기술적 위험분석 결과를 활용한 IDS 평가방법에 관한 연구

심미나*, 조상현*, 임종인*
*고려대학교 정보보호대학원
e-mail : mnshim@korea.ac.kr, shcho@dslab.kaist.ac.kr, jilim@korea.ac.kr

A Study on the results of Technical Risk Analysis based IDS Assessment Methodology

Mina Shim*, Sang-hyun Cho*, Jong-in Lim*
*Graduated School of Information Security, Korea University

요 약

현재 침입탐지시스템(IDS:Intrusion Detection System)은 다양한 평가요소들 – 탐지율, 오탐율, 새로운 공격탐지능력, 안정성 등을 기준으로 평가되고 있고, 이러한 결과는 제품의 보호수준을 결정하거나 한 조직의 정보보호장치로 적합한지를 평가하는 벤치마킹테스트의 방법으로 활용된다. 그러나, 이러한 평가의 결과는 조직의 침입탐지시스템을 구축하고자 하는 네트워크 환경하에서 각각의 침입탐지시스템이 갖는 특성에 따라 상대적인 평가는 가능하나 해당 조직의 네트워크 인프라와 위협요소, 취약점을 고려했을 때 보다 최적의 것이 무엇인지를 평가하는 방법으로는 한계가 있다. 그러므로, 본 연구논문에서는 이러한 한계를 극복하기 위한 방법으로서 조직의 정보보호 위험분석에서 도출된 해당 네트워크 환경의 자산, 위협, 취약성의 결과인 위험과 위험수준을 IDS 평가에 반영하여 조직의 환경하에 보다 적합한 침입탐지시스템 선정이 가능한 평가방법을 제안한다.

1. 서론

오늘날 네트워크 기술의 발달과 인터넷의 급격한 성장으로 네트워크 환경을 구축한 모든 조직들은 상대적으로 증가하는 취약점과 조직 내외부의 침해 위협으로부터 조직의 정보자산을 보호해야 한다는 엄청난 노력의 부담을 갖고 있다. 때문에 정보보호에 요구되는 모든 노력 즉, 비용은 체계적인 정보보호 위험의 분석을 통해 효과적인 보호장치를 적용해야 한다. 2005 년 IT 투자 동향 보고서[1]에 따르면 정보화 수준이 상대적으로 앞선 매출규모 1 천억 원 이상의 국내 주요 기업의 주요 솔루션 도입의 2 순위가 보안으로 조사되었다. 또한 국내 정보보호산업 실태조사[2]에 따르면 PKI, 암호제품에 이어 침입차단시스템의 도입이 가장 높은 증가율로 나타나고 있다. 이렇듯 위험에 대한 최우선적 대책으로 침입탐지시스템과 같은 정보보호시스템 도입을 적극 검토, 구축하고 있다.

그렇기 때문에 효과적인 투자를 위해서는 해당 조직의 위험현황을 제대로 인식하고 조직에 적합한 정보보호시스템을 도입하는 것이 매우 중요하다.

현재 침입탐지시스템 평가의 다양한 평가기준들이 제시되고 제품 성능이나 보안성 등을 평가하기 위한 방법들이 사용되고 있고, 이러한 평가방법을 활용하여 획득한 인증여부를 확인하고, 제품도입시 벤치마킹테스트를 수행하여 최선의 시스템을 도입하게 된다. 그러나, 보편적 기준 하에서 침입탐지시스템의 평가는 가능할지 모르나, 서로 다른 보안수준과 네트워크상의 특성이 존재하는 각기 다른 조직의 네트워크 환경에 어떤 제품이 가장 적합한지를 정량적으로 평가하기란 매우 어려운 일이다.

그러므로, 본 연구논문에서는 해당 조직의 네트워크환경에 존재하는 다양한 위협과 취약점을 침입탐지시스템의 평가에 반영하여 해당 조직의 위험에 가장 적합한 제품을 평가하는 방법을 제시하고자 하며, 특히 일반적으로 수행되고 있는 조직의 취약점 분석평가의 결과를 연계하는 방안을 제안하고자 한다.

2. 관련 연구

대표적인 보안솔루션의 하나인 침입탐지시스템은 그 현대적 모델을 제시했던 Denning 의 정의에서와 같이 '대상시스템에 대한 비인가된, 비정상적인 행동을 탐지하고 구별하며 이에 대응하는 기능을 가진 시스템'[3]이다. 즉, 사용자의 행위를 감시하고 침입을 탐지하기 위한 시스템이다.

