가정용 IoT 네트워크에서의 이상 징후 탐지 솔루션 제안

박연진*, 오주혜*, 이근호*, 전유부**
*백석대학교 정보통신학부
**순천향대학교 컴퓨터소프트웨어공학과 & 웰니스코칭서비스연구센터
e-mail: h_tea@naver.com, oho166@naver.com, root1004@bu.ac.kr, jeonyb@sch.ac.kr

A Solution for Anomaly Detection at Home IoT Networks

Yeon-Jin Park*, Ju-Hye Oh*, Keun-Ho Lee*, You-Boo Jeon**
*Division of Information and Communication, Baek-Seok University
**Computer Software Engineering & Wellness Coaching Services Research Center, Soon-Chun-Hyang University

요 약

인터넷의 발달이 증대함에 따라 컴퓨터를 전문적으로 사용하지 않더라도 가정에서 NAS등의 서버모델을 사용하는 경우가 많아졌다. 한번 구매하면 저전력으로 손쉽게 사용할 수 있는 대용량 서버모델의 사용자 수가 점차적으로 증가하고 있다. 이와 동시에 간단한 검색만으로 구할 수 있는 웹과 네트워크에 큰 악영향을 미치는 악성도구들도 인터넷상에 퍼지고 있다. 쉽게 얻은 해킹 도구로 간소하게 설치된 가정용 서버 등을 공격하는 빈도수가 점점 늘어나고 있는 추세이다. 본 연구는 가정용 IoT 서버 및 네트워크에서 이상 징후를 탐지하는 솔루션 모델의 구축을 제안하고자 한다.

1. 서론

컴퓨터의 보급이 점점 늘어남에 따라, 가정에서 오래된 랩 탑 및 데스크 탑이 한두 대씩 증가하고, 간단한 컴퓨팅 파워를 가진 IT기기들이 많이 증가되어가고 있다. 데이터에 대한 접근성을 위해 이러한 가정의 오래된 컴퓨터를 IIS 또는 Linux 서버로 사용하거나 가정용 NAS등을 구매하여 사용하는 경우도 역시 증가하고 있다. 이러한 가정용 서버에는 전문적인 보안 인력이 패킷을 지속적으로 지켜보는 관제를 적용하기 힘들기 때문에 보안에 대해 상대적으로 취약한 면이 있다.

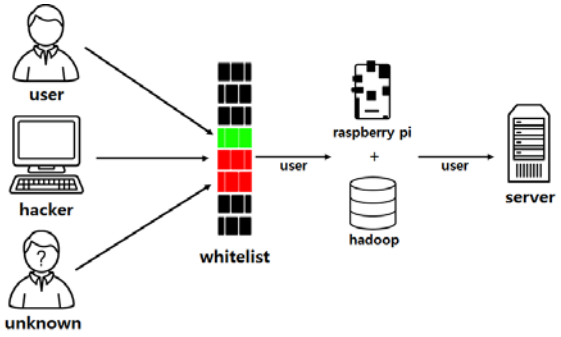
네트워크 공격은 인터넷의 보급 이후에 전통적으로 사용자들에게 공격을 가하고, 큰 피해를 입혀왔다. 몇 가지 예로 DDoS(Distributed Denial of Service) 공격, DRDoS(Distributed Reflection Denial of Service) 공격이 있다. DDoS의 유명한 예로는 2003년도 초에 Slammer 웜에 의해 발생한 대규모 트래픽이 KT DNS 서버를 다운시켜 한국에 인터넷이 마비되었던 1.25 대란도 DDos 공격의 일환으로 볼 수 있다[1]. 네트워크에 가해지는 공격은 가용자원의 급격한 소진을 유발하여 서비스 중지 등을 유발시키기 때문에 큰 피해를 입힐 수 있는 차후 공격들에 대한 사전공격의 목적으로도 사용 될 수 있다. 네트워크를 공격받은 서버모델 및 웹 사이트 등은 다른 공격을 일으키는 중간경유지로도 사용할 수 있기 때문에 가정용으로 사용되는 서버들은 해커들에게는 언제든지 공격하기 쉬운 먹잇감으로 보일 수 있다. 본 논문에서는 가정에서 저렴한 가격으로 손쉽게 설치하고 구매하며, 사용하는 데이터 보관 및 접근 구조에 대한 네트워크 이상 징후를 탐지하는 솔루션 모델을 제안하고자 한다.

2. 이상 징후 패킷

네트워크의 이상 징후를 분석하기 위해서는 특정 parameter를 정의한 후 parameter값에 대한 임계치를 정해야 한다. 잘 알려진 parameter들은 CPU Load의 양, CPU의 사용량, 패킷의 분포, 패킷의 크기 및 패킷 header의 정보, 최대치와 평균치의 집중현상, 네트워크상의 플로우가 급증되는 현상을 이용하는 플로우등이 있다. 이러한 값들은 정상적인 네트워크에 오동작을 일으켜, 네트워크의 가용자원을 고갈시키기도 하고, 피해자의 네트워크자원을 악의적인 파일을 유포하는 C&C 서버로 이용할 수 있어 제 2차, 제 3차 공격까지 야기 시킬 수 있다. 네트워크상에서 비정상적인 요구를 하거나, 특정행위를 수없이 반복해 네트워크의 자원을 고갈시키는 등의 이러한 parameter들을 조합하면 트래픽을 분석함에 있어서 트래픽 특성의 신뢰도가 높아진다[2].

