정보보호

(5111041)

과목 개요

- 학습 내용
  - Security topics including, but not limited to,
    - 보안 기술 및 원리
    - 암호 알고리듬
    - 네트워크 보안
    - 최신 보안 이슈 및 트렌드

- 평가
  - 출석 10 %, 숙제/퀴즈 10%, 중간고사 40%, 기말고사 40%

1 장

개 요

컴퓨터 보안 개요

NIST 컴퓨터 보안 핸드북[NIST95]에 따르면 컴퓨터 보안은 다음과 같이 정의된다:

"자동화된 정보 시스템내의 자원(하드웨어, 소프트웨어, 펌웨어, 정보/데이터, 통신)들의 무결성, 가용성, 기밀성을 보존하기 위해 제공되는 보호"

NIST: 미국표준기술연구소

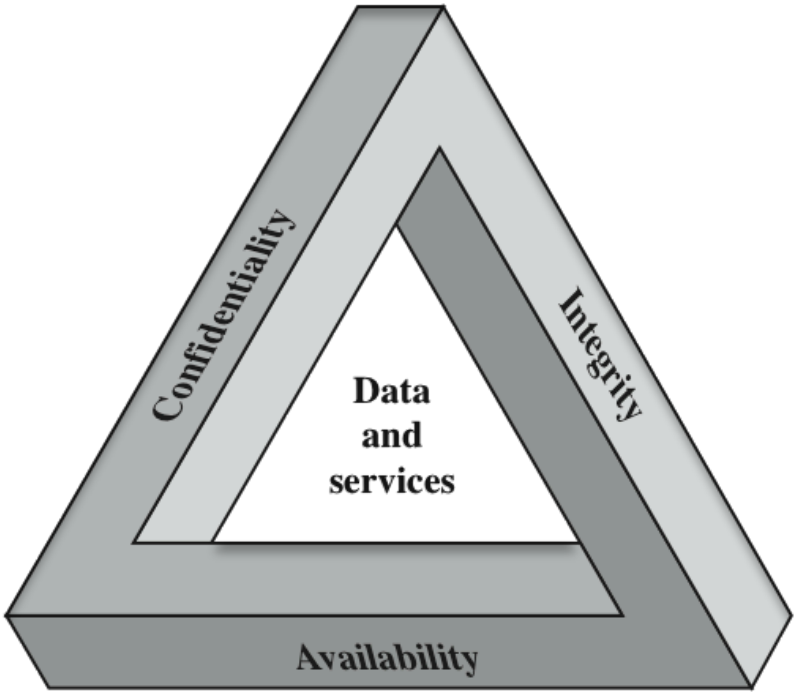


Figure 1.1 The Security Requirements Triad

CIA 3요소

- 기밀성
  - 데이터 기밀성
  - 프라이버시
- 무결성
  - 데이터 무결성
  - 시스템 무결성
- 가용성

주요 보안 개념

기밀성

- 개인 프라이버시와 소유권 정보를 보호하고, 정보의 접근 및 노출에 인가된 제한을 유지하는 것

무결성

- 정보의 부인방지와 진위성을 보증함으로써 정보의 부적절한 변경 혹은 파괴로부터 보호

가용성

- 정보에 대한 적절하고 신뢰성 있는 접근과 사용을 보증

컴퓨터 보안 과제

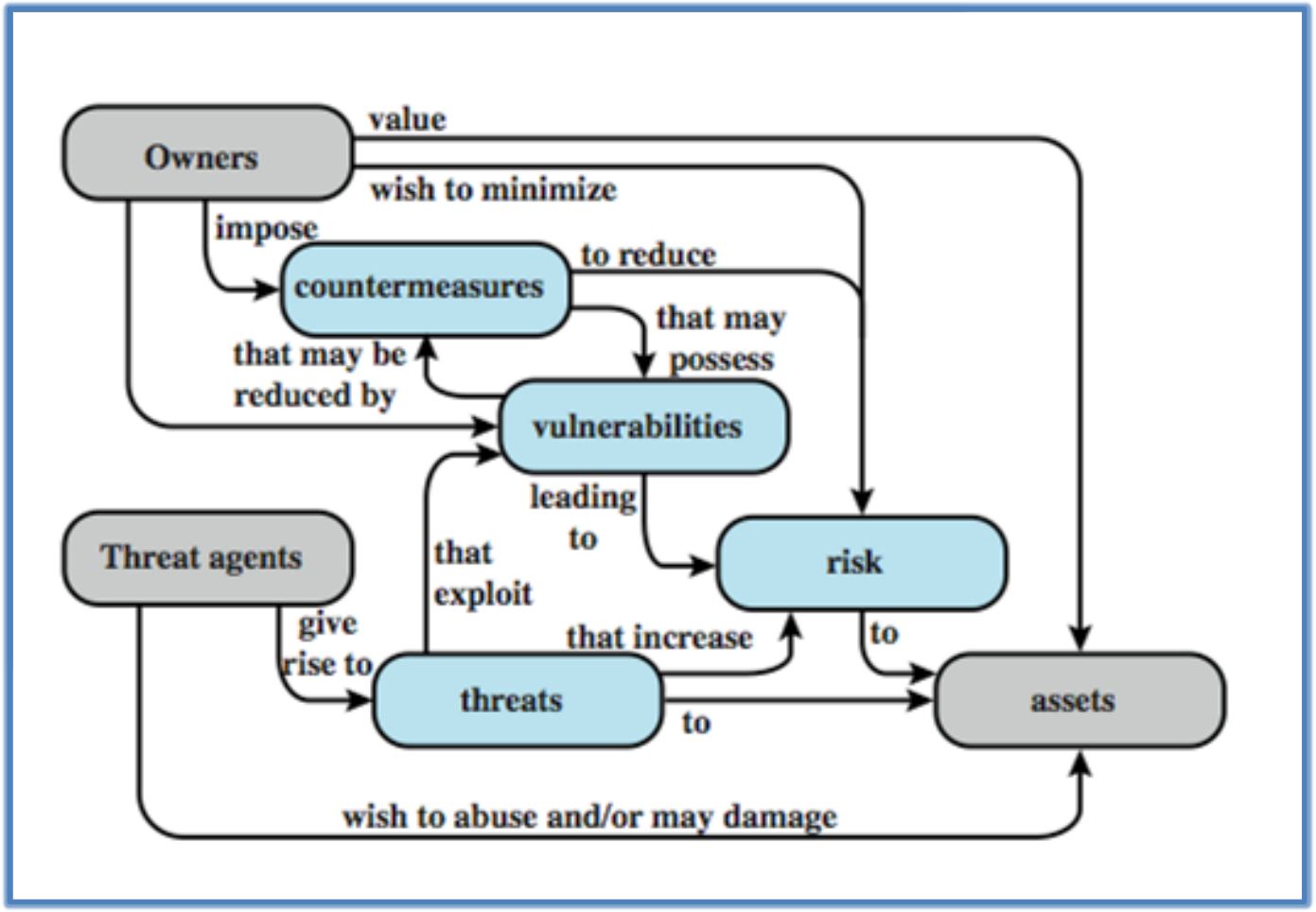
- 컴퓨터 보안은 초보자들에게 보이는 것 만큼 간단하지 않음
