제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

보안 시스템 테스트를 위한 공격 발생 테스트슈트 구현

김 환 국*, 서 동 일*, 이 상 호**
* 한국전자통신연구원 네트워크보안구조연구팀
** 충북대학교 컴퓨터공학과

요 약

현재 인터넷은 이미 일상 생활에 깊게 자리 잡았다. 이러한 인터넷을 이용해서 실생활에서 수행하여야만 했던 많은 일들을 인터넷을 통해 수행할 수 있게 되었고, 인터넷의 편리함 때문에 인터넷 사용자가 늘어났다. 그러나 인터넷 사용자의 증가와 더불어 인터넷을 통한 각종 침해사고 역시 크게 증가하였다. 따라서, 이러한 침해 공격에 대응하는 보안 시스템 개발의 기능을 테스트하기 위해 다양한 공격 패턴과 트래픽을 자동적으로 발생시키는 공격 발생 테스트 슈트가 필요하다. 본 논문에서는 다중 에이전트를 이용하여 다양한 공격 패턴 발생 테스트슈트의 설계 방법과 구현 결과를 기술하였다.

Implementation of Attack Generation Test-Suite for Security System Testing

Kim Hwan-kuk*, Seo Dong-il*, Lee Sang-ho**

ABSTRACT

Currently, internet is deeply rooted in everyday life and many things are performed using internet in real-world, increased internet user because convenience. But then, internet accident is on the increase rapidly. Therefore, it is necessary that testing system generate automatically various attack patterns and traffic. In this paper, we describe method of design and implementation about AGT(attack generation test suite : simulator) system which generate various attack patterns using multiple agents.

1. 서 론

21세기 지식 정보화 사회의 기반은 전 세계적으로 수 백 만대의 컴퓨터가 상호 연결되어 수억의 네티즌들이 사용하고 있는 인터넷이라는 데는 이론의 여지가 없다. 이러한 인터넷 망을 고도화 시키기 위한 선진 각국의 노력 또한 더한층 치열해 지고 있다. 그러나 인터넷은 누구나 쉽게 접근할 수 있는 개방 망 환경으로 인한 해킹, 바이러스 유포, 지적 재산권의 침해, 사이버 범죄에의 이용 등과 같은 정보보호 역기능의 위협도 만만치 않은 것이 현실이다.

이러한 요구에 발맞추어 각종 보안 시스템들을 개발하여 도입하기 시작하였는데, 주로 접근 제어 및 시스템 보안에 초점을 맞춘 제품들로 최근까지 시스템 하나하나가 독단적으로 설치 운

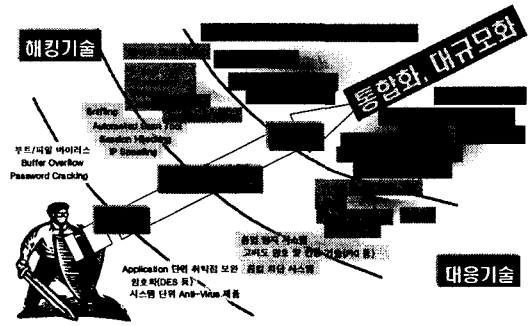
영되는 형태를 보여 왔다. 그러나 점점 사이버 테러 공격 기술의 추세가 기존의 단위 기술에서 총체적이고 유기적으로 연동되는 통합 기술로 발전하고 있으며. 특히, 신속한 전파 능력을 지닌 웜 바이러스에 시스템 및 네트워크를 파괴할 수 있는 해킹 기술을 통합하는 시도가 최근 급격히 증가되고 있어 네트워크 노드에 대한 공격과 다량의 네트워크 트래픽 발생을 동시에 시도하여 "전역적 네트워크 마비"를 일으키는 해킹이 시도되고 있으며, 이로 인해 개별적 보안 시스템으로 이를 막기에 한계에 이르게 되었다. 이렇게 날로 지능화되고 고도화되는 침해 공격에 효과적으로 대응하기 위한 보안 시스템들을 개발하는데 있어 보안 시스템들의 기능들을 테스트하고 평가하기 위한 요소 기술로 가상 공격 패킷 및 트래픽을 발생 시키는 자동화된 테스팅 도구의 개발이 필요하다[1].

따라서, 이러한 네트워크 상의 침해 행위들에 대한 대응을 수행하는 시스템들의 보안 서비스 기능들을 테스트하기 위해 다양한 공격 시나리오를 자동화된 형태로 생성시키는 도구를 설계하여 구현하고자 한다. 본 논문의 구성은 2장에서 최신 해킹 기술 동향에 대해 살펴보고, 3장에서는 공격발생 테스트슈트 설계 및 구현 방법에 대해 기술한다. 마지막으로 결론을 맺는다.

