2022-국가직-9급-정보시스템보안-나형-해설-곽후근

문 1. CPU에서 실행되는 머신 코드가 위치하는 시스템 메모리 영역은?

① 스택 ② 힙

③ 텍스트 ④ 데이터

정답 체크

(3) 실행 파일(이진 코드)가 위치한다.

오답 체크

(1) 지역 변수, 복귀 주소, 매개 변수 등이 위치한다.

(2) 동적 메모리 할당이 위치한다(C언어는 malloc/free, C++/자바에서는 new/delete).

(4) 전역 변수, 정적 변수가 위치한다.

문 2. 사용자와 운영체제 사이에서 중간자 역할을 수행하며, 명령어 해석 기능, 프로그래밍 기능, 사용자 환경 설정 기능을 제공하는 것은?

① 데몬 ② 커널

③ 프로세스 ④ 셸

정답 체크

(4) 운영체제 중 인터페이스 부분을 담당한다.

오답 체크

(1) 항상 실행중인 프로그램이다(프로세스 중 항상 실행 중임을 의미).

(2) 운영체제 중 핵심이 되는 프로그램이다(자원 관리 부분).

(3) 실행 중인 프로그램이다(보조기억장치에서 주기억장치로 올라옴).

문 3. (가)에 들어갈 용어로 옳은 것은?

> 보안 운영체제는 기존의 운영체제에 내재된 보안상의 결함으로 인한 각종 침해로부터 시스템을 보호하기 위하여 기존의 운영체제 내에 보안 기능을 통합시킨 (가) 을/를 추가로 이식한 운영체제이다. 이를 통해 사용자의 모든 접근 행위가 안전하게 통제된다. 이것은 하드웨어, 운영체제 및 기타 시스템 요소 간의 보안 인터페이스를 제공한다.

① 보안 커널 ② 접근 제어

③ 신뢰 플랫폼 모듈 ④ 하이퍼바이저

정답 체크

(1) 시스템 자원을 대한 접근을 통제하기 위한 기본적 보안 절차를 구현한다.

오답 체크

(2) 주체가 객체를 사용하는 것을 허가하거나 거부하는 기능이다.

(3) 암호화된 키, 패스워드, 디지털 인증서 등을 저장하는 안전한 저장 공간을 제공하는 보안 모듈이다.

(4) 가상 머신을 생성하고 실행하는 프로세스이다.

문 4. 보안 모델의 하나인 만리장성(Chinese Wall) 모델에 대한 설명으로 옳은 것은?

① 높은 보안 수준에서 낮은 보안 수준으로 정보가 흐르는 것을 방지하기 위한 기밀성 보장 모델이다.

② 비즈니스 입장에서 직무 분리 개념을 적용하여 이해가 충돌하는 회사 간에 정보의 흐름이 일어나지 않도록 접근을 통

제한다.
③ 무결성 중심의 상업적 모델로 내·외부의 일관성을 유지하고 비인가자에 의한 불법적인 수정을 방지한다.
④ 무결성을 위한 모델로 비인가자의 데이터 변형을 방지하기 위한 것이다.
정답 체크
(2) 충돌을 야기하는 어떠한 정보의 흐름도 차단해야 한다는 모델로 이익 충돌 회피를 위한 모델이고, 직무 분리를 접근 통제에 반영한 개념이 적용한다.
오답 체크
(1) BLP 모델에 대한 설명이다.
(3) Clark-Wilson 모델에 대한 설명이다.
(4) Biba 모델에 대한 설명이다.

문 5. 윈도시스템의 NTFS에서 폴더 및 파일 접근 권한에 대한 설명으로 옳은 것은?
① 그룹 A와 그룹 B에 속한 사용자가 그룹 A에서는 읽기 권한을 할당받고 그룹 B에서는 쓰기 권한을 할당받았다면, 사용자에게 읽기와 쓰기 권한이 모두 주어진다.
② 파일이 포함된 폴더 권한이 파일 권한보다 우선한다.
③ 권한을 중첩해서 적용할 수 있으며, 허용 설정이 거부 설정보다 우선한다.
④ 폴더 접근 권한은 그룹에게만 부여된다.
정답 체크
(1) 사용자는 A, B 그룹에 속해있으므로 A, B 그룹에 할당된 권한이 주어진다.
오답 체크
(2) 파일 권한이 폴더 권한보다 우선한다.
(3) 거부 설정이 허용 설정보다 우선한다.
(4) 사용자에게도 부여된다.

