로그 분석을 이용한 공격 트리 생성과 실시간 공격 탐지 시스템

김두회*, 김용현**, 김동화**, 신동규*, 신동일*
*세종대학교 컴퓨터공학과
**국방과학연구소
e-mail:doo6310@gce.sejong.ac.kr

Attack Tree Generation and Real-Time Attack Detection System Using Log Analysis

Duhoe Kim*, Yonghyun Kim**, Donghwa Kim**, Dongkyoo Shin*, Dongil Shin*
*Dept of Computer Engineering, Se-jong University
**Agency for Defense Development

요 약

최근 국방부는 우리 군이 운영하는 내부망이 해킹에 의해 공격당한 사실을 발표했다. 국방부는 내부망은 외부와의 망 분리를 통해 안전하게 관리되고 있다고 밝혔지만, 이번 사건으로 군에서 사용하는 내부망에도 악성코드 공격이 가능한 취약점이 존재한다는 사실이 밝혀졌다. 본 논문에서는 국방부에서 사용되는 내부망과 일반적으로 사용하는 외부망에서도 보안을 강화할 수 있는 시스템을 개발했다. 본 시스템은 공격 등급을 적용한 트리를 생성하여 일정 수준이 되면 사용자에게 알리고 공격에 이르기 전에 시스템 단에서 차단이 가능하다. 본 논문에서 개발한 시스템을 사용하면 중요한 국가기밀자료나 지적 재산이 높은 자료를 가진 국가 및 기업들이 데이터를 보호 할 수 있고 시스템이 파괴당하는 것을 사전에 방지하여 물리적인 측면도 이점을 얻을 수 있다.

1. 서론

과거부터 물리적으로 망을 외부와 분리시켜 놓는 망 구성은 국가기관이나 회사 내에서 많이 사용되어 왔다. 물리적인 망 분리는 망을 두 개로 구성하여 두 개의 모든 하드웨어 자원을 업무용, 비업무용으로 사용을 하는 것을 말한다. 비싼 구성비용과 사용자의 불편함에도 불구하고 물리적으로 외부와 망을 분리 시켜놓는 이유는 원천적으로 내부 정보를 인터넷으로 유출을 방지하기 위함이다 [1].

물리적으로 망을 분리하여 사용하는 곳은 다양한 곳이 있지만 대표적인 예로 국방부의 인트라넷을 들 수 있다. 물리적으로 망을 분리하여 사용하는 국방부는 2016년 12월 6일에 국방부 내부망이 해킹 당했다고 인정했다. 발견된 IP는 중국 선양이며 사용된 악성코드의 형태로 보아 북한의 소행이라고 추정했다. 지난해 3월에도 주요 방송국, 금융사의 전산망이 마비되었으며, 이외에도 넥슨, SK 등 대기업, 공공기관에서 내부망을 이용한 해킹이 빈번하게 일어나고 있다 [2]. 이는 내부망과 외부망의 분리만으로는 완전한 정보의 보안이 불가능하다는 것을 말하며, 망 분리 기술과 다른 새로운 보안 기술이 도입되어야 한다는 것을 의미한다. 이러한 문제점을 위해 본 논문에서는 시스템이 생성하는 로그를 비교, 분석하여 트리를 구성하고, 등급을 나누어 사용자에게 알리거나 시스템 차원에서 차단하는 시스템을 개발했다. 2장에서는 관련연구에 대해 설명하고 3장에서는 본 논문에서 개발한 시스템의 구조와 공격트리에 대해서 상세히 기술하고 4장에서는 개발한 시스템으로 실험한 내용을 기술하고 마지막 5장에서 결론과 추후 연구를 기술하며 마친다.

