어바웃 IT 기술사 7

IT 기술사 과목별 소개
- 보안

글. 강자원 컴퓨터시스템응용기술사
KBS MNC(Media Network Center)팀 (jwings@kbs.co.kr)

연재 목차

1회_ IT 기술사에 대하여(정통, 컴시응, 정관)
2회_ 기술사 수검방식 및 전략(필기, 면접)
3회_ 기술사 공부법(서브노트작성법, 마인드맵)
4회_ SW공학
5회_ 데이터베이스
6회_ 네트워크
7회_ 보안
8회_ 경영정보
9회_ 디지털신서비스
10회_ 컴퓨터구조
11회_ 알고리즘
12회_ 정보시스템감리

최근 업계 전반에서 보안 전문가들은 경계(Perimeter)의 내·외부를 막론하고 어떠한 사용자, 디바이스, 시스템도 신뢰할 수 없다는 제로 트러스트(Zero Trust) 접근방식을 중심으로 전략을 설계하고 재구성하고 있다. 보안은 최근 보안 관련 사고가 잇따름에 따라 최신 트렌드와 관련된 문제가 디지털 신서비스의 과목과 공통영역으로 많이 출제되는 추세다. 오늘날, 업무 처리를 위해 더 이상 사무실에 출근할 필요가 없게 되었다. 기술의 발전을 통해 이제 직원들은 '사무실'로 통칭하는 공간에 구애받지 않고 모바일 기기와 클라우드 소프트웨어를 통해 어디에서나 업무를 처리할 수 있게 되었다. 그러나 이러한 발전은 동시에 기업에 사이버 보안의 딜레마를 안겨준다. 보안 경계(Perimeter)는 더 이상 사무실 건물의 벽으로 국한되지 않으며, SaaS 애플리케이션, IaaS, 데이터센터, 원격 사용자, IoT 디바이스 등을 통해 중요한 비즈니스 데이터가 지속해서 전송되고 있다. 이는 사이버 범죄자가 그 어느 때 보다 광범위한 공격 표면(Attack surface)과 더 많은 진입점(Points of entry)으로 접근할 수 있게 되었음을 의미한다. 이에 대한 증거로, 2018년 사이버 공격의 34%가 내부자의 소행으로 밝혀졌다.

설상가상으로, 이러한 사이버 범죄자들은 기업 내부 보안 경계 내로 침입한 이후 적발되기 전까지 수개월에 걸쳐 기업의 민감한 중요 데이터를 유출하였고 실제로, 대부분 기업이 데이터의 유출 사실을 알아차리기까지 6개월의 시간이 걸렸다. 걱정스럽게도, 대부분의 기존 보안 인프라는 이미 세대에 뒤처져 있으며, 막아내야 할 공격의 수준보다 위험할 정도로 뒤처져 있다는 것이 사실이다. 명백히, 이제 새로운 보안 패러다임이 필요한 시기가 도래했고 이러한 흐름에 따라 기업에서 IT 기술사들은 CSO(Chief of Security Officer)로서 그 역할과 책임이 더욱 막중해졌다 볼 수 있다.

보안은 무엇인가?

보안과 보호의 의미를 구분할 필요가 있다. 정보보안과 정보보호는 어떤 의미일까? 보안(Security)이란 가치 있는 유무형 자산의 도난, 손실, 유출로부터 보호하는 것을 말하며 보호(Protection)란 주로, 보안보다 광의의 의미로 사용되며, 전체 시스템의 안정성을 확보하는 것을 의미한다. 즉, 정보보호 또는 정보보안은 정보의 수집, 가공, 저장, 검색, 송신, 수신 중 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 수단을 강구하는 것을 의미한다. 보안을 확립하는 구성요소로 말하는 방식에는 보안 삼각형이 있다. 보안 3원칙은 보안 목표이기도 하며 C.I.A Triad(보안 삼각형)로 표현한다.

