정보전을 위한 소프트웨어 순항 기반 공격 모델

An Attack Model Based on Software Cruise for Information Warfare

류 호 연* 남 영 호**
Ho-Yeon Ryu Young-Ho Nam

요 약

정보전은 새로운 전쟁 양상으로 정보보안뿐만 아니라, 국가 안보 차원에서 관심과 연구가 집중되고 있는 분야이다. 차세대 정보전에서는 방어와 공격이 모두 중요시되고 있으며 이와 같은 정보전에서 우위를 차지하기 위해서는 네트워크 및 시스템을 보호하기 위한 다양한 연구가 필요하다. 본 논문에서는 공격적 양상으로 변화해 가고 있는 정보전에 대비하여 소프트웨어 순항 기반 정보전 모델을 제안한다. 소프트웨어 순항은 소프트웨어가 네트워크를 통하여 출발지에서 지정된 목적지로 자가이동할 수 있는 소프트웨어 행위이다. 제안된 모델은 순항 특성을 지니며, 네트워크를 통해 미리 정해진 특정 목적지를 향해 가상지도를 기반으로 순항한다. 또한, 자가이동을 하는 동안 상황에 따라 미리 정의된 작업을 수행할 수 있는 기능을 포함할 수 있다.

Abstract

Information Warfare(IW), a new aspect of war, is the field centralized the concern and research in the information security and national security. Both the defense and the offensive are important in the next generation IW, and so we need to do the various research to secure the network and system for gaining the superiority of IW. This paper proposes a model for IW based on software cruise to prepare the IW that is changing the offensive aspect. Software cruise is defined as a behavior of computer programs that travel toward specific destination from a source through the network. The proposed model have the cruise property and uses the cybermap to cruise toward the destination chosen in advance. Also, while self-movement, the model can function the predefined task.

Keyword : information warfare, cyber warfare, software cruise

1. 서 론

차세대 정보전(information warfare)은 방어적인 정보보안의 개념에서 공격적인 개념을 도입하고 있는 상태이다[1,18]. 침입차단시스템이나 침입탐지시스템과 같은 유형의 보안시스템들은 정보전의 여러 양상 중, 사이버전 및 사이버 테러에서 발생하는 해킹이나 바이러스로 인한 침해사고로부터 주요 정보 및 정보시스템을 보호하는데 있어 방어적이며, 정적이다[18]. 즉, 기존의 해킹 유형이나, 바이러스 패턴을 분석하여 공격여부를 판단하며, 패킷분석 방법을 통해 공격 여부를 판단하기 때문에 해킹이나 바이러스 감염 후에야 이들 공격에 대해 대처한다. 또한, 보안시스템들을 우회하여 피해를 야기하는 해킹 기법들이 개발되면서 침해사고가 증가하고 있는 실정이다[9].

최근 각 나라들은 정보전에 대비하여 자국의 네트워크 및 시스템 보안을 위한 공격 및 방어와 관련된 신기술을 연구 개발하고 있으며, 해커를 양성하여 사이버 부대를 운영하고 있다. 해커 양성을 통해 만들어진 사이버 부대는 네트워크 및 시스템에 치명적인 바이러스와 같은 악성 코드를 개발하고, 실제 해킹에 참여한다. 그러나, 해커 양성이 갖는 문제점은 많은 교육 및 관리비용을 지불

* 정 회 원 : 경상대학교 대학원 컴퓨터과학과 박사과정
capella@edu.gsnu.ac.kr(제 1저자)
** 종신회원 : 경상대학교 컴퓨터교육과 부교수
yhnam@gsnu.ac.kr(공동저자)

하여야 하며, 해커의 활동은 정체가 추적당할 수 있는 위험이 있다. 따라서 대부분 가상 무기(cyber weapon)로서 바이러스와 웜 같은 악성 코드를 고려하고 있으며[11-13], 이에 관한 기술 개발에 전념하고 있다.

악성 코드는 이동성(mobility), 자율성(autonomous), 익명성(anonymity), 재생산성(reproduction) 등의 특성을 지니며, 이는 사이버 무기가 지녀야할 특성이기도 하다[11,13]. 그러나 악성 코드는 네트워크와 같은 가상 공간에서의 이동이 임의적이기 때문에 그 유용성을 보장받지는 못한다. 코드레드(CodeRed), 코드레드Ⅱ(CodeRedⅡ), 코드 블루(Code Blue), 님다(Nimda) 등과 같은 웜 바이러스와 1.25 대란을 야기 시킨 MS-SQL 서버 웜-슬래머(Slammer)는 큰 피해를 야기 시켰으나 그 이동이 임의적이다[4,19,20-23]. 즉, 미리 지정된 목적지나 경로에 관한 지식 또는 전략 없이 감염시킬 수 있는 모든 컴퓨터 시스템을 감염시키면서 전파된다는 것이다. 그러나, 만약 이들 악성 코드들이 목적성을 갖고 특정 시스템을 공격 할 수 있게 된다면 그 피해의 정도는 상상할 수조차 없을 것이다.

본 논문에서는 원격지 시스템으로 자가이동 가능한 순항 소프트웨어를 개발하고 실험 네트워크 상에서 그 유용성을 증명하였다. 순항 소프트웨어는 네트워크를 통해 미리 정해진 특정 목적지를 향하여 순항(cruise)하며, 이동시에 상황에 따라 미리 정의된 작업을 수행한다. 제안한 모델은 악성 코드와는 달리 지정된 목적지로 이동하며 지정된 행위를 수행함으로써 사이버전 및 사이버테러와 같은 정보전에서 공격 모델로 유용하게 활용될 수 있을 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 정보전 양상에 대하여 살펴보고 3장에서는 소프트웨어 이동 기법을 분석한다. 4장에서는 본 논문에서 제안하는 소프트웨어 순항 기반 공격 모델을 기술하고, 5장에서는 실험을 통해 그 가능성을 증명하였다. 마지막은 결론 및 향후 연구방향을 기술한다.