문 6. 다음에서 설명하는 전자우편 보안 기술은?

○ 종단 사용자에게 투명한 인증 기술을 제공하도록 설계되었다. ○ 전자우편 메시지는 전자우편 발신지 관리 도메인의 개인키에 의해 서명된다. ○ 서명은 메시지 내용 전체와 메시지 헤더의 일부를 대상으로 한다. ○ 수신 측의 MDA(Mail Delivery Agent)는 DNS를 통해 해당 공개키에 접근하여 서명을 검증할 수 있다.

① PGP ② PEM
③ MIME ④ DKIM
정답 체크
(4) 수신된 이메일이 위변조 되지 않았는지 디지털 서명을 이용해 검증하는 기술이다.
오답 체크
(1) 전자우편의 안전성을 위해 1991년 미국의 Phil Zimmermann에 의해 개발된 전자우편 보안 시스템이다.
(2) 인터넷상에서 안전한 전자우편을 제공하기 위해 제안된 인터넷 표준안을 만드는 기술위원회(IETF: Internet Engineering Task Force) 표준안이다.
(3) ASCII가 아닌 문자 인코딩을 이용해 영어가 아닌 다른 언어로 된 전자 우편을 보낼 수 있는 방식을 정의한다.

문 7. 다음에서 설명하는 윈도시스템 인증 구성 요소는?

사용자의 계정과 패스워드가 일치하는 경우 해당 사용자에게 고유의 SID(Security Identifier)를 부여하며, 파일이나 폴더에 대한 접근 허용 여부를 결정하고 이에 대한 감사 메시지를 생성한다.

① SAM ② LSA
③ SRM ④ SPI

정답 체크

(3) SAM이 사용자의 계정과 패스워드 일치 여부를 확인하여 알리면 사용자에게 SID(Security Identifier) 부여, SID에 기반하여 파일이나 디렉터리에 대한 접근(access) 허용 여부 결정하고, 이에 대한 감사(audit) 메시지 생성한다.

오답 체크

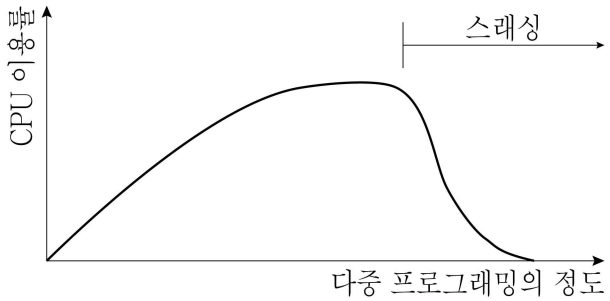
(1) 사용자/그룹 계정 정보에 대한 데이터베이스 관리, 사용자의 로그인 입력 정보와 SAM 데이터베이스 정보를 비교해 인증 여부 결정한다. 윈도우에서 패스워드 암호화하여 보관하는 파일의 이름과 동일하다.

(2) 모든 계정의 로그인에 대한 검증, 시스템 자원 및 파일 등에 대한 접근 권한 검사한다. 로컬, 원격 모두에 해당하고, 이름과 SID를 매칭하며, SRM이 생성한 감사(audit) 로그를 기록한다.

(4) IPsec을 사용하여 IP 트래픽을 터널링하는 동안 헤더에 추가 된 식별 태그이다. 이 태그는 다른 암호화 규칙과 알고리즘이 사용중인 두 트래픽 스트림을 커널이 식별하는 데 도움이된다.

문 8. (가), (나)에 들어갈 용어를 바르게 연결한 것은?

그림과 같이 다중 프로그램의 정도에 따른 CPU 이용률은 처음에는 비례해서 증가하지만 다중 프로그래밍의 정도가 어느 정도 이상으로 커지면 스래싱(thrashing)이 일어나게 되어 CPU 이용률은 급격히 떨어진다. 스래싱은 [(가)] 페이지 교체 알고리즘을 사용하면 제한할 수 있다. 또한 이 현상을 방지하기 위해서는 각 프로세스에게 할당되는 최소한의 [(나)] 개수를 보장해야 한다.



