보안제품 보호파일 기반 적합성 검증에 관한 연구

강진수, 김창수
부경대학교 전자계산학과

A study on the Appropriateness Verification based Protection Profile of Security Products

Jin-Soo Kang, Chang-Soo Park
Dept. of Computer Science, PuKyong Nat'l University

요 약

본 논문은 보안제품 적합성 검증을 위한 자동화 도구를 리눅스 기반에서 구현하였으며, 구현된 적합성 검증 자동화 도구를 이용하여 TCP/IP 5Layer중 IP Layer 이상의 계층에서 보안성을 제공하는 제품들에 대한 무결성 테스트를 실시하였다. 그리고 CC(Common Criteria) 기반의 적합성 검증 절차를 연구하여 구체적인 보안제품의 보호파일에 대한 제안을 제기했다. 구현된 적합성 검증 자동화 도구를 이용하여 개발된 보안제품의 안정성을 테스트할 수 있으리라 예상되며, 제안된 보호파일은 구체적인 평가항목으로 국가기관에서 보안제품의 평가 시 사용될 수 있으리라 예상된다.

1. 서론

네트워크 기술의 발전과 인터넷의 급속한 확장으로 전 세계는 인터넷이라는 매체를 통해서 하나로 연결되어 있으며, 최근에는 무선 인터넷 기술의 급속한 발전으로 네트워크 활용 영역을 다양한 분야로 확대시키려는 노력이 증대하고 있다. 그러나 이러한 기능과 편리성에도 불구하고 이를 불법적으로 이용하려는 침입자들도 계속 증가하는 추세에 있다.

표 1.공격수법별 침입 유형(자료제공:한국정보보호진흥원)

공격수법	2003	2004												2004년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
서용자도용	48	0	2	0										2
S/W보안오류	1,620	0	1	0										1
버퍼오버플로우	1,160	18	15	4										33
구성설정오류	9,899	563	294	53										910
악성프로그램	5,637	154	148	118										420
프로토콜취약점	0	0	0	1										1
서비스거부	30	0	0	0										0
E-mail관련	6,900	329	232	25										781
취약점정보수집	4,937	153	146	790										1,033
사회공학	0	0	0	0										0
총계	30,429	1,417	839	986										3,242

[표 1]은 공격수법별로 침입의 유형을 정리한 한국정보보호진흥원의 '2004년 3월의 통계자료이다[1]. 이 자료에서 보듯이 점차 침입의 유형이 다양해지는 추세이며, 이러한 침입에 대응하기 위한 정보보호제품의 대표적인 것으로 Firewall, IDS, VPN, 백신 S/W등의 제품들이 출시되고 있다[2]. 하지만 정보보호제품에 대한 안전성 평가가 제대로 이루어지질 않아, 일부 Firewall, IDS 제품에 대한 평가시스템을 제외한 대부분의 보안제품들에 대한 안정성 보증의 문제가 제기되고 있다. 본 논문에서는 이러한 보안제품에 대한 적합성 검증을 자동화하여 수행할 수 있는 자동화도구를 구현하였고, 이를 통하여 IP Layer 이상에서 정보보호 메카니즘을 가지는 보안제품에 대하여 적합성 검증을 수행 할 수 있다. 구현된 자동화도구를 구축한 후 보안제품에 대하여 테스트를 실시하였으며, 이러한 테스트를 바탕으로 보안제품이 가져야할 기능들에 대한 보호파일을 제안하고자 하였다[3].

2장에서는 적합성 검증에 대한 여러 나라들의 기준과 국제 공통 기준인 CC에 대해서 살펴보겠고, 3장에서는 적합성 검증 자동화도구 구현에 대해서 , 4장에서는 보안 제품에 대한 테스트 결과를 바탕으로 보안 제품의 보호파일에 대한 제안을 하겠고, 마지막으로 5장에서는 결론 및 향후연구로 논문을 맺겠다.