2. 정보전

정보전에 대한 정의는 여러 가지가 있으며 아직까지 명확하게 그 정의가 내려진 것은 없으나, 일반적으로 적의 교란, 마비, 파괴하는 행위와 군사력을 운용하는데 있어서 정보 우위를 달성하는 절차이다[3]. 즉, 미래의 정보전은 현존 군사력을 중심으로 하는 군 지휘통제시스템(C4I; Command, Control, Communication, Computer, Intelligence)이나 정보시스템에 국한된 공격 및 방어뿐만 아니라, 사이버 테러라고 하는 국가 주요 기반시설 정보시스템에 대한 공격을 포함하여 사이버공간까지 확장된 광범위한 개념으로 해석되고 있다[2,3]. 정보전의 전문가인 미 국방대학 교수 리비키는 정보전이 전쟁을 수행하는 별개의 기술이 아닌 전쟁의 한 유형으로 규정짓고, 7가지 정보전 유형을 제시하였다. 정보전 유형 7가지에는 지휘통제전, 정보기반전, 전자전, 심리전, 해커전, 경제정보전, 사이버전(cyber warfare)이 있으며, 이들은 정보의 보호, 조작, 파괴, 그리고 거부에 따라 구분된 것이다[2].

미래의 전쟁에서 정보전이 대두되고 있는 것은 정보전이 가지고 있는 여러 가지 특성[25]들로 인한 것으로 요약하면 다음과 같다.

- 정보전을 준비하고 수행하는데 드는 비용이 저렴하다.
- 사이버 공간에서는 지역적, 정치적인 전통적인 경계가 불분명해진다.
- 사이버 공간에서는 사실을 인지하는 지각능력을 쉽게 조작할 수 있다.
- 정보전을 위해서는 새로운 전략 첩보의 수집 및 분석 방법이 요구된다.
- 사이버 공간에서는 스파이 활동이나 사고 등을 정보전 공격과 구분할 수 있는 적절한 전술 경고 시스템 및 공격 평가 방법이 없다.
- 정보전에는 전선이 따로 없다. 즉, 시간적 공간적 차이를 무의미하게 한다.

정보전의 여러 유형 중 사이버공간 및 네트워크

를 기반으로 하는 유형에는 해커전, 사이버전, 사이버 테러의 개념이 있다. 해커전은 네트워크화된 정보화 사회의 취약점을 공격함으로써 물리적인 군사 시스템의 파괴보다 훨씬 결정적인 손실을 입히고자 하는 일종의 전쟁양식이다. 해커전은 공격 대상 정보 시스템의 보안 취약점을 이용하여 침투함으로써 정보 시스템을 완전히 또는 간헐적으로 마비시키거나, 자료에 무작위로 에러를 발생하도록 불법 변조하거나 유출시키고 정보를 훔치거나 악의적으로 시스템을 감시하여 정보를 수집하거나, 유해한 정보의 삽입 그리고 저장된 정보를 파괴한다. 공격 대상 정보 시스템의 접근을 위해 바이러스, 논리폭탄, 트로이목마, 스니퍼(sniffer)등과 같은 도구를 사용한다.

사이버전은 사이버 공간과 가상 인간에 대한 것으로 모든 정보전의 형태 중에서 가장 이해하기 힘든 것으로 정보 테러리즘(information terrorism), 시맨틱 공격(semantic attack), 시뮬레이션을 통한 전쟁(simular warfare), 깁슨전(gibson warfare)등을 포함한다. 사이버 테러는 네트워크를 기반으로 하여 데이터베이스화되어 있는 군사, 행정, 인적 자원 등 국가의 주요 정보를 파괴하는 것으로, 시스템뿐만 아니라 네트워크에 대한 공격도 이루어지고 있다. 향후 전쟁은 군사시설에 대한 직접적인 타격보다는 군사통신, 금융망에 대한 사이버 테러 양상을 나타낼 가능성이 크다.

본 논문에서는 정보전을 사이버 공간과 사이버 공간을 구성하는 요소들에 대한 공격과 방어 측면에서 한정한 개념으로 보고, 또한 사이버 테러, 사이버전, 그리고 정보전은 서로가 구분되는 것이기는 하지만 같은 의미로 사용하고자 한다.

3. 소프트웨어 순항

소프트웨어 이동성에 관한 연구는 순항이라는 새로운 특성에 집중되고 있다. 순항이란 네트워크를 통해 출발지(source)에서 시작하여 지정된 또는 목표로 하는 목적지(destination)로 자율적으로 이동하는 소프트웨어 특성이다[14]. 순항 특성을 갖는 소프트웨어를 사이버쉽(cybership) 또는 AMCW (autonomous mobile cyber weapon)라 한다[11,13,14]. 이러한 소프트웨어들은 비밀스러운 이동 또는 비인가된 이동을 필요로 한다. 현재 대부분의 국가들은 순항 특성을 갖는 소프트웨어를 개발하기 위해 노력하고 있으며, 이에 관한 연구 내용 및 결과들은 비밀로 취급되고 있다. 이 연구 결과들은 특정 정보 시스템을 공격, 정보 시스템을 공격으로부터 방어, 감시 및 첩보 등 다양한 분야에 활용될 수 있다.

3.1 소프트웨어 이동

소프트웨어 이동은 소프트웨어가 컴퓨터간을 이주하는 것으로, 비자가이동(nonself-movement)과 자가이동(self-movement)으로 구분될 수 있다[5].