	(가)	(나)
①	전역	프레임
②	전역	페이지
③	지역	프레임
④	지역	페이지

정답 체크

(3) 지역 : 현재 수행 중인 프로세스에게 할당된 프레임 내에서만 교체 대상을 선정하므로 스래싱을 줄일 수 있다(필요한 프레임을 유지할 수 있음).

프레임 : 물리적인 프레임의 개수를 보장해야 한다.
오답 체크
(1), (2), (4) 전역 : 모든 페이지 프레임이 교체 대상이 되면 스래싱을 줄일 수 없다(필요한 프레임을 유지 못할 가능성 존재).
페이지 : 논리적인 페이지가 아닌 물리적인 프레임을 보장해야 한다.

문 9. S/MIME에 대한 설명으로 옳지 않은 것은?
① 서명된 데이터(signed data)의 디지털 서명은 메시지 다이제스트를 서명자의 개인키로 암호화한 것으로, 서명과 함께 메시지 내용은 base64로 부호화된다.
② 서명과 봉인된 데이터(signed and enveloped data)는 서명만 하거나 암호화만 한 개체들이 중첩된 것으로, 암호화한 데이터를 서명하거나 서명한 데이터를 암호화할 수 있다.
③ 디지털 서명만을 base64로 부호화한 클리어 서명 데이터(clear-signed data)의 경우, S/MIME 기능을 갖추지 않은 수신자도 서명을 검증하고 메시지의 내용을 볼 수 있도록 지원한다.
④ X.509의 버전 3을 따르는 공개키 인증서를 사용한다.
정답 체크
(3) 메시지 내용을 볼 수 있지만 서명을 검증할 수는 없다.
오답 체크
(1) 송신자가 자신의 개인키(private key)를 이용하여 MIME 메시지에 서명한 데이터를 의미한다.
(2) 서명 및 봉인된 데이터(Signed-and-enveloped Data)란 송신자가 MIME 메시지를 암호화하고, 암호화된 MIME 메시지에 송신자 자신의 개인키(private key)를 이용하여 전자서명한 데이터를 의미한다.
(4) 암호화와 디지털 서명을 위해 공개키 인증서(공인인증서)를 사용한다.

문 10. HTTP 버전 1.1에서 정의된 요청 메시지의 메소드에 대한 설명으로 옳은 것은?
① GET이 요청하는 웹페이지의 위치는 헤더 라인 안에 명시된다.
② 서버가 보내온 쿠키를 저장했다가 반환하는 GET의 경우, 쿠키 정보는 메시지 몸체(body)에 포함된다.
③ HEAD는 서버로부터 웹페이지 자체가 아닌 웹페이지에 대한 일부 정보를 요청하기 위한 것이다.
④ PUT은 요구 메시지가 서버에 의해 제대로 처리되는가를 검사하기 위한 에코 반환 용도로 사용된다.
정답 체크
(3) 서버 측의 데이터를 검색하고 요청하는 데 사용된다.
오답 체크
(1) URL에 명시된다.
(2) URL에 명시된다.
(4) TRACE에 해당하고, PUT은 메시지에 포함되어 있는 데이터를 지정한 URI(Uniform Resource Identifier) 장소에 그 이름으로 저장한다.

문 11. 리눅스 시스템의 /etc/shadow 파일 내용에서 패스워드의 최종 변경일에 해당하는 것은?

root : 6L9~중략~ruKuT0 : 15917 : 0 : 99999 : 7 : 5 : 16070 :

① 15917 ② 99999
③ 7 ④ 16070
정답 체크
(1) 마지막 변경일에 해당한다.

오답 체크
(2) 패스워드 바꾸지 않고 최대한 사용할 수 있는 기간이다.
(3) 패스워드 최대 사용 기간에 가까워질 경우 사용자에게 미리 통지한다. 패스워드 사용 기한 며칠 전에 경고를 보낼지 지정한다.
(4) 1970년 1월 1일부터 계정이 완전 사용 정지된 기간에 대한 계산 값을 기록한다.

