차세대 공격형 정보보안 기술

장 희 진 박 보 석 김 상 욱

목 차

1. 서 론

차세대 정보전에서 정보 보안의 개념은 방어적이기보다는 공격적이게 되었다[1]. 컴퓨터 침해 사고 방지를 목적으로 침입 방지 기술에 관한 연구가 많이 수행되고 있지만 방어 수단만으로는 충분한 목적을 달성할 수 없다. 그러므로 부정행위자의 신분을 확인하여 증거를 확보하거나 상대 시스템을 위협하는 적극적인 형태의 공격형 기술이 요구된다. 그러나 대부분의 부정행위자는 추적하고자 하는 사람이 미칠 수 없는 원격 컴퓨터를 거쳐서 침입하므로 단기간 내에 신원 파악이 거의 불가능하다. 즉, 침입을 탐지함과 동시에 침입자의 접속을 차단시킴으로써 침입자가 탐지된 사실을 인지하고 차후의 접속을 중단하기 때문이다. 침입자를 차단하지 않고 그대로 방치하는 것은 자체 보안에 문제가 발생한다. 또한 사용자의 시스템을 중간 거점으로 삼아 이동하는 경우 역추적과 같은 기존의 기술을 이용한다면 역추적 소프트웨어가 설치되어 있지 않은 상태에서 부정행위자를 추적하는 것은 불가능하다. 부정행위자에 대한 정확한 신분확인을 위해서는 이러한 문제점을 해결해야 한다. 부정행위자가 인식하지 못하는 상태에서 활동을 장기간 감시할 수 있는 수단이 필요하다. 또한 부정 행위자를 추적할 수 있는 영역에 대한 제약이 최소화되어야 한다. 이러한 요구 조건을 만족하는 진보된 해킹 방지 기술이 요구된다. 이러한 기술을 통해 사용자의 시스템을 보호함은 물론 부정행위에 대한 시나리오 데이터베이스를 구축할 수 있다. 또한 부정행위자가 이동한 경로상의 원격 컴퓨터 관리자와 연락하여 공동조사가 가능하고 부정행위자의 습관을 분석함으로써 직접 신원 파악이 가능하다.

2. 정보전

2.1 정보전 개념

정보전이란 자신의 모든 중요 정보 자원 및 시스템은 적으로부터 보호하는 반면 적의 중요 정보자원 및 시스템을 파괴하거나 해를 가하여 손해를 입히고 정보의 획득과 유지에 있어서 우위를 차지하기 위한 행위를 의미한다[2].

정보전은 정보수집, 정보보호, 정보제공거부, 정보관리, 정보전송과 같은 요소를 가진다. 이들 다섯가지 요소를 어떻게 조합하는가가 정보전의 전략이다. 조직에 의해 정보가 수집되면 다음으로 고려해야 할 점은 정보를 보호하는 방법이다. 정보 인프라의 취약점은 널리 알려져 있다. 정보보호는 정보위협과 정보파괴의 두 가지 종류의 위협을 다룬다. 정보위협은 적이 조직 소유의 정보에 대한 접근이 가능한 것을 말하고 정보파괴는 적에 의한 악의적 공격의 결과 이들 정보의 손실을 포함한다. 정보제공거부는 적의 수집 시스템을 목표로 하는 일반적인 보호 외에 적의 정보 시스템에 대한 직접 공격 그리고 그 시스템에 대해 잘못된

정보를 제공하여 적을 속이고 적으로 하여금 잘못된 조치를 취하도록 하는 것을 포함한다. 조직내의 컴퓨팅과 데이터 리소스의 분산으로 발생하는 보안상의 문제들을 방지하기 위해 정보관리가 요구된다. 정확하고 신속한 정보전송은 데이터 유용성에 영향을 미치므로 조직의 전송 능력은 조직의 성패에 있어서 중요한 요소이다.