비자가이동은 특정 목적지나 경로에 관한 지식 또는 전략 없이 감염된 다른 프로그램의 이동이나 프로그램을 저장하고 있는 저장매체의 이동에 의해서 이동된다. 즉, 저장매체의 전달(delivery)과 자신의 복제(replication) 및 감염을 통해 이동된다. 전달은 악성 코드가 포함된 디스크와 같은 저장 매체의 전달에 의한 이동으로 악성 코드의 수를 증가시키지는 못한다. 복제는 악성 코드가 감염되어 있는 파일의 이메일링(emailing), 다운로딩(downloading), 업로딩(uploading) 등을 통하여 파일의 전송에 의한 이동이며, 이 수단은 악성 코드의 수를 증가시킨다. 대부분의 컴퓨터 바이러스는 비자가이동 방식으로 이동하며, 비자가이동은 특정 목적지에 도달할 가능성이 거의 없다. 즉, 오늘날 이동 능력을 갖는 바이러스나 웜들은 이동 전략이 없는 임의적 이동이며, 미리 정의된 목적을 달성하거나, 특정 목적지에 도달할 가능성이 매우 희박하다.

자가이동은 한 컴퓨터에서 네트워크상의 경로를 따라 스스로 다른 컴퓨터로 이동하는 것이다. 자가이동은 컴퓨터 시스템이 제공하는 원격 시스템 서비스들의 허점을 이용하여 그 자신의 복제본을

이동시키는 것으로 자신의 복제(replication)와 증식(mutation)에 의해 이루어진다. 인터넷 웜은 자가이동 하지만 이동 전략이 없는 임의적 이동이며, 지정된 목적지가 없는 방랑(wandering)으로 특정 목적지에 도달할 수 있는 가능성이 매우 희박하다 [5,14].

자가이동 능력을 갖는 컴퓨터 프로그램은 자율적으로 목적지로 이동할 수 있으며, 이동시에 프로그램 실행 이전에 지정하는 특정 작업을 수행한다. 컴퓨터 바이러스에 자가이동 기술이 첨가된다면 강력한 사이버 테러 무기가 될 수 있다. 따라서 정보 시스템을 보호하고 안전한 네트워크를 유지하기 위해서 미연에 자가이동 특성을 갖는 소프트웨어에 대한 철저한 분석을 수행하여 이러한 소프트웨어의 침입에 대비하여야 할 것이다.

3.2 소프트웨어 순항

순항은 소프트웨어가 네트워크를 통하여 출발지에서 지정된 목적지로 이동할 수 있는 소프트웨어 행위이다. 순항 특성을 갖는 소프트웨어를 사이버쉽이라고 하며, 사이버쉽은 순항할 때, 복제와 증식으로 자신의 수를 증가시키며, 이들의 집합을 순항 멤버(cruise member)라 한다. 하나의 순항 멤버에 속하는 모든 사이버쉽들은 동시에 순항하는 것이 아니라, 한번에 하나씩 순항한다. 자신의 임무를 수행한 멤버는 폐기되거나 파괴되고 또는 다른 멤버들과 함께 또 다른 순항을 위해 활성화된다.

사이버쉽이 이동하도록 지정된 목적지는 어떤 특정 컴퓨터, 컴퓨터의 그룹 또는 어떤 조직이 될 수 있다. 출발지는 사이버쉽이 이동을 시작 또는 발사되었던 노드이며, 역시 어떤 특정 컴퓨터, 컴퓨터 그룹 또는 어떤 조직일 수 있다. 노드는 개개의 컴퓨터 또는 조직이며, 노드의 속성으로서 순항 멤버를 발견할 수 있는 확률을 갖는다. 이러한 노드들은 출발지, 방문지, 목적지로 나뉘어진다. 출발지 노드는 사이버쉽이 발사되는 노드이며, 방문지 노드는 순항동안 사이버쉽이 방문하는 노드이다. 목적지 노드는 사이버쉽이 이동할 목적지를 나타내는 노드이며, 이것은 사이버쉽이 알아야 하는 중요한 하나의 속성이다.

4. 소프트웨어 순항 기반 정보전 모델

4.1 순항 소프트웨어 특성

순항 소프트웨어는 다음과 같은 특성을 만족하도록 설계되어야 하며, 이러한 특성들은 이동성, 자율성, 익명성, 재생산성을 보장한다.

(1) 노드 특성 분석

이동 대상 노드는 컴퓨터 시스템, 컴퓨터 그룹이며, 그중 한 대 이상의 컴퓨터가 이동의 목적지가 될 수 있다. 노드 특성 분석은 노드 정보수집과 노드 식별 기능을 수행한다. 노드 정보수집에서는 순항 소프트웨어가 방문한 노드의 도메인 이름, IP 주소, 설치된 장치들의 일련번호, 설치된 응용 소프트웨어, 등록된 사용자 정보, 운영체제 정보 등을 수집한다. 이들 정보는 목적지 노드의 식별과 다음에 방문할 노드의 결정을 위해 사용되고, 노드의 IP 주소는 가상지도에 저장된다.

노드 식별은 방문하는 노드들의 특성을 결정하는 행위를 말한다. 즉, 수집된 노드 정보는 이동 방향 및 목적지 결정에 사용된다. 방문 노드에서 수집된 특성 정보들은 먼저, 가상지도상의 목적지 정보와 비교된다. 수집된 노드들 중, 목적지 정보와 일치하는 노드가 있다면 순항은 중단될 것이다. 그러나 목적지 노드가 수집된 노드 정보에 포함되어 있지 않은 경우에는 각 노드에 대해 게이트웨이인지 아닌지를 평가한 후, 이동 여부를 결정한다. 다음으로 나머지 수집된 노드들에 대해 이동 가능성을 조사한다. 이때, 노드 특성 정보들 중 IP 주소를 비교하여 계층별 주소체계를 이용하여 동일 계층의 주소를 가진 호스트에 대해 우선적으로

이동을 시도한다. 식별에 의해 목적지에의 도달 또는 다음 이동 대상 노드가 결정되면, 가상지도 상의 정보는 갱신된다.