2. 최신 해킹 기술 동향

최근의 해킹 기술 특징을 살펴보면, 단일 기법 중심의 해킹/바이러스 기술이 점차 통합화, 고도화, 해킹 매체 및 목적이 다양화되고 있다.

해킹의 공격 대상은 개별 시스템/서버 중심에서 개인 PC 공격을 활용하여 인터넷에 연결된 네트워크를 대상으로 하고 있다. 그리고, 해킹에 의한 피해 정도는 지엽적인 소규모 수준에서 광역적인 대규모 수준으로 변하고 있다. 또한, 공격의 목적이 개인적이 아닌 정치·사회, 군사·산업적 목적으로 악용되어 네트워크 또는 특정 서비스의 기능을 마비 및 파괴시키는 핵티비즘(Hacktivism)의 형태로 변화하고 있다[2].



(그림 1) 최근 해킹 기술 동향

■ 악성코드(웜/바이러스)의 증가

초기 웜은 컴퓨터의 메모리에서 자기 복제를 통해 컴퓨터 부팅을 방해하는 프로그램으로서 피해범위는 개별 시스템으로 한정되며, 디스켓을 통한 느린 전파가 전부였다. 그러나, 네트워크 컴퓨팅 기술의 비약적인 발전으로 인하여 피해범위가 인터넷과 연결된 컴퓨터 전체의 영역으로 확장되고 악성코드의 전파 수단으로 e-mail과 인터넷이 사용되면서 피해범위가 네트워크를 통한 동시 다발적으로 광범위하게 이뤄지고 있다. 또한, 해킹에 이용되는 기술들의 통합화가 이뤄지고 있다.

■ 어플리케이션 해킹의 증가

최근 주요기관이 침입차단시스템 설치 운영 등 보안관리 강화로 인하여 해커들이 직접 침투하기 어려운 환경이 되고 있다. 그러나 외부에 공개되는 웹 포트(80번)을 이용한 공격과 사고가 급증하고 있다. 즉, 기존의 침입차단시스템과 침입탐지 시스템은 어플리케이션 계층에서 발생되는 해킹에 대응할 수 있는 보안 메커니즘이 취약하다. 따라서, 웹 어플리케이션에서의 버그나 CGI 프로그래밍 기법이 보안의 취약성을 낳게 된다.

■시스템공격에서대규모네트워크공격

해킹은 기존의 개인적인 호기심을 만족시키고 자신을 과시하기 위해 특정 시스템에 접근해 파괴하던 형태에서 정치, 사회, 군사, 경제적인 목적 달성을 위한 시스템, 네트워크의 주요자원을 악용하는 형태로 변화하고 있다. 특히 네트워크 또는 특정 서비스의 기능을 마비시킴으로 인터넷 자체를 불가능하게 하고 있다. 지난 1.25 인터넷 대란의 원인인 슬래머 웜과 국내 ISP의 대형 백본 망에서 송수신되는 트래픽 중 약 10%가 정상적인 서비스와 무관한 트래픽 이라는 사실을 통해 대규모 피해를 유발시키는 웜의 증가 및 개별 시스템 공격에서 네트워크 대역폭을 고갈시키는 유형의 네트워크 공격이 크게 증가되고 있음을 알 수 있다.

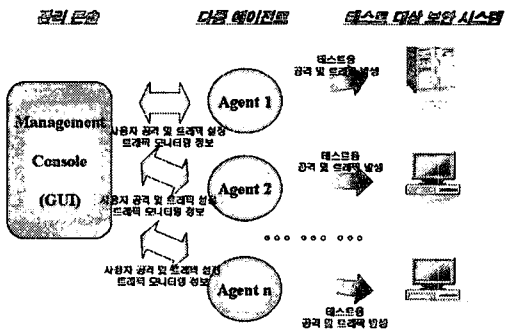
■무선랜관련취약점공격증가

무선랜 환경이 확대되면서 무선랜 프로토콜 아키텍처의 취약점을 이용한 무선랜 해킹도 늘어나고 있다. 무선랜 해킹의 대표적인 기법은 무선 액세스포인트의 인증구조를 이용하는 것으로서 이 기법은 무선랜 사용자가 액세스 포인트에 접속할 때 가상의 액세스 포인트를 경유해 해커가 사용자 중요정보를 모니터링하게 된다. 무선랜 해킹 툴로는 에어잭, 에어 스너트, 더블유잭, 몽키잭, WEP크랙 등이 있다.