2.2 정보전 대응기술

정부, 군, 산업 조직의 대규모 상호연결된 통신 정보시스템에 대한 의존도가 증가하였다. 중요 시스템의 기밀성, 무결성, 또는 가용성에 손실이 오는 경우 경제적, 국가적으로 심각한 영향을 초래한다. 그러므로 중요 시스템에 대한 침입을 정확하게 탐지하고 재빨리 대응하는 기술이 요구된다. 표 1 은 사이버 공격에 대한 대응 기술들이다[3].

침입 탐지는 대응 과정의 첫 번째 단계이다. 탐지 이후의 조치는 침입자의 의도를 파악하고 손해 범위를 점검하고 시스템에 끼치는 영향을 확인해야 한다. 그리고 무엇보다도 침입자의 신분을 확인하여 근본적인 조치를 취하는 것이 요구된다.

표 2 정보전 대응 기술

분류	대응 기술
보호(Protect)	- 암호(Encryption) - 침입차단시스템(Firewall) - 인증(Authentication)
탐지(Detect)	- 악의적 소프트웨어(Malicious S/W) - 네트워크 현황/토폴로지(Network Status/Topology) - 전조(Precursors), 침입(Intrusions) - 자원 오용(Misuse of Resources) - 자료 상관성/집합(Data Correlation/Aggregation) - 자료 시각화(Data Visualization)
반응(React)	- 대응(Response) : 접속 종료, IP 주소 봉쇄 - 복구(Recovery) 및 재구성(Reconstitution)
공격(Attacks)	- 컴퓨터 바이러스(Computer viruses), 웜(Worm) - 트로이 목마(Trojan horses), 트랩 도어(Trap doors) - 침입자 유인

침입자 의도를 결정하는 과정은 자료 상관성, 침입탐지 시스템 결과, 감사 로그, 그리고 다른 유용한 정보들을 바탕으로 추론된다. 현재 침입자 의도를 식별할 수 있는 도구는 사실상 존재하지 않으며, 거의 인적 자원에 집중되어 있는 실정이다. 손해의 범위는 대응 방법을 결정하는데 주요한 요인이 된다. 예를 들어 중요하지 않으며 기능이 협소한 호스트에 대한 공격 대응은 거의 미비하거나 없을 수 있다.

3. 정보 시스템 보호 기술

3.1 침입 탐지 기술

침입 탐지(Intrusion Detection)는 인가된 사용자 혹은 외부의 범법자들에 의해 컴퓨터 시스템의 허가되지 않은 사용이나 오용 그리고 악용과 같은 침입을 확인하기 위해 시도된 시스템이다. 현재 다양한 접근 방법들이 활용되고 있으며, 핵심 기법은 예외 발견과 오용 발견이며, 그리고 기타 패턴 인식, 네트워크 모니터링 기법 등이 있다.

예외 탐지(Anomaly Detection)는 침입자가 정상적인 사용자와는 다른 행동 패턴을 갖는다

는 가정하에서 사용자의 패턴을 비교하여 침입을 확인하는 방법이다. 로긴 시간, 로긴 세션의 존속 시간 등과 같은 사용자의 행동에 대한 프로필 정보를 생성한다. 이 방법은 OS 감사 기록에 의존적이므로 분석을 위해 시스템 과부하를 발생시켜 실시간 감사 자료 검토 능력 상실케 된다. 오용 탐지(Misuse Detection)는 사용자의 활동을 기록한 침입 서명을 검색하고 알려진 공격자의 행동과 사용자 행동을 비교하여 침입을 발견한다. 이 기법들은 감사 기록 자료에 의존적이므로 시스템 성능을 저하시킬 수 있다. 패턴 인식(Pattern Recognition)은 일련의 침투 시나리오가 시스템에 코드화하여 확장된 시간 주기, 일련의 사용자 세션 또는 다중 공격을 통해 나타나는 공격자를 확인하는 방법이다. 이 기법은 잠재적으로 많은 양의 감사 자료를 검토해야 하는 필요성을 감소시키지만, 생성된 시나리오가 시스템 의존적이므로 공격 특징이 일치하지 않으면 침입 발견이 어려운 단점이 있다.