(2) 가상지도

가상지도는 지정된 특정 목적지를 대상으로 하는 것으로, 지정된 특정 목적지를 대상으로 하는 정보전에서의 공격모델에서 방랑을 막고 목적지로의 최적 경로를 선택하기 위해 사용된다. 가상지도는 순항 소프트웨어 설계자가 제공하는 목적지 정보와 네트워크 경로상의 컴퓨터 시스템 정보, 네트워크 경로 정보를 포함한다. 가상지도상의 정보는 순항 시스템의 시작 또는 순항 시에 작성 및 변경된다. 목적지에 대한 정보 수집이 가능한 경우 순항 이전에 미리 작성될 수 있으며 정보가 존재하지 않는 경우에는 순항 시에 순항 시스템에 의해 작성된다. 또한, 순항 중에는 네트워크의 상태가 유동적이며 순항 전에 수집된 목적지에 대한 정보가 유효하지 않을 수 있기 때문에, 순항 시스템이 자동으로 가상지도 상의 정보를 갱신하여 목적지로의 이동시의 방랑을 막고 최적 경로를 선택하는데 사용한다. 순항 소프트웨어는 가상지도상의 정보를 기반으로 이동하며, 이동 시, 가상지도 정보는 갱신된다. 가상지도상에 포함된 기본 정보는 다음과 같으며, 순항 목적과 목적지에 따라 포함되는 정보는 달라질 수 있다.

① 목적지 정보 : 순항의 목적지는 유일하며, 가상지도 상에는 목적지에 대한 호스트 이름, IP 주소, 운영체제, 방화벽 시스템, 그리고 특정 응용 코드와 같은 목적지 특성 정보를 포함한다.
② 네트워크 경로상의 컴퓨터 시스템 정보 : 가상지도 상에 포함되는 네트워크 경로 상에 존재하는 컴퓨터 시스템에 대한 정보는 호스트 이름, IP 주소, 및 특성 분석 정보이며 현재 노드에서 다음 노드로 이동시에 갱신된다.
③ 네트워크 경로 정보 : 가상지도는 한 세그먼트에서 다른 세그먼트로 이동시에, 게이트웨이 정보를 저장하여 동일 세그먼트로의 재이동을 방지한다.

(3) 자가이동

자가이동은 하나의 컴퓨터 시스템 상에서 다른 컴퓨터 시스템으로 네트워크를 통해 스스로 자신의 복제본을 이동시킬 수 있는 특성을 말한다. 자가이동은 순항 특성을 지니는 것으로 방랑이 아닌 목적지를 갖는 유한한 이동성을 갖는다. 자가이동 기법은 이동 대상 또는 목적지의 운영환경에 따라 다른 기법을 사용할 수 있어야 하며, 순항의 목적이나 사용 환경에 따라서 변경 가능해야 한다. 다양한 자가이동 기법이 개발된다면 순항 소프트웨어의 자가이동시에 목적지까지의 이동 경로 상에서 발견될 확률을 줄일 수 있을 것이다.

(4) 증가 제어

순항 소프트웨어는 목적지로의 순항을 위해 하나 이상의 순항 멤버를 이동 경로 상의 노드들에 이동시킨다. 오직 하나의 순항 소프트웨어를 이용하여 목적지에 도달하는 경우보다 여러 개의 순항 멤버를 이용하여 목적지에 도달하는 경우, 목적지 도달 가능성이 증가하기 때문이다[14]. 그러나 하나의 노드에 존재하는 순항 소프트웨어의 수를 제한하지 않는 경우 네트워크 상에 무수히 많은 순항 멤버가 존재하게 되는 문제가 발생하여 목적지 도달 전에 발견될 우려가 있으므로 증가제어가 필요하다. 증가제어는 한 노드에 존재할 수 있는 자가이동 코드의 수를 제어하는 것으로, 다음과 같은 절차를 따른다.

① 특정 노드에 존재할 수 있는 자가이동 코드의 최대수를 설정한다.
② 특정 노드로 이동할 자가이동 코드는 먼저 루프백 주소(127.0.0.1)에 대해 소켓을 설정하고 자가이동 코드 수의 정보를 소켓을 통해 주고받는다.

③ 어떤 시점에서 자가이동 코드의 수가 최대수보다 커진다면 나머지 자가이동 코드는 자가 파괴 된다.

(6) 자가 증식

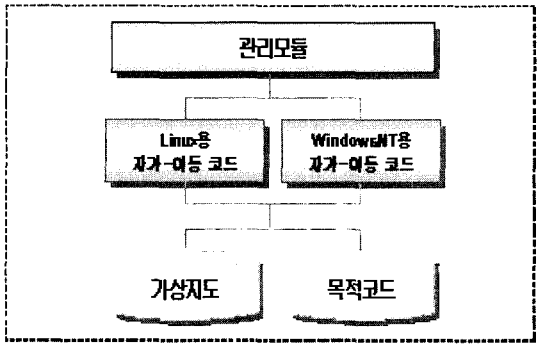
순항 소프트웨어는 특성 변화를 통해, 이동 중 발견될 수 있는 확률을 줄일 수 있어야 한다. 이미 증식엔진(mutation engine)이 개발되어 사용 중에 있으며, W32/leaves와 같은 웜 바이러스에서는 특성 변화를 통해 탐지를 어렵게 하기도 했다.

(7) 자가 방어

자가이동코드는 이동 시, 시스템 관리자에 의해 발견되는 경우 자가이동코드의 분석을 방지하기 위하여 여러 가지 자가 방어 기술을 이용한다. 자가이동 코드는 자신의 존재를 숨기기 위해 자신의 이름을 변경하는 방법을 이용할 수 있으며, 코드의 분석을 방지하기 자가이동 코드 내에 포함된 자체 암호화 함수를 이용할 수 있다. 암호화 함수는 텍스트 수준의 코드 암호화 방법을 이용한다.

