KIPS Tr. Comp. and Comm. Sys.
Vol.4, No.6 pp.205~212 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2015.4.6.205

Analysis and Response of SSH Brute Force Attacks in Multi-User Computing Environment

Jae-Kook Lee† · Sung-Jun Kim† · Joon Woo†† · Chan Yeol Park†††

ABSTRACT

SSH provides a secure, encrypted communication channel between two end point systems using public key encryption. But SSH brute force attack is one of the most significant attacks. This kind of attack aims to login to the SSH server by continually guessing a large number of user account and password combinations. In this paper, we analyze logs of SSH brute force attacks in 2014 and propose a failed-log based detection mechanism in high performance computing service environment.

Keywords : Intrusion Detection, SSH, Brute Force Attack, Supercomputing, Attack Analysis

다중 사용자 컴퓨팅 환경에서 SSH 무작위 공격 분석 및 대응

이 재 국† · 김 성 준† · 우 준†† · 박 찬 열†††

요 약

SSH 서비스는 공개키를 이용하여 두 시스템 사이의 안전하고 암호화된 통신 채널을 제공한다. 그러나 이 서비스를 악용한 SSH 무작위 공격(SSH brute force attack)과 같은 해킹 시도가 지속적으로 발생하고 있다. SSH 무작위 공격은 사용자의 계정과 패스워드 조합을 추측하여 SSH 서버에 지속적으로 로그인을 시도한다. 본 논문에서는 2014년 국가 슈퍼컴퓨터를 대상(Target)으로 발생한 SSH 무작위 공격을 분석하고 이와 같이 공격을 탐지하고 대응하기 위한 실패로그 기반의 방법을 기술한다.

키워드 : 침입 탐지, SSH, 무작위 공격, 슈퍼컴퓨팅, 공격 분석

1. 서 론

기후 연구, 분자 모델링, 물리적 시뮬레이션, 암호 해독, 지구 물리학 모델링, 자동차 및 항공 우주선 설계, 재무 모델링, 데이터 마이닝 등 고도로 계산 집약적인 연구를 수행하기 위하여 초고성능의 슈퍼컴퓨터를 이용한다. 한국과학기술정보연구원(KISTI) 국가슈퍼컴퓨팅연구소(NISN: National Institute of Supercomputing and Networking)에서는 국가 슈퍼컴퓨터를 구축하여 운영하고 있다[1]. 1988년 슈퍼컴퓨터 1호기를 시작으로 1997년 슈퍼컴퓨터 2호기, 2002년 슈퍼컴퓨터 3호기, 현재는 공유 메모리형의 GAIA 1, GAIA 2 시스템과 클러스형의 TACHYON 1, TACHYON 2 시스템으로 구성된 슈퍼컴퓨터 4호기(KISTI-4)를 운영 중이다(2009년 구축)[2]. NISN은 슈퍼컴퓨팅서비스를 제공하기 위하여 원격 접속 서비스인 SSH(Secure Shell Protocol) 서비스를 허가하고 있다. SSH 서비스는 유닉스 기반의 운영체제를 사용하는 서버를 원격에서 접근하기 위한 표준화된 프로토콜로서 공격자가 관리자(root) 비밀번호(password) 획득을 목적으로 공격대상으로 삼기에 매력적인 서비스이다. 과거 바이러스, 웜, 분산서비스거부(DDoS) 공격 등의 사이버 공격은 네트워크 대역폭(Bandwidth)이나 서버의 자원(Server Resource)을 소진시키는 목적으로 사용되었다. 그러나 최근에는 APT공격 등 정상적인 사용자를 가장하여 특정한 시스템을 대상으로 침입을 시도하는 공격으로 진화하고 있다. NISN은 이러한 외부의 공격으로부터 초고성능의 슈퍼컴퓨터를 안전하게 보호하고 사용자에게 보다 신뢰도 높은 서비스를 제공하기 위해 다양한 보안 장비를 24 x 7 운영 중이다[3].

본 논문에서는 2014년 NISN에서 수집한 SSH 무작위 공

† 정 회 원 : 한국과학기술정보연구원 슈퍼컴퓨팅인프라실 선임연구원
†† 정 회 원 : 한국과학기술정보연구원 슈퍼컴퓨팅인프라실 실장
††† 종신회원 : 한국과학기술정보연구원 슈퍼컴퓨팅인프라실 책임연구원
Manuscript Received : February 10, 2015
First Revision : April 9, 2015
Accepted : April 21, 2015
* Corresponding Author : Chan Yeol Park(chan@kisti.re.kr)

격(SSH Brute Force Attack) 데이터를 분석하고 이와 같은 정상적인 접속을 가장한 공격을 탐지하고 대응하기 위한 방법을 기술한다. 2절에서는 관련 연구로 SSH 무작위 공격에 대하여 기술하고 무작위 공격을 위해서 구성될 수 있는 봇넷에 대하여 소개한다. 3절에서는 NISN에서 수집한 공격 데이터를 분석하고 4절에서는 무작위 공격을 탐지하고 대응하기 위한 방법을 기술한다. 끝으로 5절에서는 결론을 맺고 향후 연구 과제를 제시한다.

