국방망에서 세션분석기반의 침입자 역추적 시스템

장희진°, 윤호상, 김상수, 박재근, 김철호
국방과학연구소
{janghj°, yunhs}@add.re.kr, wisdory@naver.com, parkjaek@korea.com, cheolkim@add.re.kr

Session Analysis based Intruder Traceback System in Defense Network

Heejin Jang°, Hosang Yun, Sangsoo Kim, Jaekeun Park, Cheolho Kim
Agency for Defense Development

요 약

21세기 정보혁명을 바탕으로 전쟁의 양상은 정보전, 네트워크 및 컴퓨터 중심의 사이버전과 같은 새로운 전쟁 패러다임으로 변화하고 있다. 이러한 정보전에 대비하여 국방정보체계에 다양한 정보보호시스템을 설치하여 사용하고 있다. 그러나 국방정보체계 환경에 현재까지 배치된 정보보호시스템들은 침해 사고에 대한 탐지 및 보고 등의 수동적인 대응만을 지원한다. 그러므로 발생한 공격에 대한 대응을 마련하더라도 동일한 공격자가 동일한 목표 시스템에 대하여 또 다른 공격 기술을 이용하여 재침입이 가능하다. 이를 방어하기 위하여 공격에 대한 능동적인 대응이 필요하다. 대표적인 능동 대응 기술인 침입자 역추적은 시스템 및 네트워크에 대하여 공격을 시도하는 침입자의 네트워크 상의 실제 위치를 추적하는 기술이다. 침해 사고를 근본적으로 차단하기 위하여 침입자의 실제 신분 확인이 필수적이다. 이를 위하여 본 논문에서는 침입자 역추적 기술을 분석하고 국방정보체계 환경을 위한 세션분석기반의 침입자 역추적 기술을 제안한다. 또한 이 기술을 기반으로 구현한 침입자 역추적 시스템을 소개한다.

1. 서 론

정보화 시대의 도래로 군도 정보체계, 지휘통제, 작전체계 등의 분야에서 정보시스템 의존도가 급증하는 추세에 있으며, 첨단 정보통신기술을 이용하여 주요 국방정보기반을 교란·마비시킬 수 있는 사이버 공격의 위협이 다양화, 고도화 되고 있다. 동일한 침입자에 의한 침해사고의 재발을 막기 위하여 탐지, 복구 등의 수동적 방어와 함께 역추적과 같은 능동적 대응이 필요하다. 능동적인 대응으로서의 침입자 역추적은 시스템 및 네트워크에 대하여 공격을 시도하는 공격자의 네트워크 상의 실제 위치를 알아내는 기술이다[1].

대부분의 침입자는 자신을 추적하기 어렵게 하기 위하여 대규모 분산 네트워크 환경의 속성을 이용하여 여러 호스트를 경유하거나 소스 호스트의 IP 주소를 변경한다[2,3]. 그러므로 현재 인터넷 환경에서는 부분적으로 침입자에 대한 추적이 가능하지만 전체 환경을 구성하는 모든 도메인에 대하여 관리자 권한을 가지지 않는 한 전체 공격경로를 파악하기는 어렵다. 현재 침입자 역추적에 대한 연구가 활발하게 진행되고 있지만 위와 같은 인터넷 환경의 근본적인 제약때문에 일정한 가정이 없다면 현재까지 제안된 역추적 기술을 지금의 환경에 적용하는 것은 불가능하다.

국방망 역시 다양한 종류의 호스트와 네트워크로 구성된 대규모 분산 네트워크 환경이지만 외부와는 분리된 폐쇄망이며, 물리적으로는 여러 개의 도메인으로 구성되지만 논리적으로는 일종의 단일망으로 볼 수 있다. 이러한 국방망 환경에서 환경의 속성과 익명성을 이용한 공격을 근본적으로 막기 위하여 국방정보체계의 호스트 또는 네트워크를 공격한 침입자를 역추적하여 신분을 확인할 필요가 있다.

본 논문에서는 국방망 환경에서 우회공격을 시도하는 침입자를 식별하는 세션분석기반의 침입자 역추적 기술과 시스템을 제안한다.

본 논문에서 제시하는 세션분석기반의 침입자 역추적 기술은 침입과 연관된 세션을 기반으로 침입자의 이동경로를 추적하므로 정확하고 신속하게 우회공격을 시도한 침입자의 이동 경로를 추적할 수 있다. 침입을 탐지함과 동시에 역추적 프로세스가 동작하므로 평상시 처리 과부하를 없애고 최소의 데이터를 기반으로 침입자를 역추적할 수 있다. 또한 침입자가 침입을 완료하기 전에 실시간으로 침입자 경로 파악이 가능하다.