- 보안 특성들에 대한 잠재공격 가능성을 반드시 고려해야 함
- 특정 서비스를 제공하기 위한 처리 과정은 예외가 발생될 수 있음
- 물리적 배치와 논리적 배치를 어떻게 하여 사용할 것인가를 판단해야 함
- 보안 메커니즘은 특정 알고리즘 혹은 프로토콜을 포함
- 공격자는 하나의 취약점만 찾아내면 되지만, 방어 측면에서는 모든 취약점을 발견하여 없애야 함
- 사용자와 시스템 매니저는 문제가 발생할 때까지 보안의 필요성에 대해 간과하고 있음
- 보안은 정기적으로 지속적인 모니터링이 요구됨
- 보안을 설계 뒷전의 업무로 간주하고 있음
- 보안은 작동의 편의와 효율성에 방해가 될 것이라는 관념이 있음

컴퓨터 보안 용어

용어	의미
공격자	시스템을 공격하거나 위협하는 존재
공격	시스템의 보안 서비스를 회피하여 보안 정책을 위반하려는 의도된 시도
대응	위해를 최소화하거나 적절한 대응을 위해 탐지, 보고하여 위협, 노출, 공격을 제거하거나 방지하는 행위, 장비, 기법
위험	특정 위협이 가져올 확률적으로 표현되는 예상되는 손실
보안 정책	시스템이나 기관이 민감하고 중요한 시스템 자원들에 보안 서비스를 제공하기 위해 명시한 규정과 업무
시스템 자원 (자산)	정보 시스템내의 데이터, 시스템의 서비스, 처리 기능, 통신 대역폭, 시스템 장비(하드웨어, 펌웨어, 소프트웨어, 문서), 시스템 장치 설비
위협	보안을 침해하고 손해를 가져올 수 있는 상황, 행위, 이벤트가 존재할 때 잠재적 보안 위반
취약성	시스템 보안 정책을 위반할 수 있는 시스템 설계, 구현, 혹은 운영, 관리상의 오류 혹은 약점