2. 관련 연구

2.1 슈퍼컴퓨팅 서비스 환경

Fig. 1은 슈퍼컴퓨터의 시스템 구조를 개념화한 것이다. 사용자는 공개키 암호화 기법을 이용하는 SSH[4, 5]를 통하여 로그인 노드(LOGIN nodes)에 접속할 수 있다. 이때 슈퍼컴퓨팅서비스 사용자 계정이 필요하다. 로그인 노드에서는 간단한 프로그램 수정 및 디버그, 배치(Batch) 작업 제출 등이 가능하다. 그러나 장시간 소요되는 프로그램 디버그나 상호작용(Interactive)이 필요한 작업은 디버그 노드(DEBUG nodes)에서 수행해야 한다. 디버그 노드는 로그인 노드를 통해서만 접속할 수 있다. 그리고 로그인 노드에서 제출된 배치 작업은 스케줄러(SCHEDULER)에 의해 계산 노드(COMPUTE nodes)에서 실행된다. 계산 노드는 사용자가 외부에서 직접 접근할 수 없다.

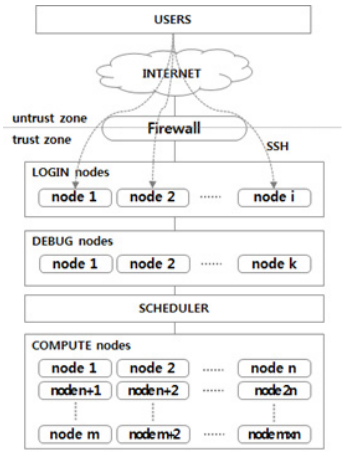

Fig. 1. Service Environment of High Performance Computing (KISTI-4)

2.2 SSH 무작위 공격 및 탐지 기법

SSH 서비스는 클라이언트가 요청하는 모든 세션에 응답하기 위해 서버는 22번 포트를 열어서 항상 수신 대기한다[6]. 최근 이 서비스를 악용한 SSH 무작위 공격이 지속되고 있다. SSH 무작위 공격은 사전 공격(Dictionary Attack)이라고도 하는데 반복적으로 사용자 계정과 비밀번호를 조합하여 불법적으로 이미 스캔 된 호스트에 관리자 및 사용자 권한을 획득하려고 시도하는 공격이다. 최근에는 분산된 무작위 공격(Distributed Brute Force Attack)을 이용하여 매우 은밀하게 공격(Stealth Attack)이 이루어지기도 한다. 이런 분산된 무작위 공격은 공격자가 노출되는 것을 회피하기 위하여 봇넷 등의 악성 호스트 그룹을 이용한다.

이와 같은 공격을 탐지하기 위한 기법은 모니터링하는 위치에 따라 크게 네트워크 기반(Network-based), 호스트 기반(Host-based), 응용 기반(Application-based)으로 분류할 수 있다. 네트워크 기반의 모니터링 방법은 SSH와 같이 암호화된 트래픽을 이용한 공격을 탐지하는 것에 한계가 있다[7]. 탐지하는 방법으로 구분하면 이상(Anomaly), 오용(Misuse), 하이브리드(Hybrid) 모델로 분류된다. 이 방법들은 대부분 기계학습(Machine Learning)과 데이터 마이닝 기법을 이용하여 공격 트래픽과 정상 트래픽을 분류한다[8-20]. 그러나 이러한 기계학습이나 데이터 마이닝 기법을 이용한 탐지 기법은 암호화 터널링을 이용한 경우 탐지에 한계가 있으며 오탐률이 상대적으로 높기 때문에 실제 상용 서비스 환경에 적용하는 것에는 충분하지 않다[7].

3. SSH 무작위 공격 분석

분석에 사용된 데이터는 NISN에서 2014년 3월부터 12월까지 수집한 시스템 접속 및 방화벽 탐지(차단) 로그이다. 1~2월 데이터는 NISN에서 2014년도 2월에 슈퍼컴퓨팅서비스의 성능을 개선하기 위하여 네트워크 및 보안 장비의 구성을 변경하였으므로 통계의 일관성을 위해서 분석에서 제외하였다.

3.1 비정상 접속 시도

사전 공격 등 SSH 무작위 공격은 슈퍼컴퓨터의 관리자 및 사용자의 계정과 비밀번호를 탈취하기 위하여 지속적으로 발생하고 있다. Fig. 2는 KISTI-4를 대상으로 하는 비정상 접속 시도 건수를 나타낸 것이다.

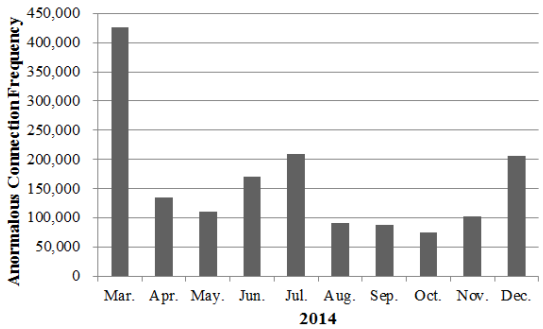

Fig. 2. Number of Abnormal Accesses using SSH Service Port in 2014 (Monthly)

3월의 경우 다른 달에 비해 2배 이상 빈도가 높았던 것을 확인할 수 있다. 3월에 발생한 비정상 접속 건수가 높은 이유를 확인하기 위하여 공격 IP 주소 TOP10으로 살펴보면 Fig. 3과 같다(보안을 위해 공격 IP 주소를 영문 대문자로

대신함). 특정 공격 IP 주소 1개에서 전체 비정상 접속의 43% 이상을 시도한 것을 확인할 수 있다. 이 공격 IP 주소는 중국에서 발생한 것으로 3월 1일에서 17일까지 지속적으로 186,000건이 넘게 공격을 시도하였다. Fig. 4는 SSH 무작위 공격을 시도한 공격 IP 주소의 개수를 나타낸 그래프이다. 12월에 공격 IP 주소의 개수가 다른 달에 비해 많았다.

