VPN의 데이터 무결성 평가를 위한 VIES 설계 및 구현

이 동 춘† · 김 점 구†† · 조 석 팔†††

요 약

인터넷을 전용망처럼 활용함으로써 비용절감과 업무효율을 증진할 수 있게 한 가상 사설망(Virtual Private Network, VPN)은 데이터의 무결성 보증이 그 핵심 기술이다. 그러므로 어떤 경우라도 VPN의 무결성 기능은 유지되어야 하며, 보안 관리자는 이를 수시로 검증하여 이상 유무를 확인 할 필요가 있다. 본 논문은 정보보호 시스템을 직접 공격하는 최근 해킹 기법에 대비하여 VPN의 보안 취약성 정보를 자동으로 수집·평가할 수 있는 VIES(VPN Integrity Evaluation System)를 개발하며, 국제공통평가기준(Common Criteria, CC)을 기반으로 평가 시나리오를 구축함으로써 평가 결과에 대한 객관적 신뢰성을 확보하고, 보안 비전문가도 쉽게 조직의 보안성 평가에 활용할 수 있는 실용성을 가질 수 있도록 하였다.

Design and Implementation of VIES for Integrity Evaluation in VPN

Dong Chun Lee† · Jeom Goo Kim†† · Sok Pal Cho†††

ABSTRACT

Guarantee of the data integrity is important to the Virtual Private Network (VPN) which can be improved cost decreasing and effective work by applying on Internet as the private network. Thus, the integrity function in the VPN must be maintained and the security manager must be check it occasionally. In this paper we propose the VPN Integrity Evaluation System (VIES) which is collecting, and evaluating automatically the vulnerable data of VPN against current hacking mechanisms in information security system. And this VIES obtain to the results which have objectivity and fairness of evaluation by driving off the evaluation scenario based on Common Criteria (CC), and general users or non-specialist can utilize easy the security evaluation of organization.

키워드 : VPN, VIES, 무결성(Integrity), 평가(Evalution)

1. 서 론

가상 사설망(Virtual Private Network, VPN)은 인터넷을 이용하여 전용선과 같은 보안성을 유지하고, 비용을 획기적으로 절감할 수 있는 기술로, 수요가 갈수록 증가하고 있다. 그러나 VPN의 활용 증가에 따른 관리와 보안성 유지, 그리고 보안성 보증을 위한 표준 평가 방법이 없으며, 이러한 현실은 VPN의 이용이 확산되면 될수록 인터넷 응용에 대한 보안 취약성은 증가하게 되는 원인이 되게 된다[15].

해킹도구가 다종 다양화되고 일반화되었으며, 정보보호시스템을 직접 공격하는 예가 많아져 최근들어 미국이나 유럽을 비롯한 선진국에서는 정보보호시스템의 보안성 인증을 위한 평가와 기존에 설치된 정보보호시스템의 보안성 유지 차원의 평가 방법에 대한 연구가 활발히 진행되고 있으며, 많은 평가 도구도 선보이고 있다. 그러나 국내는 그러한 도구가 전무한 실정으로 국내 기업체 등에서는 외국 보안 컨설팅 업체에 자사의 보안성 평가를 의뢰하거나 외국 평가 도구를 도입하여 운용하고 있다. 이와 같이 국내 기업을 외국 보안 컨설팅 회사가 보안성 평가를 할 경우 국내 기업 기밀이 외국에 유출될 우려가 있으며, 외국의 기존 평가 도구를 사용할 경우 그 사용 방법이나 평가 결과에 대한 다음과 같은 문제점이 있을 수 있다[14].

1) 보안 비전문가는 분석 결과를 해석하기가 어렵다. 그러므로 일반적인 국내환경에서는 외국 컨설팅에 계속 의존하여야 하는 상황이 발생할 수 있다.
2) 취약성 정보 수집 방식을 대부분 질문 방식에 의존하고 있어, 다양한 정보 시스템 환경에 대하여 질문 내용이 모두 동일한 비중으로 적용됨으로 인하여 정확한 시스템 환경을 분석 시스템에 적용하기가 어렵다.
3) 정보 시스템 환경이 네트워크 위주로 변화함에 따라 분석 도구도 이를 반영하여야 함에도 불구하고 외국의 많은 자동 보안성 분석 도구들은 이를 반영하지 않고 있다.

※ 본 논문은 2001년도 과학재단의 지역대학 우수과학자 지원에 의하여 연구되었음(R05-2001-000-00981-0).
† 정 회 원 : 호원대학교 컴퓨터학부 교수
†† 종신회원 : 남서울대학교 컴퓨터학과 교수
††† 정 회 원 : 성결대학교 컴퓨터 및 정보통신학부 교수
논문접수 : 2002년 3월 21일, 심사완료 : 2002년 8월 6일

4) 보안성 분석 도구 사용자 위주의 환경이 반영되지 않고, 정보시스템에 대한 보안성 평가 위주의 도구 개발로 시스템 관리자, 시스템 사용자, 단말기 사용자, 보안 관리자 등이 도구 사용을 기피하는 현상이 발생한다.