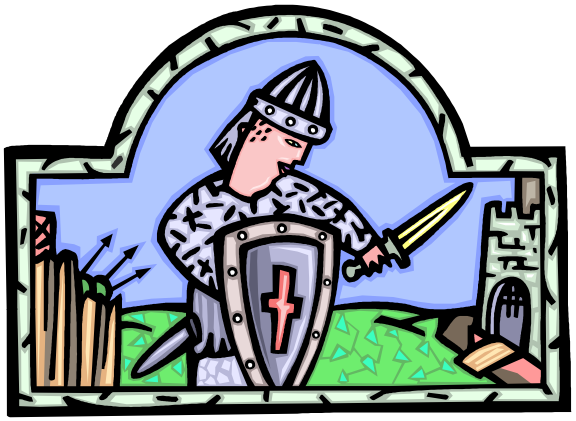
소스: RFC 2828, internet Security Glossary May 2000

보안의 개념과 관계


Owners
value
wish to minimize
impose
countermeasures
to reduce
that may
possess
that may be
reduced by
vulnerabilities
leading
to
Threat agents
that
exploit
risk
give
rise to
that increase
to
threats
to
assets
wish to abuse and/or may damage

취약성, 위협 및 공격

- 취약성의 범주
  - 오류 (무결성 상실)
  - 유출 (기밀성 상실)
  - 작동 불가 혹은 속도 저하 (가용성 상실)



- 위협
  - 취약점을 악용하는 위협
  - 보호해야 할 자산에 해를 끼치는 위협
- 공격 (위협을 이행하는 행위)
  - 수동적 공격 – 시스템 자원에는 영향을 미치지 않는 공격
  - 능동적 공격 – 시스템 자원을 변경하거나 시스템 동작에 영향을 미치려는 시도
  - 내부공격 – 보안 경계 내에서의 공격
  - 외부공격 – 보안 경계 외부에서의 공격

위협의 결과	위협행위(공격)
▪ *비인가 노출 (unauthorized disclosure)* 허가되지 않은 데이터에 대한 접근을 획득하게 되는 상황 혹은 이벤트 → 기밀성	- 노출(exposure): 민감한 데이터가 비인가 된 존재에게 직접 노출 - 도청(interception): 인가된 송수신자 사이에 전송되는 민감한 데이터에 대한 직접적 접근 - 간섭(interference): 비 인가된 사용자의 통신의 특성과 부산물 등을 이용한 민감한 데이터에 대한 간접적인 접근 - 침입(intrusion): 비 인가된 사용자가 시스템 보안 보호벽을 뚫고 민감한 데이터에 대해 접근
▪ *기만(deception)* 인가된 사용자가 잘못된 데이터를 옳은 데이터로 착각하는 환경 혹은 이벤트 → 무결성	- 매스커레이드(masquerade): 비인가된 사용자가 인가된 사용자인 것으로 가장 - 변조(falsification): 잘못된 데이터가 인가된 사용자를 속임 - 부인(repudiation): 행위에 대해 부인함으로써 다른 사용자를 속임
▪ *분열(disruption)* 시스템 서비스와 기능들의 바른 동작을 막는 환경 혹은 이벤트 → 가용성, 무결성	- 무력화(incapacitation): 시스템 컴포넌트 불능화를 통해 시스템 동작을 방해하거나 중단시킴 - 오염(corruption): 시스템 동작, 기능, 데이터를 원치 않는 방향으로 변경 - 방해(obstruction): 시스템 동작을 막아서 시스템 서비스 수행을 중단시키는 위협행위
▪ *횡령(usurpation)* 비 인가된 사용자에게 시스템 서비스나 기능을 초래하는 환경이나 이벤트 → 무결성, (기밀성)	- 전용(misappropriation): 시스템 자원에 대해 허가되지 않은 논리적, 물리적 점유 - 오용(misuse): 시스템 보안에 해롭게 동작하는 기능이나 서비스를 수행하는 시스템 컴포넌트의 초래