이 밖에도 인스턴트 메신저를 이용한 공격, Peer-to-Peer 응용 프로그램을 이용한 공격, PDA을 이용한 공격 등 고성능/고도화 해킹 기술이 출현하고 있으며, 해킹을 이용한 매체 및 목적이 다양화되고 있다.

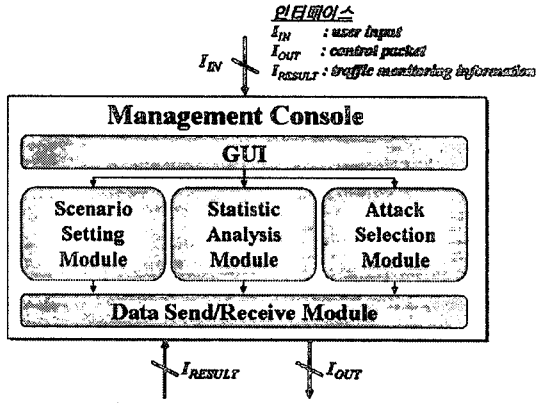
3. 공격 발생 시뮬레이터 구조 및 설계

본 논문에서 설계하는 공격 발생 테스트슈트(AGT : Attack Generation Test suite)는 네트워크를 통한 다양한 네트워크 공격 패킷 및 트래픽을 자동화된 형태로 발생시켜 각종 보안 시스템을 테스트하는데 사용하기 위한 도구이다.



(그림 2) AGT의 시스템 구성도

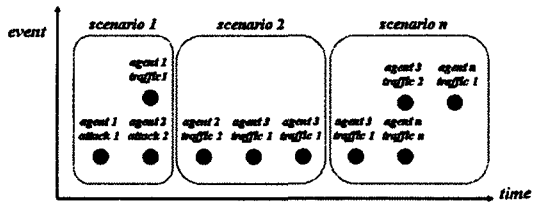
보안 시스템 테스트용 공격 발생 테스트슈트(AGT)는 관리콘솔과 에이전트로 구성되며, 하나의 관리콘솔에 다중 에이전트가 연결 구성될 수 있다. 그림2는 AGT의 시스템 구성도이다.



(그림 3) 관리콘솔 블록 구조도

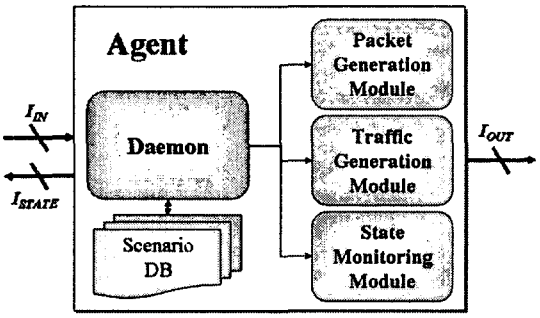
관리콘솔(Management Console)은 다양한 공격 유형과 트래픽 발생 유형을 선택하기 위한 공격 선택모듈(ASM : Attack Selection Module), 다양한 에이전트에 다양한 공격 시나리오를 설정할 수 있는 시나리오설정모듈(SSM : Scenario Setting Module), 설정된 공격 패턴과 트래픽들의 발생 현황을 보여주는 통계분석모듈(SAM :

Statistic Analysis Module), 관리 콘솔에서 설정된 내용을 해당 에이전트에 제어 신호를 보내고, 패킷 발생 정보를 수신하기 위한 데이터 송수신 모듈(DSRM:Data Send/Receive Module)로 구성한다(그림3).



(그림4) 시간에 따른 공격 시나리오 발생도

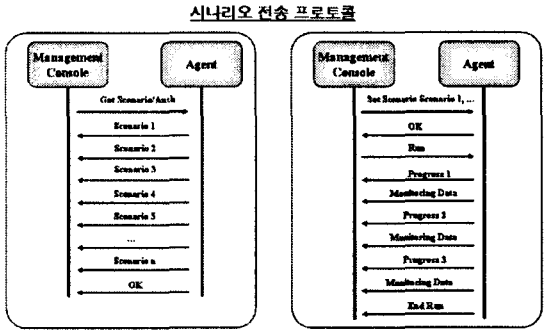
AGT는 관리콘솔에서 제어패킷을 다중 에이전트로 전송하여 여러 가지 형태의 공격 시나리오에 따른 공격 패턴/트래픽 발생이 가능하도록 설계하였다. 다음 그림4는 설정된 시간에 따라, 다수의 에이전트에서 다양한 공격 패턴/트래픽 발생을 위한 공격 시나리오에 대한 내용을 나타낸 것이다. x축은 시간(time)이며, y축은 발생시간에 따라 발생되는 공격 이벤트를 가리킨다.



