미수 공격의 목표를 예측하기 위한 공격트리 시스템

송경진, 신동규, 신동일
세종대학교 컴퓨터공학과
e-mail:yoroos@gce.sejong.ac.kr

Attack Tree System for Predicting Target of Attempted Attack

Song Kyoungjin, Shin Dongkyoo, Shin Dongil
Dept of Computer Engineering, Se-jong University

요 약

정보통신 시스템이 나날이 발전하고 거대화되면서 해킹시도 또한 기하급수적으로 늘어나고 있다. 그러나 해킹 시도의 대다수는 성공으로 이어지지 않고, 단순의 탐색 경우가 대다수이다. 따라서 미수로 끝난 공격에서 공격 경로 및 공격 목표를 예측함으로써 추가적인 공격에 대비할 수 있는 시스템을 구축할 필요성이 있다. 그러므로 본 논문에서는 포렌식 분석, 해커의 문서, 보안 보고서 등을 토대로 공격 행위, 공격 결과 및 목표 등과 같은 공격 정보를 수집하고 공격트리를 만들어 레지스트리 정보, 프로세스 정보, 보안 로그 등과 같은 시스템 정보를 토대로 공격 목표를 찾는 시스템을 제안한다.

1. 서론

정보통신 시스템이 나날이 발전하고 거대화되면서 해킹시도 또한 기하급수적으로 늘어나고 있다 [1, 2]. 하지만 모든 해킹 시도는 성공으로 이어지지 않을뿐더러 단순한 탐색을 위한 해킹 시도인 경우도 많다. 예를 들어 다중 취약점 스캔 공격, 특정 취약점 스캔 공격, 은닉 스캔, 네트워크 구조 스캔 등이 있다 [3]. 이러한 탐색을 위한 해킹 시도인 경우 차후 더 위협적인 공격이 시도 될 수 있다. 그렇기 때문에 추가적인 위험을 방지하지 않으면 더 큰 위협이 될 수 있다. 그러므로 미수로 끝난 공격에서 공격 경로 및 공격 목표를 예측하여 추가적인 공격에 대비할 수 있는 시스템이 필요하다.

본 논문의 구성은 다음과 같다. 2장에서는 공격정보를 수집하는 방법에 관해 설명한다. 3장에서는 공격 트리를 구성하는 방법과 구축된 시스템을 기반으로 공격의 목표를 예측하는 방법에 대해 설명한다. 마지막 4장에서는 결론을 내리며 향후 연구에 대해 설명한다.

2. 관련 연구

공격 목표를 예측하기 위해서는 사전의 공격 방법에 대해서 수집 및 분류를 해야 한다. 이러한 공격 방법을 수집하기 위해서는 주로 포렌식 분석 기술, 해커의 문서, 보안 보고서, 보안 실무자의 경험 등이 필요하다. 앞에서 서술한 방법을 토대로 공격 행위, 공격 결과 및 목표 등과 같은 데이터를 수집한다. 단 데이터를 수집할 때는 공격에 관련된 모든 데이터를 수집해야 한다. 그 이유는 공격자가 사용할 수 있는 방법을 고려할 때 범위를 한정할 수 없기 때문에 모든 공격에 관한 모든 데이터가 존재해야 한다. 수집된 데이터는 데이터베이스에 저장되어 공격트리를 만드는데 사용되고, 후에 공격 목표를 예측할 때 시스템 정보를 기반으로 공격에 대한 노드를 찾기 위해 사용된다.

3. 시스템 설계

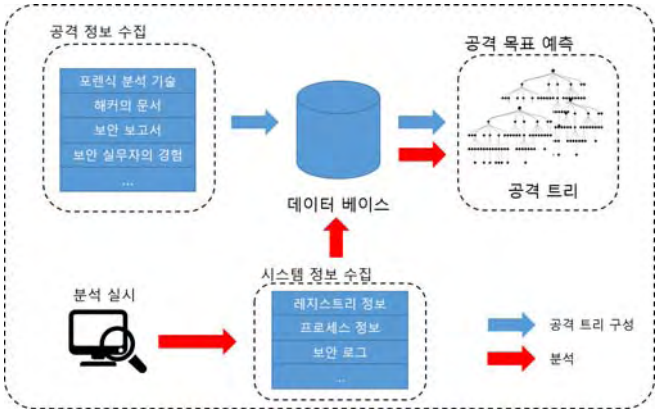
본 논문에서 제안하는 시스템을 사용하기 위해선 공격 정보 수집 과정이 필요하다. 이러한 수집 과정에서는 주로 포렌식 분석 기술, 해커의 문서, 보안 보고서, 보안 실무자의 경험 등을 통해 작성된다. 공격 정보를 수집하고 공격 트리를 구성한 후 분석을 실시하였을 때 수집 된 시스템 정보를 기반으로 공격 트리들에서 해당 노드들을 탐색 후 탐색 된 노드들을 기반으로 공격 목표를 예측한다.