3.2 침입자 역추적 기술

침입자를 역추적하기 위해 로그, 호출자 판별, 모니터링과 같은 기술들이 사용된다. 로그 기반의 역추적은 시스템이 기본적으로 제공해 주는 로그파일을 분석함으로써 침입 호스트를 확인한다. 사용자의 로그인/로그아웃 일시 기록, 프로세스 기록, 라우터 정보 등이 추적의 기본 정보로 사용된다. 시스템 관리자가 많은 수작업을 해야하므로 침입자가 자신의 자취를 은폐할 수 있는 충분한 시간을 제공할 뿐만 아니라 관리자의 경험에 의존하므로 정확한 침입자 역추적 및 피해분석이 어렵다. 호출자 판별(Caller Identification) 기술은 네트워크를 통해 시스템에 로그인 할 경우, 이전의 경로 정보를 전송하도록 하는 방법이다. 경로 정보는 다른 호스트에서 접속을 시도한 시점에서 작성되며, 하나 이상의 호스트를 경유하여 접속하는 경우에는 현재까지의 경로 정보가 해당 호스트에 전달된다. 제공되는 데이터가 인접 시스템에 대한 정보에 한정되어 있기 때문에 침입자가 지나쳐온 모든 경로를 추적하기에는 부적합하므로 경로 정보가 로그인 할 때 전송되도록 확장한다. 경로 정보의 인증을 위해서 접속 요구를 받는 호스트가 접속을 요구한 사용자의 ID를 알아내기 위해서 각 호스트마다 호출자 판별 서버(Caller Identification Server)가 설치되어야 한다. 모든 호스트에 이러한 판별 서버가 있어야하므로 현실적으로 적용이 어렵다. 침입 탐지 및 역추적을 위해서 사용자의 행위 및 시스템 상태가 모니터링 되어야한다. 이러한 모니터링 기술은 호스트 레벨 모니터링과 네트워크 레벨 모니터링으로 나뉘어 진다. 호스트 레벨의 모니터링은 주로 터미널 가로채기 방법을 이용하여 이루어진다. 이러한 시스템의 예로는 UNIX 시스템을 대상으로 하는 ttywatcher[4]와 ttymon[4]이 있고 Linux 시스템을 대상으로 하는 linspy[5]등이 있다. 이들은 단일 시스템 상에서 사용자를 모니터링하고 제어하는 도구이다. 네트워크 레벨에서의 모니터링은 네트워크 레벨에서의 부정행위자의 모든 로그온을 감시할 수 있으므로 다른 기계에 접근할 필요가 없다. 부정행위자가 새로운 연결을 시작하면 관리자는 부정행위자가 로그온한 호스트에 접근할 필요없이 단지 부정행위자에 대한 연결만을 감시하면 된다. TCP dump[5], Etherfind[6], Netlog[6], SNIF[7] 같은 도구들이 이런 기능의 일부를 제공했지만 감시할 로그온 연결을 지정하지 않으므로 네트워크 상의 모든 패킷 정보가 입력되어 연관된 자료를 걸러내고 유용한 정보를 추출하는 것이 어렵다. 그러므로 실시간 분석을 통한 정보 제공이 이루어지지 않았다. 그리고 부정행위자에 대해 감시와 모니터링만 수행할 뿐 조치를 취할 수는 없다.

4. 공격형 정보보안 기술

부정 행위자에 대한 신분 정보를 획득하기 위한 기본 전제는 부정 행위자의 호스트에 직접 접근 가능해야 한다. 그러나 기존의 역추적을 이용한 신분 확인은 모든 호스트에 역추적 모듈이 있어야 하는 제한이 있다. 따라서 역추적 뿐만 아니라, 부정행위자의 접속 경로를 미

행하여 호스트들에 직접 접근함으로써 보다 정확한 신분 정보 및 증거를 수집할 수 있다.