Table 1.2

위협 결과

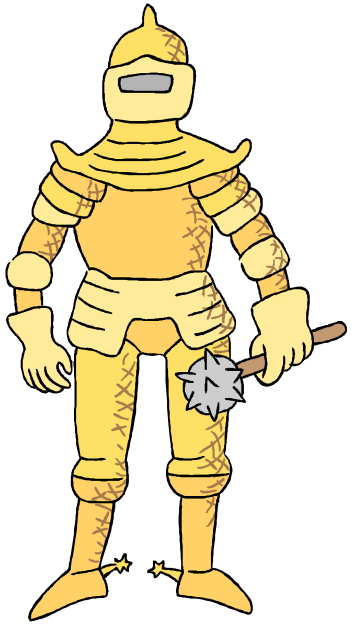
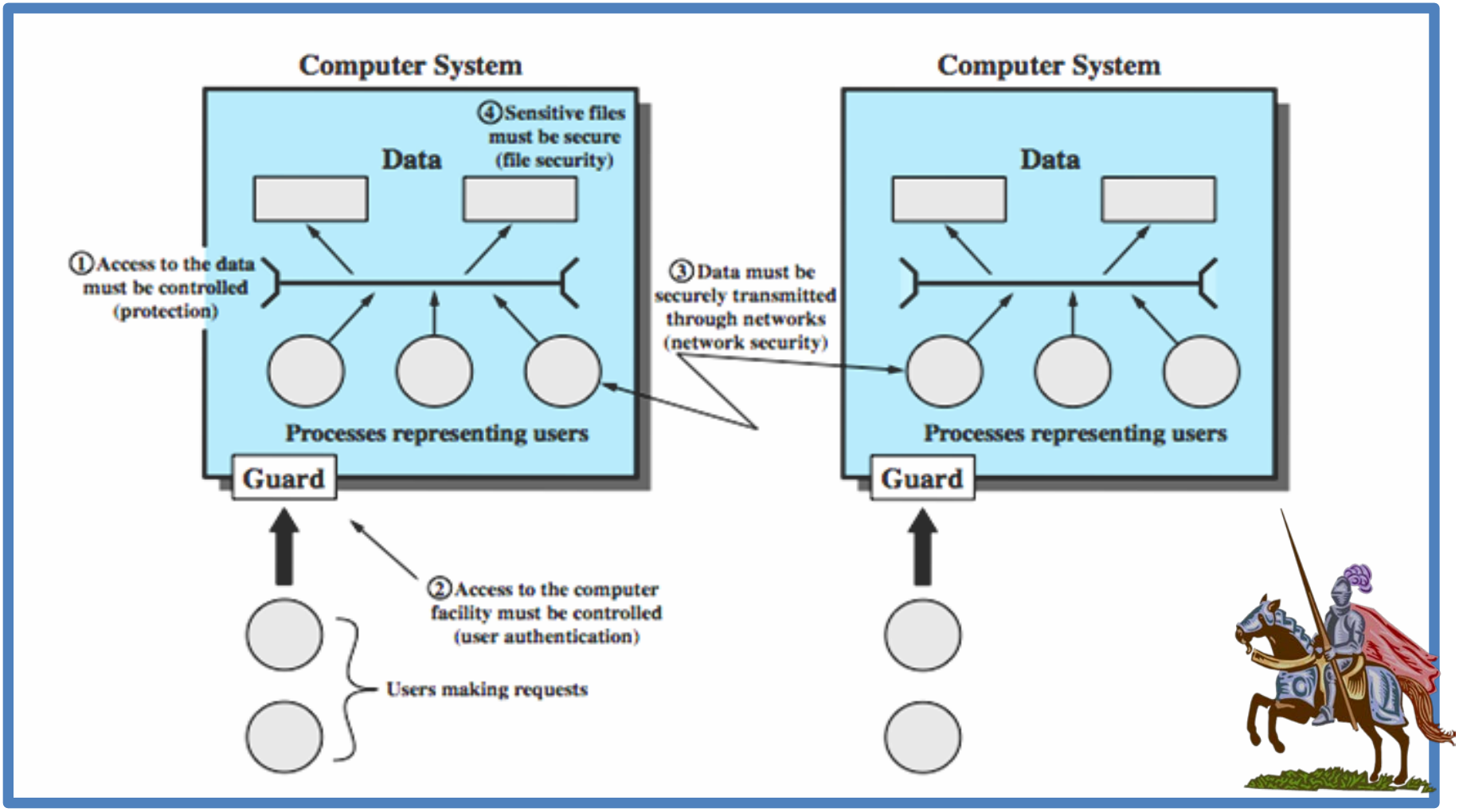
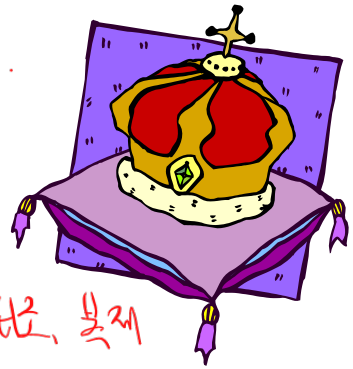


