시스템 보호를 위한 에이전트 기반의 능동 보안

박지철[+], 김희연[+], 신 원[+], 이경현[ǂ]
+ 부경대학교 전자계산학과, ǂ 부경대학교 전자컴퓨터정보통신공학부

Mobile Agent based Active Security for System Protection

Ji-Choul Park[+], Hee-Yeon Kim[+], Weon Shin[+]and Kyung-Hyune Rhee[ǂ]
+ Dept. of Computer Science, PKNU
ǂ Division of Electronic, Computer and TeleCommunication Engineering, PKNU

요 약

다양한 네트워크 시스템이 구축됨에 따라 시스템 해킹 사례도 비례해서 증가하고 있다. 점차 분산화, 자동화, 에이전트화되고 있는 공격 기법에 대하여, 본 논문에서는 최근 네트워크를 통하여 이루어지는 시스템 공격 기법을 살펴보고 그 동향을 분석한다. 그리고, 이를 효과적으로 대응하고 방어할 수 있는 새로운 개념인 능동 보안(Active Security)의 개념을 살펴보고, 핵심 기술인 이동 에이전트의 도입 및 적용에 대하여 논의한다.

1. 서론

최근 인터넷을 통한 많은 위협 및 범죄가 등장하고 있으며 이를 통한 막대한 시간 및 경제적인 피해가 보고되고 있다. 과거 미국의 Yahoo나 CNN 등 유명한 전자상거래의 대표적인 사이트가 서비스 거부 공격(Denial of Service)을 당한 것은 네트워크를 통한 공격이 얼마나 심각한 정도에 다다랐는지 보여주는 단적인 예이다.

많은 가상기업 및 인터넷관련 기관들이 자신의 정보와 시스템을 보호하기 위한 노력을 기울이고 있으며 네트워크 및 시스템 보안 문제에 많은 관심을 가지고 주목하고 있다. 그러나 이러한 노력에도 불구하고 현재 시스템의 취약점을 이용하는 공격용 프로그램들은 날로 복잡하고 정교해지고 있으며 새로운 공격 기법들이 속속 등장하고 있다. 따라서 이러한 공격에 대처하기 위한 새로운 방어 방법들이 개발되고 그 방법에 대응하기 위한 발전된 공격방법이 역시 개발되고 있는 실정이다. 최근 보고 되고 있는 해킹 피해 건수는 매년 3배 이상의 증가 추세를 보이고 있으며, 과거의 잘 알려진 공격이 아니라 새로운 공격 기법들이 시도되고 있고, 점차 은닉화, 분산화, 에이전트화, 자동화되고 있는 추세이다[1].

본 논문은 전통적인 공격 기법과 최근 동향, 앞으로의 공격 방향에 대하여 분석하고 이를 효과적으로 대응하기 위한 능동 보안을 소개하고 그 핵심 기술인 이동 에이전트 기술의 도입 및 적용을 고려한다.

2. 공격 방법 및 동향

2.1 전통적인 공격 기법

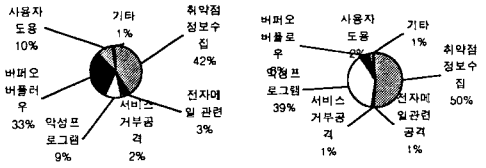
전통적인 네트워크 공격은 그 절차 및 기법이 이미 잘 알려져 있어 잠재적인 취약점을 방어하기 위한 수단이 많이 강구되어 왔다. 일반적인 공격절차는 가장 먼저 공격대상에 대한 "정보수집 단계"이며, 그 다음 수집한 정보를 바탕으로 "시스템 침입 단계"를 거치게 된다. 그리고 지속적인 침입 및 다른 시스템의 공

격을 위한 "공격 전이 단계"를 거치게 된다[2].