문 12. PKI에 대한 설명으로 옳지 않은 것은?
① 인증기관(CA), 등록기관(RA), 키 분배 센터(KDC)로 구성된다.
② 이용자는 공개키를 이용하기 전에 CA의 인증서 폐기 목록(CRL)을 조사해서 해당 인증서의 유효성을 확인할 필요가 있다.
③ CA의 공개키에 대해 다른 CA가 디지털 서명을 하는 것으로 그 CA의 공개키를 검증할 수 있다.
④ CA의 개인키가 노출된 경우에는 그 사실을 CRL을 사용해서 이용자에게 통지할 필요가 있다.
정답 체크
(1) 인증기관, 등록기관, 이용자, 저장소로 구성된다.
오답 체크
(2) CRL(주기적 확인)과 OCSP(실시간 확인)를 사용한다.
(3) 계층형 PKI에 해당한다.
(4) CA의 개인키가 노출되면 공인인증서는 폐기가 된다.

문 13. 인증을 받은 사용자가 여러 정보 시스템에 재인증 절차 없이 반복해서 접근할 수 있도록 해주는 것은?
① OTP ② SSO
③ Challenge & Response ④ CAPTCHA
정답 체크
(2) 모든 인증을 하나의 시스템에서 한다는 의미이다. 시스템이 몇 대가 되어도 하나의 시스템에서 인증에 성공하면, 다른 시스템에 대한 접근 권한도 모두 얻는다. 이러한 접속 형태의 대표적인 인증 방법으로는 커버로스(Kerberos)를 이용한 윈도우의 액티브 디렉토리(Active Directory)가 있다. 지식 기반 인증에 사용된다.
오답 체크
(1) 고정된 비밀번호 대신 사용되는 매번 새롭게 바뀌는 일회용 비밀번호이다. S/KEY 방식, 시간 동기화 방식, 챌린지/응답 방식, 이벤트 동기화 방식 등이 있다. 소지 기반 인증에 사용된다.
(3) 검증자가 요구하는 임의의 요청(도전)에 대해서도 정확한 인증 정보(응답) 제공을 요구함으로써 실체를 인증하는 방법이다.
(4) 어떠한 사용자가 실제 사람인지 컴퓨터 프로그램인지를 구별하기 위해 사용되는 방법이다. 사람은 구별할 수 있지만 컴퓨터는 구별하기 힘들게 의도적으로 비틀거나 덧칠한 그림을 주고 그 그림에 쓰여 있는 내용을 물어보는 방법이 자주 사용된다.

문 14. 공격 대상이 되는 서버에서 먼저 공격자 PC로 연결하게 하여 방화벽 보안 정책을 우회하는 공격은?
① 리버스 텔넷 ② 쿠키 변조
③ 명령 삽입 ④ 파일 업로드
정답 체크
(1) 웹 서버의 텔넷(Telnet)이 열려있어도, 방화벽으로 인해 공격자가 외부에서 접근할 수 없다(방화벽의 인 바운드 정책). 방화벽의 아웃 바운드 정책이 없다면 웹 서버에서 공격자에게 리버스 텔넷을 시도할 수 있다.

오답 체크

(2) 쿠키를 안전한 알고리즘으로 암호화하지 않는 경우 공격자가 쿠키 인젝션 등과 같은 쿠키 값 변조를 통해 다른 사용자로 위장 및 권한 변경을 할 수 있다.

(3) 코드를 추가하여 실행 순서를 바꾼다. 해당 취약점은 SQL, LDAP, Xpath, NoSQL 등에서 발견된다.

(4) 공격자가 시스템 내부 명령어를 실행시킬 수 있는 웹 프로그램(ASP나 JSP, PHP)을 제작하여, 자료실과 같은 곳에 공격용 프로그램을 업로드 하는 공격 방식이다.

문 15. (가) ~ (다) 안에 들어갈 용어를 바르게 연결한 것은?

함수 P가 함수 Q를 호출하기 위해, P는 Q에 전달할 인수를 스택에 넣는다. Q를 호출하는 call 명령어를 수행하면 [(가)]가 스택에 저장된다. Q는 [(나)]를 스택에 넣는다. 프레임 포인터 레지스터 값을 현재의 포인터 값으로 설정하고, 스택 포인터를 아래로 움직여 [(다)]를 저장할 공간을 할당하고, Q의 코드를 수행한다. 컴파일러의 최적화 기능에 따라 실제 배치는 차이가 있을 수 있으나, 저장된 [(가)]와 [(나)]에 겹쳐 쓰기는 스택 버퍼 오버플로 공격의 핵심이다.