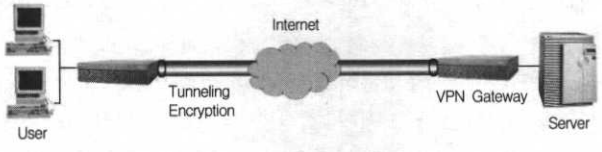
따라서 본 논문은 VPN의 보안 취약성 정보를 자동으로 수집·평가할 수 있는 방법을 제안하고, 제안된 내용을 설계·구현한 VIES(VPN Integrity Evaluation System)를 개발하였다. 제안된 VIES는 보안 비전문가도 쉽게 조직의 정보보호시스템 보안성 평가에 활용할 수 있으며, 평가 결과에 대한 객관적 신뢰를 가질 수 있도록 1999년 6월에 국제표준평가기준(ISO/IEC15408)으로 공식 인정된 국제공통평가기준(Common Criteria, CC)을 기반으로 하였다.

본 논문의 구성은 2장에서 VPN의 기술과 기존 평가 도구들에 대해서 고찰하였고, 3장에서는 VIES의 설계 및 구현을 하였고 기존 도구들과 비교 분석을 하였다. 마지막으로 4장에서는 본 논문의 결론과 향후 연구방향에 대해서 기술하였다.

2. VPN의 관련연구

2.1 VPN 구성 요소

물리적인 VPN 제품의 구성요소는 (그림 1)과 같이 VPN 게이트웨이와 VPN 클라이언트로 나눌 수 있으며, 외부 사용자와 네트워크 연계 시 보안성 증대를 위한 터널링 기술, 전송시 데이터 보호와 네트워크 침입의 원천 봉쇄를 위한 암호화 기술, 그리고 외부 사용자 인증기술 등의 논리적 구성요소로 나눌 수 있다[9].



(그림 1) VPN의 일반적인 형태

(1) 터널링 기술 : (그림 1)과 같이 인터넷망에 논리적으로 가상적인 터널을 형성해 정보를 주고받을 수 있는 기술로서, 송신측에서 수신측까지 암호화된 통신 프로토콜로 보안 세션을 구성하게 된다.

(2) 암호화 기술 : 터널링 기술뿐만 아니라 신뢰성 있는 보안 성능을 제공해주는 기술이 암호화 기술이며, 터널링이 이루어지기 위해 종단을 정의하고 상호 키를 교환하여, 터널을 형성한다.

(3) 인증 기술 : 수신자 혹은 중간 전달자 측에서 데이터의 헤더에 표기된 송신자가 실제 송신자인지 확인하여 인증된 사용자에 대해서만 접근을 허가하는 기술로서 IPSec을 사용할 경우 게이트웨이(Gateway)와 사전 협상이 필요하다.

2.2 VPN의 데이터 무결성 제공 방법

2.2.1 해쉬함수(Hash Function)

해쉬함수는 암호학적으로 전자서명의 효율성 증대와 중요 정보의 무결성 확인, 그리고 메시지 인증을 위해 가장 흔하게 사용된다. 어떤 메시지에 대한 무결성을 확인하는 방법은 우선 송신자는 메시지와 함께 그 메시지의 해쉬값을 함께 보내게 되며, 수신자는 메시지를 동일한 해쉬함수로 압축(Message Digest, MD)한 후 송신자로부터 받은 해쉬값과 비교함으로써 값이 같다면 수신자는 그 메시지가 변조되지 않은 원래의 메시지임을 인정하게 된다. 일방향 해쉬 알고리즘은 다음과 같은 세 가지 조건을 만족하여야 한다[11].

(1) 해쉬 값을 이용해 원래의 입력 값을 추정하는 것은 계산상으로 불가능하여야 한다.

(2) 입력값과 해당 해쉬 값이 있을 때, 이 해쉬 값에 해당하는 또 다른 입력 값을 구하는 것은 계산상으로 불가능하여야 한다.

(3) 같은 해쉬 값을 갖는 두 개의 다른 입력 값을 발견하는 것은 계산상으로 불가능하여야 한다.

2.2.2 메시지 인증코드

무결성을 검사하는 방법 중 비밀키에 의한 방법을 메시지 인증 코드(Message Authentication Codes, MAC)라고 한다. 일반적으로 인증 코드는 비밀키를 공유하고 있는 쌍방간의 데이터 전송의 유효성을 확인하기 위하여 사용한다. 일방향 해쉬함수를 MAC로 바꾸는 쉬운 방법은 해쉬 값을 대칭 알고리즘으로 암호화하는 것이다.

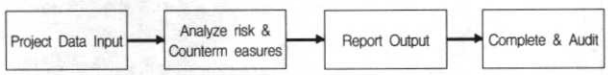
2.3 기존 보안성 평가 도구

미국의 대표적 보안성 프로그램들로는 BDSS, Buddy, Control-It 등이 있고, 영국의 프로그램들로는 AnalyZ 등이 대표적 시스템이다.

2.3.1 AnalyZ

가. 시스템 구조

(그림 2)의 Project Data Input은 위험관련질문을 통한 시스템 관련 정보를 입수하는 단계이다. Analyze Risks & Countermeasures는 입수된 정보를 토대로 위험분석기법을 이용한 위험수준측정 및 위험대책을 제시한다. Report Output은 결과를 정리 및 출력해 주며, Complete & Audit은 Project Data Input 단계와 Analysis Risks & Countermeasures 단계를 통해 얻어진 자료를 검증하고 선택되어진 위험대책을 저장한다[7].



