한국콘텐츠학회 2003 춘계종합학술대회 논문집 Vol.1 No.1

해킹 기법을 이용한 보안 시스템 설계 및 방안

서 복 진, 김 삼 수
예원대학교 정보 경영학부

Bok-Jin Seo, sam-su Kim
School of Information and Management, Yewon Univ.

요 약

인터넷과 네트워크기술이 발전함에 따라 전자적 거래 등의 사이버마켓에 관한 응 용분야가 운영되고 있으며, 실제 오프라인 마켓 보다 더 많은 수익을 내는 쇼핑몰 운영업체들이 나타나고 있다. 또한 원격지의 구매자로부터 인터넷 뱅킹에 의한 쉽고 빠른 결재 방식으로 인하여 구매, 결재에서 배송까지 하나의 프로세스라인을 구축하고 있다. 이에 따른 사용자 정보를 보호하기 위한 여러 가지 암호화 기법들이 연구 및 도입되고 있다. 따라서 인증 되지 않은 외부 침입자로부터 시스템의 정보보호를 위하여 침입탐지 시스템 및 암호화, 복호화 알고리즘을 적용하여 소프트웨어 측면에서의 보안기법과 Firewall 등의 하드웨어적인 보안기술이 도입 및 실용화 되고 있는 것이다.

본 논문 에서는 우리 주변에서 발생 하고 있는 해킹 사고 사례와 나날이 발전해가는 해킹 방법의 동향, 이러한 불법 침입을 이용한 침입 탐지 기법들과 네트워크에 관련한 침입탐지 방안기술 그리고 라우터 장비에서의 침입탐지 방안을 제시 하였다.

1. 서론

정보화 사회의 활성화와 정보통신 인프라로서 인터넷의 중요성이 급속히 부각되고 있으며, 이를 통한 중요 정보의 유출 문제가 나날이 심각해지고 있다. 더욱 현재의 정보통신 기반 구조로는 서로 밀접하게 연관된 단위구조들로 연관되어 있어 네트워크 구조의 복잡도 증가로 인한 문제가 확산되고 있다 특정 단위구조에 대한 사이버 테러 발생 시 연결된 구조로의 피해 확산이 우려될 뿐 아니라, 실제 피해규모도 추산하기 어렵고, 이에 따른 효율적인 차단 및 복구에도 어려움이 가중되고 있는 실정이다[1].

정보통신과 컴퓨터기술의 발전은 불법침입으로 인한 정보파괴와 컴퓨터 바이러스 등에 의한 역기능이 날로 증가하고 인터넷과 같이 범세계적인 네트워크로 연결되어 있는 정보 시스템에 대한 위협 역시 급속히 증가하고 있는 추세이다. 이러한 이유로 비밀성, 신뢰성 등의 정보보호 서비스에 대한 요구가 증대되어 정보보호 기술 및 정보보호 제품에 대한 수요가 점차 확대되어 가고 있다.[2]

또한, 컴퓨터 네트워크를 통한 원격지간의 비대면 거래방식은 시대가 바뀜에 따라 피할 수 없는 현실이 되었으며,[3] 특히 인터넷의 확장으로 인한 외부인의 시스템 불법침입, 중요정보의 유출 및 변경·훼손·불법적인 사용, 컴퓨터 바이러스 및 서비스 거부 등 역기능들이 날로 증대되어 피해규모가 심각한 수준에 이르고 있다. 특히 컴퓨터 시스템의 침해사고가 국내·외에서 빈번히 일어나고 있는 지금 이에 대한 대응책이 어느 때 보다 절실

히 요구되고 있다.[4]