2.2 최근 동향

'00년은 '99년의 572건에 비하여 3배 이상 늘어난 1943건의 해킹사고가 보고되었다. 또한 '01년 3월까지 1083건의 피해로 '00년의 절반이상을 넘어 서고 있다. 이러한 현상은 미국, 영국, 일본도 마찬가지로 전세계적으로 해킹사고는 크게 증가하고 있다는 것을 알 수 있다. 이러한 해킹사고의 급증 원인은 아래 세 가지의 원인을 들 수 있다[1].

- 네트워크로 연결되는 개방된 정보시스템과 사용자의 지속적인 증가
- 해커들의 자유롭고 빠른 정보의 교환
- 정보시스템 관리자의 시간적, 기술적 역량 부족

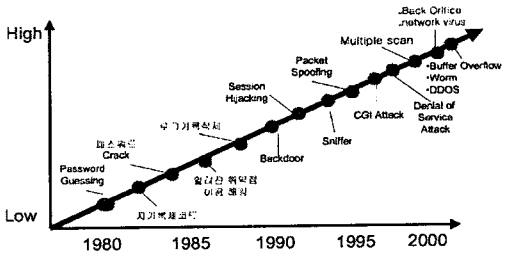


<그림 1> 1999, 2000년 해킹기법 현황

해킹 발생 건수의 증가와 함께 해킹 기법도 점점 지능화, 고도화 되어가고 있는데, CERCC-KR에 보고된 최근 해킹 기법별 현황을 <그림 1>에서 살펴보면 취약정보수집이 50%로 가장 많은 해킹사고가 접수되었으며 악성프로그램이 39%로 두 번째로 많은 사고가 접수되었고, 버퍼오버플로우가 6%, 사용자 도용 2%, 서비스 거부공격, 전자메일관련 공격, 기타가 1%의 순으로 보고되고 있다[1]. 여기서, 취약정보수집은 실질적 공격을 수행하기 이전의 "정보수집 단계"이며, 실제 시스템에 침해를 가하는 "시스템 침입 단계"에 해당하는 방법으로는 "악성프로그램"이 가장 많은 공격기법으로 사용되고 있다는 것을 알 수 있다.

2.3 새로운 공격 기법의 등장

오늘날 네트워크 기술의 발전과 정보보호의 중요성 인식으로 인하여 침입차단시스템(Firewall) 및 침입탐지시스템(Intrusion Detection System)이 보급되어 다양한 공격에 대응하는 기술이 보편화되고 있다. 이를 극복하기 위한 공격자들의 노력은 전통적인 공격모델의 변화를 가져오게 되었고, 정보보호 시스템을 무력화시키고 성공적으로 시스템에 침입하기 위한 새로운 기술 및 도구들이 최근 몇 년간 지속적으로 개발되고 있으며, 다음과 같은 방법들이 사용된다. <그림 2>는 연대별 해킹 기법의 변화를 그림으로 보여준다



<그림2 > 해킹 기법의 변화

- 분산 공격(Distributed Attack) : 여러 호스트에서 하나의 공격 대상 네트워크를 스캔하여 보다 빠르고 다양한 정보를 획득하여 IDS의 대응을 무력화시키는 방식이다. 특히, 에이전트 형태의 공격 도구를 이용하게 되면 공격자는 시스템에 로그인하지 않고 원격에서 다수의 에이전트를 통제하여 쉽게 정보를 수집하거나 공격할 수 있게 된다.
- DDoS(Distributed DoS) 공격 : 최초로 에이전트 개념을 도입한 공격 방법으로 시스템 취약성을 이용하여 공격한다. 자동화, 분산 공격 기능 등을 가진다.
- 인터넷 웜(Internet Worm) : 자동으로 임의의 공격 목표를 정한 후 공격이 성공하면 바로 그 곳에서 다른 곳으로의 공격을 시도하기 때문에, 비슷한 취약점을 가진 호스트가 목표가 된다. 또한 병렬 형태의 공격패턴을 제공하여 침입 탐지의 위협을 피할 수 있도록 한다.
- 에이전트 형태의 백도어(Backdoor) : Covert Channel을 사용하여 CMP, UDP, IP, TCP 등의 프로토콜 계층과 http, Mail, DNS 등 응용프로그래밍 계층에서도 구현이 가능하며, 파이어월 또는 IDS를 우회할 수 있는 수단을 제공한다.
- 악성 에이전트: 바이러스의 확산기능, 트로이 목마의 스파이 기능, 에이전트의 원격제어 기능, 시스템 침입기능 등 다양한 기능을 가지고 있으며, 모든 특성을 가진 악성 에이전트도 존재한다.