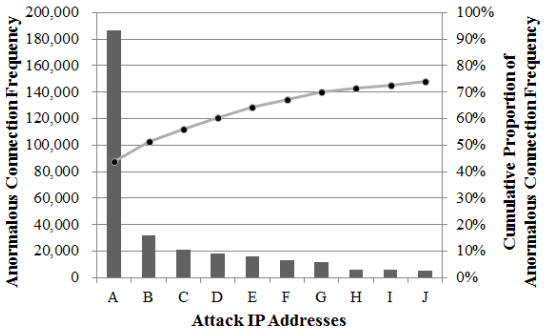

Fig. 3. Frequency and Cumulative Proportion of Anomalous Connections in Mar. 2014 (TOP 10 IP Address)

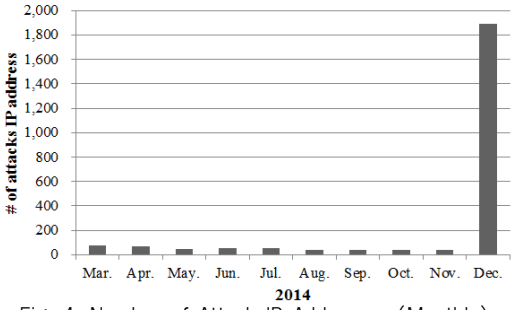

Fig. 4. Number of Attack IP Addresses (Monthly)

Fig. 2와 Fig. 4를 비교해보면, 3월은 비정상 접속 시도 건수는 많으나 공격 IP 주소의 개수는 적은 반면에 12월에는 접속 시도 건수는 많지 않으나 공격 IP 주소의 개수는 다른 달에 비해 15배 이상 증가한 것을 확인할 수 있다.

Fig. 5는 공격 IP 주소가 많았던 12월의 공격 IP 주소 개수를 일별로 상세화한 그래프이다.

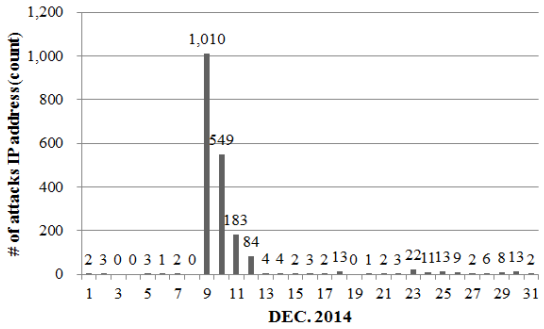

Fig. 5. Number of Attack IP Addresses (Daily, Dec. 2014)

9일부터 12일까지 공격 IP 주소의 개수가 집중된 것을 확인할 수 있다. 다른 공격 패턴과 다르게 이 기간의 공격은 여러 개의 좀비 PC를 이용한 분산된 무작위 공격으로 추정할 수 있다.

3.2 공격 계정

SSH 무작위 공격은 서버에 접속하기 위한 계정과 비밀번호를 무작위로 생성하거나 미리 정의된 사전을 이용하여 공격을 하게 된다. Fig. 6은 12월 9일부터 12일까지 공격 IP 주소의 개수가 많았던 기간에 사용된 계정의 분포를 나타낸 것이다. Table 1에는 공격에 사용된 계정에서 Fig. 6의 범례에 나타나지 않은 계정을 추가로 나타냈다.

Table 1. Residual Accounts that are Used to SSH Brute Force Attack (11~12 Dec. 2014)

Day	Accounts
11	a, ftp, default, vyatta, alex
12	zhangyan, dff, test, ubuntu, git, boot, 123456, 123, xbmc, debug

이 기간(9~11일)에 'root' 계정이 가장 많이 사용된 것을 확인할 수 있다. 특히 9일은 99%가 'root' 계정으로 접속을 시도하였다.

3.3 공격 지속성

공격 지속성은 공격을 시도한 IP 주소에서 얼마 동안 계속적으로 접속을 시도하는지를 나타낸다. Fig. 7은 공격 IP 주소별 공격 지속시간을 나타낸 분포도이다. x축은 공격 IP 주소를 임의로 배열하였다(보안상 x축 항목은 표기하지 않음). 공격 지속시간은 Equation (1)과 같이 공격 시작시간(t_s)부터 종료시간(t_e)까지의 차이를 나타낸다. 단위는 시간(Hours)이다.

$$\Delta t = (t_e - t_s) \times 24$$
$$\text{TYPE}[t_s | t_e] = YYYYMMDD\ HH{:}MM{:}SS \qquad (1)$$

지속시간이 가장 짧은 것은 순간적으로(1초 이하, 0.00001) 23개의 접속시도를 한 공격 IP 주소이고, 가장 긴 지속시간을 갖는 것은 1개월(30일, 737.37389) 이상 지속하면서 595개의 접속을 시도한 공격 IP 주소이다. 그리고 SSH 무작위 공격을 하는 경우 Fig. 7에서 보는 것과 같이 대부분 10시간 이상 지속되는 것을 확인할 수 있다. 평균(average)도 65시간 이상 지속된다. 평균은 Equation (2)와 같이 최솟값과 최댓값을 제외하고 평균을 구하였다.