2. 적합성 검증 기준

2.1 ITSEC

유럽에서는 영국, 독일, 프랑스, 네덜란드가 1989년부터 ITSEC (Information Technology Security Evaluation Criteria) 계획을 설계하기 시작하여 정부 및 상용 정보보호 시스템의 효율적 평가 인증 및 상호인정 토대 구축을 목적으로 CESG, CCSC의 두 기관이 공동으로 참여하여 민간용 컴퓨터 시스템에 대한 평가를 수행하도록 하였다. ITSEC은 최초의 정보보안 상용제품 평가 기준이었던 TCSEC과의 호환 등급이 정의될 수 있을 정도로 많은 공통점을 가진다.

2.2 TCSEC

미국에서는 미 국방부 지침 5125.1 : 안전한 컴퓨터 평가기준 제정 및 평가업무 명시에 따라 1983년 TCSEC(Trusted Computer System Evaluation Criteria) 초안(Orange Book)이 제정되었으며 TPEP(Trusted Product Evaluation Program)로 하여금 TCSEC의 모든 등급 평가를 위한 평가 절차를 규정하도록 하였다. 정부 기관 NSA(National Security Agency)가 평가 및 인증을 해, 현재까지 100이상의 제품·시스템이 인증을 취득하고 있다. 그 후, 1992년에 민수용 제품까지 적용 확대할 수 있도록 개정된 FC(Federal Criteria)의 Draft가 만들어졌으나, 같은 시기에 시작한 CC(Common Criteria) 작성으로 인해 방향을 전환하여 FC 작성은 중단되었다

TCSEC의 등급은 C1, C2, B1, B2, B3에서 가장 높은 등급인 A1과 부적격 등급인 D급으로 이루어져 있다.

2.3 CTCPEC

캐나다에서는 1986년 캐나다 정부의 정보 및 자산 보호를 위한 정책 및 표준 필요성이 대두됨에 따라 캐나다 정부의 보안정책 발표가 있은 후에 1988년 CSSC(Canadian System Security Centre)설립하여 캐나다 자체의 평가기준 및 평가능력 배양에 힘을 기울이게 되었다. 이에 따라 1989년에 최초로 Canadian Criteria 1.0이 발표된 것을 시작으로 1990년에 발표된 Canadian Criteria 2.0이 실제 평가에 최초로 사용되게 되었다. 1993년에는 Canadian Criteria 2.1을 확장하여 CTCPEC(Canadian Trusted Computer Product Evaluation Criteria : Version 3.0)을 발표하게 되었다. 8단계의 평가등급을 각각 T0에서 T7까지 부여하고 T0를 부적격 등급으로 지정하였으며 기준이 되는 평가지침서는 미국의 TPEP를 공동으로 운영하고 있다.

2.4 CC

CC(Common Criteria)는 많은 IT 보안 평가 기준을 통합해 제정된 것으로, 1999년 6월, ISO/IEC 15408 국제 규격으로서 승인되었다. CC는, 유럽의 ITSEC, 미국의 TCSEC (통칭 오렌지 북), 그리고 캐나다의 CTCPEC를 포함하고 있다[4].

CC의 구성을 살펴보면 Part Ⅰ, Ⅱ, Ⅲ의 세 가지 분야로 구성되어 있으며 각각의 분야는 다음과 같은 역할을 가지고 있다.

Part1에서는 CC가 전제로 하는 보안 개념이나 평가 개념 등에 대해서 기록하고 있다. Part2에서는 제품이나 시스템이 갖추어야 할 보안 기능(감사, 암호, 사용자 데이터 보호 등)에 관한 조건이 규정되어 있다. Part3에서는 Part2의 기능 요건을 실제 환경에 확실히 부합하도록 하기 위한 요건이 규정되어 있다. 또한 개발자가 평가자에게 제출해야 할 문서나, 평가자가 실시하는 평가 내용이 규정되어 있다. 제품이나 시스템의 기능 요건의 보증범위를 표현하는 척도로서 각 보증 요건의 부분집합이라고 하는 형태로 7 계층의 평가 보증 레벨 즉, EAL (Evaluation Assurance Level)이 정의되어 있다. 이에 따르면 EA1 등급(최저)에서부터 EA7(최고)까지의 평가 등급을 가지고 있으며, EA0는 부적합 등급을 나타내고 있다. 이를 통해 CC에 의해 객관적 보안 평가 결과를 비교하는 것이 가능하게 된다.