(그림 2) AnalyZ 보안성 분석 체계

나. 특 징

AnalyZ는 비교적 사용이 용이하고 위험분석 과정이 간단하다. AnalyZ의 자체 보안구조 또한 만족할 만 하다. 그러나 위험 질문의 유형이 지나치게 외국 전산환경 및 상업조직 등에 편중되어 있어 국내 실정에 정확히 맞지 않는 점이 단점이라 할 수 있겠다.

2.3.2 BDSS(Bayesian Decision Support System)

가. 시스템 구조

BDSS는 정성적 외형 요소의 전반적인 구조와 정량적 취약성 및 위협의 행렬, 그리고 1900여개의 제한된 대응책 등을 60여개가 넘는 위협요소에 대하여 비용 효과를 포함하여 분석한다. BDSS는 운영상에서 발생될 수 있는 작은 위험요소들과 치명적인 주요 위험요소들의 관리체계를 지원함으로써, 정보시스템 환경운영의 비용 효과를 향상시킨다. BDSS는 위험을 받아들이거나, 피하거나, 이동시키는데 대한 결정을 만들기 위하여, 위험 관리능력을 직접적으로 지원한다[8].

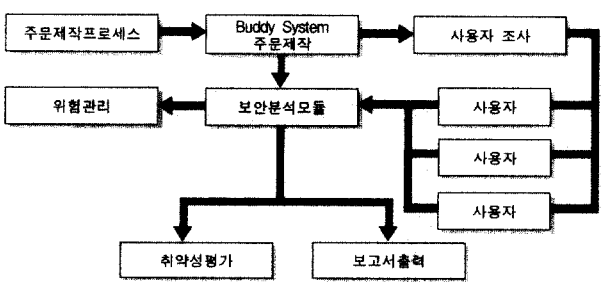
나. 특 징

BDSS는 여러 위협, 자산, 대응책, 시나리오 등을 그래프에 근거한 종합적인 보고서를 산출한다. 이는 관리자로 하여금 분석결과의 이해를 돕고, 위험관리결정에 정확성과 확신성을 향상시킨다. BDSS는 정량 및 정성 분석 기술의 전문가에 의해 디자인되어졌으며, 기존 방식의 복잡하고 모순적이며 비효율적인 분석과정을 개선하였다.

2.3.3 BS(Buddy System)

가. 시스템 구조

BS의 전체 구조는 (그림 3)과 같이 3개 주요 부문으로 구성되어 있다. 보안 분석 모듈, 운용 모듈, 그리고 사용자 질문 모듈 등이다. 보안 분석 모듈은 취약성 분석, 위협과 대응책 확인, 그리고 기대 손실 값의 결과를 산출하는 분석 알고리즘을 이용한다. 운용 모듈은 보안 대응책의 실시, 감독 등 보안 관리 운영의 대부분을 조정한다. 모듈이 지니고 있는 과거 분석 로그는 향후 분석 자료로 쓰이며, 분석 결과에 대한 위험 관리자의 결정은 감리 평가를 위하여 기록되고 운영된다[13].



(그림 3) BS 구조

또한 운영 모듈은 BS을 분석 대상 시스템의 환경에 맞추기 위하여 각각의 위협 요소와 대응책에 대한 무게 값을 변환시킬 수 있는 특성화 과정을 지원한다.

나. 특 징

사용자 질문 모듈은 시스템 사용자의 이해를 돕고 쉽고 정확한 답변을 유도하고 있다. 또한 소형과 중·대형 등의 시스템 기종에 따라 시스템 사용자나 운영자로부터 시스템의 상태를 파악할 수 있게 하여준다. 분석을 진행하면서 보안 관리자에 의해 제안된 보안 규정의 정확한 준수를 위하여 질문 모듈을 통한 분석 조사는 전산망을 통하여 정기적으로 이루어진 후 보안 분석가에게 보내질 수 있다. 질문 모듈을 통하여 조사되고 수집된 시스템의 정보는 분석 모듈로 이식된다.

결과 및 보고 과정을 통하여 7개의 주요 보안 분석 보고서가 산출된다. 보안 분석 보고서, 사용자의 시스템 정보 종합, 취약성 종합, 감리·준수 측정, 다중 시스템 취약성 분석, 보안 관리 보고서, 그리고 현존 대응책 보고서 등이다. 결론에 따라 보안 관리자는 대상 시스템의 각 책임자로 하여금 적정한 조치를 요구하게 된다.

3. VIES 시스템

VIES는 앞서 언급한 기존 보안성 평가 도구의 문제점들을 보완하고, CC의 평가기준을 바탕으로 전송데이터가 VPN을 통해 전송되는 과정에서 데이터의 변조와 재전송이 있었을 때 VPN이 그것을 제대로 감지하고 있는지를 평가하는 시스템이다. VIES는 데이터 무결성에 대한 평가를 자동화함으로써 VPN 제품들이 제대로 감지하는지 여부를 실시간으로 평가 할 수 있으며, 수시 또는 정기적으로 VPN에 대한 데이터 무결성을 검증하여 조직의 신뢰성 향상과 안전한 보안 서비스를 제공을 보증할 수 있게 한다.