$$average = \frac{\sum_{k=1}^{n} \Delta t_k - (\Delta t_{\max} + \Delta t_{\min})}{n-2}, \qquad (2)$$
$$\Delta t_{\max} = Maximum(\Delta t_1, \Delta t_2, ..., \Delta t_n)$$
$$\Delta t_{\min} = Minimum(\Delta t_1, \Delta t_2, ..., \Delta t_n)$$

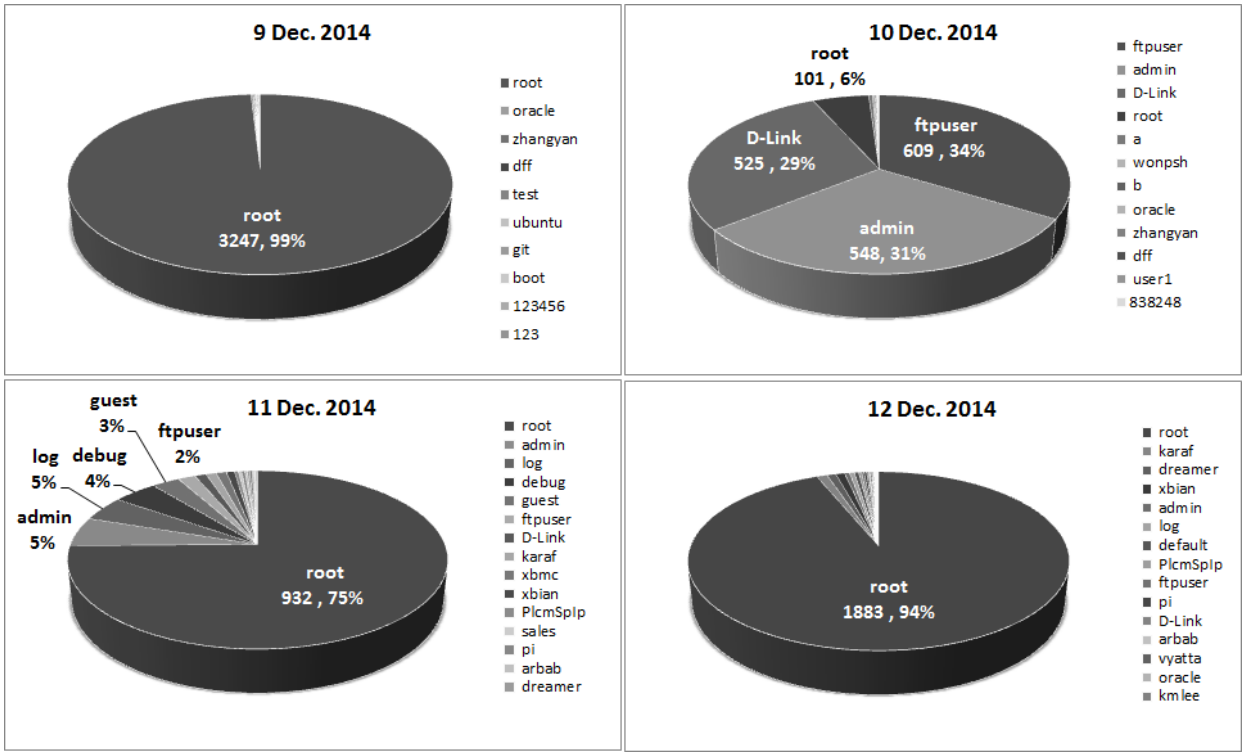

Fig. 6. Proportion of Used Accounts to SSH Brute Force Attack (9~12 Dec. 2014)