신분확인 시스템[8]은 가상 잠복 모드, 미행 모드, 복제 모드, 탐문 모드로 동작된다. 침입탐지 시스템에 의해 부정행위자로 판명될 경우, 가상 잠복 모드로 전환하여 부정 행위자가 가상의 공간에서 해킹하는 동안 부정행위자의 모든 행위를 감시하면서 역추적한다. 부정행위자가 다른 호스트로 이동할 때 미행 모드에서 부정행위자의 기본 인증 정보와 이동 경로를 획득한다. 이들 정보를 기반으로 복제 모드와 탐문 모드로 전환한다. 복제 모드에서는 부정행위자의 이동 경로에 또 다른 거점을 확보하기 위해서 신분확인 시스템을 복제한다. 탐문 모드는 부정행위자에 대한 현재 호스트에서의 신분 정보와 행위 정보를 수집하고, 백도어와 같은 호스트 보안 취약점을 검사한다. 그림 1은 부정행위자 신분확인 시스템의 동작을 나타낸다.

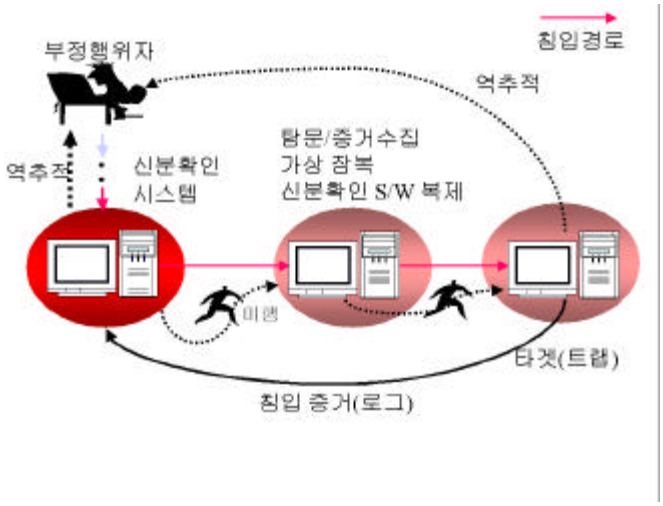

그림 1 부정행위자 신분확인 시스템

4.1 가상 잠복

침입탐지 시스템에 의해 침입이 감지되었을 경우, 시스템에는 피해없이 부정 행위자의 침입 방법, 침입 경로 등의 부정 행위자의 신분 확인을 위한 정보를 획득하기 위해 가상 잠복 모드가 구동된다. 그림 2는 가상 잠복 모드의 개요이다.

가상 잠복 모드에서 주요한 역할을 하는 것이 가상쉘과 쉐도우 운영체제이다. 가상쉘은 부정행위자에게 가상 환경을 제공하기 위한 커널과 사용자 간의 인터페이스이다. 응용프로그램 레벨에서 커널을 제어하는 것이 불가능하므로 커널에 대한 입출력이 가상쉘에서 필터되고 변경된다. 필터된 명령이 시스템에 영향을 주는 시스템 명령인 경우 쉐도우 OS를 통해 커널에 대해 수행함으로써 시스템에 피해를 주지 않으면서 부정 행위자에 대한 로그를 확보하고 또한 부정 행위자 신분 확인을 위한 시간을 얻을 수 있다. 가상쉘은 기존의 쉘을 캡슐화한다. 쉐도우 OS는 ASCII 코드 또는 바이너리 파일의 실행 요청에 대해 가상 파일 시스템을 지원한다. 부정행위자의 파일 컴파일 또는 실행과 같은 사용자 명령을 커널로 직접 전달하기 전에 쉐도우 OS는 텍스트 파일의 내용 또는 바이너리 파일의 경로를 변경한다. 지정된 디렉토리 이상의 디렉토리에 대한 접근을 거부하는 chroot()에 의해 부정행위자의 실제 파일 시스템으로의 접근을 막고 가상 파일 시스템을 제공한다. 이런 메커니즘을 통해 실제 파일 시스템은 보호된다.