3.1 시스템 설계

3.1.1 요구 분석

VPN 평가 과정 중 데이터 무결성에 대한 평가는 VPN의 역할을 제대로 수행하는지의 여부와 관리자의 오용, 환경 설정, 실수 등으로 인하여 안전한 데이터 전송이 되는지 여부를 평가한다. VIES는 VPN의 데이터 무결성 평가가 주목적이므로 데이터 근원지에서 목적지로 전송되는 패킷을 중간 가로채기와 변조, 재전송을 할 수 있는 기능을 가져야 한다. 그 밖의 기본적인 요구사항은 다음과 같다.

(1) 기존 보안성 평가 도구의 문제점들을 보완하고, CC의 평가기준을 바탕으로 한 표준화된 한국형 자동화 데이터 무결성 평가가 이루어질 수 있어야 한다.

(2) 평가 결과는 날짜별로 저장되어야 하며, 데이터 변조 시

간, 재전송 시간이 출력되어야 한다.

(3) 수시, 정기적, 그리고 반복 평가의 편의성 제공과 도구 사용자 인증이 필요하다.

(4) 평가 대상에 대한 무결성 기능의 정확한 동작 여부를 평가할 수 있어야 하며, 지속적으로 발전하고 있는 VPN 제품과 더불어 새로운 기능 추가를 할 수 있는 확장성이 고려되어야 한다.

(5) 수행 후 결과 분석을 쉽게 할 수 있도록 리포트 기능, 출력 기능 등의 부가적인 기능을 활용할 수 있어야 한다.

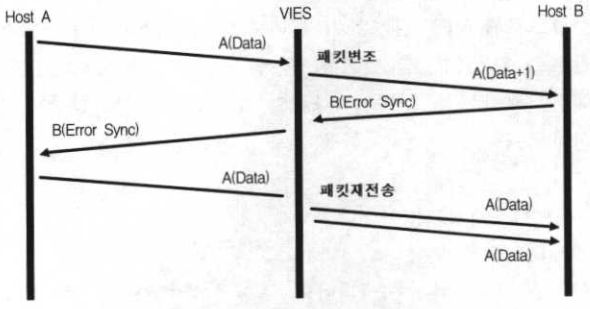
(6) 사용자의 인터페이스를 시각화하여 활용의 편리함을 제공한다.

3.1.2 VPN의 데이터 무결성 평가

가. IPSec의 터널링 무결성 평가

IPSec은 네트워크 통신의 패킷처리 계층 보안을 위해 지금도 발전되고 있는 표준으로서 VPN구현에 가장 널리 사용되고 있는 보안 프로토콜이다. IPSec은 터널링뿐만 아니라 이에 필요한 각종 암호기술이나 무결성, 인증 등을 위한 총체적 보안을 제공하는 현존하는 가장 강력한 VPN구현 기술이다[9].

VIES에서는 이러한 IPSec이 적용된 환경 하에서의 데이터 통신의 무결성을 검증하기 위해서 게이트웨이의 커널을 패치하여 패킷 변조 기능을 (그림 4)과 같이 커널에 포함시킨다. 그리고 IPsec이 적용된 환경에서 게이트웨이를 통하여 통신을 하도록 하고, 게이트웨이에서 Attack을 했을 경우와 하지 않았을 경우 수신측에서 데이터의 무결성을 검사하는 것을 보인다.



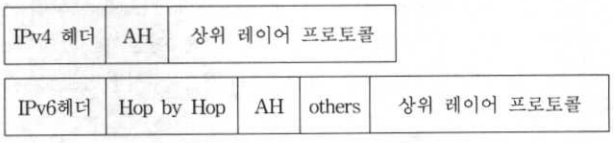
(그림 4) 패킷 변조와 패킷 재전송

나. 패킷 재전송 평가

인증헤더는 IP 데이터그램을 인증하기 위해 필요한 정보를 포함하며, 헤더 정보는 송신자가 인증된 데이터그램을 송신하기 직전에 구성하고 수신한 다음에 해제된다. 인증헤더를 사용함으로써 메시지 인증을 담당하는 코드에 의해 계산되어진 각 필드의 합산 값으로 수신자가 확인하여 데이터 무결성을 보장받으며, 데이터 인증 시에는 인증 시 필요한 키와 인증 알고리즘을 SA(Security Association)와 연계, 지정된 알고리즘을 수행하여 보장받는다. 또한 인증헤더에 있는 일련번호의 값으로서 재전송 방지를 할 수 있다[10].

AH(Authentication Header)는 받은 데이터의 근원지를 인증하기 위해서 MD5나 SHA-1과 같은 해쉬 알고리즘을 사용하여 데이터의 무결성을 보장하며, 또한 일련번호를 부여하면서 재전송공격을 방지할 수 있다. IPv4일 경우에 (그림 5)와 같이 AH는 IP 패킷의 IP헤더 뒤에 추가함으로서 인증을 보장하고, 터널링이 되었을 때 내부 IP헤더를 보호하게 된다.

그러므로 VIES에서의 패킷 재전송에 대한 평가는 패킷 제어모듈에서 전송되어지는 패킷과 동일한 일련번호의 패킷을 재전송모듈에서 재전송 공격케함으로써 재전송 되었을 때의 VPN이 이를 발견하는 지 여부로 패킷 재전송 평가를 하게 된다.

