시뮬레이션을 이용한 Network의 취약성 진단 및 능동적인 Network 보안에 대한 연구

김재희*, 지승도*, 박종서*, 이장세*, 정정례*

*한국항공대학교, 컴퓨터공학과

Diagnostication of Network vulnerability by Simulation and Dynamic Network Security

Jae-Hee Kim, Jong-Sou Park, Sung-Do Ji, Jang-Se Lee, Jeong-Rae Jeong

Dept. of Computer Engineering, HanKuk Aviation Univ.

요 약

현대 사회는 정보시스템 및 정보통신망에 대한 의존도가 높아지고 있으며 이러한 기반시설들이 국가의 안보에 막대한 영향을 미친다. 그에 대비하여 사회 여러 분야에서 Hacking 및 사이버테러 등 주요 기반구조 침해위협을 방지하기 위해서 많은 노력이 이루어지고 있으며 본 논문에서는 시뮬레이션을 이용한 Network의 취약성 진단 시스템 및 Real Network의 능동적인 구성설정의 변경을 통한 보안성 향상에 대한 연구를 통하여 기존의 보안도구 보다 한 차원 진보된 성능의 시스템을 제안한다. 본 시스템은 네트워크의 변화에 대해 수동적인 기존의 보안 도구에 비하여 시뮬레이션이라는 기법을 이용하여 Network의 변화에 마추어 원하는 시기에 수시로 바뀌는 네트워크 취약성의 정도를 측정할 수 있고 취약성에 대한 대응정책을 토대로 Real Network를 구성하는 각 Component들의 구성설정을 적절하게 변화시켜 줄 수 있는 Agent 시스템으로 Network을 능동적으로 Control하여 보다 효율적인 방법으로 보안성을 강화시킬 수 있으며 네트워크/시스템의 보안성이 현저하게 향상될 수 있을 것이다.

I. 서론

정보화의 진전에 따라 사회시설이 전반적으로 정보통신기반 기술을 이용하여 자동화되고, 이에 따라 점점 더 정보시스템 및 정보통신망에 대한 의존도가 높아지고 있으며 이러한 기반시설들이 국가의 경제 및 안보에 막대한 영향을 미친다. 그러므로 급증하고 있는 Hacking 및 사이버테러 등 주요 기반구조 침해위협을 방지하기 위해서는 주요 기반구조를 소유, 운용 및 관리하는 공공기관 및 산업체의 보호노력에 대한 통합 및 조정이 절실히 요구된다[1,2].

더욱이 Hacking과 Cracking이 대중적으로 유행하고 있는 시점에서 현대의 네트워크에서 보안은 가히 뚫으려는 Hacker와 그 공격을 방어하려는 시스템 보안 관리자 사이의 다툼이라고 볼 수 있다. 그 입장에서 시스템 보안 관리자는 창과 방패의 측면에서 볼 때 방패이며 Hacker에 비해서 항상 수동적인 입장인 것이 사실이다. 아무리 기존 Hacking 방법에 대하여 완벽한 네트워크/시스템 보안을 해놓았다고 하여도 Hacker가 새로운 방법을 발견하여 보안 관리자가 모르는 방법으로 Hacking을 시도한다면 그 시스템은 어느 누구도 지키기 힘들게 된다. 그리고 현실적으로 보안 관리자들은 다양한 Hacking에 대한 지식이 부족하고 회사에서의 업무로 인하여 공개된 새로운 Hacking 방법의 출현과 그것에 대한 보안기술을 습득하기 힘든 것이 사실이다. 그리하여 보안 관리자가 자신이 관리하는 네트워크와 보안에 관련한 지식이 완벽하지 않더라도 그를 대신하여 원하는 시기에 시시각각 전반적인 네트워크/시스템의 취약성을 평가해 줄 수 있으며 동시에 그 취약성에 대한 대응정책을 제공해 줄 수 있는 시스템과 그 대응정책을 토대로 Real Network에 적절한 대응을 Dynamic하게 적용시켜 줄 수 있는 시스템이 존재한다면 네트워크/시스템의 보안성이 현저하게 향상될 수 있을 것이다.

기존의 네트워크 모델링 및 시뮬레이션의 연구는 알려진 공격 뿐 아니라 기호적 시뮬레이션을 통하여 정교한 모델링을 구현하고 그것을 이용하여

가상의 공격 시나리오의 자동생성에 대하여도 연구가 되어있다[3]. 이런 연구가 진행된 상태에서 그것을 이용하여 현재의 네트워크와 그와 함께 구성되어 있는 시스템들의 상태 정보를 수집하고 네트워크/시스템의 취약성의 정도를 판단한다. 그 후 수집된 정보를 토대로 Network Component들의 구성설정을 능동적으로 변환하여 보안성의 향상을 꾀할수 있으며 정해진 정책에 따라 전체적인 취약성의 정도를 현저히 줄일 수 있다.