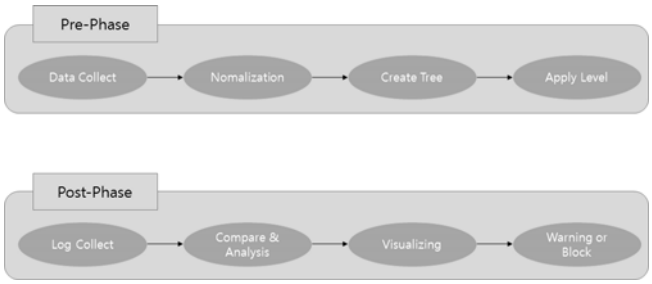
2. 관련 연구

국방부나 기업에서는 인트라넷이란 내부망을 주로 사용한다. 인트라넷은 기업이나 연구소, 국방부, 공공기관 등에서 내부의 모든 업무를 LAN환경에서 처리하기 위한 폐쇄적인 망 구성 기술을 말한다. 인트라넷은 TCP/IP프로토콜을 지원하는 환경으로 구성된다. 기존에 사용하던 인터넷 브라우저를 사용하며 여러 가지 독자적인 시스템들을 웹 환경으로 통일하여 효율성을 얻을 수 있다 [3]. 하지만 이러한 특징적인 구조가 특정한 공격에 취약해지는 단점이 있다. 이러한 구조에 적합한 공격으로 ARP Spoofing과 Backdoor를 들 수 있다. ARP Spoofing은 LAN환경에서 ARP 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법이다. 이 공격은 데이터 링크상의 프로토콜인 ARP 프로토콜을 이용하기 때문에 인트라넷처럼 구성 된 근거리상의 통신환경에서만 사용할 수 있는 공격이다. ARP 프로토콜은 요청 또는 응답메시지의 발신자를 인증하거나 제공된 정보의 무결성과 유효성을 확인하는 매커니즘이 없으므로 공격을 당하게 되더라도 사용자가 알 수 있는 경우가 많다 [4]. Backdoor는

컴퓨터나 다른 시스템에 대해 보안 메커니즘을 우회하여 원격 액세스를 얻기 위한 방법이다. Backdoor는 주로 사회 공학적 해킹 기법을 이용하여 설치된다, 주로 상대방의 권한을 이용하거나, 전화나 이메일을 통해 그들의 약점과 도움을 이용한다. 사회 공학적 해킹 기법 이외에도 소스코드의 컴파일 된 부분에 Backdoor를 삽입하도록 컴파일러를 수정하는 방법도 있고, 바이러스 같은 자동화 된 프로그램을 사용하여 Backdoor를 설치할 수 있다 [5]. Backdoor와 ARP Spoofing과 같은 다양한 공격들을 시각화하려면 그래프나 트리 같은 구조가 필요하다. 본 논문에서는 트리구조를 이용하여 계층마다 레벨을 부여 하는 방식을 사용하기 때문에 Attack Tree가 적합하다. Attack Tree를 구성하기 위해선 정형화 된 공격 데이터 리스트가 있어야 한다. 공격자가 원하는 파일, 설정, 로그 등으로 구성될 수 있으며, 구성되는 트리는 반드시 이진트리일 필요는 없다 [6]. 본 논문에서 루트노드는 공격자가 원하는 최종 공격 목표를 나타내고 자식 노드는 공격자가 목표를 달성하기 위한 필수 과정이며, 부모 노드에 존재하는 모든 취약점에 대한 유형이 자식 노드로 포함되어 구성한다.

3. 실시간 공격 탐지 시스템

그림 1은 본 논문이 설계한 실시간 공격 탐지 시스템의 전체 구조도를 두 단계로 나누어 간소화 한 것이다.



(그림 1) 실시간 공격탐지 시스템 구조도

실시간 공격 탐지 시스템은 크게 두 가지 단계로 실행한다. Pre-Phase는 사용자가 사용하기 이전에 해야 하는 전처리 과정이다. Pre-Phase를 통해 각 시스템에 맞는 트리를 설계하고 적용할 수 있다.