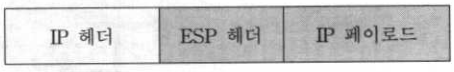


(그림 5) IPv4와 IPv6에서의 AH 구조

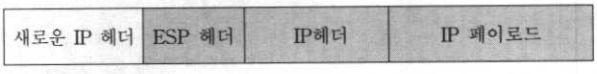
다. 데이터 기밀성 평가

ESP(Encapsulation Security Payload)는 암호화 기법을 사용하여 AH에서 제공하지 못한 기밀성을 제공한다. 또한 무결성과 재전송 방지의 기능을 제공하는 프로토콜로서 사용하는 암호 알고리즘에 따라 인증 기능까지 제공할 수 있다. 인증헤더와 마찬가지로 ESP 키 관리는 철저한 보안이 되어야 하며, 키 관리 메커니즘과 보안프로토콜 메커니즘이 독립적으로 구현된다[11].

트랜스포트 모드에서 ESP의 기능은 (그림 6)에서 처럼 원래의 IP 헤더는 보호하지 않고 IP 페이로드만을 보호하지만 터널 모드에서는 기존의 IP 헤더와 페이로드는 보호하고, 새로운 IP헤더는 보호하지 않는다. 또한 트랜스포트 모드는 데이터그램과 IP 헤더는 계속 유지되고, 원래 IP 데이터그램의 페이로드와 ESP 트레일러(Trailer)가 암호화되기 때문에 IP 헤더가 전송되는 동안 공격자에 노출될 수 있다. 반면 (그림 7)의 터널 모드에서는 새로운 IP헤더가 만들어져서, 원래 IP 데이터그램과 ESP 트레일러는 암호화된다. 따라서 전송되는 동안 공격자가 헤더의 내용을 볼 수 없게 된다.



(그림 6) 트랜스포트 모드 ESP 구조



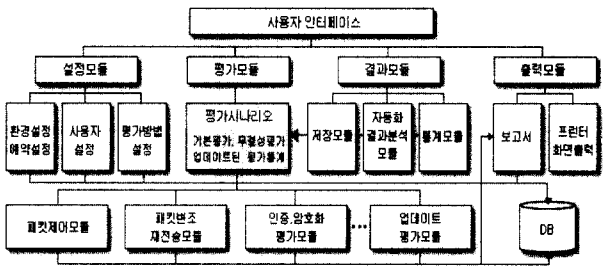
(그림 7) 터널 모드 ESP 구조

VIES는 VPN 호스트간에 전송되는 패킷에 AH헤더와 ESP 헤더가 IP헤더에 추가되었는지 전송 패킷의 프로토콜번호를 확인하고, 패킷제어모듈에서 수신측으로 보내지는 IP패킷의 헤더를 제외한 임의의 위치를 변조하여 수신측으로 보내에 VPN이 이를 찾아내는지를 확인함으로써 VPN의 기밀성 보증 여부를 평가한다.

VIES 평가 모드에서 공통적으로 패킷 변조에 대한 정보를 보안 관리자가 평가 시 입력을 통해 동적으로 설정하고 변경된 패킷에 대한 정보를 보여주기 위해 커널과 사용자 간에 정보를 주고받는 방법을 커널 모듈을 통하여 구현하고, 변조하는 패킷의 변조위치와 패킷 번호, 변조 위치 등을 사용자 입력을 통해 동적으로 설정하여 무결성 보장 여부를 실시간 측정하도록 하였다.

3.1.3 시스템 구조

(그림 8)은 시스템의 기본구조를 나타낸다. 사용자 인터페이스, 설정모듈, 평가모듈, 결과모듈, 그리고 출력모듈로 크게 분리되며, 모든 모듈에서 저장되어지는 데이터베이스는 시스템을 유기적으로 동작할 수 있게 한다.



(그림 8) VIES시스템 기본 구조

VIES의 기본 구조는 시스템의 기본 동작을 위한 인터페이스를 중심으로 평가 설정 기능을 제공하며, 평가 결과를 나타낼 수 있는 결과 표시 창과 기본 데이터 입력, 그리고 사용자 인증을 제공한다.

(1) 설정모듈 : 이 모듈은 관리자가 환경설정에서 정기적인 검사나 혹은 시간을 예약했을 경우 평가에 대한 환경설정과 예약설정을 포함하며, 관리자가 아닌 일반 사용자가 사용할 수 없도록 사용자를 설정하는 모듈이 있다. 또한 평가방법설정모듈은 저장되어진 항목정보에 따라 평가를 실시하며, 이 모듈에 대한 설정은 모두 데이터베이스에 저장되어 관리된다.