	(가)	(나)	(다)
①	반환 주소	P의 스택 프레임 포인터	지역 변수
②	반환 주소	Q의 스택 프레임 포인터	지역 변수
③	P의 스택 프레임 포인터	지역 변수	반환 주소
④	Q의 스택 프레임 포인터	지역 변수	반환 주소

정답 체크

(1) 반환 주소 : 호출을 마치고 돌아올 주소를 저장한다.

P의 스택 프레임 포인터 : 현재 어디를 수행중인지를 저장했다가 나중에 호출을 마쳤을 때 해당 위치부터 다시 수행한다.

지역 변수 : 스택에는 지역 변수가 저장된다(스택 포인터가 해당 위치를 가리킨다).

오답 체크

(2), (4) Q의 스택 프레임 포인터 : Q에서 다른 함수를 호출했을 때 저장되지만, 현재 상태에서는 저장할 필요가 없다.

(3) 순서가 바뀌었다.

문 16. FTP에 대한 설명으로 옳지 않은 것은?

① 데이터 연결 시 평문으로 데이터를 전송한다.

② 데이터 연결은 송수신 모두 지정된 포트 20번을 통해서만 가능하다.

③ 사용자 계정의 패스워드는 암호화되지 않은 상태로 전달된다.

④ FTP를 이용하여 클라이언트는 서버의 파일을 읽고 서버에 파일을 저장할 수 있을 뿐만 아니라 서버의 파일 목록을 볼 수도 있다.

정답 체크

(2) active 또는 passive 모드에 따라 포트를 변경할 수 있다(1024번 이후 포트).

오답 체크

(1), (3) 암호화를 수행하지 않는다.
(4) 클라이언트의 파일 목록을 볼 수도 있고, 서버의 파일 목록을 볼 수도 있다.

문 17. SQL 뷰에 대한 설명으로 옳지 않은 것은?
① 사용자가 뷰를 통해서만 데이터에 접근하게 함으로써 기본 테이블에 대한 보안성을 높일 수 있다.
② 뷰가 정의된 기본 테이블이 확장되거나 뷰가 속해 있는 데이터베이스에 테이블이 늘어난다고 하더라도 기존의 뷰를 사용하는 프로그램이나 사용자는 영향을 받지 않는다.
③ 필요한 데이터만 뷰로 정의해서 처리할 수 있기 때문에 사용자 권한 관리가 용이하다.
④ 대부분의 경우 삽입, 삭제, 갱신 연산에 많은 제한이 따르며 질의문이 복잡해지는 단점이 있다.
정답 체크
(4) 질의문이 간단해진다.
오답 체크
(1) 데이터를 숨길 수 있다.
(2) 뷰를 원래 정의된 것에 변경되지 않는다.
(3) 뷰를 통해 권한을 관리하면 필요 이상의 권한을 줄 필요가 없다.

문 18. 리눅스에서 제공하는 특수 권한에 대한 설명으로 옳지 않은 것은?
① 숫자로 나타내면 접근 권한의 맨 앞자리에 Set-UID는 4, Set-GID는 2, Sticky-Bit는 1로 표현된다.
② Set-UID를 설정하면 소유자 실행 권한 자리에, Set-GID를 설정하면 그룹 실행 권한 자리에 s 혹은 S가 표시된다.
③ Sticky-Bit는 공유를 목적으로 파일에 설정하는 특수 권한으로, 설정 시 소유자 실행 권한 자리에 t 혹은 T가 표시된다.
④ Set-UID가 설정된 파일이 실행되는 동안에는 파일을 실행한 사용자의 권한이 아니라 파일 소유자의 권한이 적용된다.
정답 체크
(3) 제3자 실행 권한 자리에 t 혹은 T가 표시된다.
오답 체크
(1) 4000, 2000, 1000으로 표기된다.
(2) 파일 소유자 권한 또는 파일 그룹 권한으로 권한이 변경된다.
(4) 사용자가 어떤 일을 수행하기 위해 일시적으로 권한 상승을 하기 위해 사용한다.

문 19. 다음에서 설명하는 웹 취약점 점검 방법과 해당 취약점을 바르게 연결한 것은?