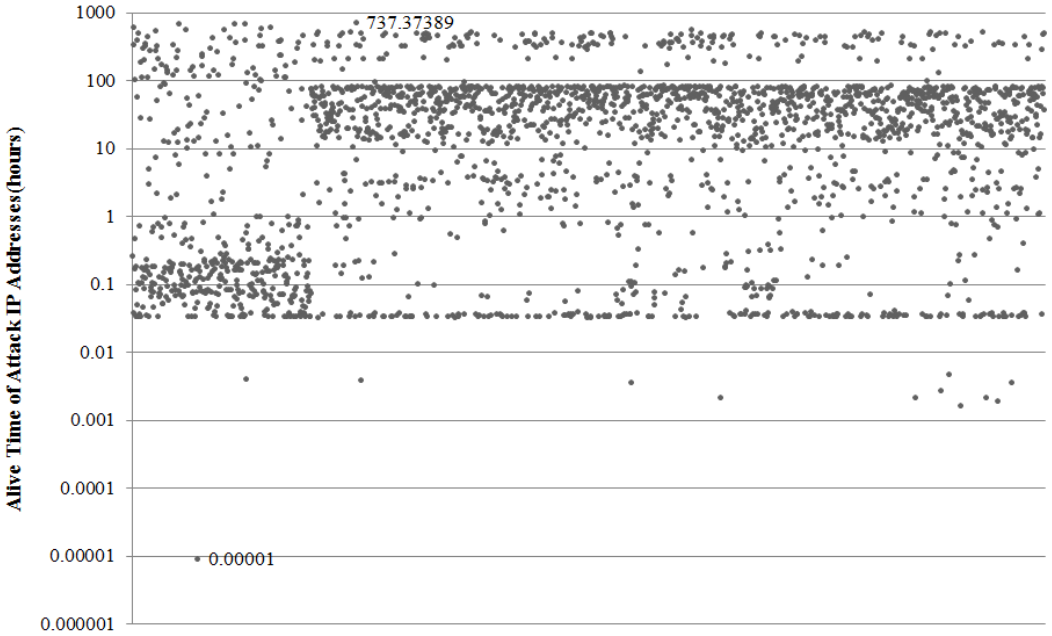

Fig. 7. Distribution of Alive Times of Brute Force Attack IP Addresses

3.4 공격 국가

Fig. 8은 공격 IP 주소 개수가 많은 TOP 10 국가를 나타낸다. 중국, 미국, 독일 3개국에서 발생한 공격 IP 주소가 전체의 50% 가까이 된다. 더 나아가 TOP 10 국가가 전체 공격 IP 주소의 71% 이상을 차지한다.

Fig. 9는 비정상 접속 시도 횟수가 많은 TOP 10 국가를 나타낸다. 중국에서 시도한 건수가 전체 비정상 접속 시도의 47.35%로 절반 가까이 차지하는 것을 볼 수 있다. TOP 10 국가로 확대하면 전체 비정상 접속 공격 시도의 83.57%가 된다.

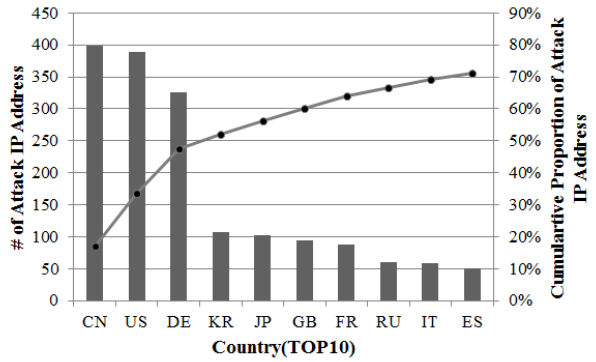

Fig. 8. Number of Attack IP Address and Cumulative Proportion (TOP 10 Countries)

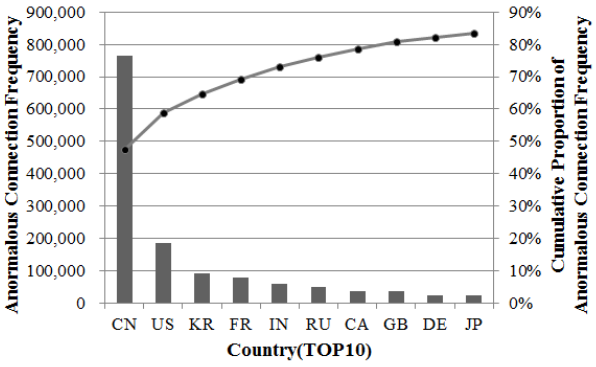

Fig. 9. Frequency and Cumulative Proportion of Anomalous Connections (TOP 10 Countries)

4. 실패로그 기반 침입탐지 및 대응

SSH 무작위 공격을 분석하여 공격의 지속 시간과 공격에 사용된 사용자 계정, 공격지 IP 주소의 국가별 통계 등 공격의 특징을 확인하였다. 이러한 정상적인 서비스를 가장한 공격을 탐지하기 위하여 첫째, 평균 65시간에 이르는 공격 지속 시간을 고려하여 타임 윈도(Time Windows)를 조정하여야 한다. 둘째, root, ftpuser, admin 등 SSH 무작위 공격에 가장 많이 사용되는 사용자 계정에 대한 탐지를 강화해야 한다. 끝으로 국내 공격자뿐만 아니라 해외, 특히 중국의 공격이 두드러지게 나타나므로 이 부분도 설계에 반영해야 한다.

4.1 설계

SSH 무작위 공격을 탐지하기 위해서 본 논문에서는 응용 기반의 SSH 서비스 로그를 통합하고 출발지 IP 주소나 사용계정 등 특정 구분자로 군집화(Clustering)하여 분석하는 실패로그 기반의 탐지 기법을 제안한다. 제안하는 기법은 2단계로 동작한다. 첫 번째는 탐지 단계로 시스템 접속 로그를 실시간으로 통합, 수집하고 분석하는 단계이다. 이 단계는 접속 실패가 계속되는 출발지 IP 주소나 사용 계정을 분석함으로써 공격이 의심되는 출발지 IP 주소를 찾아낸다. 두 번째는 대응 단계로 의심되는 출발지 IP 주소를 확인하고 공격인지 아닌지 판단하는 단계이다. 이 단계에서는 실제 서비스되고 있는 시스템이므로 오탐률(False Positive)을 최소화하기 위하여 관리자가 직접 확인하여 최종 공격 여부를 판단한다.

Fig. 10은 탐지하고 대응하는 절차를 도식화한 것이다. 사용자의 접점이 되는 시스템들의 SSH 접속 로그를 통합하여 수집(Log collector)하고 파싱(parsing) 하여 보안 로그 데이터베이스(Security Log DB)에 저장한다. Table 2는 파서에 의해 파싱 된 접속 로그 테이블의 구조를 나타낸다. 출발지 IP 주소의 국가를 확인하기 위하여 국가코드를 테이블 필드에 추가한다.