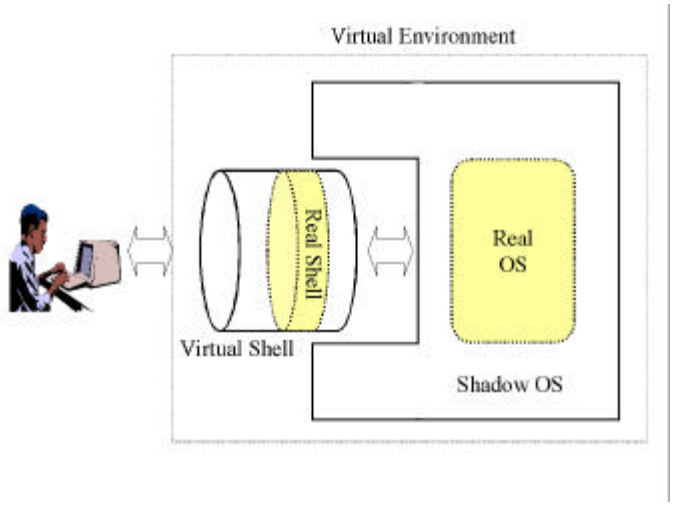

그림 2 가상 잠복 모드 개요

4.2 미행

부정 행위자로 의심되는 사용자의 신분 확인을 위해 역추적을 통해 침입 경로를 알아낼 뿐 아니라 침입자임을 확신할 수 있는 증거 수집과 타겟 호스트에 대한 피해를 최소화하기 위해 사용자의 행위를 추적할 필요가 있다. 이를 위해 터미널 모니터링이 시도된다. 사용자의 터미널을 모니터링하기 위한 여러 가지 방법이 제시되었지만 지금까지의 방법은 단순히 부정행위자를 감시할 뿐 모니터링 행위 자체가 부정행위자에게 노출된다. 사용자의 신분확인을 위해서는 우선 충분한 시간확보가 요구된다. 이러한 관점에서 볼 때 노출된 모니터링 행위는 의미가 없다. 그러므로 새로운 방식의 모니터링이 요구된다.

부정행위자를 감시하기 위해 부정 행위자가 신분확인 소프트웨어가 있는 호스트를 거쳐서 다른 호스트에 침입하는 경우 그 경로를 추적하기 위해 미행한다. 미행의 결과 부정 행위자의 이동 경로와 행위 로그를 신분확인시스템이 획득하게 된다. 또한 복제를 위한 인증정보 획득이 미행을 통하여 이루어진다. 주요 감시 대상이 되는 명령 또는 이벤트들을 미리 정의하여 필터하고 그 결과는 관리자가 미리 설정한 행위 정책, 기존에 수집된 정보들과 비교, 분석된다. 필터된 결과 사용자의 행위가 시스템에 심각한 영향을 미치는 행위인 경우는 세션을 끝내거나 메시지를 보내는 등의 적절한 조치를 취하도록 하는 개발이 향후 요구된다. 그 외 부정 행위자의 행위 증거 또는 인증 정보로 기록할 필요가 있으면 로그로 남기거나 새롭게 수행된 부정 행위 시나리오거나 새롭게 발견된 부정 행위자인 경우 데이터베이스에 등록하도록 하는 조치도 개발이 가능하다.

4.3 복제

신분확인 시스템이 이미 설치된 호스트에 대해 터미널을 사용하지 않을 경우 부정 행위자에 대한 더 이상의 추적은 불가능하다. 정확한 신분 확인을 위해 더 많은 정보를 획득할 필요가 있다. 이를 위해 또 다른 신분 확인의 거점을 확보할 필요가 있다. 호스트 레벨에서 행위 감시가 수행되다가 부정 행위자가 다른 호스트로 이동하는 경우 이를 추적하기 위해 네트워크 레벨의 감시가 수행된다. 이로서 획득된 인증정보로 이동한 호스트에 미행과 탐문을 위한 모듈을 복사한다. 부정 행위자가 이동한 호스트에서 관리자의 권한을 획득하는 경우 관리자 권한을 가진 터미널로 부정 행위자에게는 에코(echo)되지 않게 한 후 명령을 전송하여 복사된 모듈을 컴파일하고 데몬의 형태로 백 그라운드 실행함으로써 이동한 호스트에서의 부정 행위자 미행과 탐문이 계속된다. 탐문 모듈은 이동한 호스트에서 데몬으로 수행되