II. 지능형 보안관리 시스템 개요

1. 보안 모델링과 시뮬레이션

모델링과 시뮬레이션 연구는 많은 응용 분야에서 이용되고 있지만 정보 보호 분야의 경우 가상 공격과 방어의 복잡성, 방대한 탐색 공간, 공격과 방어에 대한 정보의 부족 등으로 타 분야에 비해서 연구가 미진한 상태이며 특히, 국내의 경우, 보안 모델링에 관한 연구는 전무한 실정이다. 대표적인 보안 관련 모델링에 관한 연구는 Cohen, Amoroso, Nong Ye의 연구로 요약된다.

지금까지의 Cohen, Amoroso, Nong Ye의 연구는 네트워크 보안 모델링에 있어서 나름대로의 연구결과들을 제시하고 있지만 원인-결과 모델에 의한 가상 공격과 방어의 표현은 너무 단순하게 표현했기 때문에 실제 적용을 하는데 어려움이 있으며, 침입 모델에 대한 연속적인 행동은 침입 모델에 대한 행동을 보이는 장점을 가지는 반면, 보안 메커니즘 중심의 표현으로 인해 컴퓨터 시뮬레이션 접근이 분명치 않은 단점을 가진다. 마지막으로 Nong Ye의 접근은 복잡한 시스템에 대한 단계적 접근이 돋보이지만 이러한 단계를 적용한 모델링 및 시뮬레이션 기법에 대한 구체적인 예시가 없는 실정이다[3].

본 연구에서는 가상 공격에 대한 명령어 수준의 접근을 통해서 Nong Ye가 가장 바람직한 단계로 제안한 기능단계의 모델링을 시도하여 시스템을 구현하였으며 시뮬레이션 후 Real Network로의 적용의 흐름의 개요를 간단하게 그림으로 표현하면 다음과 같다.[4]

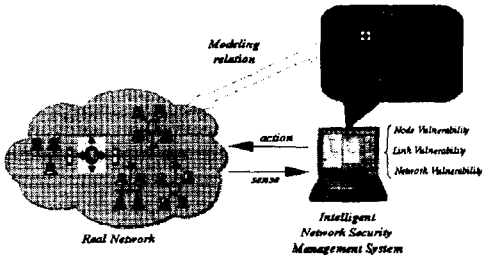

그림 1 지능형 보안관리 시스템의 개요

2. 취약성 분석 및 대응 전략

본 장에서는 Unix host, Router, X-terminal, Windows NT, Windows 98, Web Server 등을 포함하는 네트워크를 구성하는 구성원의 구성설정 오류 등에 의한 보안 취약성을 분석하여 시뮬레이션 기반의 취약성 분석을 위한 노드, 링크, 네트워크 취약성과 대응전략에 대한 개념을 정의하고 모델링하였다.[4]

1) 노드 취약성

노드 취약성은 네트워크상의 구성원들이 갖는 취약성 항목들에 대한 종합적인 취약성 값을 나타낸다. 이를 위하여 우리는 먼저 취약성 항목별 값의 범위를 0 ~ 1 사이의 값으로 정의하였으며, 이 값은 시뮬레이션 평가를 통하여 얻을 수 있다.

2) 링크 취약성

전 세계적인 인터넷 구축에 따른 접속점 증가에 따른 접근 경로의 다양화로 링크 취약성 분석이 필수적이며, 이에 따라 본 연구에서는 노드 취약성과 같이 링크 취약성을 0 ~ 1 사이의 값으로 정의하였으며, 이 값은 시뮬레이션 평가를 통하여 얻을 수 있다.

충분한 반복적인 시뮬레이션을 통해 얻은 통계치를 이용하는 방법으로 공격이 시도된 링크별로 다양한 취약성을 평가함으로써, 접근 경로상의 취약성 및 대응책을 효과적으로 분석할 수 있다.

3) 네트워크 취약성

네트워크 취약성은 네트워크 단위로 그룹화하여 통합한 취약성 매트릭스를 말하는데, 이는 네트워크의 전반적인 취약성에 대한 종합 평가를 위한 방편으로 사용될 수 있다. 네트워크 취약성은 해당 노드와 링크의 취약성 값들에 대한 산술평균으로 간단히 얻을 수 있다. 그러나 이 경우, 단순한 산술평균에 의한 산정보다는, 해당 노드별 역할에 따른 중요도에 대한 가중치를 두어서 종합 평가하는 것이 보다 합리적이다.

4) 대응전략

공격을 방지하기 위하여 자원을 변경하는 행동(명령어)의 집합을 대응 전략으로 정의하고 자원의 취약성에 따른 대응 전략을 명세하여 데이터베이스로 관리함으로써, 시뮬레이션을 통하여 분석된 취약성에 따른 대응 전략을 생성한다. 또한, 생성된 전략을 적용한 후 시뮬레이션을 통하여 생성된 전략을 평가함으로써 정책에 부합하는 최적의 대응 전략을 수립할 수 있다.