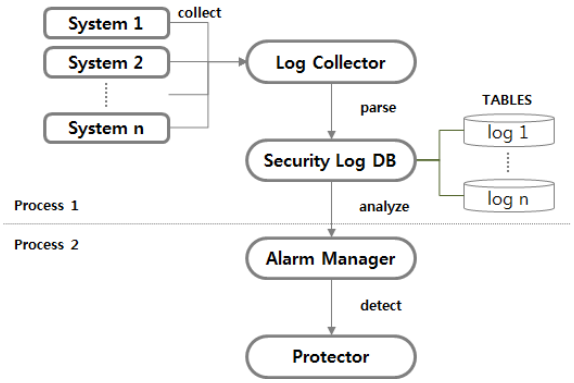

Fig. 10. Flow Chart of Failed-log Based Detection and Response Mechanism against Brute Force Attacks

수집된 보안 로그는 분석기(Analyzer)에 의하여 일정 간격으로 분석하여 특정 조건에 해당하는 이벤트가 Equation (3)과 같이 임계값(Threshold) 이상 발생하면 경고 메시지(Alarm Manager)를 발생한다. 이때 $\triangle t$는 공격의 평균 지속시간을 고려한다. 그리고 사용자 계정에 따라 이벤트의 임계값을 차별화한다. 알람이 발생하면 바로 차단을 하는 것이 아니라 관리자에 의하여 오탐 여부를 확인하고 공격인 경우에만 방화벽에서 차단하도록 정책을 설정한다.

Table 2. Field of SSH Connection Log Table in the Security Log DB

Field	Explanation	Format
Num	Index Number	Number
Date	Log Collection Time	YYYYMMDD HH:MM:SS
Src. IP	Source IP Address	A.B.C.D
Host	Target System Name	String
User ID	Account Information	Login Accounts
Auth. Result	Result of Authentication	Success(Y)/Fail(N)
Country	Country of Source IP Address	Country Code

$$\frac{\sum_{i=1}^{n} f(e_i)}{\Delta t} > Threshold, \quad (3)$$
$$\Delta t = size\ of\ Time\ Sliding\ Window$$
$$f(e_i) = failed\ Authentication\ Event\ with\ same\ Src.\ IP\ \text{or}\ User\ ID$$

4.2 구현

SSH 접속 로그는 syslog에 의해 로그 수집기에 전달되고 로그 수집기는 각 시스템별로 구별하여 로그를 저장한다. 로그는 일정 시간 간격으로 파싱하여 데이터베이스에 저장된다. (Fig. 11)은 보안 로그 데이터베이스에 저장된 SSH 접속 테이블의 일부를 나타낸 것이다. 출발지 IP 주소(Src. IP)는 보안을 위해서 일부 음영 처리하였다.

Num	Date	Src.IP	Host	User ID	Auth Result	Country
13635206	2014-12-09 13:02:26	32.34	gaiab	root	N	IL
13635197	2014-12-09 13:02:27	22.49	tachyonc	root	N	US
13635200	2014-12-09 13:02:50	13.246	gaia	root	N	TR
13635198	2014-12-09 13:03:01	140.243	tachyonc	root	N	RU
13635196	2014-12-09 13:03:24	68.22	tachyonc	root	N	IL
13635208	2014-12-09 13:03:30	.201.210	gaiad	root	N	IT
13635204	2014-12-09 13:03:31	17.226	gaiab	root	N	US
13635218	2014-12-09 13:03:33	.195.51	tachyon2c	root	N	NO
13635211	2014-12-09 13:03:34	'.189.175	tachyon2a	x993jhc	Y	KR
13635220	2014-12-09 13:03:39	.124.178	tachyon2d	root	N	CN
13635219	2014-12-09 13:03:52	27.221	tachyon2d	root	N	FR
13635217	2014-12-09 13:04:17	9.162	tachyon2c	root	N	LT
13635221	2014-12-09 13:04:18	.105.151	tachyon2d	root	N	US
13635266	2014-12-09 13:04:50	.105.151	tachyon2d	root	N	US
13635239	2014-12-09 13:04:50	46.94	gaiac	root	N	DE
13635268	2014-12-09 13:05:25	78.186	tachyon2d	root	N	US
13635235	2014-12-09 13:05:45	233.100	gaia	root	N	IT
13635253	2014-12-09 13:06:03	52.116	tachyon2b	root	N	CN

Fig. 11. SELECT query result of SSH connection log table

Table 3은 실패 로그 기반의 SSH 무작위 공격 탐지 기법을 구현한 소스코드의 일부를 나타낸 것이다. 프로그램을 시작하면(00) 보안 로그 데이터베이스에 접속하고(02~03) 이전에 검사했던 다음부터 진행하기 위하여 SSH 접속 로그 테이블에서 위치를 찾는다(04~12). Equation (3)에 일치하는 공격을 탐지하기 위하여 데이터베이스 질의문(Query)을 생성하고(14), 실행한다(15). 결과가 존재하는 경우 공격자 IP 주소를 이용하여 메시지를 생성하고(17~18), 경고 메시지를 송신한다(19). 질의문을 생성하는 단계(14)에서 출발지 IP 주소와 사용자 계정을 이용하여 군집화한다.

송신된 메시지는 Fig. 12와 같이 내용을 확인할 수 있는 창에 나타난다. 관리자는 메시지를 확인하고 해당 의심 IP 주소가 공격인 경우 차단하여 추가적인 공격으로부터 피해를 예방한다.