며 부정 행위자에 대한 정보를 수집한다. 미행 모듈이 이동한 호스트에서 데몬으로 수행됨으로써 부정 행위자가 신분 확인 시스템이 설치된 호스트를 거치지 않고 이동한 호스트만을 경유하는 경우에도 미행이 가능하다. 수집된 정보는 주기적으로 또는 필요에 따라 신분확인 시스템 서버로 전송된다.

4.4 탐문

부정행위자의 일반 신분정보와 침입 호스트에서의 부정행위를 검사하는 것을 탐문이라 한다. 탐문에서는 부정행위자의 신분 정보 중에서 부정 행위자의 일반정보 및 부정 행위자가 수행했을 것으로 추정되는 비실시간 부정 행위를 추출한다. 탐문 모드에서는 탐문 동작과 함께 부정행위자가 재차 원격 로그인 했을 때 부정행위자의 행위를 추적하고 감시할 수 있도록 신분확인용 백도어를 설치한다. 이것은 부정행위자의 정보를 비동기적으로 원격에서 감시하여 침입 증거를 수집하기 위한 것이다. 탐문에서 수집하는 부정행위자 신분 정보에는 계정 정보, 환경 및 프로파일 정보, 부정행위자의 로그, 부정행위자가 한 백도어, 부정행위자의 침입도구, 부정행위자 유인용으로 생성한 파일 등이 있다. 탐문을 수행하는 기본적인 메커니즘은 파일 시스템의 무결성을 검사, 패턴 분석, 포트 검색이다.

5. 결론

본 고에서는 정보전의 개념과 지금까지 개발된 대응기술 그리고 차세대 공격형 정보보안에 대하여 기술하였다. 미래의 정보전에서는 상대방으로부터 자신의 중요한 정보 시스템을 보호하기 위해 공격적인 형태의 보호 기술이 요구된다. 국내에서도 정보전에 대비한 정보보안 기술이 개발되고 있다. 하지만 여전히 정보통신 기반구조 보호에서 초보적인 단계에 머무르고 있다. 앞으로 정보보호 기술 개발, 관련법, 제도의 정비 그리고 과감한 투자, 인력 양성 및 관련 산업 육성이 요구된다.

참고문헌

[1] Winkler J.R., OShea C.J. and Stokrp M.C., “"Information Warfare, INFOSEC and Dynamic Information Defense,"” Proceedings of National Information Systems Security Conference, December 1996

[2] Reto E. Haeni, "Information Warfare: an introduction," Information Warfare Conference, 1995

[3] Richard Brackney, "Cyber-Intrusion Response," Proceedings of IEEE Symposium on Reliable Distributed Systems, October, 1998

[4] Russel D. and Gangemi G., Computer Security Basics, OReilly & Associates, 1991.

[5] Simson, G. and Gene, S. Practical Internet and UNIX Security, O'Reilly & Association, 1996.

[6] Stallings, W. Network and Internetwork Security Principles and Practice. New Jersey, NY: Prentice-Hall, 1995.

[7] Alves-Ross J., “"An Overview of SNIF: A Tool for Surveying Network Information Flow,"”Proceedings of the Internet Society Symposium on Network and Distributed System Security, February, 1995

[8] 김상욱, 박보석, 장희진, 김건우, 박정현, 임채호, "미행에 의한 부정행위자 신분확인," 한국정보과학회 가을 학술발표 논문집, pp327-329, 1999