2.1 침입탐지시스템 평가 기준 및 방법

정보보호제품의 평가는 특성상 보안성(security)이 필수적으로 제공되어야 하며, 외국의 경우 TCSEC, ITSEC, CC 등으로 평가 및 인증이 이루어지고 있다.[4] 보안성은 성능과 서로 트레이드오프(trade-off)의 관계를 가지기 때문에 균형을 맞추는 것이 중요한데, 침입탐지시스템의 정량적 평가를 위한 방법론 연구를 통하여 이미 다양한 평가기준들이 제시되고 있다. 즉, 침입탐지시스템이 갖는 특징들에 의해 다음과 같은 평가기준이 제시되고 있다. [5]

- Coverage: IDS 가 이상적 조건에서 탐지할 수 있는 공격 결정을 위한 척도(Signature-based IDS 의 signature 개수, Non-signature-based IDS 에서의 알려진 공격 외 탐지 가능한 공격 개수)
- 오탐율(Probability of False Alarms): 특정 time frame 동안 주어진 환경에서 IDS 에 의해 생성되는 false positive rate 를 결정하는 척도
- 공격탐지율(Probability of Detection): 특정 time frame 동안 주어진 환경에서 IDS 에 의해 올바르게 공격이 탐지되는 비율을 결정하는 척도
- 저항성(Resistance to Attacks Directed at the IDS): IDS 의 올바른 운영을 방해하는 공격자 시도에 얼마나 견딜 수 있는가를 나타내는 척도
- 안전성(Ability to Handle High Bandwidth Traffic): 거대 볼륨 트래픽에서 IDS 가 얼마나 잘 동작하는지를 나타내는 척도
- 연계성(Ability to Correlate Events): IDS 가 공격 이벤트와 얼마나 잘 연계되는지를 나타내는 척도
- 새로운 공격탐지율(Ability to Detect Never Before Seen Attacks): IDS 가 그전에 발생하지 않았던 공격을 얼마나 잘 탐지해 내는가를 나타내는 척도
- 공격식별(Ability to Identify an Attack): 일반명이나 취약점명을 갖고 각각의 공격을 분류하거나, 공격유형을 할당함으로서 탐지된 공격을 IDS 가 얼마나 잘 식별할 수 있는지를 나타내는 척도

현존하는 평가방법론 또한 점차 발전하고 있는데, 1990 년대 초반 University of California at Davis(UCD)의 오용행위 기반 성능평가 연구를 시작으로 하여 IBM Zurich, MIT Lincoln Laboratory(MIT/LL), Air Force Research Laboratory (AFRL)와 같은 연구기관에서 연구가 이루어지다 MITRE, Neohapsis/Network-Computing, The NSS Group, Network World Fusion 와 같은 기업으로 점차 확대되고 있다.

- UC Davis 방법론: 순수침입/오판 테스트, 배경잡음테스트, CPU 부하 테스트, 고용량 테스트 등 평가항목으로 Telnet 세션 기록 및 재생을 통한 정상/오용행위 생성을 통한 성능평가
- IBM Zurich Lab 방법론: 배경잡음 테스트 평가항목으로 사용자 명령을 기록하고 재생하는 방법으로 정상행위를 생성, FTP 의 오용행위 생성 등을 통한 성능평가
- MIT/LL 방법론: 배경잡음 및 탐지회피공격테스트를 평가항목으로 실제 사용자 네트워크 트래픽 기록 및 재생을 통해 다양한 운영체제 및 어플리케이션 오용행위와 시나리오기반 비정상 행위를 생성하여 성능평가
- AFRL 방법론: 실제 사용자 네트워크 트래픽을 기록 및 재생하는 방법으로 배경잡음 및 탐지회피공격테스트를 대상으로 테스트베드 제어 네트워크와 평가 데이터 이동 네트워크를 구분하여 오용행위 탐지시스템의 성능평가

이들 평가방법은 앞의 평가 기준들 중 일부를 각각의 제품특성을 고려하여 평가하는데, 조직의 제품 구매자나 보안분석가들이 조직에 적합한 제품선택에 필요한 평가결과를 얻기에는 아직 부족함이 있다.[5] 하나의 평가항목이 정확한 평가결과를 보여준다고 하더라도 서로 다른 네트워크 환경의 조직에서 동일한 효과의 평가결과를 기대하기 어렵고, 포괄적이고 정량적인 평가방법이라 할 수 없기 때문이다.