4.2 순항 소프트웨어 설계

본 논문에서 설계한 순항 소프트웨어는 앞 절에서 언급한 순항 특성을 갖는 것으로 자가이동을 위해 이미 알려져 있는 시스템 취약성을 이용한다. 실제 네트워크에서는 다양한 보안 시스템들을 이용하여 침해사고를 예방하고 있으나, 이러한 보안 시스템들에 대한 우회 기법이 존재하며 이는 자가이동 기법 선택 시 함께 고려되어야 할 사항이므로 본 논문에서의 순항 소프트웨어 설계에서는 고려하지 않았다. 순항 소프트웨어는 출발지가 Linux인 상태에서 세 가지 이동 패턴 중 노드의 운영체제 특성에 따라 선택적으로 실행된다. 세 가지 이동 패턴은 Linux 서버에서 Linux 서버로의 이동, Linux 서버에서 windowsNT 서버로의 이동, windowsNT 서버에서 windowsNT 서버로의 이동으로 구분된다. 순항 소프트웨어는 관리모듈, Linux용 자가이동 코드, windowsNT용 자가이동 코드, 가상지도, 및 목적코드로 구성된다. 그림 1은 순항 소프트웨어의 프로토타입을 나타낸 것이다.



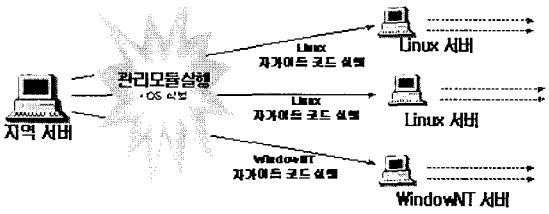
〈그림 1〉 순항 소프트웨어 프로토타입

(1) 관리모듈

순항 소프트웨어의 시작으로, 현재 위치한 노드에서 다음과 같은 절차를 수행한다.

① 현재 호스트 정보 및 이동 대상 호스트 정보 수집
② 운영체제 식별
③ 가상지도 정보와 정보 비교
④ 운영체제에 따라 자가이동 코드 실행

Linux용 및 windowsNT용 자가이동코드는 운영체제의 종류에 따라 선택적으로 실행되며 자가이동은 여러 가지 방법을 통해서 가능하다. 본 논문에서는 Linux 시스템의 경우에는 RPC 메커니즘과 FTP 서비스 취약점을 이용하여 자가이동하고, windowsNT(NT4.0, IIS4.0. Service pack4.0/5.0, Option Pack 4.0) 시스템의 경우에는 IIS의 유니코드 버그를 이용하여 윈도우 tftp를 실행시켜 자가이동 코드를 이동시키고, IIS 클라이언트 요구 메소드를 통하여 자가이동 코드를 원격 실행시키는 방법을 이용한다. 이동이 성공하는 경우, 자가이동 코드의 모든 내용이 그 노드로 이동하게 된다.



〈그림 2〉 순항 소프트웨어 이동 모형

(2) Linux용 자가이동 코드

관리모듈에서 식별한 이동 대상 호스트의 운영체제가 Linux인 경우에 실행되는 것으로, RPC 메커니즘과 FTP 서비스 취약점을 이용하여 이동한다. Linux용 자가이동 코드 프로토타입은 그림 3과 같으며, 그림 4는 Linux용 자가이동 코드의 이동 모델을 나타낸 것으로 이동 절차를 보이고 있다. 예를 들어, FTP를 이용하는 경우의 이동 절차는 다음과 같다.

① 수집된 호스트 정보에 대해 포트 스캐닝을 수행하여 21번 포트를 사용하는 FTP 서비스의 실행 유무를 검사한다.

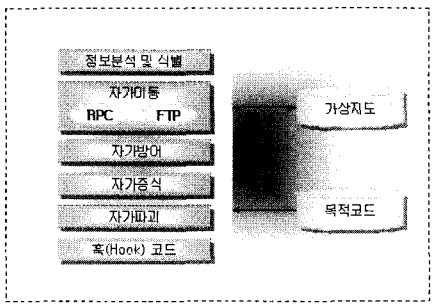
② FTP 서비스가 실행 중이라면, FTP 서비스의 보안 취약점을 이용하여 쉘을 획득한다. 즉, 버퍼 오버플로우를 이용하여 /bin/bash 또는 /bin/sh을 획득한다.

③ 원격 컴퓨터로 훅 프로그램을 전달하고, 컴파일 한 후, 실행되어 지역 컴퓨터에 있는 자가이동 프로그램 파일을 소켓을 통하여 원격 컴퓨터로 복사한다.

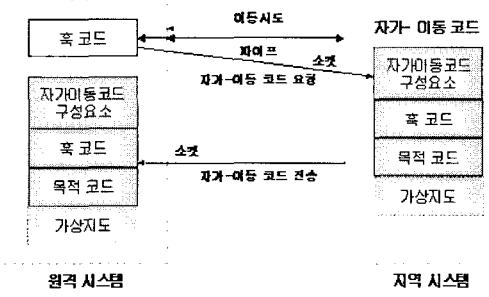
④ 지역 컴퓨터 내의 자가이동 프로그램 파일을 삭제하고, 프로세스를 kill 한다.

(3) windowsNT용 자가이동코드

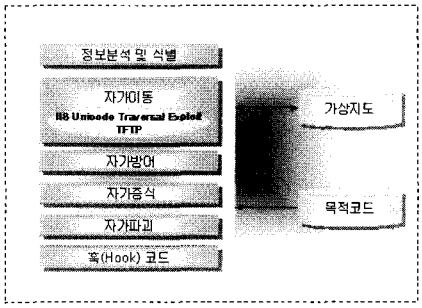
관리모듈에서 식별한 이동 대상 호스트의 운영체제가 windowsNT인 경우에 실행되는 것으로, windowsNT용 자가이동 코드 프로토타입은 그림 5와 같다. 그림 6은 windowsNT용 자가이동 코드 이



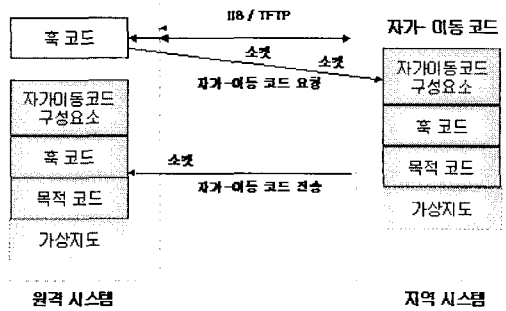
〈그림 3〉 Linux용 자가이동 코드 프로토타입



〈그림 4〉 Linux용 자가이동 코드 이동 모델



〈그림 5〉 windowsNT용 자가이동 코드 프로토타입



〈그림 6〉 Windows용 자가이동 코드 이동 모델

동 모델을 나타낸 것으로 이동 절차를 보이고 있다. 예를 들어, IIS 유니코드 취약점을 이용하는 경우의 이동 절차는 다음과 같다.