3. 취약성 보안

현재 구성되어 있는 전체적인 네트워크의 상황을 시뮬레이션하여 측정한 취약성의 정도를 보안하기 위하여 규정된 정책에 적합하게 본 시스템에서 생성된 대응전략을 기준으로 Real Network를 구성하고 있는 각각의 Component(Router, Firewall, IDS, Host 등등)들의 기능과 구성설정 등을 생성, 수정, 변경하여 전반적인 네트워크의 보안성 향상을 목적으로 하

는 것이 기본적인 개념이다.

III. 지능형 보안관리 시스템 구조

본 논문에서 제안하는 지능형 네트워크 보안 관리 시스템은 기존의 다양한 보안 기능이 있는 도구 즉, 방화벽, IDS, Router, Host 등과 연동하여 정보를 수집하고 이들에 적용 가능한 전략을 수립하여 적용함을 전제로 한다. 개략적인 흐름을 보면, 네트워크는 정상적인 사용자와 비정상적인 사용자 즉, 공격자에 의하여 사용되이질 수 있으며 이에 따른 네트워크 상의 취약성 변화를 네트워크 보안 관리 시스템이 전체적으로 모니터링한다. 모니터링 된 자료를 토대로 네트워크의 취약성을 정량적으로 분석하고 관리자의 정책을 반영하여 최적의 방어 전략을 계획한다. 이어 계획된 전략은 Security Agent의 명령을 통해 각각의 Network Component들에게 전달되고 변경된 Network Component들의 방어기능에 의하여 네트워크가 안전하게 관리됨으로써 지능적이고 능동적인 보안 관리가 이루어진다.[4]

1. 전체적인 구조와 동작

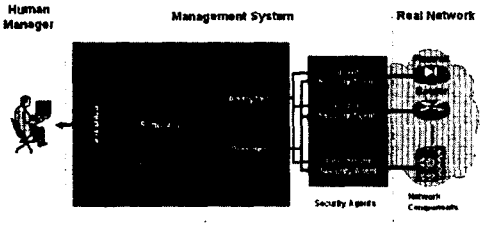

그림 2 지능형 보안관리 시스템 전체 구조도

2. 모듈의 기능

- Interface : 관리자와 시스템간의 정보전달을 용이하게 하기 위한 GUI(Graphic User Interface)
- Analyzer : 취약성 매트릭스를 이용하여 시뮬레이션의 결과를 정량적으로 분석하는 모듈
- Planner : Simulator를 통하여 평가하고 정책을 반영하여 방어 전략을 수립하는 모듈
- Simulator : 네트워크의 상황을 모니터링한 후 그 정보 및 방어전략을 이용하여 시뮬레이션을 수행하는 모듈
- MB : 시뮬레이션을 위한 네트워크 구성원을 모델링 해놓은 모델베이스
- Command-DB : 명령이 모델링을 통해 구성된 명령이 데이터베이스
- Attack-DB : 명령어의 집합으로 구성된 공격 시나리오 데이터베이스
- Vulnerability-DB : 취약성 분석을 위한 취약성 데이터베이스
- Defense-DB : 방어전략 생성을 위한 전략 데이터베이스
- Security Agents : Network component(기존 보안 도구)와 연동하기 위하여 상태를 점검하며 생성된 방어전략을 Network component에 적용, 관리하기 위한 Agent
- Network Components : Real Network를 구성하는 개체들로 Router, Firewall, IDS, Host Server 등을 포함

IV. 능동적 네트워크 제어

1.Active Network Component Control

현재 구성되이 있는 Network의 상황과 Network을 구성하고 있는 Component들 중에 필요한 것들의 구성설정을 파악하고 지능형 보안관리 시스템을 이용해 해당 Netwok이 지니고 있는 취약성을 분석한 후 본 시스템에서 생성된 대응전략을 이용하여 조정할 필요성이 있는 Component들을 정책에 맞는 적절한 구성설정의 변경만으로 최적의 보안성을 제공할 수 있도록 각각의 Component별 정책을 구분한다. 그 후 해당 Component를 관리하는 Security Agent가 각 Component의 기능적 구성을 변경할 수 있도록 명령을 전달한 후 각각의 Component에 적합한 명령을 실행시킨다. 이런 흐름을 통하여 Component를 능동적으로 제어가 가능하며 결국 전체적인 네트워크를 원하는 정책에 적합하게 Contorl할 수 있으며 그것을 통하여 전체적인 네트워크의 보안성을 향상시킬 수 있다.