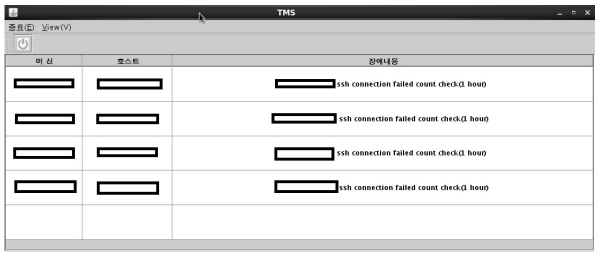

Fig. 12. Confirm Malicious Event Messages

Table 3. Source Code of the Failed-log Based Detection Method

```
(00) public static void main(Stringp[] args) {
(01)  try {
(02)   dbconn = DriverManger.getConnection();
(03)   stmt = dbconn.createStatement();
       // connect to DB
(04)   if((line = br.readLine()) != null) {
       // calculate the inspection location
(05)     pos = line; // start position
(06)   }
(07)   br.close();
(08)   query = "select max() as cnt from Table";
(09)   rs = stmt.executeQuery(query);
(10)   if ( rs.next() ) {
(11)     max_v = rs.getInt("cnt");
         // end position
(12)   }
(13)   if ( rs != null ) rs.close();
(14)   query = "select ip, count(*) as cnt from \
           Table where Auth.result = 'N' and Num > \
           " + pos + " and Num <= " + max_v + \
           "group by ip having cnt >= Threshold";
       // create a DB query for detecting
       // SSH brute force attacks
(15)   rs = stmt.executeQuery(query);
       // execute the query
(16)   while ( rs.next() ) {
(17)    String ip = rs.getString("ip");
(18)    String send_msg = ip + \
                "ssh connection failed count check";
        //create a event message
(19)    System.out.println(send_msg);
        // send the attack event message
(20)   }
(21)   if ( rs != null ) rs.close();
(22)  }
(23)  catch (Exception e) { e.printStackTrace(); }
(24) }
```

5. 결론 및 향후 연구

SSH 무작위 공격과 같이 정상적인 서비스를 가장한 슬로우 공격(Slow Attack)은 DDoS 공격 대응 시스템이나 시그니처 기반의 침입 차단 시스템 등과 같은 보안 장비에서 탐지하는 것은 쉽지 않다. 본 논문에서는 KISTI에서 운영중인 슈퍼컴퓨터 KISTI-4를 대상으로 2014년 수집된 SSH 무작위 공격을 분석하였다. 분석을 통하여 공격을 시작한 IP 주소는 평균 65시간 이상 지속적으로 무작위 공격을 시도하는 것을 확인할 수 있었고, 공격에 사용되는 계정 중 'root', 'admin', 'ftpuser' 등이 상위에 존재하는 것과 중국발 공격이 많이 발생한 것을 확인하였다. 이와 같은 분석을 통하여 본

논문에서는 시스템 접속 로그를 IP 주소나 사용자 계정으로 군집화하여 공격을 탐지하는 실패로그 기반 기법을 제안하였다. 그리고 설계 및 구현 단계에서 실패로그를 확인하기 위한 타임 윈도 및 임계값에 이를 반영하였다. 그리고 출발지 IP 주소의 국가코드 필드를 데이터베이스에 적용하였다.

NISN은 보다 안전한 서비스 제공을 위하여 사용자 계정과 패스워드를 통한 인증에 추가로 OTP(One Time Password) 인증을 적용하였다. OTP 인증 방법은 사전 공격이나 무작위로 계정과 비밀번호를 유추하는 SSH 무작위 공격으로부터 시스템을 안전하게 보호할 수 있다. 그러나 지속적인 접속 시도는 서버에 부하를 줄 수 있으므로 제안한 기법을 통하여 탐지된 공격 IP 주소를 방화벽에서 차단하여 시스템 자원이 소모되는 것을 방지하였다. 그리고 무작위 공격에 가장 많이 사용되는 계정인 'root'로의 직접적인 접속을 SSH 서비스 설정 변경('PermitRootLogin no')을 통하여 차단하여 운영 중이다.

향후 제안한 기법의 임계값 및 타임 윈도에 따른 성능 분석에 관한 연구를 계속할 것이며, 유입되는 패킷을 자동으로 분석하고 시그니처(Signature)를 추출하여 방화벽 이전단에서 유입되는 공격을 차단하거나 특정 시점에 해외 특정 국가에서 발생하는 공격을 능동적으로 차단하도록 하는 등 보안 장비(방화벽 등)에 발생할 수 있는 부하를 줄일 수 있는 선필터(Pre-Filter) 기법에 관한 연구도 지속할 것이다.

References

[1] Chan Yeol Park, JunWeon Yoon, Tae-Young Hong, and Joon Woo, "Pattern Analysis of Jobs on Supercomputer Tachyon2," *Journal of Supercomputing Information*, Vol.2, No.1, Apr., 2014.

[2] Bu Young Ahn, Ji Hoon Jang, Sun Il Ahn, Myung Il Kim, Noo Ri On, Jong Hyun Hong, and Sik Lee, "Study of High Performance Computing Activation Strategy," *International Journal of Multimedia and Ubiquitous Engineering*, Vol.9, No.6, 2014.

[3] Jae-Kook Lee, Chan Yeol Park, Sung-Jun Kim, and Joon Woo, "Performance Analysis and Improvement of Network Firewalls in the KISTI-4 Supercomputing Service Environment," *Journal of Supercomputing Information*, Vol.2, No.2, Oct., 2014.