① 두 시스템간에 소켓을 설정한다.
② 원격 시스템상의 실행 가능 디렉토리를 찾는다.
③ 윈도우 쉘을 실행 가능 디렉토리로 옮긴다.
④ 실행 가능 디렉토리로 옮긴 윈도우 쉘상에서 유니코드 버그 명령을 통해 tftp를 실행시켜 자가이동 코드를 업로드시킨다.
⑤ 실행 가능 디렉토리에 있는 윈도우 쉘을 이용하여 자가이동 코드를 실행시킨다.

(4) 가상지도

가상지도는 자가이동코드의 목적지 정보와 네트워크 경로상의 노드 즉, 컴퓨터 시스템 정보, 네트워크 경로 정보를 저장한다. 저장된 가상지도 정보는 목적지를 식별하고, 자가이동코드의 이동 방향을 결정하는데 사용된다. 또한, 가상지도상의 정보는 사전 작성되거나 자가이동 중에 작성되어 갱신될 수 있다. Linux용 자가이동코드와 windowsNT용 자가이동코드는 가상지도상의 정보를 기반으로 이동하며, 이동 시, 가상지도 정보는 갱신된다. 가상지도에는 목적지 정보, 네트워크 경로상의 컴퓨터 시스템 정보, 네트워크 경로 정보, 이동 결정 정보 등이 포함된다. 이들 정보들은 순항 소프트웨어 내에 독립된 데이터 파일로 존재하며, 자가이동시에 수집되는 각 노드의 목적지 식별 및 이동 방향 결정에 따라 갱신된다.

가상 지도를 위한 자료구조에는 dhost, vgatelist, hostlist 가 있다. 자료구조 dhost는 목적지 호스트 정보를 저장하는 것으로, 호스트 이름, IP 주소, 특정 응용 프로그램 식별 코드 및 게이트웨이 주소를 저장한다. 목적지 정보는 자가이동 전 자가이동 코드 설계자에 의해 정의된다. 자료구조 vgatelist는 네트워크 이동 시에 경유했던 게이트웨이 정보를 저장한다. 저장되는 정보는 게이트웨이 주소와 트래픽 정보이다. 자료구조 hostlist는 동일 네트워크 내에서 수집된 호스트 정보를 저장하기 위한 것으로, 한 호스트에서 다른 호스트로의 이동 시에 그 정보를 유지한다. 저장되는 정보는 도메인 네임, IP 주소, 플래그 정보이다.

```
struct dhost {
        char *d_name;
        int d_addr;
        int d_gateway;
        char *d_os;
};
struct vgatelist {
                int g_addr;
                int g_traffic;
        struct vgatelist *next;
};
struct hostlist {
        char *hostname;
        int n_addr;
        int flag;
        char *os;
        struct hst *next;
};
```

가상지도는 가상지도 설계자에 의해 작성될 수 있으며, 이동시에 순항 소프트웨어에 의해 자동으로 정보의 추가 및 갱신이 이루어질 수 있다. 가상지도 초기화 및 갱신 과정은 다음과 같다.

① 자가이동 전, 가상지도 설계자에 의해 제작된다.
② 이동시에 자가이동 코드에서 수집된 한 네트워크 내의 호스트 정보들은 가상 지도상의 목적지 정보와의 비교 후, 식별된다. 만약 목적지로 식별되는 호스트가 존재하지 않는 경우에는 그 네트워크의 게이트웨이 호스트 정보만 가상지도에 추가한다.
③ 한 네트워크에서 다른 네트워크로의 이동시에는 가상지도 상의 게이트웨이 정보의 플

래그 필드 정보를 이용하여 이전에 방문한 적이 있는 네트워크로의 이동을 방지한다.

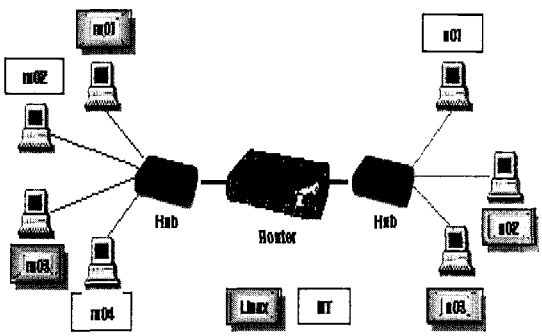
(5) 목적코드

목적코드는 자가이동코드의 목적에 따라 추가될 수 있는 부분으로, 그 내용은 달라질 수 있다. 사이버테러에서 공격을 위한 프로그램, 사이버테러에 대한 공격 후 시스템이나 네트워크 복구 및 감시를 위한 프로그램, 혹은 시스템 및 네트워크의 보안 레벨 테스트를 위한 프로그램 등이 포함될 수 있다.

5. 실 험

5.1 실험 환경

본 논문에서는 간단한 실험 네트워크를 구축하여 구현한 순항 소프트웨어에 대한 시뮬레이션을 수행하였다. 실험환경은 Linux와 windowsNT 서버로 구성된 지역 네트워크를 구성하였으며, 침입탐지 시스템, 침입차단 시스템 등과 같은 보안 시스템들은 고려하지 않았다. 실험 대상 네트워크 환경은 그림 7과 같이 이더넷 방식의 호스트 컴퓨터로 구성되어 있으며, 두 개의 세그먼트가 라우터를 통하여 연결되어 있다.