최근 발견되는 이러한 형태의 공격도구들은 다음과 같은 공격기법의 새로운 추세인 분산화, 에이전트화, 자동화, 은닉화의 특성을 가진다.

- 분산화 : 침입탐지시스템 등의 정보보호 시스템을 우회하기 위하여 많은 수의 시스템에서 단일의 시스템 또는 다수의 시스템을 공격하는 방법을 사용한다.
- 에이전트화 : 최근의 공격기법에서는 원격으로 조

정 가능한 에이전트형 백도어를 설치하고 이를 이용하여 다른 시스템을 공격하는 방법을 사용한다. 이는 공격자가 매번 로그파일에서 자신의 흔적을 지워야만 하는 번거로움을 없애주며, 많은 시스템을 이용하여 분산 공격을 수행할 때 매우 효과적인 방법이다.

- 자동화 : 인터넷 웜 및 윈도우용 공격도구, 그리고 최근 침해사고에서 발견되는 자동 공격 스크립트의 증가는 공격도구들이 자동화되고 있다. 이러한 자동화는 분산 네트워크 공격을 가능하게 한다.
- 은닉성 : 에이전트를 이용한 분산 공격기법에서 공격자의 위치를 은닉시킬 수 있도록 에이전트와 공격자간의 통신이 암호화 및 터널링 기법을 사용하여 탐지하기 어렵도록 한다.

3. 능동 보안(Active Security)

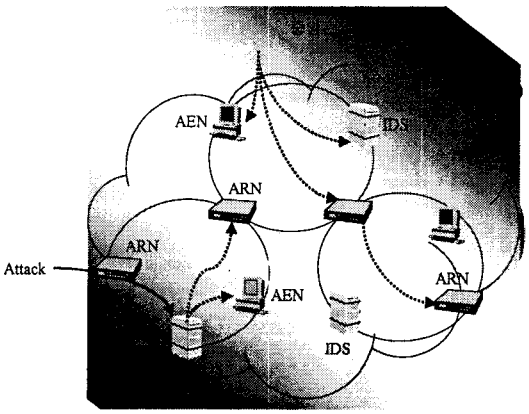
3.1 개념

구축된 네트워크를 보호하기 위한 다양한 정보보호 기술들이 적용되고 있으나 계속해서 조직화, 분산화, 자동화되는 고도의 공격 기법에 대항하기에는 현실적으로 불가능하다. 따라서, 특정 호스트에 대한 공격 탐지 및 대응 기술에 기반하는 단순하고 수동적인 기본 보안 방법의 단점을 극복하기 위하여 "능동 보안(Active Security)"[3]이 제안되었다. 능동 보안은 각 보안 시스템을 통합하고 전체 네트워크 차원에서 공격자에 대하여 효과적으로 대응하기 위한 적극적인 보안 방법으로 기존 보안 방법과 비교하여 다음과 같은 요구 조건을 만족해야 한다[4].

- 시스템 공격에 대하여 수동적 대응뿐만 아니라 능동적 대응이 가능해야 한다.
- 시스템 또는 내부망 보안에서 전체 네트워크에 대한 보안이 가능해야 한다.
- 보안 시스템의 독립적인 운용에서 상호 결합적인 운용이 가능해야 한다.
- 공격 및 시스템 대응 방법에 대하여 구체적인 기술과 수용이 가능한 유연한 보안 시스템 구조를 가져야 한다.
- 새로운 보안 정책 및 기술의 수용이 용이한 개방적 실행 구조를 가지는 보안 시스템이어야 한다.