본 논문에서의 연구는 위와 같은 이론으로 실제 모든 Network Component의 능동적 제어를 대표하기 위하여 Router를 원격지에서 동적으로 제어하는 Agent를 구현하였으며 Router의 여러 기능을 이용하여 네트워크 상의 취약성을 보안하였다.

2. RCS(Router Control System) 구조와 흐름

RCS는 Router를 명령어 파일 형식에 적합하게 동적으로 제어할 수 있는 기능을 가진 시스템이며 RCS Agent 의 기능은 지능형 네트워크 시스템에서 생성된 대응전략 파일을 토대로 정책파일로 변환, 그 내용을 각 Component에 적합한 명령이로 바꾸어 그것을 각각의 Router를 Control할 수 있는 시스템인 RCS로 보내어 각 Component의 구성설정을 정책에 맞게 재설정하게 된다. 이 과정에서 불필요하거나 취약한 네트워크의 노드 또는 링크가 있다면 그곳에 해당하는 Routing Table이나 또는 Access List를 이용하여 원하는 IP또는 해당 IP의 Port를 Blocking할 수 있게 되므로 네트워크의 보안성을 상황에 맞게 한 층 강화시킬 수 있다.

RCS Agent와 RCS 사이의 구조는 다음과 같다.

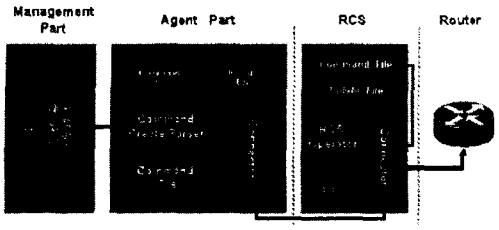

그림 3 RCS Agent와 RCS의 구조도

3. 모듈 기능

- Command DB : Router에 적합한 명령어를 생성하기 위해 Router의 명령어 형식을 가지고 있는 DB
- IP List DB : Router IP, RCS IP 등의 각종 IP 정보를 가지고 있는 DB
- Command Create Parser : 대응전략 정책 파일을 기초로 Router에게 전달할 명령어를 Command DB를 참고하여 생성하는 모듈
- Connector : 각각의 연결해야할 시스템 사이를 연결시켜주는 모듈로서 Telnet, Socket, COM Port등을 통하여 연결할 수 있는 접속 모듈
- Command File : Command Create Parser에 의해 생성되며 Router에 직접 입력할 명령어들이 집합된 파일
- Delete File : RCS가 Router에 적용시켜 놓은 Command들을 삭제하며 원상복귀 시킬 수 있게 해주는 명령어 집합 파일
- RCS Operator: Command DB를 기준으로하여 Router에게 직접 명령을 내릴수 있는 모듈
- Log : Router에게 행해지는 모든 명령과 행동 그리고 결과의 정보를 담고 있는 Log

V.결과 및 응용분야 고찰

본 논문에서는 수시로 바뀌는 네트워크의 취약성의 변화를 한번의 구성설정을 통해 보안기능을 제공하는 보안도구를 이용하여 전반적인 네트워크의 보안성을 제공하기에는 한계가 있으며 또한 관리자의 미숙은 제대로 된 보안성능의 효과를 제한할 수 있다. 그러므로 현재의 네트워크의 취약성의 변화에 항시 대처할 수 있도록 스스로 네트워크의 취약성을 평가할 수 있는 시스템을 시뮬레이션을 이용하여 설계, 구현하였고 이를 통하여 나온 대응전략을 토대로 보안도구의 성능을 정책에 맞게 제대로 발휘할 수 있도록 조절하는 시스템 Agent의 이론을 제안하며 대표적인 Agent로 Router를 능동적으로 제어하는 RCS를 설계, 구현하여 보았다.

향후 연구과제로는 모든 Component를 제어할 수 있는 Agent의 설계, 구현과 표준화 방향의 제안에 대한 연구와 개발. 그리고 지능형 보안관리 시스템 이외의 다른 시스템(ESM 등등)과의 인계를 통한 연구와 개발이다.

Acknowledgements

본 연구는 정보통신부 ITRC사업의 지원을 받아 진행되었음.

참고문헌

[1] Longstaff T. A., Chittister, C., Pethia, R. and Haimes Y., "Are We Forgetting the Risks of Information Technology", IEEE Computer, pp.43-51, December, 2000.

[2] 이철원, 김홍근, 정보보증: "컴퓨터보안의 새로운 패러다임", 정보과학회지, 제18권 제1호, pp.53~61, 2000년 1월.

[3] 이민우 : "기호적 시뮬레이션을 이용한 가상 공격 시나리오 자동 생성에 관한 연구", 한국항공대학교 공학석사 학위논문, pp 1~15, 2002년 2월.

[4] 지승도외 몇명, "지능형네트워크보안관리시스템개발",신기술개발사업보고서, 산업자원부, 2002. 9.