또한, 제품을 구매하는 조직은 기능 및 성능 요구사항(requirements)을 가장 잘 만족하는 제품을 선택하기 위해 벤치마킹테스트를 수행한다. 그런데 이때 필요한 표준화된 평가방법론이나 기준의 부재로, 일반적으로 표준에서 요구되는 요구사항들보다 다양한 기능 위주의 평가가 되기 쉽고[4], 특정 제품에 편향된 평가항목을 배제하기 어려울 수 있다.

2.2 침입탐지시스템 BMT 방법 사례

본 연구에서는 ISS 사의 침입탐지시스템 BMT 평가를 예로 한다. BMT 시 평가자/피평가자는 협의 하에 탐지대상 취약점 항목을 선정, 이를 대상으로 테스트를 수행한다.

(그림 1) BMT 평가항목(예시)

수행결과는 다음의 기준에 따라 0~5 로 점수화된다.

- 5 점: 매우 우수함
- 4 점: 우수함
- 3 점: 보통 – 기본기능 제공
- 2 점: 부족함 – 불충분한 기능 제공

- 1 점: 매우 부족함
- 0 점: 해당사항 없음

결과적으로 BMT 평가항목의 선택이 최종결과에 매우 중요하게 작용할 수 있으며, 평가항목 선정의 적합성에 대한 객관적 근거가 부족하다.

2.3 위험분석

존재하는 정보자산의 위험요소를 식별하고 평가하여 그 위험요소를 적절하게 통제하는 수단을 합리적, 체계적으로 구현,운영하는 전반적 행위 및 절차를 위험분석이라 한다. 위험분석은 자산, 위협, 취약점, 대응책을 요소로 이루어진다. 대상자산의 가치를 산정하고(자산분석), 발생했거나 발생 가능한 위협과 자산에 미치는 영향을 분석하고(위협분석), 자산의 속성과 중요도를 바탕으로 자산이 갖는 약점인 취약점을 파악하여(취약점분석) 결과적으로 대응책을 분석(대응책분석)하는 과정이다.[6]

취약점은 자체로 큰 위험이 되지 않으나 존재하는 위협요소에 따라 침해의 원인을 제공하기 때문에 이러한 취약점 분석은 위험분석에서 가장 중요하다.

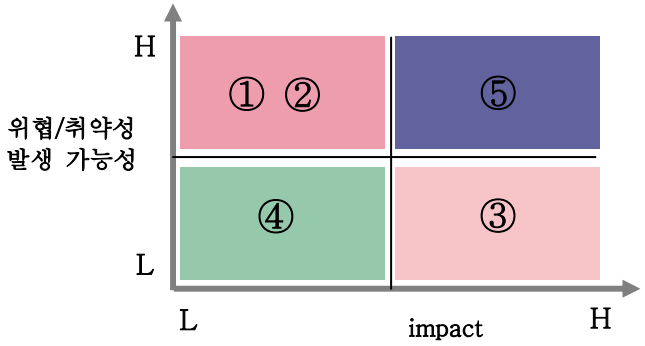
기술적 취약점 분석의 과정은 다음과 같다.

① 취약점 파악: 잘 알려진 시스템 및 네트워크 취약점 항목을 포함한 세부항목 도출

② 취약점 속성 파악: 취약점과 자산, 위협, 대응책의 관계 파악하여, 취약점의 속성을 특정짓는 속성 파악

③ 위험수준 산출: 자산의 잠재적 취약점 수준을 파악하고 대응책 수립 위한 우선순위 고려

우선순위는 파악된 결과를 종합하여 선정하게 되는데, 이는 한 조직의 위험을 관리하는데 있어 중요한 한가지는 존재하는 위험 중 무엇을 어떻게 관리하는 것이 가장 비용-효과적인지를 파악하기 위한 것이다.



① 위협/취약점 감소
② 원하지 않는 사고의 감지/대응/복구
③ 위험전이
④ 위험수용
⑤ 위험회피

즉, 상기 그래프에서와 같이 1 과 2 에 해당하는 항목을 관리대상으로 선정하면 보다 효과적인 위험관리가 가능하다.