그림 1.3
컴퓨터 보안 범위



컴퓨터와 네트워크 자산과 위협예제



	가용성	기밀성	무결성
하드웨어	장비가 도난 되거나 불능 상태가 되어 서비스가 제공되지 않음		
소프트웨어	프로그램이 삭제되거나 사용자 접근이 거부됨	소프트웨어 불법복제	수행중인 프로그램이 변경되거나 의도되지 않은 작업을 수행
데이터	파일이 삭제되어 사용자 접근이 거부됨	데이터 불법도청, 통계적 분석으로 데이터 내용이 분석	기존 파일이 수정 혹은 새로운 파일이 위조됨.
통신라인	메시지가 삭제됨. 통신라인 혹은 네트워크가 불통됨	메시지 불법도청, 트래픽 패턴이 관찰됨	메시지가 수정, 지연, 재정렬, 복제. 허위 메시지가 제작

소극적 공격과 적극적 공격

- 소극적 공격은 시스템으로부터 정보를 도청하여 얻거나 그 결과로 얻은 정보를 사용하는 시도들을 말하며, 시스템 자원에는 영향을 끼치지 않는 공격을 의미함
  - 탐지가 어려움
  - 탐지보다는 예방을 강조
  - 소극적 공격의 2가지 종류:
    - 메시지 내용 방출
    - 공격을 위한 트래픽 분석
- 데이터 흐름의 변경을 포함하는 적극적 공격
  - 예방이 어려우며 이를 탐지하여 복구가 필요함
  - 적극적 공격의 4가지 종류:
    - 위장
    - 재전송
    - 메시지 변조
    - 서비스 거부

표 1.4
(FIPS PUB 200)
보안 요구사항

접근 제어(Access Control): 시스템 정보의 접근을 허가된 사용자, 인가된 사용자를 대신한 역할을 수행하는 프로세스, 장비(다른 정보 시스템 포함), 또는 인가된 사용자가 허가한 기능과 트랜잭션에게만 허용.

인식과 교육(Awareness and Training): (i) 정보 시스템의 사용자와 관리자가 그들의 행위에 대한 보안 위험과 관련 법규, 규정, 정보 시스템의 보안 정책을 인식; (ii) 보안 관련 업무 수행을 위해 부여된 임무에 적절한 훈련

회계 감사와 책임(Audit and Accountability): (i) 모니터링, 분석, 조사, 불법적 행위, 부적절한 정보 시스템 행위 보고를 위해 감사보고서를 생성, 보호, 유지; (ii) 정보 시스템 사용자들의 행동을 개별적으로 추적하여 그들의 행위에 책임을 지도록 함

증명, 인증, 보안 평가(Certification, Accreditation, Security Assessments): (i) 보안 제어가 시스템내의 어플리케이션에 효과적인지 주기적으로 평가; (ii) 조직의 시스템의 결점과 취약점을 보완하기 위해 고안된 행위를 개발하고 구현; (iii) 조직의 정보 시스템 및 연결된 관련 시스템 연결의 작동에 권한 부여; (iv) 제어상의 효율성을 지속시키기 위해 정보 시스템의 보안 제어를 모니터링

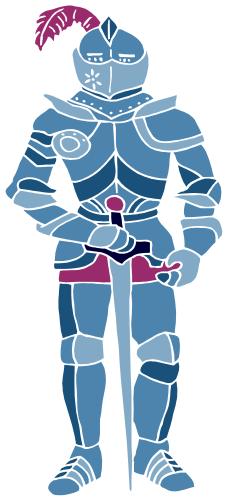
환경 설정 관리(Configuration Management): (i) 기존 구성과 조직의 정보 시스템(하드웨어, 소프트웨어, 펌웨어, 문서)의 재고를 확립하고 유지; (ii) 조직의 정보 시스템내의 정보 기술 생산품들에 대한 보안 환경 설정을 확립하고 강화