국제적인 공통 기준으로 설계된 CC에서는 다른 나라에서 실시되고 있는 정보 기술 보안 평가에 대해서 공통적인 보안 기능 조건을 제공함으로써 각국에서 사용되는 평가기준 레벨 설정에 도움을 주고 점검 및 유지하는 기능도 가능하게 된다. 또한 CC 의 중요한 목표로 보안 평가 결과의 국제적인 상호 승인을 가능하게 하는 것이 포함된다. 공식적으로 국제 공통 평가기준 승인 협정(Common Criteria Recognition

Arrangement - CCRA)에 조인하고 있는 미국, 영국, 캐나다, 독일, 프랑스, 오스트레일리아, 뉴질랜드 등의 국가에서는 다른 협정국에서 CC를 이용하여 평가되고 인정된 IT 제품을 다시 평가하는 노력을 생략할 수 있으므로 상당한 비용 절감 효과를 가질 수 있다.

3. 적합성 검증 자동화도구 구현

본 논문에서는 송신자와 수신자 사이 중간노드에 변조서버를 위치시켜 패킷을 변조함으로 보안제품이 변조된 패킷에 대하여 정확하게 반응하는지를 테스트 하였다.

3.1 변조서버

본 연구에서 사용한 변조서버는 리눅스 기반의 시스템으로 [그림 1]와 같이 리눅스 패킷 전송의 원리를 이용하여 패킷을 변조한다[5]. 리눅스 시스템은 패킷을 수신하여 자신의 주소와 일치하면 패킷을 상위계층으로 전달하고 자신의 주소와 일치하지 않으면 임시버퍼로 전달하여 다른 목적지로 전송한다. 본 연구에서는 수신된 패킷에 대하여 변조작업을 수행한 후, 변조된 패킷을 목적지로 전달함으로써 무결성 테스트를 수행 하였다. 이때 변조작업은 임시버퍼의 패킷에 대해 수행된다. 변조된 패킷을 수신한 서버는 설치된 보안 SW가 제대로 무결성을 검사할 경우 이를 폐기하거나 경고의 반응을 보이게 될 것이며, 무결성을 체크하지 못할 경우 아무런 경고 없이 패킷을 수신하여 정상처리 할 것이다[6].

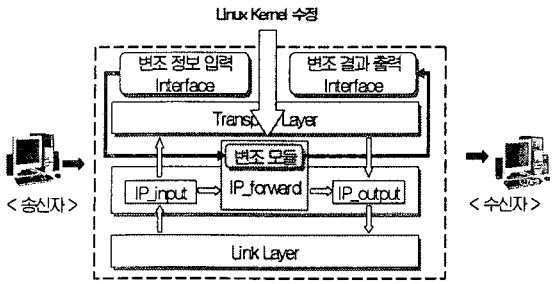

그림 1. 적합성 평가 변조서버 모듈구조

3.2 변조정보 입력 인터페이스

변조 정보 입력 인터페이스는 [그림 3]과 같이 사용자가 직접 변조에 대한 정보를 입력할 수 있으며 변경하고자 하는 패킷의 목적지 주소, 근원지 주소, 패킷 번호, 패킷 변조 위치 등을 입력하게 된다.