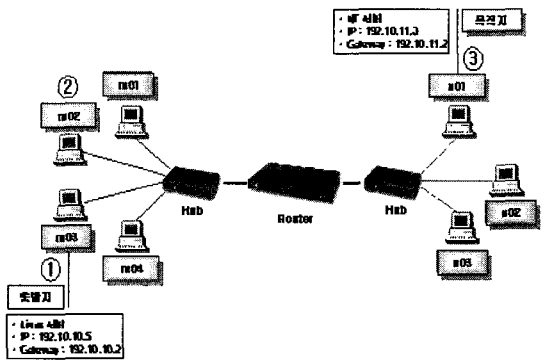


〈그림 7〉 실험 네트워크 환경

5.2 실 험

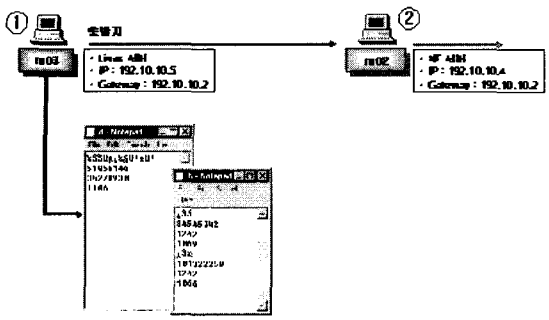
본 논문에서는 실험 네트워크 환경에서 자가이동 기술을 통한 특정 목적지 방문이 가능함을 보임으로써 정보전 대응 모델로서의 가능성을 제시한다.

Linux 서버인 ①번 노드는 출발지 노드로서 자가이동코드가 실행되는 노드이다. 자가이동코드 실행 이전에 가상지도 설계자에 의해 가상지도가 작성되며, 목적지 컴퓨터가 지정된다. 본 실험에서는 NT 서버인 ③번 노드가 목적지이다. 따라서 시뮬레이션은 ①번 출발지 노드에서 시작된 자가이동코드가 ③번 목적지 노드를 식별하여 방문함으로써 완료된다. 시뮬레이션에서 목적지에 대한 IP 주소 및 운영체제 정보는 이미 알고 있는 것으로 하였다. 그림 8은 다른 네트워크로의 자가이동 시의 경로를 보여준다.



〈그림 8〉 다른 네트워크로의 자가이동

출발지 ①번 노드에서 자가이동 코드가 실행되면 가상지도 상의 목적지 정보를 읽어 들여 다음 이동 대상 노드를 결정하게 된다. 다음 이동 대상 노드는 현재 노드에서 이동 가능한 노드들 중에서 선택된다. 실험에서는 ①번 Linux 서버에서 ②번 NT 서버로 이동하였으며 그 결과는 그림 9과 같다. 그림 9에서 텍스트 파일 d는 목적지 정보, h는 이동 경로상에 위치한 노드 정보를 나타낸다.



〈그림 9〉 다른 네트워크로의 자가이동

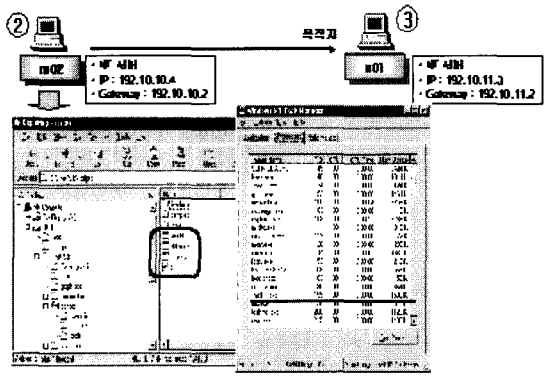
그림 10은 목적지 ③번 노드에 자가이동 코드 및 가상지도 정보가 전달되어 수행중인 상태를 나타낸 것이며, 그림 11은 목적지 ③번 노드에서 자가이동코드의 수행이 완료된 상태를 보인 것이다. 자가이동코드의 수행이 완료된 시점에서는 자가파괴에 의해 이동 흔적을 찾아 볼 수 없다. 즉, 목적지 노드로의 이동시에 기록되는 여러 가지 로그 정보는 자가이동코드에 의해 자동삭제 됨으로, 그 흔적이 남지 않게 된다.

6. 결 론

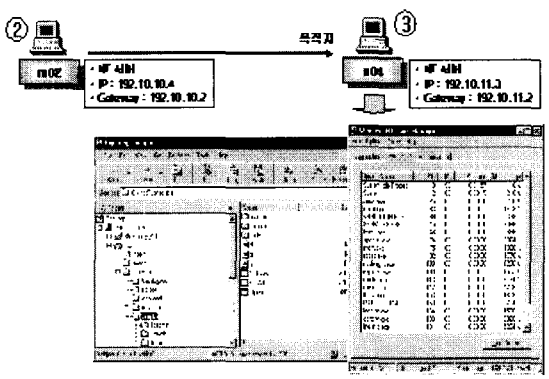
현대 사회는 정보사회로서 정보와 정보 시스템이 국가나 사회 조직의 생존에 결정적인 요인으로 작용하며 정보의 우위를 누가 점유하느냐 하는 것이 주요 관심의 대상이 되고 있다. 이러한 상황은 국가나 사회 여러 조직 및 기구들이 정보 시스템에 더욱 의존하게 만들었으며 필요한 정보를 선점하거나 상대측의 중요한 정보를 파괴함으로써 상대적인 우위를 자치하려는 양상을 보이고 있다. 즉, 정보 시스템에 침입하여 정보를 삭제 또는 변조하거나 정보 시스템의 기능을 중지시키는 등의 사이버전 및 사이버테러와 같은 정보전 양상을 보이고 있다.