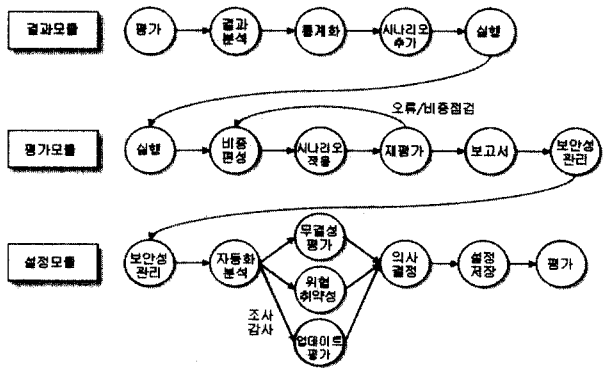
(2) 평가모듈 : 이 모듈은 VIES의 핵심적인 모듈로서 평가 시나리오에 근거한 기본평가, 무결성 평가, 업데이트되어진 평가모듈을 수행한다. 세부적으로 패킷제어모듈은 근원지에서 목적지로 이동하는 패킷 중에 VPN을 설정한 패킷을 제어하여 데이터베이스에 저장된 설정에 따라 패킷변조·재전송 모듈이 유기적으로 작동된다. 패킷변조·재전송 모듈은 패킷 변조를 선택하였을 때와 패킷 재전송 선택을 했을 때 실행되는 모듈이다. 패킷 제어모듈에서 전달되어진 패킷을 우선 저장하고 패킷을 변조 혹은 재전송 후 DB(Data Base)에 변조된 정보를 또 다시 저장하게 된다. 설정모듈에서 선택되어진 시간과 간격을 출력모듈을 통하여 결과 창에 보여주게 된다.

(3) 결과모듈 : 이 모듈은 평가에 대한 저장과 결과 분석, 결과 통계 모듈로 나뉘어지며 결과분석이 자동적으로 이루어져 평가시나리오에 전달된다. 통계모듈은 날짜와 시간에 대한 결과를 통계화시켜 보고서 출력에 그래프로 보여진다.

(4) 출력모듈 : 이 모듈은 평가모듈에 대한 결과모듈이 보고서 폼 양식으로 출력되며 프린터출력과 화면출력을 담당하는 모듈이다. 저장되어진 평가결과에 대하여 날짜별, 시간별로 그래프로 구현하는 기능이 있다.

3.1.4 시스템 기능 흐름

(그림 9)는 각 모듈별 유기적인 기능 흐름을 보여주고 있다. 결과모듈은 평가에 대한 결과를 자동으로 분석, 통계화하여 시나리오를 추가할 수 있도록 하였고, 평가모듈에서는 그 시나리오가 적용되어 실행되어질 수 있는 기능이 있다. 설정모듈 또한 평가모듈과 관련되며 자동화된 분석, 무결성과 관련된 최신의 기능을 조사, 그리고 평가 시스템의 감사를 통하여 모듈을 업데이트 할 수 있다. 그리고 그 설정 값은 데이터베이스에 저장되어 다음 평가에 적용하게 된다.



(그림 9) 시스템 기능 흐름도

3.2 시스템 구현

3.2.1 시스템 구현 환경

VIES를 이용하기 위한 평가 환경 구성은 게이트웨이 역할을 하는 시스템에서 송신지와 수신지의 주소가 VPN을 적용한 호스트인지를 판단하여 IP 패킷을 변조, 혹은 재전송하여 무결성 평가를 수행하게 된다. 게이트웨이를 구성하기 위해서는 전송 데이터를 실시간으로 분석하여 패킷 변조와 재전송을 할 수 있도록 모듈이 탑재되었으며, 그 모듈은 gcc로 설계되었다.

VIES는 <표 1>과 같이 리눅스 환경에서 gcc로 게이트웨이 역할의 모듈을 구성하였으며, 인터페이스는 J-Builder 5.0으로 윈도우 환경에서 비전문가도 실행할 수 있도록 하였다.

〈표 1〉 VPN 데이터 무결성 평가 소프트웨어 사양

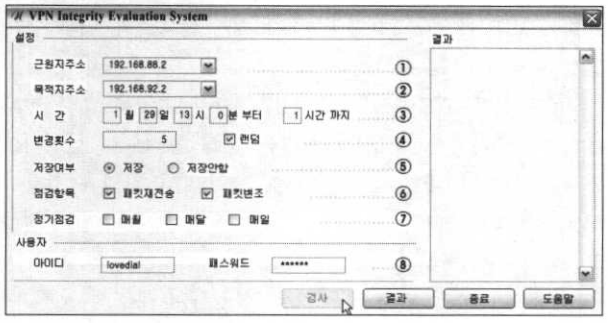
구 분	게이트웨이	클라이언트
운영체제	Linux Red Hat 7.0	Windows 9X, 2000, XP
CPU	Pentium 이상	Pentium 2 이상
Memory	32M 이상	32M 이상

3.2.2 시스템 실행 환경

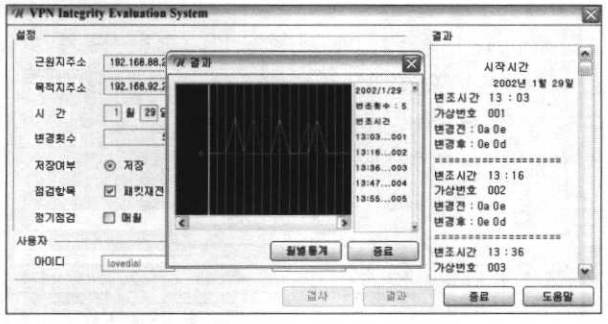
실행환경 인터페이스의 구성은 (그림 10)과 같이 테스트할 근원지 주소, 목적지 주소, 프로그램이 동작할 시간과 변경횟수 등을 입력받는다.