비상 계획(Contingency Planning): 조직의 정보 시스템에서 중요한 정보 자원의 가용성과 비상시 동작의 연속성을 위한 비상시의 대응, 백업, 사후 복구 방안을 확립, 유지, 구현

식별 및 인증 (Identification and Authentication): 정보 시스템의 사용자, 사용자의 프로세스, 장비를 식별, 이러한 사용자, 프로세스, 장비를 조직의 정보 시스템 접근허가를 위한 전제조건으로 증명

사고 대응(Incident Response): 충분한 준비, 탐지, 분석, 억제, 복구를 포함하는 조직적인 사고 처리 능력. 적합한 조직의 관리자에게 추적, 문서, 보고

유지(Maintenance): (i) 조직의 정보 시스템에 대한 주기적이고 적절한 유지 및 보수; (ii) 정보 시스템 유지 보수를 수행하기 위한 도구, 기법, 메커니즘, 인력에 대한 효과적인 제어



미디어 보호(Media Protection): (i) 문서나 전기적인 정보 시스템 미디어 보호; (ii) 정보 시스템 미디어의 정보 접근을 허가된 사용자에게 제한; (iii) 폐기나 재사용 전에 정보 시스템 미디어 삭제

물리적 환경적 보호(Physical and Environmental Protection): (i) 정보 시스템과 장치, 허가된 개인에 대한 운영 환경에 대한 물리적 접근 제한; (ii) 물리적 생산설비 보호와 정보 시스템의 인프라 지원; (iii) 정보 시스템에 지원 유틸리티 제공; (iv) 환경적 위험으로부터 정보 시스템 보호; (v) 정보 시스템 설비에 적절한 환경 제공

계획 (Planning): 정보 시스템의 보안 제어와 개인의 행동 규정에 대한 개발, 문서화, 주기적 업데이트, 구현

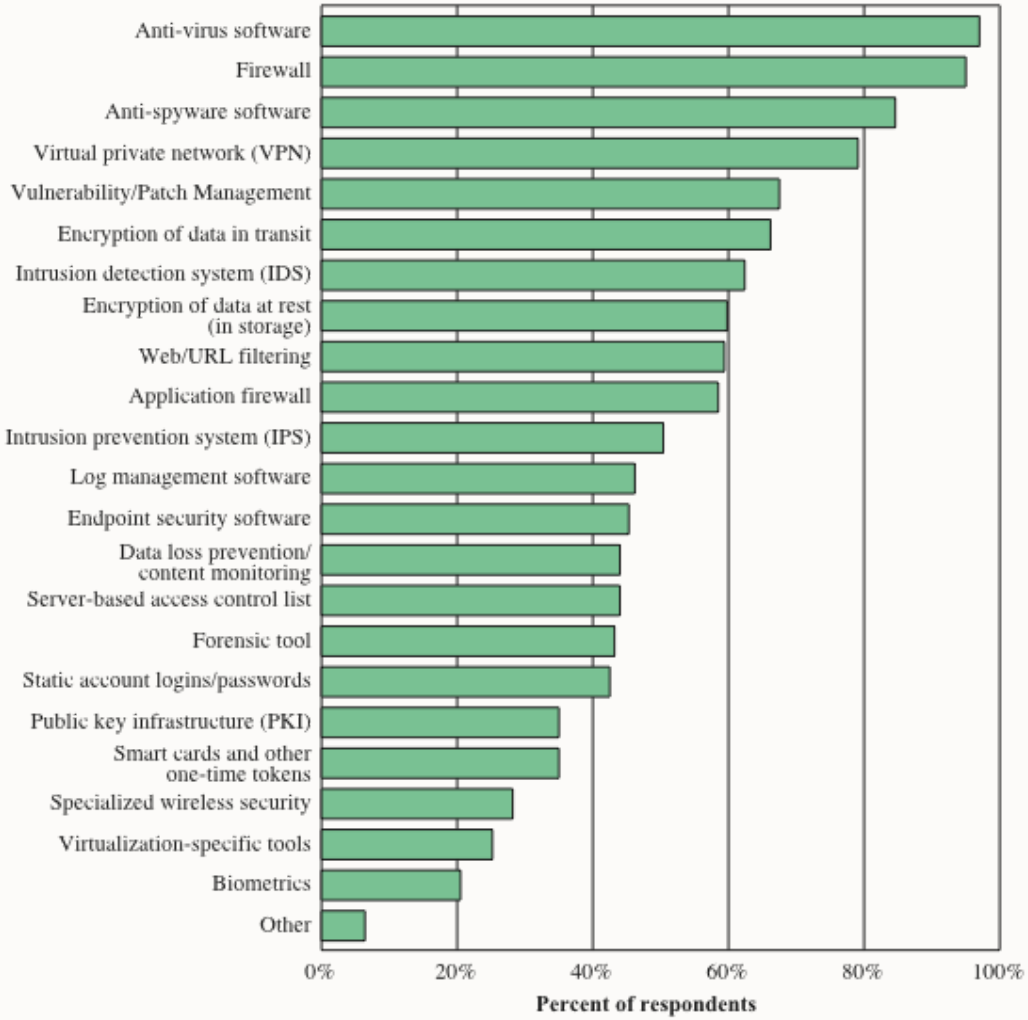
개인 보안(Personnel Security): (i) 조직에서 책임위치를 차지하는 개인이 신뢰할 수 있고 직위의 보안 규정을 만족; (ii) 조직의 정보와 시스템이 개인의 행동에 보호; (iii) 보안 정책과 절차를 준수하는데 실패한 개인에 대한 공식적인 제재 조치.

