Analysing a router dynamically

제출일자 : 2017년 0월 00일 0요일

학 과 : 컴퓨터공학과

담당교수 : 신영주 교수님

학 번 : 2016722092

성 명 : 정동호

**목차**

[1 SNMP란 3](#_Toc491244024)

[1.1 SNMP 버전들 3](#_Toc491244025)

[1.2 SNMP로 할 수 있는 일들 4](#_Toc491244026)

[1.2.1 네트워크 구성 관리 4](#_Toc491244027)

[1.2.2 성능 관리 4](#_Toc491244028)

[1.2.3 장비 관리 4](#_Toc491244029)

[1.2.4 보안 관리 4](#_Toc491244030)

[1.3 SNMP 망구성 5](#_Toc491244031)

[1.4 SNMP 프로토콜 동작 5](#_Toc491244032)

[1.5 SNMP 메시지 5](#_Toc491244033)

[2 MIB 8](#_Toc491244034)

[3 SMI 9](#_Toc491244035)

[3.1 Basic Data Types 9](#_Toc491244036)

[4 PySNMP 9](#_Toc491244037)

[4.1 기본 Get 예제 10](#_Toc491244038)

[4.2 외부MIB 로드하기 11](#_Toc491244039)

[5 Reference 11](#_Toc491244040)

# 개요

기하급수적으로 발전하는 네트워크는 현대 사회에 필수적인 존재가 되었다. 따라서 개인의 생각, 계획, 사상이나 조직간의 기밀, 중요한 내용들 또한 네트워크를 통해 흐를 수 있으며 문제는 이전부터 제기되어 왔던 소위 빅 브라더라 불리는 국가의 감시이다. 이는 터무니 없는 얘기가 아닌데 2013년 6월 10일 NSA와 GCHQ 등의 정보기관들이 전세계 통화기록과 인터넷 사용정보등의 개인 정보를 PRISM이라는 프로그램을 통해 무차별 수집, 사찰해온 사실이 내부 고발로 인해 폭로된 적 있으며 대한민국의 경우 국가정보원에서 도청을 위한 해킹 프로그램을 구입한 것이 사실로 밝혀진 적 있다.

이처럼 국가나 어떤 집단에 의해 네트워크가 도청 될 수 있다는 것은 큰 문제이다. 그러므로 이를 해결하기 위해 라우터 상에서 동작하는 백도어를 탐지하는 것이 이번 연구의 궁극적인 목표이다. 라우터에 숨어있는 백도어를 탐지하기 위해 여기서는 SNMP 프로토콜을 활용하여 라우터 인터페이스 간 흐르는 트래픽을 분석해 백도어를 식별하는 동적인 접근 방법을 택하였다.

정상적인 라우터라면 인풋과 아웃풋이 크게 차이 나지 않겠지만 도청을 위한 라우터의 경우 모든 패킷을 수용할 수 없으므로 주기적으로 이를 어딘가로 내보내야 한다. 이 때 인풋과 아웃풋이 크게 차이가 날것이라 가정하고 연구를 진행하였다. 또한 MIB는 표준 MIB만을 사용하였으며 연구는 직접 국가기관의 도청 프로그램을 구할수 없어 실제 네트워크 장비가 아닌 Dyamips를 통한 가상 환경에서 진행되었다.