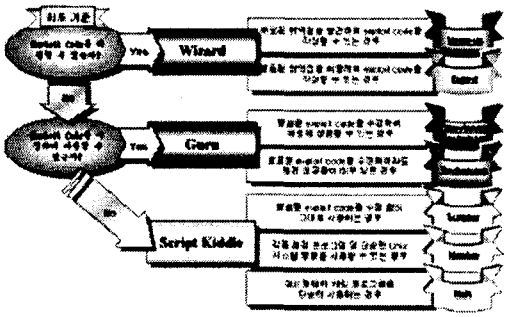
최근 네트워크나 시스템에 대한 크래킹 Cracking 이나 잘못된 조작 등에 의한 피해 사례는 대표적인 정보보호 시스템인 침입차단 시스템(방화벽)이 설치된 네트워크 도메인에서도 많이 발생하고 있다. 이는 지금까지 침입차단 시스템만으로 자신의 네트워크를 안전하게 관리 할 수 있다고 믿고 있는 일부 보안 관리자들을 당혹스럽게 만드는 일임에는 틀림없다. 따라서 보안 관리자는 자신이 관리하고자 하는 네트워크의 환경과 자료의 중요도에 따라 보안 정책을 수립하고 이에 맞는 다양한 보안제품을 철치, 운영하여야 한다. 이종의 분산 환경에서 다양한 보안 시스템에 대한 효율적인보안 관리를 위해서 관리자는 보안 시스템들이 설치된 네트워크 환경에 대한 사전에 전문적인 보안 지식을 갖고 있어야하며, 개방형 네트워크 환경의 경우 새로운 보안 시스템이 추가되면 새로운 보안 정책과 기술을 적용해다 한다. 이는 전산망 운영 기관의 보안 관리 비용을 가중시키ㅇ며 체계적이고 일괄적인 보안 정책 및 기술 구현을 불가능하게 하여 오리려 보안 문제를 야기 시키는 역기능을 초래 할 수 있다. 그리고 보안 제품의 개발과 공급이 다수의 공급자에 의해서 공급되므로 서로 상이한 특성을 갖는 보안 시스템들로 구성된 보안 고리 구조의 효율적인 운용과 유지에 상당한 어려움이 있다. 이에 복잡하고 다양한 방식의 보안관리 및 통신망 관리체계의 집중화, 자동화된 관리체제의 집중화, 자동화된 곤리 체계로의 전환, 그리고 이종간의 보안 시스템들에 대한 통합적인 관리를 위한 정책 관리가 요구되고 있다[5][6].

본 논문 에서는 우리 주변에서 발생 하고 있는 해킹 사고 사례와 나날이 발전해가는 해킹 방법의 동향, 이러한 불법 침입을 이용한 침입 탐지 기법들과 네트워크에 관련한 침입탐지 방안기술 그리고 정책기반의 네트워크 관리(PBNM : Policy-based Network Manage- ment)모델에 대한 연구에 대해서 살펴보고 향후 방향과 계획에 대해 언급하고자 한다.

2. 해킹 시나리오 분류

내부망의 보안 수준을 평가하기 위해서 해커 및 해킹 수준 분류를 바탕으로 하여, 테스트를 위한 해킹 시나리오를 분류하였다. 이는 제안한 평가 방법에서 테스트를 위한 공격수준이 지침이 된다.

다음의 <그림 1>에서는 해커/해킹 기법의 분류



<그림 13>해커/해킹 기법 분류 및 레벨 정의

및 레벨을 정의 하였다.

다음의 <표 1>에서는 해킹 시나리오는 크게 3개의 부분으로 분류 하고, 각각의 분류된 해킹 시나리오는 단계별로 해커/해킹 수준에 따라 공격방법을 기술 하였다.

분류	공격단계	공격수준		
scenario Ⅰ	1. 정보수집 (시스템 취약성) 2. 불법적인 권한 획득 3. Sniffer 설치 4. Backdoor 설치 5. 구체적인 피해 행위 6. 침입흔적 제거	Low Script Kiddie 수준의 공격 기술 사용	Medium Guru 수준의 공격 기술 사용	High Wizard 수준의 공격 기술 사용
scenario Ⅱ	1. 정보수집(네트워크 취약성) 2. DoS 또는 DDoS			
scenario Ⅲ	1. 바이러스 또는 웜 공격			

<표 1> 해킹시나리오 분류

2.1 해킹 시나리오 I

일반적인 해킹 공격 기법으로 주로 시스템 취약성에 대한 정보수집, 부럽ㅂ적인 권한 획득, 스니퍼 설치, 백도어 설치, 구체적인 피해행위, 침입흔

적 삭제 등의 순서를 취하고 있다.