[4] Steve Mansfield-Devine, "Interview: Tatu Ylönen, SSH communications Security," Computer Fraud & Security, May, 2012.

[5] Gene Schultz, "Using ssh: Do security risks outweigh the benefits?," *Network Security*, Vol.2004, Issue.10, Oct., 2004.

[6] Dusi, M., M. Crotti, F. Gringoli, and L. Salgarelli, "Tunnel hunter: Detecting application-layer tunnels with statistical fingerprinting," *Computer Networks*, Vol.53, Issue.1, 16th, Jan., 2009.

[7] Mehdi Barati, Azizol Abdullah, NurIzura Udzir, Mostafa Behzadi, Ramlan Mahmod, and Norwati Mustapha, "Intrusion Detection System in Secure Shell Traffic in Cloud Environment," *Journal of Computer Science 10*, 2014.

[8] Stanislav Ponomarev, Nathan Wallace, and Travis Atkison, "Detection of SSH Host Spoofing in Control Systems Through Network Telemetry Analysis," Cyber and Information Security Research Conference, 8-10th, Apr., 2014.

[9] Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari, and Joaquim Celestino Junior, "An intrusion detection and prevention system in cloud computing: A systematic review," *Journal of Network and Computer Applications 36*, 2013.

[10] Chirag Modi, Dhiren Patel, Bhavesh Borisaniyam, Hiren Patel, Avi Patel, and Muttukrishnan Rajarajan, "A survey of intrusion detection techniques in Cloud," *Journal of Network and Computer Applications 36*, 2013.

[11] Zigang Cao, Shoufeng Cao, Gang Xiong, and Li Guo, "Progress in Study of Encrypted Traffic Clasification," in ISCTCS 2012, May, 2012.

[12] Zubair M. Fadlullah, Rarik Taleb, Athanasios V. Vasilakos, Mohsen Guizani, and Nei Kato, "DTRAB: Combating Against Attacks on Encrypted Protocols Through Traffic-Feature Analysis," *IEEE/ACM Transactions on networking*, Vol.18, No.4, Aug., 2010.

[13] Laurens Hellemons, Luuk Hendriks, Rick Hofstede, Anna Sperotto, Ramin Sadre, and Aiko Pras, "SSHCure: A Flow-Based SSH Intrusion Detection System," *LNCS*, Vol. 7279, 2012.

[14] Anna Sperotto, Ramin Sadrem, Pieter-Tjerk de Boer, and Aiko Pras, "Hidden Markov Model modeling of SSH brute-force attacks," *LNCS*, Vol.5841, 2009.

[15] Dusi, M., M. Crotti, F. Gringoli, and L. Salgarelli, "Tunnel hunter: Detecting application-layer tunnels with statistical fingerprinting," *Computer Networks*, Vol.53, Issue.1, 16th, Jan., 2009.

[16] Akihiro Satoh, Yutaka Nakamura, and Takeshi Ikenaga, "SSH Dictionary Attack Detection based on Flow Analysis," in 12th International Symposium on Applications and the Internet, 2012.

[17] Xiaoqiao Huang, Hongbin Guo, "Construct the Secure Shell Transport Model and Analyze Its Security Performance," Procedia Environmental Sciences 11, 2011.

[18] Woosuk Kim, Sunghoon Kang, Kyungshin Kim, and Seungjoo Kim, "Detecting ShellCode Using Entropy," *KIPS Tr. Comp. and Comm. Sys.*, Vol.3, No.3, 2014.

[19] Aly M. El-Semary, Mostafa Gadal-Haqq M. Mostafa, "Distributed and Scalable Intrusion Detection System Based on Agents and Intelligent Techniques," *Journal of Information Processing Systems*, Vol.6, No.4, Dec., 2010.

[20] Ill Young Weon, Doo Heon Song, and Chang Hoon Lee, "A Combination of Signature-based IDS and Machine Learning-based IDS using Alpha-cut and Beta pick," *The KIPS transactions, Part C*, Vol.12C, No.4, 2005.

이 재 국

e-mail : jklee@kisti.re.kr
2012년 충남대학교 컴퓨터공학과(박사)
2010년~2013년 한국인터넷진흥원
기술개발팀 책임연구원
2013년~현 재 한국과학기술정보연구원
슈퍼컴퓨팅인프라실 선임연구원
관심분야 : 시스템 및 네트워크 보안

우 준

e-mail : wjnadia@kisti.re.kr
2000년 한남대학교 컴퓨터공학과(석사)
2010년 충남대학교 컴퓨터공학과(박사수료)
2000년~현 재 한국과학기술정보연구원
슈퍼컴퓨팅인프라실 실장
관심분야 : 병렬컴퓨팅, I/O

김 성 준

e-mail : sjkim@kisti.re.kr
2002년 한남대학교 컴퓨터공학과(석사)
2013년 충남대학교 컴퓨터공학과(박사수료)
2004년~현 재 한국과학기술정보연구원
슈퍼컴퓨팅인프라실 선임연구원
관심분야 : 로그 분석, 시스템 모니터링

박 찬 열

e-mail : chan@kisti.re.kr
2000년 고려대학교 컴퓨터학과(박사)
2002년~현 재 한국과학기술정보연구원
슈퍼컴퓨팅인프라실 책임연구원
관심분야 : 병렬 및 분산 시스템