(1) 근원지 주소 : 변조하고자하는 VPN 패킷의 근원지 주소
(2) 목적지 주소 : 변조하여 보낼 주소
(3) 시간 : 평가 예약을 할 수 있으며 시간 간격 동안 변경횟수 받아들여 변조한다.
(4) 변경횟수 : 정해진 시간에 대한 변조 혹은 재전송 횟수를 정하게 된다. 숫자가 높을 수록 평가결과의 신뢰도가 높아진다. 랜덤을 선택할 경우는 주어진 시간에 난수를 발생시켜 평가를 하게 되고 선택되지 않았을 경우에는 일정한 시간을 간격으로 평가된다.
(5) 저장여부 : 결과를 저장할 경우 선택을 한다.
(6) 점검항목 : 전송되어지는 패킷에 대한 패킷변조와 패킷재전송을 선택할 수 있다.
(7) 정기점검 : 예약하는 경우 맞춰놓은 날짜와 시간에 검사를 할 수 있다.
(8) 사용자 로그인 : 관리자만 사용할 수 있도록 지정되어진 ID와 패스워드를 입력한다.

(그림 11)은 평가 결과를 그래프로 나타내고 있다. 시간별로 패킷변조와 패킷재전송에 대한 그래프가 존재하며 오른쪽에는 날짜와 시간, 횟수가 나타난다. 월별 통계를 선택하게 되면 월별 실행된 날짜와 횟수가 그래프로 나타나게 된다.



(그림 10) VIES의 실행 화면



(그림 11) VIES의 결과 화면

3.3 시스템 운용 결과 분석

3.3.1 시스템 비교 분석

<표 2>는 기존 보안성 평가 도구와 VIES를 비교 분석한 것이다. AnalyZ는 사용자체는 비교적 용이하고 분석도 간단하지만 보안성에 대한 질문의 유형이 국내 실정에 적합하지 않다. 또한 보안성 분석을 위한 자료 수집도 사용자에게 의존하고 있어 한계성을 보인다.

〈표 2〉 보안성 평가 도구 비교

구 분	VIES	BUDDY System	BDSS	AnalyZ
사 용 법	비전문가 용이	비교적 용이	전문가 용이	비교적 용이
시스템가격	저가	중가	고가	상당 고가
방 법 론	정성	정성	정량/정성	정량/가능
유 지 비	저렴하다	비교적 고가	상당 고가	상당 고가
특 성	• 공공기관에서 개발(비영리) • 국내최초(한글화, 위험분석 기본기능) • NCA 개발 표준과 연계가능	• 민간기업에서 개발 • 미 연방정부 정보보안관리 규정 만족	• 위험의 기술적 측정을 그래픽화 • 주요 위험요소들의 관리가 지원되어 운영비 효과 향상	• 자료입력의 순위 체계로 최대한 정확한 자료 제공 • 질문을 통해 결과를 도출하기 위해 위험질문의 분석 필요
신 뢰 도	• 시험적용 필요	• 미 연방정부를 포함한 20여개 이상의 공공기관에서 사용	• 축적된 DB와 Bayesian 모델과 결합하여 신뢰성 향상	• 질문의 유형을 세부항목으로 나뉘어 정확한 답변 유도.
보 안 관 리	적용가능	적용	적용	적용
단 점	• 정보수집을 위한 DB의 부족	• 분석가에 의한 자료 점검이 필요	• 이산적인 수량가치와 관리가 어렵고 높은 비용과 노동비용이 들어간다.	• 자료수집에 있어 사용자의 주관적 입장이 개입

버디 시스템은 비교적 저렴한 가격에 이용하기 쉬운 장점이 있어서 공공기관 등에 많이 사용되어지지만 분석 오류를 줄이기 위해 분석가가 필요하다. BDSS는 정량분석과 정성분석을 지원하며, 취약성도 자동으로 분석하여 대응책도 제시해주지만 유지비가 높아서 작은 조직에서는 경제적인 부담이 클 수밖에 없다.

반면에 제안된 VIES는 국내 최초 한글화 보안성 분석을 기본으로 제공되어지며 비전문가도 사용하기 편리하게 구성되어 있다. 현재는 정성적 방법론을 기본으로 하지만 향후 정량적 분석법도 적용할 방침이며, 정보 수집을 위한 데이터베이스가 부족한 것이 단점이다.

3.3.2 시스템 운용 효과 분석

VPN을 사용하는 기업이나 기관들이 정보가 누출되는지의 여부를 확인하고 신뢰할 수 있다는 것은 사용자와 개발자의 경쟁력 향상을 제공한다. 또한 제안된 평가 모델은 테스트 과정을 자동화하며 평가 결과를 통계화 할 수 있기 때문에 효율적인 관리를 할 수 있다.

