(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 제한적인 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.

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 Private MIB을 식별하였으며, 그 중 가변 길이 값 입력으로 받는 MIB을 식별하였다. 가변길이 MIB은 아래 표와 같은 형식을 가진다.

Table 1. 가변길이 MIB 상세 구성요소

ENTERPRISE	PRIVATE	OID	Length
1.3.6.1.4.1		*	N Val ₁ ...Val _n

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

II. Background

1. SNMP

SNMP는 ‘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