3.1 Pre-Phase

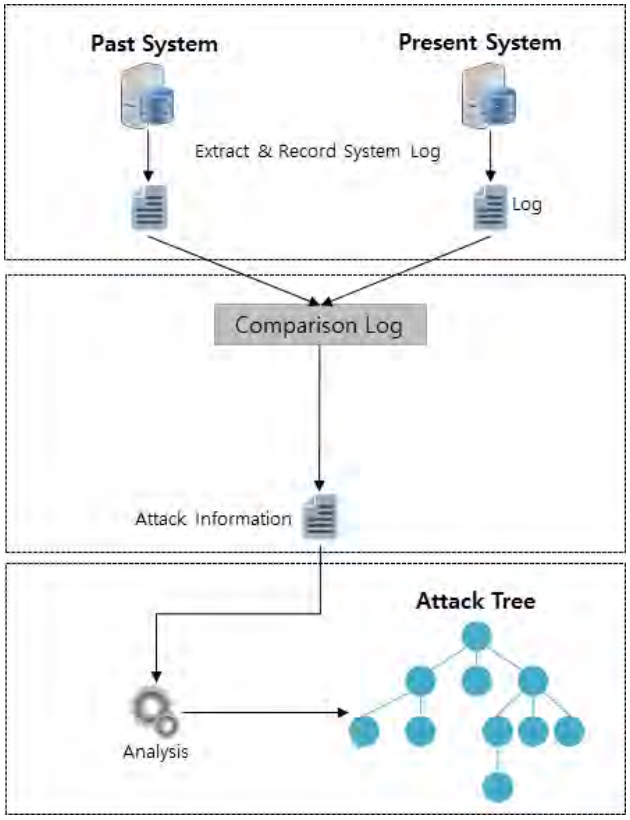
그림 2는 Pre-Phase의 상세 구조이다.

(그림 2) Pre-Phase 과정

Data Collect는 공격에 관련된 데이터를 수집하는 단계이다. 공격행동, 공격도구, 공격효과, 포렌식 도구 등 공격에 관련된 모든 데이터를 수집한다. Nomalization은 앞에서 수집한 데이터를 모아서 정규화하여 리스트화 한다. 정규화한 리스트로 트리를 구성한다. 가장 상위에는 공격자의 목표가 노드가 되고 그 하위에는 상위 목표를 달성하기 위한 공격 방법들이 자식노드로 들어간다. 한 가지 목표를 달성하기 위한 목표는 여러 가지 경로가 있기 때문에 트리는 이진트리일 필요가 없다. 다음 노드로는 공격방법의 수단이 노드가 되고 그 수단을 달성하기 위한 노드들이 수단노드들의 자식 노드를 생성하게 된다. 공격마다 트리가 하나씩 생성되며 공격 경로에 따라 마지막 차수의 자 노드 숫자가 결정된다. Attack Tree에서 레벨을 적용하는데, 가장 상위단계에 있는 노드를 Level1을 부여한다. 그 하위 노드는 Level2 하위의 하위노드는 Level3으로 오름차순으로 레벨을 부여한다. 어떠한 이벤트가 발생했을 때 공격자의 행위가 높은 레벨이면 사용자에게 통지하고 공격 목표에 가까운 낮은 레벨이 나오면 시스템 차원에서 프로세스를 종료시키거나 피해를 입지 않도록 시스템을 자동으로 종료시킨다.

3.2 Post Phase

그림 3은 Post Phase의 세부 단계이다.



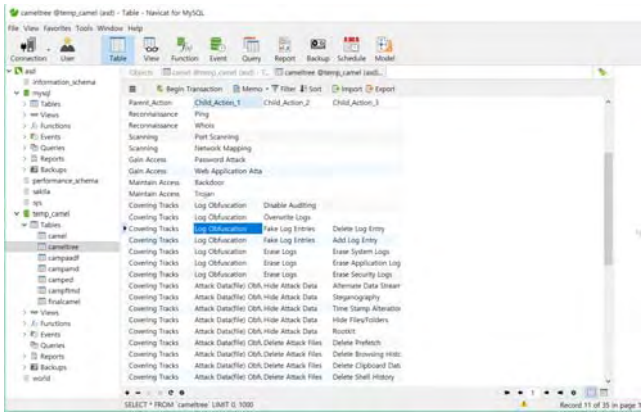
(그림 3) Post-Phase 과정

Log Collect에선 로그 비교를 위해서 공격을 당하지 않은 안전한 상태의 로그가 필요하다. 따라서 과거에 수집해 놓은 로그 데이터가 필요하다. 기존에 저장해둔 로그와 실시간으로 유입되는 로그를 비교, 분석하여 공격이 일어