본 논문의 2장에서는 침입자 역추적 기술의 개념과 우회공격에 대한 역추적 기술에 대한 관련연구를 소개한다. 3장에서는 세션분석기반의 침입자 역추적 기술을 제시하고 4장에서는 이를 기반으로 구현한 침입자 역추적 시스템을 소개한다. 5장에서는 향후 연구방향을 제시하며 결론을 맺는다.

2. 침입자 역추적 기술

2.1 침입자 역추적 기술의 개념 및 분류

침입자 역추적은 시스템 및 네트워크에 대하여 공격을 시도하는 침입자의 네트워크 상의 실제 위치를 탐색하는 기술이다. 침입자 역추적 기술은 크게 우회공격 역추적 기술과 IP 패킷 기반의 역추적 기술로 분류된다. 우회공격 역추적은 침입자가 여러 호스트를 경유하여 우회 공격을 시도하는 경우, 침입자의 실제 위치를 추적하는 기술이다. IP 패킷 기반의 역추적은 IP 주소가 변경된 패킷의 실제 송신지를 추적하는 기술이다. 본 논문에서 제시하는 기술은 우회 공격을 대상으로

한다.

2.2 우회공격에 대한 역추적 기술

침입자는 추적 자체를 어렵게 하기 위하여 여러 호스트를 경유하여 공격을 수행한다. 하나의 호스트에서 다른 호스트로 이동할 때 두 호스트 간에 TCP 연결이 생성된다. 이 연결을 유지한 상태에서 또 다른 호스트로 로그인하여 이동하면 두번째 TCP 연결이 생성된다. 이렇게 여러 호스트를 경유할 때 생성되는 TCP 연결의 순서화된 집합을 연결체인이라 한다. 우회공격에 대한 역추적이란 침입이 탐지된 현재 호스트로부터 시작하여 침입자의 연결 체인을 구성하여 침입자가 공격을 시작한 소스 호스트의 IP 주소를 알아내는 것이다. 우회공격에 대한 역추적 기술은 대표적으로 호스트 기반의 기술, 네트워크 기반의 기술이 있다.

호스트 기반 연결 역추적은 인터넷 상의 모든 호스트에 역추적 모듈을 설치하고 이들의 상호작용을 통하여 침입자를 추적하는 기술이다. 호스트에서 발생하는 로그 기록 등의 다양한 정보를 바탕으로 침입자를 추적한다. 이러한 기술을 구현한 시스템의 예로는 Distributed Intrusion Detection System(DIDS)[4], Caller Identification System(CIS)[5], CallerID[6] 등이 있다. 이 기술을 이용하여 침입자를 성공적으로 추적하기 위해서는 인터넷 상의 모든 호스트에 역추적 모듈을 설치해야한다. 비록 이것이 가능하더라도 임의의 호스트에 대한 무결성을 유지하기 어려우므로 호스트 기반의 역추적은 현재 환경에 구현하기는 어렵다.

네트워크 기반의 연결 역추적은 라우터와 같이 네트워크 상에 송수신되는 패킷을 확인할 수 있는 위치에 역추적 모듈을 설치하고 패킷들로부터 정보를 추출하여 역추적을 수행하는 기술이다. 연결에서 같은 방향으로 움직이는 패킷들을 패킷 스트림이라한다. 연결 체인에서는 침입에 사용된 연결과 그것의 모든 업스트림 연결에는 같은 패킷 스트림이 전송되며 이러한 속성을 이용한 것이 네트워크 기반의 침입자 역추적이다. 네트워크 기반 침입자 역추적 기법으로는 썸프린트(Thumbprint) 기술[6], 타이밍(Timing) 기반의 기술[7] 등이 있다. 이 기술들은 동일한 연결 체인에 속하는 연결들을 찾을 수 있다고 하더라도 네트워크에 송수신되는 패킷들로부터 획득한 정보를 비교할 때 발생하는 순서 관계 문제를 해결하기 어렵고, 오탐 및 과탐이 발생하기 쉬우며 네트워크에서 발생하는 모든 연결에 대한 정보를 수집 기록해야한다. 이와 같은 문제점 때문에 네트워크 기반의 역추적 기술 또한 현재 환경에 적용하는데는 무리가 있다.

3. 세션분석기반의 침입자 역추적 기술

연결체인을 구성하는 모든 세션연결에는 동일한 패킷이 전송되므로 일정시간내에 전송되는 데이터의 양이 유사하다. 이는 같은 연결체인을 구성하는 세션이라면 그 세션들을 구성하는 패킷들의 데이터바이트는 다른 세션에 대하여 각각 대응하는 데이터바이트를 가진다는 것을 뜻한다. 국방망에서의 침입자 추적을 위한 세션분석기반의 침입자 역추적 기술은 연결체인을 구성하는 세션들의 각 대응하는 데이터바이트 간의 전송시간의 평균과 분산이 유사한 값을 가진다는 사실을 기반으로 침입자를 추적한다.