3.1 Attack Tree

공격 트리의 구조는 노드, 간선, 커넥터로 구성되어 있다. 각 노드는 수집된 데이터를 바탕으로 하나의 공격을 나타내고 있으며, 공격 트리의 최상위 노드는 공격자가 원하는 최종 목표로 설정되고, 상위 노드에서 하위 노드로 내려 갈수록 상위 노드의 공격에 이르기 위한 공격으로 분해되는 과정을 반복하며 트리를 구성한다. 한 가지 목표를 달성하기 위한 공격 방법은 여러 가지가 될 수 있지만, 모든 공격이 달성되어야만 상위 공격에 이르는 것은 아닐 수도 있다. 따라서 간선은 AND와 OR 연산을 가지는 각

각의 커넥터를 가질 수 있으며, 공격의 진행 상태를 표시한다. 2개 이상의 자식 노드들을 가진 노드의 공격 목표를 달성하기 위한 전제조건으로 자식 노드 중 1개만 선택 실행이 가능한 경우를 OR로 묘사하고 모든 자식 노드들이 반드시 실행되어야 하는 경우를 AND로 묘사한다 [4]. 본 논문에서는 이러한 공격트리를 이용한 미수 공격의 목표 예측 시스템을 제안한다.

3.2 시스템 구성도



(그림 1) 시스템 구성

본 시스템은 크게 공격 트리 구성 단계와 분석 단계 두 가지 단계로 구성 된다. 공격 트리 구성 단계에서는 데이터를 수집하고 데이터베이스에 저장하며 저장된 데이터를 토대로 공격 트리를 구성한다. 그리고 분석 단계는 분석을 실시하였을 때, 시스템 정보를 수집하여 데이터베이스의 정보와 비교하여 공격 트리에서 해당 노드를 찾아 공격 목표를 예측한다. 예측 결과 도출을 위해 사용되는 기준은 전체 노드 중에 시스템 정보를 기반으로 찾은 노드 수의 비율 그리고 분석을 실시하였을 때 시도 되었던 공격 빈도 수 이다. 이러한 기준을 통해 분석 한 결과로 공격 목표를 예측한다. 공격 목표 예측 결과는 하나가 아닐 수도 있으며 가장 확률이 높은 순으로 정렬된 결과를 제공한다.

4. 결론

본 연구에서는 공격 정보를 수집하여 데이터베이스를 만들고 데이터베이스를 이용해 트리를 만들었다. 이 트리를 이용하여 공격 목표를 예측하고 추가적인 피해를 막을 수 있는 시스템을 제안 하였다. 본 시스템을 이용하면 공격자의 공격 목표를 예측하고 추가적인 피해를 방지할 수 있는 효과를 기대해 볼 수 있다. 논문에서 제안한 시스템은 결과적으로 공격의 목표를 예측하지만 어떠한 공격은 다양한 공격의 자식 공격이 될 수 있으므로 공격 목표 결과가 하나가 아닌 복수가 나올 수 있다. 향후에는 다수의 공격 목표가 나오는 경우를 줄이기 위해 공격 트리를 생성할 때 중복된 공격 정보를 최소화 하여 생성한 트리를 이용해 최소의 결과를 도출하는 시스템을 연구하려고 한다.

Acknowledgement

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD160066BD).

참고문헌

[1] 장문수, 구향옥, 오창석. "유해 트래픽 분석을 이용한 침입 방지." 한국컴퓨터정보학회논문지 , 10.4 (2005.9): 173-179. Print.

[2] 주, 박창욱, 이수진, 임재성. "사이버 방어작전 프레임워크 기반의 공격그룹 분류 및 공격예측 기법." 정보과학회논문지 : 컴퓨팅의 실제 및 레터, 20.6 (2014.6): 317-328. Print.

[3] 유일선, and 조경산. "정보보안: 네트워크 취약점 검색 공격에 대한 개선된 탐지시스템." 정보처리학회논문지 C 8.5 (2001): 543-550.

[4] Schneier, Bruce. "Attack trees." Dr. Dobb's journal 24.12 (1999): 21-29.