나거나 관련된 공격에 관련된 행위가 포착된다면 사용자에게 알린다. 사용자에게 알리는 내용에는 공격과 공격에 관한 정보, 포렌식 도구, 해결방안 등을 포함한다. 이미 공격이 시작된 후거나 공격 행위가 발전하여 실제 공격이 이루어지기 직전까지 도달하여 공격트리에서 지정한 위험도가 높은 레벨에 접근했다면 시스템 차원에서 프로세스를 종료하거나 프로그램을 종료시킨다.

4. 실험

본 논문에서 진행한 실험은 Windows 10을 운영체제로 사용하였고, MYSQL과 Java를 이용하였다. 실험에 앞서 트리를 만들 수 있게 데이터베이스를 구성해야 한다. 그림 4는 본 논문에서 트리 구성을 위해 입력한 데이터베이스이다.



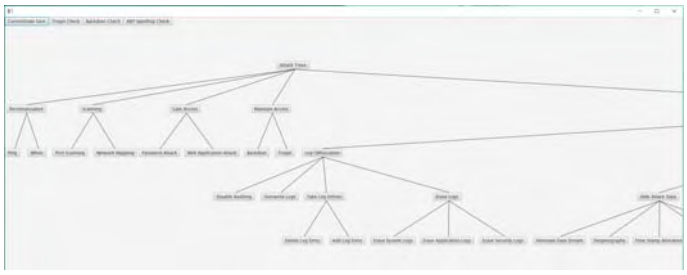
(그림 4) 트리 구성을 위한 데이터베이스

프로그램의 구성은 두 가지가 있다. 각 두 가지 프로그램은 가장 처음에 실행시켜 로그를 저장해 두는 프로그램과 저장한 이후에 실시간으로 로그를 수집하고 비교, 분석하는 프로그램으로 구성하였다. 그림 5는 공격당하지 않은 시스템에서 비교, 분석할 로그들을 미리 저장하는 프로그램을 실행 시킨 화면이다.

```
Save LIVEinfo to C:₩ForPeace₩dump
************************************************************
Dumping... (1/7)
Dumping... (2/7)
Dumping... (3/7)
Dumping... (4/7)
Dumping... (5/7)
Dumping... (6/7)
************************************************************
Finish!
************************************************************
BUILD SUCCESSFUL (total time: 0 seconds)
```

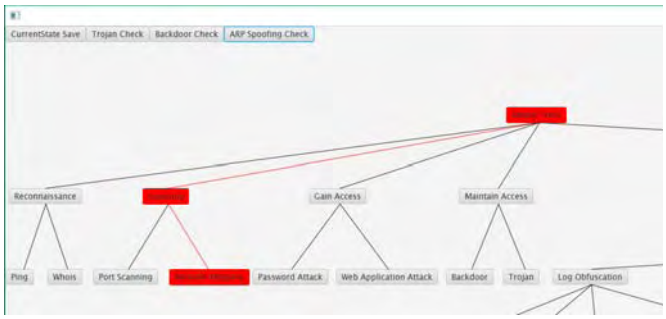
(그림 5) 로그 저장 프로그램

실험방식은 공격이 일어나지 않았을 때의 로그를 저장한 뒤 시스템에 직접 공격을 발생시킨 뒤 두 번째 프로그램을 실행시켜 공격이 일어났는지 확인 하였다. 공격은 ARP Spoofing과 Backdoor공격을 사용해 보았으며 프로그램의 작동여부를 위해 시스템 종료는 하지 않았다. 그림 6은 저장해 둔 데이터베이스를 사용하여 트리로 시각화한 프로그램이다. 이 프로그램에서 실시간으로 로그 저장이 가능하며, 실험을 위해서 버튼을 따로 만들어 놓아 실험에서 사용하는 공격만을 추출하게 설계했다.