〈표 3〉 도입 효과 분석

구 분	직접적인 효과	간접적인 효과
항 목	• 보안관리 효율 증대 • 보안성 평가 비용 절감 • 비전문가 활용가능	• 생산성 향상 • 신뢰성 증대 • 정보 보호의 제고 • 경쟁력 향상
특 성	• 경비 절감 효과 • 소극적인 효과	• 업무 효율의 제고 • 적극적인 효과

4. 결 론

VPN은 인터넷을 이용하여 전용망과 같은 보안성을 유지하고, 비용을 획기적으로 절감할 수 있는 기술이다. 그럼으로 VPN의 데이터 무결성 확보는 매우 중요하다. 그러나 VPN을 비롯한 정보보호시스템이 예상치 못한 보안 문제가 발생하거나, 인터넷과 같은 공중망 보안취약점을 위협함으로써 작게는 개인에서부터 크게는 국가·사회 간접자원에 이르기까지 심각한 문제가 야기될 우려가 있다. 국내·외적으로 정보보호시스템의 성능과 신뢰성이 사용자로 하여금 충분히 검증될 수 있도록 객관적 평가 결과를 제공해 줄 수 있는 도구가 절실히 요구되며, 특히 보안 전문가가 턱없이 부족한 국내의 경우 보안성 평가 자동화 도구는 더욱 절실하게 요구되어지고 있다.

따라서 본 논문은 정보 통신망 정보보호 대책의 일환으로 국제공통평가기준을 기반으로 VPN의 데이터 무결성 평가와 취약성 정보수집을 자동화할 수 있는 VIES를 개발하였다. 그리고 이를 이용함으로써 망 차원의 데이터 무결성 보증이 용이하도록 하고, 나아가 기업이나 공공기관의 VPN 도입 확산과 국내 정보보호 산업의 활성화에 기여할 수 있을 것이다. 또한 VIES는 비전문가도 쉽게 조작할 수 있도록 인터페이스와 도움말 기능을 한글화하였고, 평가 결과 역시 최대한 그래픽 기능을 이용하여 시각화하였다. 이 논문에서는 VPN의 정보보호서비스 중 데이터 무결성만을 제한적으로 평가하고 있다.

향후 연구 방향은 정보보호 서비스 전반을 보증할 수 있는 통합평가 도구의 개발에 대한 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] Syngress Media, "Mission Critical Internet Security," PGW (C), 2000.

[2] W. Richard Stevens, "UNIX Networking Programming," 2nd Ed., Vol.1, 1998.

[3] Robert L. Ziegler, "Linux Firewalls," New Riders, 1999.

[4] Sean Walton, "Linux Socket Programming," SMS, 2001.

[5] Jackson K. M., Hruska J. and Parker, D. B., Computer Security Reference Book, CRC Press, 1992.

[6] John Chirillo "Hack Attacks Revealed," WILEY, 2001.

[7] AnalyZ Demonstration Copy User Guide, Zergo Limited, June, 1993.

[8] Welcome to the World of BDSS, and OPA Inc. The Integrated Risk Management Group, OPA Inc., Jan., 1995.

[9] ZUM Strarten hier kicken, "IP VPN Solution for Service Provider," Cisco Systems, 1999.

[10] Kent, S., and R. Atkinson, "IP Authen. Header," RFC 2402, Nov., 1998.

[11] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload(ESP)," RFC 2406, Nov., 1998.

[12] Frederick G. Tompkins, How to Select Risk Analysis Software Package, Datapro, McGraw-Hill, Dec., 1995.

[13] Zenkins, Buddy, Security Analysis and Management Manual, Countermeasures Inc., 1994.

[14] 한국전산원, "정보시스템 보안을 위한 위험분석 소프트웨어(V.1.0) 개발 연구", 1996.

[15] 한국정보보호진흥원, "국제공통평가기준(V.2.0)", 1998.

[16] 한국정보보호진흥원, "네트워크 취약성 분석 및 평가 S/W 개발", 1999.

[17] 펜타 시큐리티 시스템(주), "자동화된 위험분석 툴의 구현", 2000.

이 동 춘

e-mail : edch@sunny.howon.ac.kr

연세대학교 컴퓨터과학과 공학박사

1989~현재 호원대학교 컴퓨터학부 정교수

JPDC, JHSN, ETT, JoIN, Perform. Eval.(SCI급) 국제논문지 심사위원

관심분야 : 무선통신(IMT-2000, Wireless IP, Wireless ATM)의 위치관리 기법과 성능분석, 무선통신보호

김 점 구

e-mail : jgoo@nsu.ac.kr

1990년 광운대학교 전자계산학과 이학사

1994년 광운대학교 대학원 전자계산학과 이학석사

2000년 한남대학교 대학원 컴퓨터공학과 공학박사

1990년~1994년 (주)제성프로젝트 연구원

1995년~1998년 (주)시사 컴퓨토피아 인터넷사업부장

1999년~ 현재 남서울대학교 컴퓨터학과 조교수

관심분야 : 정보보호, 컴퓨터네트워크, 무선통신

조 석 팔

e-mail : spcho@sungkyul.edu

1976년 광운대학교 전자통신과 공학사

1987년 한양대학교 전자통신과 공학석사

1992년 경희대학교 전자공학과 공학박사

1976년 Control Data Corp. Computer SE.

1984년 삼성전자 정보통신 연구소 연구실장 (수석 연구원)

1995년~현재 성결대학교 컴퓨터 및 정보통신공학부, 정보통신전공 교수

관심분야 : 컴퓨터네트워크, 무선통신, 통신보호