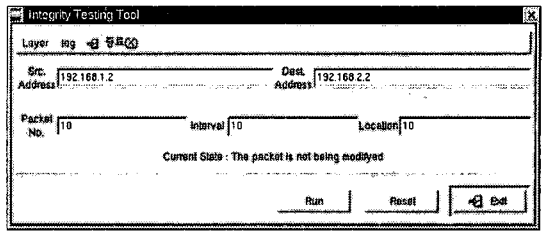

그림 2. 변조 정보 입력 인터페이스

4. 적합성 검증 테스트

4.1 테스트 환경 및 테스트

본 논문에서는 [그림 3]와 같은 테스트 환경을 구축한 후 보안제품의 적합성 검증을 실시하였다. 각각의 클라이언트와 서버 단에는 TCP/IP 5layer중 IP Layer 이상 계층에서 보안을 수행하는 어떤 보안제품도 위치 할 수 있으며 변조서버를 거쳐 수신 측에 패킷이 도달 하였을 때 나타나는 반응을 기록하였다[7].

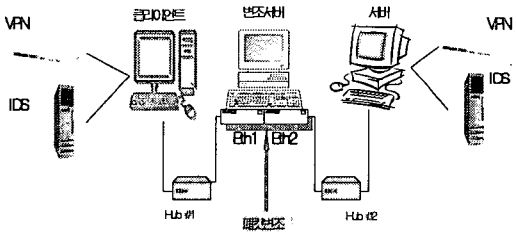

그림 3 . 적합성 검증 자동화 시스템 구성도

[표 2]은 해당 테스트 환경에서 SSL보안제품을 테스트한 결과 이다.

표 2. ssl 보안제품 테스트 결과

넘버	Server OS	Server Program	Client OS	Client Program	변조감지 여부	반응메세지
3.13	윈도우 2000	IIS+SSL	파란 Linux 7.3	모질라 1.0	감지	incorrect Message Authentication Code
3.13	윈도우 2000	IIS+SSL	윈도우 2000	Explore 5.0	감지	시스템 오류에 전달된 데이터 영역이 너무 작습니다
3.13	윈도우 2000	IIS+SSL	윈도우 2000	Nescape 7.01	감지	암 수 없는 메시지 인증코드를 사용한 메시지를 받았습니다
3.19	파란 Linux 7.3	Apache+SSL	윈도우 2000	Explore 5.0	감지	요청한 서버드를 사용할 수 없거나 잘못 수 없습니다
3.19	파란 Linux 7.3	Apache+SSL	윈도우 2000	Nescape 7.01	감지	암 수 없는 메시지 인증코드를 사용한 메시지를 받았습니다
3.21	파란 Linux 7.1	Apache+SSL	파란 Linux 7.1	Nescape 7.01	감지	암 수 없는 메시지 인증코드를 사용한 메시지를 받았습니다
3.27	윈도우 2000	Apache+SSL	윈도우 2000	Explore 5.0	감지	시스템 오류에 전달된 데이터 영역이 너무 작습니다
3.28	윈도우 2000	Apache+SSL	윈도우 2000	Nescape 7.01	감지	암 수 없는 메시지 인증코드를 사용한 메시지를 받았습니다
4.8	윈도우 2000	Apache+SSL	윈도우 2000	Zone Alram	감지않음	개인용 방화벽세팅후 변조되었어 도 어떠도 반응 없음
4.10	윈도우 2000	Apache+SSL	윈도우 2000	Black ICE	감지않음	개인용 방화벽세팅후 변조되었어 도 어떠도 반응 없음
4.11	윈도우 2000	Apache+SSL	윈도우 2000	Snort 2.8	감지않음	alert을 하지 않으며 에러 log가 남지 않음

각각의 테스트 결과 보안제품별로 나타나는 반응 메세지들이 다름을 알 수 있었다. 변조패킷에 대하여 해당하는 메시지를 보여주는 보안제품이 있는 반면 에러 내용 없이 패킷을 거부한 경우도 있었다.

4.2 보안제품 보호파일

이러한 보안제품의 보증에 관한 연구가 국내외적으로 많이 수행되고 있는데 대표적인 국제표준으로 CC(Common Criteria)가 존재한다. [그림 4]는 CC의 Firewall에 관한 PP(Protection Profile)를 나타내고 [그림 5]은 KISA(한국정보보호진흥원)의 Firewall PP를 보여주고 있다.