2.2 해킹 시나리오 II

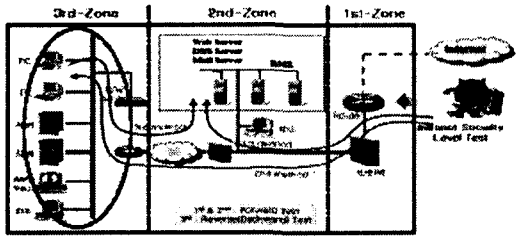
최근에 유행했던 서비스 거부공격(DoS)과 분산 서비스거부공격(DDoS)의 형태의 공격 방법으로, 다른 시스템을 해킹하기위한 선행 작업 및 네트워크 취약점을 부석하고 정보를 수집한다.

2.3 해킹 시나리오 III

바이러스와 인터넷 웜의 형태의 공격방법으로 이 방법은 인터넷 확산 속도 때문에 매우 심각하며, 신종 바이러스 및 인터넷 웜 또한 최근에 큰 문제가 되고 있다.

3. 네트워크 테스트 모델

내부망의 보안 수준을 평가하기 위한 네트워크의 구축 상태 및 테스트 모델을 제시한다. 이것은 평가 방법에 대한 전반적인이해를 돕고 실제로 네트워크를 구축하기 위한 것이다. 아래의 <그림 2>에서 네트워크는 외부 망과 1지대, 2지대, 3지대의 내부 망으로 구성할 수 있으며, 내부 망의 방어 수준 테스트는 해킹 공격 방법에 의해서 수행하게 된다. 1지대는 라우터와 방어벽이 있으며, 2지대는 DMZ(웹, 메일, DNS서버 등)가 있으며, 3지대는 일반 서버들이 존재한다각 지대별 보안 솔루션으로 침입탐지시스템, 침입차단시스템 및 백



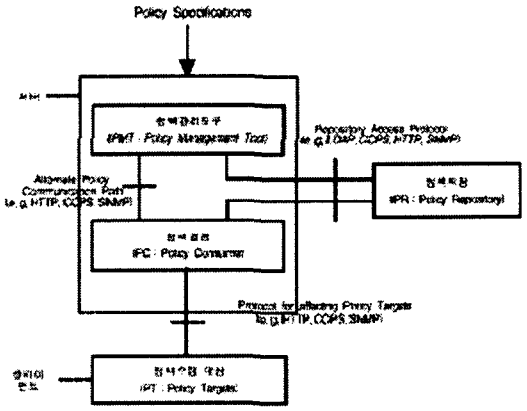
<그림 14> 네트워크 테스트 모델

신 등을 사용하였다. 지대별 구분을 기준으로 침투경로를 설정하고, 그것을 순방향 공격(Forward Attack : FA)과 역방향 공격(Backward Attack : BA)으로 구분하였다. 보안수준이 높을수록 역방향 공격이 어렵다[11].

4. PBNM의 개요

정책 기반 통신 시스템은 IETF표준화 문서중 "Policy FrameWork"에 기능이 정립되어 있다[8][9]. 정책기반의 네트워크관리[10]는 네트워크에서 제공하는 QoS[11], 정보보안 및 자원을 공통된 형태로 제공하고, 이를 효율적으로 관리하는데 있다. 이에 정책기반의 네트워크 관리 시스템은 정책규칙(Policy Rule)을 제정하고, 정책에 따라 네트워크를 운영하기 위해서는 통신망 구성장치를 실시간으로 모니터링 하여, 동적으로 변화되는 정보를 신속하게 정책 기반 관리 시스템에게 전송해야한다.

다음<그림 3>은 정책 기반 관리시스템의 프레임워크를 나타낸 것이다.



<그림 15> 정책기반 관리시스템의 프레임워크

IETF의 정책 FrameWork 규격에서는 기능적 컴포넌트로 정책 관리도구(Policy Management Tool), 정책정보 저장(Policy Repository), 정책 결정(policy Consumer), 정책수행 대상장치(Policy Target)의 4개의기능을 블록으로 구성되어 있다.