3.2 구조 및 동작

능동 보안은 단순한 보안 체계의 범위를 넘어서는 "Security Infrastructure"로써 시큐리티 하부구조, 시큐리티 시스템, 각 시스템의 실행 구조, 시스템 간의 통신 방법, 이기종 간 동작에 대한 조정 체계, 프로그래밍 언어, 프로토콜 등으로 구성된다. 능동 보안은 각 보안 시스템 간의 통합을 통하여 전체 네트워크 상에서 공격자를 효과적으로 대응하기 위한 기능인 ARN(Active Response Network)과 시큐리티 환경 변화에 쉽게 대처 가능하도록 각 시큐리티 구조를 유연하고 개방적으로 구현하기 위한 AEN(Active Execution Node)으로 나누어 진다. 또한, 능동 보안을 적용한 네트워크는 시큐리티 정보를 상호 결합하여 관리자에게 보고하고 해당 시큐리티 관리 영역 내에서 통합된 대응 방안을 결정하여 수행할 수 있는 SMD(Security Management Domain)로 구성된다. 다음 <그림 3>은 능동 보안 네트워크의 구조의 한 예를 보여준다.



<그림 3> Active Security 구성 예

외부 네트워크에서 공격을 탐지한 경우 IDS는 독립적으로 대응 방안을 모색할 수도 있고, 주위의 ARN 및 AEN에 그 사실을 보고한다. 공격이 탐지된 네트워크에 소속한 ARN은 대응 방안을 독자적으로 결정할 수도 있고 중앙 관제 시스템에 그 사실을 통보하여 더 나은 대응 방안을 요청할 수도 있다. 또한, 중앙 관제 시스템에서는 전체 SMD에 변화된 시큐리티 환경, 새로운 공격 기법에 대한 대응 방안 등의 사실을 알리기 위해 각 ARN에 배포하고 AEN을 통하여 수행할 수 있도록 한다.

4. 이동 에이전트 기술의 도입 및 적용

주어진 작업을 수행하기 위해 네트워크로 연결된 시스템 사이를 스스로의 판단 하에서 이동하는 에이전트를 특히 "이동 에이전트"라고 정의한다[5]. 이것은 사용자를 위해 자동적으로 행동하는 프로세스이다. 이러한 이동 에이전트는 기존 통신 체계 하에서 발생

하는 막대한 통신 비용 절감, 분산 처리, 협동 작업 수행, 작업의 비동기 수행 등의 요구를 수용하는 해결책으로서 등장하게 되었다.

능동 보안의 동작에서 각 ARN은 다른 ARN과 상호 정보 교환을 위한 통신이 필수적이고, 각 AEN은 해당 프로그램 코드를 받아 수행할 수 있는 실행 환경이 반드시 구축되어야 한다. 즉, 이동 에이전트가 ARN 상에서 이동하면서 능동 보안에 대한 여러 자료를 배포하거나 공격 사실을 이웃 ARN에 알리는 역할을 수행하며, AEN 상에서 이동 코드를 직접 수행하면서 공격 패턴의 탐지, 탐지된 공격에 대한 대응 절차, 수집된 정보의 리포트 등을 직접 수행하게 된다. 따라서, 이동 에이전트에 대한 인증을 포함하여 에이전트 정보보호, 실행 환경 보호, 안전한 에이전트 이전 등이 함께 구현되어야 한다. 능동 보안에 적용하기 위한 이동 에이전트의 요구사항은 다음과 같다.