(그림 5) 에이전트 블록 구성도

공격 발생 에이전트는 관리콘솔과 제어 패킷을 송수신하며 통신을 하고, 선택된 시나리오에 따라 시나리오 DB의 시나리오를 설정하고 결과를 보내는 데몬(Daemon) 모듈, 설정된 공격유형에 따라 다양한 공격 패킷들을 생성하는 공격생성 모듈(PGM:Packet Generator Module), 설정된 트래픽 양에 따라 TCP/UDP 트래픽을 발생시키는 트래픽생성모듈(TGM:Traffic Generation Module), 발생된 공격 패킷과 트래픽의 현재 상태와 진행 상황을 모니터링하는 상태모니터링모듈(SMM:State Monitoring Module)로 구성된다.

다음 그림 6은 관리콘솔과 에이전트 간에 시나리오 전송 프로토콜 구조이다.



(그림 6) 시나리오 전송 프로토콜

에이전트 내 데몬은 Socket을 열고 관리콘솔의 명령을 기다리는 프로세스로 TLS 상호 인증을 기본으로 한다. 상호 인증에 의해 인증 및 암호화가 수행되고 이에 따라 통신이 수행된다. 데몬에 전송되는 Scenario는 그림 6과 같이 전송된다. 프로토콜은 Get/Set/Run으로 구분된다.

- Get : 서버에 있는 Scenario를 가져옴
- Set : 사용자가 선택한 시나리오
- Run : 현재의 선택 사항을 실행

다음 표1은 AGT에서 동작 가능한 시나리오 목록이다. Scanning과 Exploit을 이용한 공격에 대한 Signature 테스트, 우회에 대한 Evasion 테스트, False Positive 가 많이 나오도록 유도하는 False Positive 유도 테스트를 수행하는 공격 생성 패턴과 테스트 대상 시스템의 성능 테스트를 수행하는 트래픽 생성 시나리오 두 종류로 구분한다.

구분	계열	서비스
공격 생성	Exploit	BIND
		finger
		FTP
		HTTP
		RPC
		Windows
	False Positive	
	IDS Evasion	Fragment
		URL Obfuscation
	Network	DOS
		Reply Test
	SANS Top20	
	Scan	IP Integrity Checker
		Nessus test
		Nethios scan
		Port scan
		SNMP Probe
		SSH scan
트래픽 생성	TCP 관련	TCP 25%
		TCP 50%
		TCP 75%
	UDP 관련	UDP 25%
		UDP 50%
		UDP 75%

(표 1) 공격 시나리오 목록

4. 결론

본 논문에서는 네트워크 침입대응을 위한 보안 서비스를 제공하는 네트워크 보안 시스템 기능들을 테스트하기 위해 다중 에이전트 방식을 이용한 공격 발생 테스트슈트(AGT : Attack Gene-ration Test suite)를 설계하여 구현한 내용을 기술하였다. AGT 시스템은 다양한 공격 패턴 발생, TCP/UDP 등의 다양한 트래픽 발생, 보안 노드들의 취약성 공격 시나리오를 자동화된 형태로 생성시키는 기능을 가지고 있으므로, 구현된 시스템을 이용하여 네트워크 보안 시스템들 개발에 있어 성능 및 기능 평가 및 문제점 파악에 이용 가능할 것이다.

참고문헌

[1] 김거우,김환국,김정녀, "대규모 트래픽 폭주 공격에 대한 지능적 대응 방안", 한국인터넷정보학회지 3월호 특집, 2004.3.

[2] 서동일, "차세대 해킹대응 기술", 제8회 정보보호심포지움, 2003.7.

김 환 국

1998년 : 한국항공대학교 전자계산학과 이학사

2000년 : 한국항공대학교 컴퓨터공학과 공학석사

2000. 9.~2002. 4. 이레스페이스

2002. 5.~현재 한국전자통신연구원 네트워크보안구조연구팀

서 동 일

1989년 : 경북대학교 전자공학과 공학사

1994년 : 포항공과대학교 정보통신학과 공학석사

2002년 : 충북대학교 전자계산학과 (박사과정 수료)

1989. 1.~1992. 2. : 삼성전자종합연구소

1994. 3.~현재 한국전자통신연구원 네트워크보안구조연구팀장

이 상 호

1976년 : 숭실대학교 전자계산공학사

1981년 : 숭실대학교 대학원 시뮬레이션 공학석사

1989년 : 숭실대학교 대학원 컴퓨터네트워크 공학박사

1981년 ~ 현재 충북대학교 컴퓨터과학과 교수