위험 평가(Risk Assessment): 조직의 운영(미션, 기능, 이미지, 평판), 조직의 자산, 개인, 정보 시스템 동작 결과, 관련된 정보의 처리, 저장, 전송에 대한 위험을 주기적으로 평가

시스템과 서비스 획득(Systems and Services Acquisition): (i) 정보 시스템의 보호를 위해 충분한 자원을 할당; (ii) 정보 보안을 고려한 시스템의 라이프 싸이클 사용; (iii) 소프트웨어 사용과 설치 제한; (iv) 아웃소싱되는 제3자는 정보, 어플리케이션, 서비스에 대한 보안을 측정하는 적절한 도구사용

시스템과 통신 보호(System and Communications Protection): (i) 조직의 정보 시스템의 외부 경계와 내부의 주요 지점에서의 통신을 모니터, 제어, 보호; (ii) 조직의 정보 시스템의 효과적인 정보 보안을 증진시키는 구조적 설계, 소프트웨어 개발 기법, 시스템 공학 원칙사용

시스템과 정보 무결성(System and Information Integrity): (i) 정보와 시스템 오류에 대한 시기 적절한 식별, 보고, 교정; (ii) 정보 시스템내의 적합한 지점에 유해 코드에 대한 보호 제공; (iii) 정보 시스템 보안 경고에 대한 모니터와 적합한 대응에 대한 권고



Source: Computer Security Institute 2010/2011 Computer Crime and Security Survey

Figure 1.5 Security Technologies Used

보안 기술

컴퓨터 보안 전략

명세서 / 정책

하고자 하는것은 무엇인가?

구현 / 메커니즘

어떻게 하는가?

정확성/ 확실성

잘 동작되고 있는가?

보안 정책

- **시스템이나 조직이 민감하고 치명적인 시스템 자원에 제공하는 보안 서비스 방법에 대한 일반적 형식의 규칙이나 관행**

- 고려 사항:
  - 보호하고자 하는 자산의 가치
  - 시스템 취약점
  - 잠재적인 위협과 공격 가능성
- 고려해야 할 절충사항:
  - 사용의 용이성 VS 보안성
  - 보안 비용 VS 오류 및 복구 비용

보안 구현

탐지

- 침입 탐지 시스템
- 서비스 공격 부인 탐지

대응

- 탐지를 통해 공격을 중지시키고 더 큰 손상을 방지함

복구

- 백업시스템의 사용

예방

- 보안 암호 알고리즘
- 암호키에 대해 비인가 된 접근 방지

보증과 평가

- 보증
  - 시스템과 정보를 보호하는 보안 수단의 확신 정도
  - 시스템 설계와 시스템 구현을 보증함
- 평가
  - 컴퓨터 제품이나 시스템을 특정 기준에 준하여 검사하는 과정
  - 테스트 및 공식적인 분석 또는 수학적 기법으로 평가가 이루어짐