그림 1 은 세션분석기반의 침입자 역추적 동작 및 알고리즘을 나타낸다. 그림에서 굵은 선으로 표시한 것이 침입자의 연결체인이고 호스트 간의 하나의 연결을 세션연결이라고 한다. 두 호스트 간의 세션연결은 (IP 주소, 포트 번호)로 구성된다. 그림과 같이 침입자가 호스트 A에서 B를 거쳐 C로 이동한다고 가정할 때, 두 개의 세션 (A,100)-(B,300)와 (B,500)-(C,600) 이 생성되고 이들 세션연결은 하나의 연결체인을 구성하므로 일정한 시각에 유사한 양의 데이터가 전송된다. 그 외의 사용자에 의한 세션연결 (A,200)-(B,400)에는 전혀 다른 데이터가 전송된다.

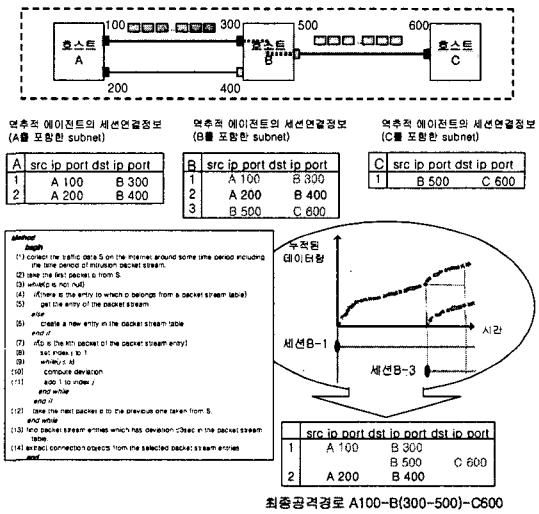

그림 1 세션분석기반의 침입자 역추적 알고리즘

침입이 탐지되는 순간, 일정한 시각동안 또는 일정한 양의 데이터가 모일 때까지 모든 세션정보를 수집한다. 침입 세션과 비교할 세션을 선택하고 두 세션을 구성하는 각 대응패킷간의 전송시간을 계산한다. 비록 하나의 연결체인을 구성하는 세션일지라도 호스트의 운영체제 및 사용하는 어플리케이션의 종류, 연결 방법에 따라 전송되는 패킷에는 차이가 있을 수 있다. 즉, 패킷들이 일대일로 대응할 수도 있지만 하나의 패킷이 두개 이상의 패킷으로 나누어지는 경우, 여러 개의 패킷이 하나로 합쳐지는 경우 등이 발생할 수 있으므로 이러한 모든 경우를 고려하여 대응패킷을 계산한다. 두 세션의 각 대응패킷간의 전송시간의 평균과 분산을 계산하여 일정 범위내에 속하면 동일 연결체인에 있다고 판단한다. 또 다른 비교세션을 선택하여 동일한 과정을 반복하고 유사한 값을 가지는 세션들을 연결하여 침입의 근원지를 알아낸다.

4. 시스템 프로토타입

4.1 시스템 동작 및 구조

제안한 세션분석기반의 침입자 역추적 기술을 적용하여 시스템을 구현하였다. 본 시스템은 공격을 시작한 호스트 및 사용자를 추적하여 식별하는 시스템으로서 하나의 역추적 매니저와 각 망을 관리하는 다수의 역추적 에이전트로 구성된다. 그림 2는 침입자 역추적 시스템의 동작을 나타낸다.

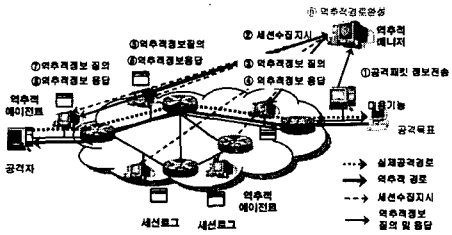

그림 2 세션분석기반의 침입자 역추적 시스템 동작

침입이 탐지되면 역추적 매니저는 침입 이벤트가 발생한 망의 역추적 에이전트에게 역추적을 지시한다. 역추적 에이전트는 망에서 수집된 데이터를 이용하여 침입을 역추적하고 역추적 매니저에게 결과를 알린다. 역추적 매니저는 이 결과를 기반으로 연관된 망의 또 다른 역추적 에이전트에게 역추적을 지시한다. 이 과정을 반복하여 침입 경로뿐만 아니라 침입의 근원지를 알아낸다. 그림 3은 침입자 역추적 시스템의 구조이다.