3. 제안 평가방법 및 절차

앞 절에서 소개한 바와 같이 위험분석의 결과로 해당 조직의 효과적인 위험관리의 대상선정이 가능한데, 이를 침입탐지시스템 평가방법에도 이를 적용하고자 한다. 즉, 이미 NSTL 이나 ICSA 와 같은 제품테스트 기관의 평가결과에 추가하여, 조직의 적합성 여부를 판단할 때 보다 객관적 결과를 기대할 수 있게 한다.

3.1 제안 평가방법

첫째, 알려져 있는 CVE(Common Vulnerabilities and Exposure)와 같은 취약점리스트를 바탕으로 BMT 평가항목과 기술적 취약점분석 평가항목을 통일하여 적용, 상호 연계성을 높인다.

둘째, 취약점분석 평가의 결과로 얻어지는 위험관리의 우선순위 즉, 각 취약점 항목의 위험도를 파악한다. 위험관리의 대상이 되는 취약점 항목은 IDS 평가항목 선정시 반영하고, 해당 위험도는 IDS 평가항목의 가중치로 적용하여 계산한다. 이로써, BMT 결과는 해당 조직에 존재하는 네트워크의 위험특성을 효과적으로 반영하게 된다.

3.2 제안 평가절차

- 관리대상 평가항목 도출: 취약점 평가결과 도출된 관리대상 항목을 대상 BMT 평가항목 선정
- 평가항목에 대한 탐지시험: 선정된 평가항목을 토대로 테스트를 실시하여 탐지능력 측정
- 탐지시험 결과값 산정: 테스트결과값 계산
- 위험도 반영한 결과값 계산: 관리대상 취약점 항목의 위험도를 BMT 결과의 평가항목 각각의 가중치로 계산하여 최종 결과값 계산

4. 위험 기반 IDS 평가방법론

4.1 관리대상 평가항목 도출

알려진 취약점분석 평가항목을 대상으로 위험분석을 수행하고 관리대상항목과 위험도가 표시된다.(*표)

(위험분석 점수는 10 점측도를 사용한 경우이며, 1~3: Low, 4~7:Mid, 8~10:High 로 분류)

취약점 항목		결과	위험도
대항목	세부항목		
Telnet	세션하이제킹 존재(1)	5	M*
	Root 사용자 패스워드 노출(2)	5	M*
	전송 데이터 노출(3)	7	H*
데몬버전	SNMP Read/Write	2	L

(표 1) 취약점분석 결과표(예시)

전체 BMT 평가항목	선정대상
PHP Buffer Overflow 탐지	-
Telnet Login 시도 탐지(1)	O
XXX Buffer Overflow 탐지	-
Telnet Login ID 입력 탐지(2)	O
Answerbook Admin Access 탐지	-
Telnet Password 입력 탐지(3) …	O

(표 2) BMT 평가항목 선정표(예시)

4.2 평가항목에 대한 탐지시험

표 2 에 선정된 평가항목(O 표시)으로 BMT 실시

4.3 탐지시험 결과값 산정

테스트결과값을 계산한다. 이때 탐지성공(O)는 1, 실패(X)는 -1 로 산정한다. (결과값 산정의 기준은 점수화 기준에 따라 차이가 있을 수 있는데, 본 연구에서는 가상실험에 의해 본 방법을 채택하였음)

BMT 평가항목	탐지유무	탐지 결과값
세션 하이제킹 존재(1)	O	1
Root 사용자 패스워드 노출(2)	O	1
전송 데이터 노출(3)	O	1
SNMP Read/Write	X	-1

(표 3) BMT 평가 탐지결과표(예시)

4.4 위험도 반영한 결과값 계산

선정된 취약점항목의 위험도를 4.3 의 결과값에 가중치로 적용하여 최종결과값을 산정한다. 위험도는 H:3, M:2, L:1 로 계산하며, 최종점수는 2 + 2 + 3 + (-1) = 6 이 된다. (항목별 최종결과값:탐지결과값 * 위험도)

BMT 평가항목	탐지 결과값	위험도	최종 결과값
세션 하이제킹 존재(1)	1	M	2
Root 사용자 패스워드 노출(2)	1	M	2
전송 데이터 노출(3)	1	H	3
SNMP Read/Write	-1	L	-1