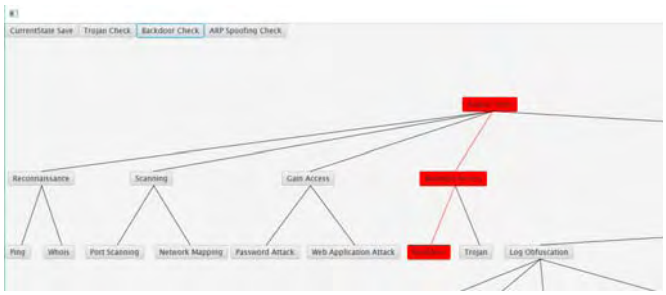
(그림 6) 데이터베이스를 이용해 트리를 그린 결과

그림 7의, 그림 8 는 사용자의 시스템에 공격을 진행한 뒤 두 번째 프로그램의 결과이다. 그림 7은 정상적인 사용자의 시스템에 ARP Spoofing 공격 후 프로그램을 실행한 결과이고 그림 8은 Backdoor 공격을 실행한 후 프로그램 실행 결과이다. ARP Spoofing과 Backdoor는 국방부의 인트라넷과 같은 내부망에 공격이 가능하기 때문에 실험에 사용했다.



(그림 7) ARP Spoofing 검출 결과

ARP Spoofing 공격은 주로 같은 망에 있는 게이트웨이의 맥주소와 공격자의 맥주소를 동일시 시켜 데이터 패킷을 가로채는 공격 수단을 사용하였다. 이러한 공격수단은 같은 내부망에 같은 주소가 있는지 체크하는 것으로 간단하게 해결할 수가 있으므로 안전한 상태의 데이터가 필요 없이 실시간으로 수집한 맥주소만으로도 판별이 가능하다.



(그림 8) Backdoor 검출 결과

그림 8은 Backdoor공격의 검출 결과이다. Backdoor는 공격자가 사용자의 시스템을 원격조종하거나 데이터를 우회해서 가져갈 수 있다. 이를 위해선 현재 사용 중인 포트 이외에 다른 포트를 열어서 공격자의 시스템과 통신해야 한다. 이 프로그램에서는 Backdoor를 검출 할 때 공격이 들어오기 전에 저장했던 안전한 데이터와 실시간으로 열린 포트를 비교해서 Backdoor의 여부를 알아낸다.

5. 결론

본 논문은 국방부에서 사용하는 인트라넷이나 사내에서 사용하는 내부망에서 사용할 수 있는 실시간 공격 탐지 시스템을 개발했다. 본 논문에서 제안한 시스템을 사용하면 내부망에서 외부로의 정보 유출을 막을 수 있다. 또한 공격자로부터의 시스템 파괴도 사전에 방지함으로써 물리적인 측면에서도 이점을 볼 수 있다. 추후 연구로는 각 시스템마다 프로그램을 설치하지 않고 따로 분리하여 여러 대의 로그를 한 시스템에서 수집하여 처리하는 방식으로 변경하는 방법을 연구하고, 이외에 다른 공격들을 방어하는 방법을 더 추가하여 완전한 보안프로그램으로 개발하는 것이다.

ACKNOWLEDGMENT

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD160066BD).

참고문헌

[1] Lee Y. and Yoo S., "The construction of logical, physical network separation by virtualization," *Korea Convergence Security Association*, vol. 14, no. 2, pp. 25-33, 3, 2014.

[2] Lee M., "A study for national cyber security and defense," *The Korea Contents Society*, 2013, pp. 18-22.

[3] Dick S., "Designing the new intranet", 2002.

[4] Talal A., Durando D., "Securing ARP in Software Defined Netwrorks," *Local Computer Networks 2016 IEEE 41st Conference on*, 2016.

[5] Salimi E., Arastouie N., "Backdoor detection system using artificial neural network and genetic algorithm," *Computaional and Information Sciences,* 2011.

[6] Mateski Mark, "Cyber threat metrics" *Sandia National Laboratories*, 2012.