■ 관리도구(Policy Management Tool)

정책 기반의 통신망 관리 운영 상태 감시 혹은 관리를 위한 작업과 관련하여, 규칙을 변환 및 검증, 정책규칙 자료검색, 그래픽으로 표시된 정책규칙을 특정한 정보로 변환하는 등의 기능 수행

■ 정책정보 저장(Policy Repository)

PDP(Policy Decision Point)또는 정책서버라고도 하며, 정책데이터베이스내의 정보가 변했다는 것을 인지하여 정책데이터베이스로부터 정책 정보

를 검색하고 정책을 정책 클라이언트가 받아들일 수 있는 형태나 구문으로 변환 후 정책 클라이언트로 전송한다.

■ 정책 결정(policy Consumer)

정책 저장소(는 정책 규칙을 데이터베이스로 객체지향 개면에 입각하여 중앙 혹은 지역적으로 분산 형태로 저장 및 관리를 담당한다.

■ 정책수행 대상장치(Policy Target)

정책클라이언트라고도 하며, 정책결정으로부터 전송된 정책 규칙정보를 자체 시스템에서 적합한 형태로 저장하여 이를 수행한다. 수행된 결과를 정책기반 서버에 보고하거나 혹은 동적으로 처리되는 중요한 정보를 보고하는 기능을 수행한다. 또한 동적인 네트워크 상태를 모니터링 하는 정책결정과 함께 정책 서버를 구성한다[7].

4. 결론

본 논문에서는 해킹 시나리오 기법과 네트워크 테스트 모델, 정책기반 관리시스템을 한층 더 안전한 정보 보호를 위하여 살펴보았다. 해킹시나리오Ⅰ의 시스템 취약점을 이용한 경우와 시나리오Ⅱ의 너트워크취약점을 이용하는 공격 시나리오Ⅲ의 바이러스 및 인터넷 웜을 이용한 공격 등에 대한 대부분의 방어가 되어있으나 새로운 해킹 공격 및 바이러스 공격에 대해서는 보안성을 유지하지 못하는 수준이다.

그러나, 한층 더 안전한 보안대책을 세우기 위해서는 공격방법에 대한 연구와 보안장비, 정책 그리고 관리자의 및 개개인의 수준향상이 요구된다.

참고문헌

[1] 한국정보통신진흥원, http://www.certcc.or. kr

[2] C. Pfleeger, "Security in Computing Second Edition", Prentice Hall, 1997

[3] 최영철, 홍기융, 이홍섭 "전자서명법과 전자서명 인증관리체제", 한국정보보호센터 정보과학회지 제 18권 제1호 통권128호 , 2000. 1. ISSN 1015-9908 P13

[4] 한국정보보호센터, "실시간 네트워크 침입탐지 시스템 개발에 대한 연구", Dec., 1998

[5] 이동성, 김동수, 홍승선, 정태명, "웹 기반의 방화벽 통합보안관리시스템 개발", 한국정보처리학회논문지, 7권 10호 pp3171-3181, 2000

[6] D. Y. Lee, D. S. KIM, K. H. Pang, H. S. Kim, T. M. Chung, "A Design of Scalable SNMP Agent for managing Heterogeneous Security Systems," NOMS(Network Operations and Manage- ment Symposium)2000, pp. 293- 294 April 2000.

[7] 이동영, 김동수, 정태명" 이종의 보안시스템관리를 위한 정책기반의 통합보안관리시스템의 계층적 정책모델에 관한 연구" 정보처리학회 논문지 제8-C권 5호, pp607-614 2001.10

[8] M. Stevens, "Policy Framework,"Internet Draft, draft-oeft-policy-framework- 00.txt, Sep. 1999

[9] B. Boore, et., "Policy Core Information Model- Version 1 Specification," Internet Draft, draft- policy-core-info- model-06.txt, IETF, May. 2000.

[10] Susan Hinrichs, "Policy-Based Management : Bridging the Gap," Computer Security Applications Confe- rence, 15th Annual, pp.209-218., 1999

[11] Raju Rajan, Diesh Verma, Sanjay Komat, Eyal Felstaine, Shai Herzog, "A Policy Framework for Integrated and Differentiated Services in the Internet," Journal of IEEE Network, Sep/Oct. 1999.

[11] 서동일, 최병철, 손승원, 이상호, "해킹기법을 이용한 내부망 보안 평가방법" 정보처리학회 논문지C 제9-C권 제3호, 2002. 6.