(가) "../"를 이용해서 임의의 경로가 포함된 값으로 웹페이지 파라미터를 변조한 후 해당 경로의 파일 내용이 표시되는지 확인
(나) 사용자 입력값을 전달받는 게시판, 자료실 등에 〈script〉alert()〈/script〉와 같은 스크립트를 입력한 후 실행 여부 확인
(다) 인증 후 정상적으로 세션이 발행된 페이지의 정보를 취득하고 일정 시간 후에 재전송했을 때 정상 처리가 되는지 확인

(가) (나) (다)

① 경로 추적	CSRF	불충분한 인증 및 인가
② 경로 추적	XSS	불충분한 세션 관리
③ 디렉터리 인덱싱	XSS	불충분한 인증 및 인가
④ 디렉터리 인덱싱	CSRF	불충분한 세션 관리

정답 체크

(2) 경로 추적 : 웹 어플리케이션 서버의 파일 또는 디렉토리에 대한 접근이 제한적이지 않고 허용이 되어 있어 공격자로부터 경로가 탈취되어 중요 정보획득 및 변조가 가능한 취약점을 의미한다.

XSS : 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 주로 여러 사용자가 보게 되는 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다. 이 취약점은 웹 애플리케이션이 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타난다. 이 취약점으로 해커가 사용자의 정보(쿠키, 세션 등)를 탈취하거나, 자동으로 비정상적인 기능을 수행하게 할 수 있다. 주로 다른 웹사이트와 정보를 교환하는 식으로 작동하므로 사이트 간 스크립팅이라고 한다.

불충분한 세션 관리 : 동일한 세션 아이디를 발급하거나 세션 타임아웃을 너무 길게 설정하였을 경우 공격자가 다른 사용자의 세션을 재사용하여 해당 사용자의 권한을 탈취할 수 있는 취약점이다.

오답 체크

(1), (3), (4) CSRF : 웹 사이트 취약점 공격의 하나로, 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 특정 웹 사이트에 요청하게 하는 공격이다. 즉, 일단 사용자가 웹 사이트에 로그인한 상태에서 CSRF 공격 코드가 삽입된 페이지를 열면, 이후에는 사용자의 행동과 관계없이 사용자의 웹 브라우저와 공격 대상 웹 사이트 간의 상호 작용이 이루어진다.

불충분한 인증 및 인가 : 인증이 미흡할 경우 공격자가 파라미터로 전달되는 값을 수정하여 사용자 도용 및 개인정보 노출 문제가 발생할 수 있는 취약점이다.

디렉토리 인덱싱 : 서버내의 모든 디렉터리 및 파일에 대해 인덱싱이 가능하여 모든 파일에 대한 목록을 볼 수 있는 취약점을 의미한다.

문 20. 보안 요구 조건을 명세화하고 평가 기준을 정의하기 위한 ISO 표준인 공통 기준(CC)에서는 요구 조건을 기능적 요구 조건과 보증 요구 조건으로 나누고 있다. 기능적 요구 조건에 해당하지 않는 것은?

① 식별과 인증 ② 암호 지원

③ 보안 감사 ④ 취약점 평가

정답 체크

(4) 보증 요구 조건은 다음과 같다(가변).

•ASE(Security Target Evaluation): 보안목표명세서 평가
•ADV(Development): 개발
•AGD(Guidance Documents): 설명서
•ALC(Life Cycle Support): 생명주기 지원
•ATE(Tests): 시험
•AVA(Vulnerability Assessment): 취약성 평가
•ACO(Composition): 합성
•APE(PP Evaluation): 보호프로파일 평가
•ADO(Delivery and Operation): 배포 및 운영
•ACM(Configuration Management): 형상 관리
•ACE(PP Configuration): 보호프로파일 설정

•AMA(Maintenance of assurance): 보증 유지

•그 외…

오답 체크

(1), (2), (3) 기능적 요구 조건은 다음과 같다(고정).

CC 2부 보안기능 클래스
FAU(Security Audit) 보안 감사
FCO(Communication) 통신
FCS(Cryptographic Support) 암호 지원
FDP(User Data Protection) 사용자 데이터 보호
FIA(Identification & Authentication) 식별 및 인증
FMT(Security Management) 보안 관련
FPR(Privacy) 프라이버시
FPT(Protection of the TSF) TSF 보호
FRU(Resource Utilisation) 자원 활용
FTA(TOE Access) TOE 접근
FTA(Trusted Path/Channel) 안전한 경로/채널