3. 제안사항

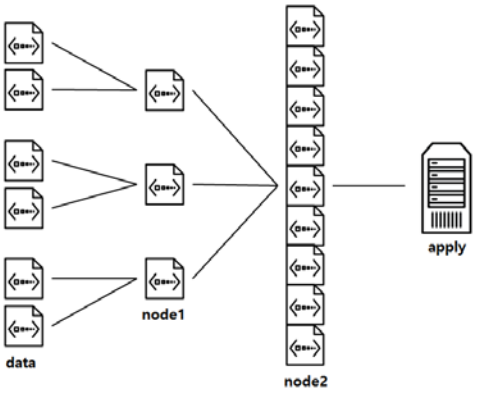
가정용 컴퓨터에서 사용가능한 이상 징후 탐지 모델은 다음과 같다.



(그림 1) Following an Anomaly Detection Model

저전력 미니컴퓨터인 라즈베리파이에 하둡을 설치한다. 하둡은 서버와 연결되어있으며, 서버와 같은 네트워크상에 존재한다. 서버에 접속하여 데이터를 요구하는 사용자들이 접속하는 기준은 인가된 사용자만 네트워크에 접속 할 수 있는 화이트 리스트 방식을 기준으로 한다. 화이트 리스트 방식 기반의 탐지 및 대응방법은 화이트리스트에 없는 비정상 사용자로부터의 공격을 탐지하고 차단하는 것이 가능하지만 정상사용자로 위장하여 등록한 후에 플러딩 공격할 시에는 대응 할 수 없다는 문제점이 있다[3]. 또한 서버의 사용자는 여러 위치와 여러 네트워크를 사용하기 때문에 화이트 리스트 기반만 사용해서는 악성 이용자를 필터링 할 수 없다. 따라서 추가적으로 하둡을 사용하여 악성 사용자들의 로그를 분석한다.

대용량 네트워크 공격 로그들을 분석해본 결과 TCP-Connect-Dos, TCP-ACK-Flooding, TCP-Fin-Flooding, TCP- SYN-Flooding등의 패킷을 확인 할 수있다[4]. 이 로그들의 공통점은 특정 동작을 요구하는 패킷들을 대량 전송하여 자원을 낭비시키는 공격이다. 어떤 한 종류의 패킷이 가용자원의 임계치를 넘게 요구할 때 자동적으로 그 근원지를 차단하는 방식을 사용한다면 대다수의 네트워크 공격을 막을 수 있다. 또한 계속 서버에 오는 로그들을 하둡에 지속적으로 저장시켜 주기적으로 분석 후 적용하는 컨볼루션 네트워킹 방식을 사용한다면, 네트워크 공격으로부터 안전한 시스템을 구축 할 수 있을 것이다.



(그림 2) Convolutional Network

3. 결론

본 논문에서는 라즈베리파이와 하둡을 사용하여 가정용 서버 및 개인 NAS등에 들어오는 공격에 대한 대응 및 이상 패킷 탐지모델을 제안하였다. 이 모델은 저·전력, 저가의 미니컴퓨터인 라즈베리파이를 이용하였으며 계속 사용함에 따라 데이터가 축적, 융합되어 점점 정교해진다. 보안에 대한 전문적 지식이 없는 가정에서 구축 후 지속적으로 약간의 관리만 해준다면 가정에서 네트워크 공격을 받아서 서비스가 중지되는 일이나 다른 큰 네트워크 공격을 위한 중간 기점으로 활용되는 일을 막을 수 있을 것이다.

감사의 글

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2016-H8601-16-1009). 또한 2016년 산학협동재단 지원으로 수행된 연구임.

참고문헌

[1] Choi Hyun-sang, Park Hyun-do, Lee Hee-jo, “A Study on Amplification DRDos Attack and Defenses”, JKIIECT, Vol. 8, No. 5, pp. 429-437, 2015

[2] Lee Jong-yeub, Mi-sun Yoon, Lee Hoon, "Monitoring and Investigation of DoS Attack", KNOM Review, Vol. 6, No. 2, pp. 21-32, 2004

[3] Jin-hee Kim, Bon-seung Koo, Byeng-hee Roh, “Detection and Countermeasure Sheme using Counting Bloom Filter agaist SIP DDoS Attacks by Whitelist Users”, Korean Institute of Next Generation Computing, Vol. 11, No. 5, pp. 25-35, 2015

[4] Jyun-yung Choi, “Integrated analysis of bulk network attack logs”, Korea Information Science society, Vol. 12, pp. 701-703, 2014