(표 4) BMT 평가 점수산정표(예시)

5. 기존 방법과의 비교

유사한 수준의 A 와 B 사의 침입탐지시스템이 있는데, 비교를 위해 전송데이터 노출에 대한 탐지능력만 다르다고 가정하자. (A 는 탐지가능, B 는 탐지불능) 표 5 와 같이 테스트결과를 얻었고, 도출된 위험도가 다음과 같다. 위험도를 반영한 경우와 그렇지 않은 경우 어떻게 수준이 달라지는지 최종점수를 비교해보자

BMT 평가항목	A 제품 탐지 결과	B 제품 탐지 결과	위험도
세션 하이제킹 존재	O	O	H(3)
Root 사용자 패스워드 노출	X	X	M(2)
전송 데이터 노출	O	X	H(3)
SNMP Read/Write	O	O	L(1)

(표 5) 탐지결과 및 위험도(예시)

5.1 기존 평가방법에 따른 비교

BMT 평가항목	A 제품 최종 결과값	B 제품 최종 결과값
세션 하이제킹 존재	1	1
Root 사용자 패스워드 노출	0	0
전송 데이터 노출	1	0
SNMP Read/Write	1	1

(표 6) 탐지결과값(예시)

A 는 3 점, B 는 2 점으로 최종점수가 차이가 거의 나지 않고, 처음 가정처럼 유사한 수준으로 파악된다.

5.2 제안 평가방법에 따른 비교

BMT 평가항목	A 제품			B 제품		
	탐지 결과 값	위 험 도	최종 결과 값	탐지 결과 값	위 험 도	최종 결과 값
세션 하이제킹 존재	1	3	3	1	3	3
Root 사용자 패스워드 노출	-1	2	-2	-1	2	-2
전송데이터 노출	1	3	3	-1	3	-3
SNMP Read/Write	1	1	1	1	1	1

(표 7) A,B 제품 최종결과표(예시)

위험도 반영 시 A 제품의 최종점수는 3 + (-2) + 3 + 1 = 5 점이고, B 제품은 3 + (-2) + (-3) + 1 = -1 점이다.

5.3 두 방법의 결과 비교

결과에서와 같이 기존방법으로는 1 점 차이가 났으나, 제안방법에서는 6 점의 차이로 위험도에 따라 어떤 제품이 적합한지를 판단할 수 있다. 여러 실험치를 사용해본 결과 취약점 분석결과 위험도가 낮은 조직보다 높은 조직에서 기존방법과 큰 차이를 보여 결과비교가 쉬웠다. 즉, 위험도반영이 평가에 중요한 잣대임을 보여준다.

6. 결론 및 향후 계획

기존의 BMT 평가방법을 통해서는 조직의 네트워크가 갖는 위험을 효과적으로 반영한 결과를 얻는다는 객관적 근거를 제시하기 어려웠다. 그러나 위험도 기반 평가방법을 통하여 이러한 문제를 상당히 해결할 수 있을 것이고, 조직에 맞는 침입탐지시스템 선정이 가능해 진다는데 의미가 있다.

그러나 본 논문에서 제시한 대로 위험분석과 침입탐지시스템 평가에 동시에 적용할 수 있는 통일된 취약점목록 개발과 결과값 산정 방정식은 좀더 보완되고 개선되어야 할 것이다. 그러므로 향후 남은 과제를 수행하고 실제 실험을 통해 보다 타당한 제안의 근거를 마련하는 것을 향후 계획으로 진행할 것이다.

참고문헌

[1] 2005 년 IT 투자동향 보고서, KIPA, 백영란, 2004. 10
[2] 2004 국가정보보호백서, 국가정보원
[3] D.B.Chapman and E.D.Zwicky, Building Internet Firewalls, O'Reilly & Associates, 1995
[4] 정보보호제품 성능시험동향 분석, 정보보호학회지 제 12 역, 정태인, 김진호, 신용녀, 박희운, 2002. 10
[5] Peter Mell(NIST ITL) and Richard Lippmann(MITLL), An Overview of Issues in Testing Intrusion Detection Systems, DARPA Project, 2002
[6] 한국정보통신기술협회, 공공정보시스템 보안을 위한 위험분석 표준-위험분석 방법론 모델, 2000. 3