본 논문은 소프트웨어 순항 기반 정보전 공격 모델을 제안하였다. Linux와 windowsNT 서버들의 네트워킹 환경에서 원격지 시스템으로 스스로 이동할 수 있는 순항 소프트웨어 시스템을 개발하였으며, 순항 소프트웨어는 노드의 특성 분석 및 식별, 자가이동을 위한 가상지도 등의 특성을 지니며 이는 실험을 통해 그 유용성을 증명하였다.

향후에는 다양한 자가이동 기법과 자가방어를 위한 암호화 기법에 대한 연구가 이루어져야 하며, 보안 시스템이 존재하는 네트워크 상에서의 순항 소프트웨어의 사용을 위한 전략이 연구되어야 할 것이다. 또한, 정보전에 능동적으로 공격 및 방어할 수 있는 대응 구조를 정의하여 정보전 대응모델과 통합되어 운영될 수 있는 정보전 방어 모델이 제시되어야 할 것이다.



〈그림 10〉 다른 네트워크로의 자가이동



〈그림 11〉 다른 네트워크로의 자가이동

참 고 문 헌

[1] Winkler J.R., Oshea C.J. and Stokrp M.C., "Information Warfare, INFOSEC and Dynamic Information Defense," Proceedings of NISSC, Dec. 1996.

[2] M. Libicki, "What Is Information Warfare?," Strategic Forum, No. 28. May 1995.

[3] Edward Waltz, "Information Warfare : Principles and operations," Boston/London: Artech House, 1998

[4] Lenny Zeltser, "The Evolution of Malicious Agents," http://www.zeltser.com/agents, May 2, 2000

[5] Bob Page. "A Report on the Internet Worm," ftp://coast.cs.purdue.edu/pub/doc/morris_worm/worm.paper, 7 Nov. 1988

[6] Eugene H. Spafford, "The Internet Worm Program : An Analysis," Purdue Technical Report CSD-TR-823, Nov. 29, 1988.

[7] Donn Seeley, "A Tour of the Worm," Proceedings of 1989 Winter USENIX Conference, USENIX Association, San Diego, CA, Feb. 1989.

[8] Hyacinth S, Nwana, "Software Agents: An Overview," Knowledge Engineering Review, Vol. 11, No. 3, Setp. 1996, pp. 1-40.

[9] CERT/CC. Overview of Attack Trends, May 2002.

[10] Harold Thimbleby, Stuart Anderson and Paul Cairns, "A Framework for Modeling Trojans and Computer Virus Infection", Computer Journal, Vol. 41, No. 7, 1999, pp. 444-458.

[11] Sung Moo Yang, "AMCW : A New Weapon for the New Millennium," http://www.sungyang. org, Jan. 1998.

[12] Ivan Krsul, "Computer Vulnerability Analysis," Purdue University, Apr. 1997.

[13] Sung Moo Yang, "Autonomous Mobile Cyber Weapon," http://www.sungyang.org, Sept. 1999.

[14] Sung Moo Yang, "The Behavior Cruise," http://www.sungyang.org, Nov. 1996.

[15] Max Vision, "Lion Internet Worm Analysis," http://www.whitehats.com/library/worms/lion/, 2001. 4. http://www.certcc.or.kr/paper/incident_note/2001//in2001_009.html, 2001. 7. 20

[16] Kari Miettinen, "Security Issues in Agent Technology," Research Seminar on Agent Technology, Department of Computer Science, University of Helsinki, Finland, Dec. 11, 1998

[17] Stan Franklin, Art Graesser, "Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents," Preceedings of the Third International Workshop on Agent Theories, Architectures, and Languages, Springer-Verlag, 1996.

[18] 장희진, 박보석, 김상욱, "차세대 공격형 정보보안 기술," 정보처리 제7권 제2호, 2000. 3

[19] Red 웜 확산에의한 피해증가 http://www.certcc.or.kr/paper/incident_note/2001/in2001_008.html, 2001. 6. 29

[20] 새로운 CodeRed II웜 http://www.certcc.or.kr/paper/incident_note/2001/in2001_010.html, 2001. 8. 5

[21] Code Blue Worm의 출현 및 대응방법 http://www.certcc.or.kr/paper/incident_note/2001/in2001_013.html, 2001. 9. 15

[22] 전익수, 이환희, Nimda Worm(W32/Nimda worm) http://www.certcc.or.kr/paper/incident_note/2001/in2001_015.html, 2001. 9. 19

[23] MS-SQL 서버 웜 - 슬래머(Slammer) 공격기법 분석 및 사고대응 http://www.certcc.or.kr/paper/incident_note/2003/in2003_001.pdf, 2003. 1. 28

[24] 이현우, "향후 인터넷 웜 발전방향 및 대응방안," SecurityMap.Net, 2001. 11. 15

[25] 박상서, "정보전: 새로운 전쟁 패러다임," 공군 창군 50주년 기념국제 학술 세미나 논문집, 교리 발전 분야, pp. 25-86. 1999.

◐ 저 자 소 개 ◑

류 호 연
1998년 경상대학교 컴퓨터과학과 졸업(이학사)
2000년 경상대학교 대학원 컴퓨터과학과 졸업(공학석사)
2000~현재 경상대학교 대학원 컴퓨터과학과 박사과정
관심분야 : 순항 소프트웨어, 소프트웨어공학, 정보전, 보안,
E-mail : capella@edu.gsnu.ac.kr

남 영 호
1989년 경상대학교 전자계산통계학과 졸업(이학사)
1991년 중앙대학교 대학원 전자계산학과 졸업(공학석사)
1994년 중앙대학교 대학원 컴퓨터공학과 졸업(공학박사)
1995~1996 신라대학교 전자계산학과 전임강사
1996~현재 경상대학교 컴퓨터교육과 부교수, 경상대학교 컴퓨터정보통신 연구소원
관심분야 : 순항 소프트웨어, 무선 프로토콜 검증
E-mail : yhnam@gsnu.ac.kr