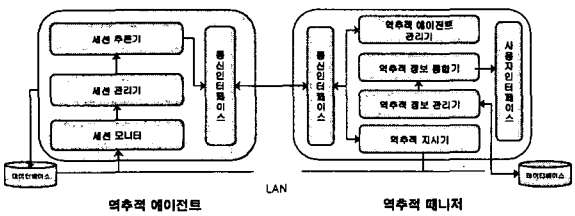

그림 3 세션분석기반의 침입자 역추적 시스템 구조

역추적 매니저는 침입 이벤트 수신, 역추적 에이전트에게 역추적 지시, 역추적 결과 통합 및 추론 기능을 제공하며 역추적 에이전트는 세션수집 및 역추적 수행과 역추적 결과 송신 기능을 지원한다.

4.2 구현

침입자 역추적 시스템의 주요 모듈은 Linux와 Unix 운영체제를 설치한 펜티엄 IV급 이상 PC를 기반으로 구현하였다. 세션정보와 역추적 정보 등을 저장하기 위한 데이터베이스로는 MySQL을 사용하였고 사용자 인터페이스는 JAVA를 이용하여 구현하였다. 그림 3은 침입자 역추적 시스템의 역추적 결과 화면이다. 구현화면의 위쪽 창은 침입자 역추적의 결과를 시각적으로 보여주고 아래쪽 창은 침입자 역추적 경로에 대한 상세한 정보를 제공한다.

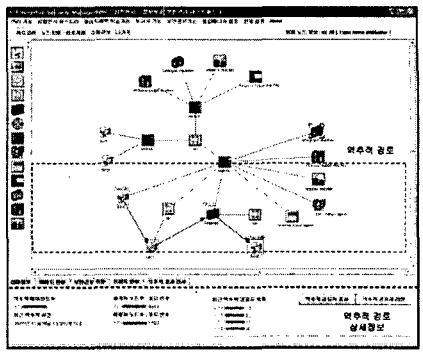

그림 4 구현화면

5. 결론

대규모 분산 네트워크 환경이지만 폐쇄망과 논리적인 단일망이라는 국방정보체계의 환경 속성을 기반으로 침입자를 추적하는 세션분석기반의 침입자 역추적 기술을 제안하고 시스템으로 구현하였다. 본 논문에서 제안하는 역추적 기술은 침입과 연관된 세션정보만을 수집, 분석하여 침입자를 추적하므로 정확하고 신속하게 우회공격을 시도한 침입자의 이동경로를 실시간으로 파악할 수 있다. 이로써 침입의 근원지를 밝힐 수 있고 침입에 취약한 호스트 및 네트워크를 확인할 수 있다.

향후 세션분석기반의 침입자 역추적 기술을 보완하여 공격자 신분확인의 정확도를 높이며 DDoS, DRDoS 공격을 포함한 DoS 공격을 역추적하는 IP 패킷 기반의 역추적 기술도 함께 개발하여 상호 보완할 수 있도록 연구 개발을 진행할 예정이다. 또한 국방정보체계 환경의 변화와 함께 능동 네트워크; 무선 네트워크 환경에서의 침입자 역추적에 관한 연구도 진행할 계획이다.

참고문헌

[1]S.S. Chen and L.T. Heberlein, "Holding Intruders Accountable on the Internet." *Proceedings of the IEEE Symposium on Security and Privacy,* pp. 39-49, 1995.

[2]D. Schnackenberg, K. Djahandari and D. Sterne, "Infrastructure for Intrusion Detection and Response," *Advanced Security Research Journal,* Vol. 3, pp. 17-26, 2001.

[3]H.Jang and S.Kim, "Real-Time Intruder Tracing through Self-Replication," *Information Security, LNCS2433, Springer,* pp. 1-16, September 2002.

[4]S. Snapp et al., "DIDS(Distributed Intrusion Detection System) Motivation, Architecture, and an early prototype," *Proceedings of National Computer Security Conference,* pp. 167-176, 1991.

[5]H. Jung, H. Kim, Y. Seo, G. Choe, S. Min, C. Kim, "Caller Identification System in the Internet Environment," *Proceedings of USENIX Security Symposium,* 1993.

[6]S. S. Chen, "Distributed tracing of intruder", *Thesis of masters degree,* Department of Computer Science, U.C.Davis. 1997.

[7]Y.Zhang and V.Paxson,"Detecting Stepping Stones," *Proceedings of USENIX Security Symposium,* August 2000.