- 시큐리티 관련 연산의 성능
- 각 구성 요소들 간의 상호운용성
- 시큐리티 기능의 확장성
- 새로운 기능 추가에 대한 유연성
- 공격 대응의 확실성, 효율성
- 시큐리티 기반 구조 구성의 단순화
- 시큐리티 기반 구조의 관리

능동 보안을 도입한 시스템은 해당 기능을 구현한 코드(즉, 이동 에이전트)의 다운로드 및 실행이 가능한 유연하고 개방적인 실행 구조를 가져야 한다. 이를 통하여 새로운 공격 기법이 등장하였을 경우 대응 방법을 기술한 코드를 다운로드받아 실행함으로써 침입 탐지 및 차단을 수행할 수 있다. 즉, 각 능동 보안 시스템이 새로운 기능을 수용하여 전체 시스템에 대한 확장성을 확보하고 시스템 전반의 보안 수준을 한층 더 높일 수 있는 동적인 시스템을 구성할 수 있게 된다. 최근 전체적인 구조의 능동 보안에 대한 연구가 진행되고 AEN을 위한 부분으로써 Active Network에 이동 에이전트를 도입하여 실시간 동작을 위한 성능의 최적화, 다양한 위협에 대한 시큐리티, 여러 통신 구조의 효율적인 지원을 위한 활발한 연구가 진행되고 있다. 또한, ARN을 위해서 다양한 네트워크 구성 시스템들의 통합, 노드들 간의 신뢰성 확보, 안전한 통신을 위한 암호화 기능 등이 포함되어야 한다.

5. 결론

본 논문에서는 2장에서는 최근 성행하고 있는 시스템 공격 기법을 분석하였다. 이를 위하여 전통적인 공격 기법과 그 동향을 살펴보고 공격 기법의 시대적 변화에 따르는 공격 기법의 특성을 분석하였다. 3장에서는 새로운 보안 기반 구조를 제시하는 능동 보안의 개념을 소개하고 세부적인 구조와 동작을 논의하였다. 4장에서는 능동 보안에서의 이동 에이전트의 역할과 적용을 위한 요구사항을 제시하였다.

능동 보안은 특정 호스트에 대한 공격 탐지 및 대응 기술에 기반하는 단순하고 수동적인 기본 보안 방법의 단점을 극복하기 위하여 제안되었다. 능동 보안은 각 보안 시스템을 통합하고 전체 네트워크 차원에서 공격자에 대하여 효과적으로 대응하기 위한 적극적인 보안 방법으로, 기존 보안 방법과 비교하여 보안 기반 구조에 유연성을 부여하여 기존의 공격 및 새로운 공격에 대한 효과적이고 강력한 대응이 가능한 장점을 가지고 있다. 이 점을 기반으로 네트워크 기반의 정보보호 시스템에 새로운 방향을 제시할 것으로 예상된다. 따라서, 국내 실정에 맞는 체계적이고 구체적인 능동 보안에 대한 보안 기반 구조, 구성 요소 기술 등이 여러 기관의 협력 속에서 이루어져야 할 것이다. 특히, 능동 보안 구성 요소 기술 중 핵심 기술인 이동 에이전트에 대한 실행 환경 보호, 이동 에이전트 실행 보호, 이동 에이전트 간의 보호에 대한 연구 등도 선행되어야 할 것으로 사료된다.

참고문헌

[1] CERTCC-KR, http://www.certcc.or.kr/

[2] 신원, 윤희영, 이경현, "네트워크를 통한 시스템 침입에 대한 고찰", 「'2000 한국멀티미디어학회 춘계학술발표회 논문집」 pp.86-89, 2000.

[3] G.Escelbeck, "Active Security - A Proactive Approach for Computer Security System", Journal of Network and Computer Application, Vol.23, 2000.

[4] Sigcomm Review, "Active Network과 Security 기술 기반", Vol.1 No.1, 2000.

[5] 박영호, 신원, 이경현, "이동 에이전트 시스템 시큐리티", 「'2000 한국통신정보보호학회 종합학술발표회 논문집」, pp.164-171, 2000.

[6] DARPA, DARPA Information Survivability Program, http://www.darpa.mil/ito/research/is/