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL	T.LOWEXP	T.CRYPTPRO
O.IDAUTH	X											
O.SINUSE		X	X									
O.MEDIAT				X	X	X						
O.SECSTA	X								X			
O.ENCRYP	X						X					X
O.SELPRO	X								X	X		
O.AUDREC								X				
O.ACCOUN								X				
O.SECFUN	X		X							X		
O.LIMEXT	X											
O.EAL											X	

Table 6.1 – Summary of Mappings Between Threats and IT Security Objectives

그림 4. CC Firewall PP

TSF 보호	FPT_AMT.1					X		X							
	FPT_RVM.1							X							
	FPT_SEP.1							X							
	FPT_STM.1			X											
	FPT_TST.1	X	X			X		X							
안전한 경로/채널	FTP_ITC.1	X	X												

그림 5. KISA Firewall PP

하지만 이러한 PP의 구성은 추상적인 개념으로만 구성되어 있기 때문에 실제 보안성을 테스트를 수행하는 기관에서 바로 활용하기가 싶지 않다. 따라서 본 논문에서는 보안제품의 테스트 수행 시 직접 적용할 수 있는 항목들을 도출해 내고자 시도하였다. 아래 항목들은 보안제품 테스트를 수행한 결과 나타난 결과를 바탕으로 도출한 권고사항이다.

① 정확한 에러 원인 표시

테스트결과 error 원인 표시 없이 서비스만 제공하지 않는 보안제품이 있었음.

② illegal packet drop 정책

illegal packet에 대해서 receive 정책이 아닌 drop 정책 필요[7]

③ error log 정보 database화

발생한 error에 대해서 접근자의 정보를 토대로 error log 생성필요

이러한 사항들은 PP와는 다르게 실제 기능을 하는지 여부를 명확하게 확인할 수 있으므로 보안제품의 적합성 테스트에 바로 적용 할 수 있을 것이라 예상된다.

5. 결론 및 향후연구

본 논문에서는 보안제품의 적합성 검증을 위한 자동화도구에 대해서 연구하였다. 구성한 자동화도구는 리눅스 커널을 수정하여 구성했으며 중간노드에 변조서버를 위치시켜 패킷의 정보를 임의적으로 변경하여 보안제품이 정확히 변조된 패킷에 대해서 반응하는지의 여부를 살펴보았다. 덧붙여 보안제품의 국제표준인 CC에 대해서 살펴보았고 추성적인 CC의 보호파일(PP)에 대한 적용하기 어려운 점을 고려하여 구체적인 보안제품이 가져야 될 항목들에 대해서 권고사항을 제시하였다. 향후 연구로 보다 많은 보안제품에 대한 테스트 수행을 실시하여 , 구체적이고 다양한 권고사항을 도출해 내야 될 것이다. 덧붙여 보안제품의 성능적인 측면 또한 개발 시 고려해야 될 중요한 사항으로 이부분에 대한 추가적인 연구가 필요할 것이라 예상된다[9].

[참고문헌]

[1] 한국정보보호진흥원 "3월 해킹바이러스 통계 및 분석 월보" 2004.3

[2] 포항공과대학 전자계산소,"Security plus for Unix",1998

[3] 김태호 "네트워크 보안제품 적합성 검증을 위한 무결성 검증 도구 설계 및 구현" 이학석사 학위논문 2002.3

[4] [Common Criteria] http://csrc.nist.gov/cc

[5] Gerhard Mourani "Securing & Optimizing Linux the ultimate solution", 한빛미디어, 2003

[6] W.Richard Stevens "Unix Network Programming" ,Prentice hall PTR, 1998

[7] W.Richard Stevens "TCP/IP Illustrated volume1" , 1998

[8]Seny Kamara,Sonia Fahmy,Eugene Schultz, Florian Kerschbaum and Michael Frantzen,"Analysis fo vulnerabilities in Internet firewalls",Computers & Security,2003

[9] 문종옥,김종수,정기현,임강빈,주민규,최경규,"IDS의 성능 향상을 위한 패킷 폐기방안" 과기부 국가지정연구사업,2002