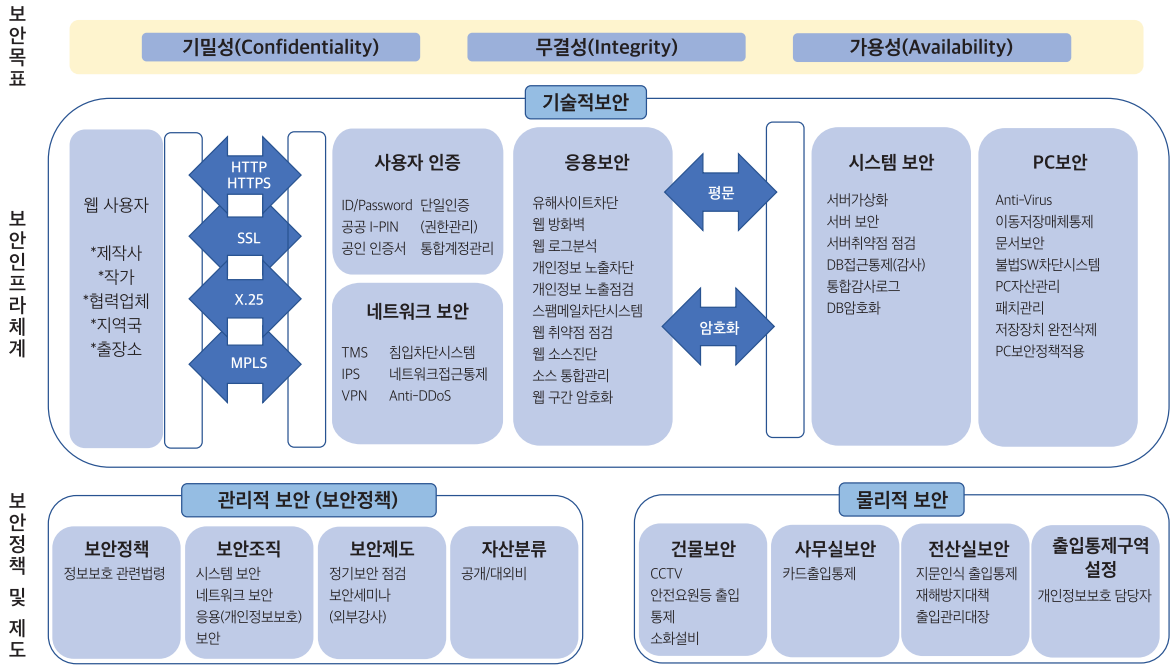
1. 기밀성(Confidentiality)은 인가된 사용자만 정보자산에 접근하는 것을 의미하고
2. 무결성(Integrity)은 적절한 권한을 가진 사용자에 의해 인가된 방법으로만 정보를 변경할 수 있도록 하는 것이며
3. 가용성(Availability)은 정보자산에 대해 적절한 시간에 접근 가능한 것을 의미한다.

조금 더 쉽게 설명해보면, 기밀성이란 방화벽 암호나 패스워드 같은 것들인데 정당한 사용자만 접근할 수 있게 해서 정보를 안전하게 보호하는 것을 말한다. 도청, 도난 등의 기법으로 침해될 수 있다. 무결성은 오직 정부(적절한 권한을 가진 사용자)만이 한국은행을 통해(인가된 방법으로만) 만들거나 바꿀 수 있고 그렇지 않은 경우 (무결성이 훼손될 경우) 위조지폐로 취급돼 엄중한 처벌을 받을 수 있는 경우로 정보가 변조되지 않도록 보호하는 것을 의미하며 마지막으로 가용성은 예를 들어 24시간 편의점에 밤이든 낮이든 무엇인가 필요할 때 항상 얻을 수 있는 상황 즉 언제나 가용을 의미하는 것으로 내가 원할 때 얼마든지 서비스를 이용할 수 있는 것을 의미한다.

보안 아키텍처를 통해 본 보안 과목의 세부 범위

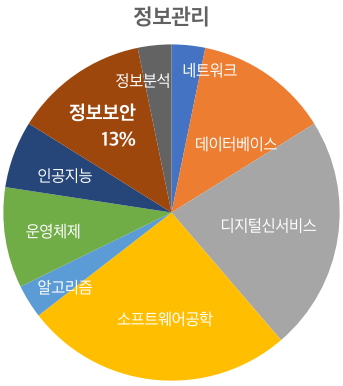
아주 간단히 우리 기업의 정보보안 아키텍처를 외부와 내부 그리고 연계하는 구역을 기준으로 나누게 된다면 다음 표와 같다. 그리고 각각 세부적으로 해당하는 섹션을 시스템 관점으로 분류해보았고 그에 상응하는 기술들을 열거해 보았다. 본인이 사용하는 서비스와 응용프로그램들을 떠올려보면 해당하는 것들이 어느 섹션에 어느 기술에 속하는지 아주 쉽게 이해가 될 것이다. 이렇게 보안 과목을 준비할 때는 러프하게 표와 같이 준비해볼 수도 있지만 다음과 같이 전사적인 보안 거버넌스 관점의 아키텍처를 설계한다면 다음장의 아래표와 같을 것이다. 전사적인 보안 거버넌스란 기업이 보안에 대해 목표와 정책을 수립하고 이에 따라 해당 기술의 아키텍처를 적용한 보안 참조모델 또는 전체적인 구조와 틀이라 이해하면 되겠다. 이렇게 보안 거버넌스 또는 보안 참조모델이 있는 기업의 보안은 매우 탄탄하다 볼 수 있다. 해당 정책을 가지고 그 정책에 따라 룰을 적용하는 것은 매우 일관

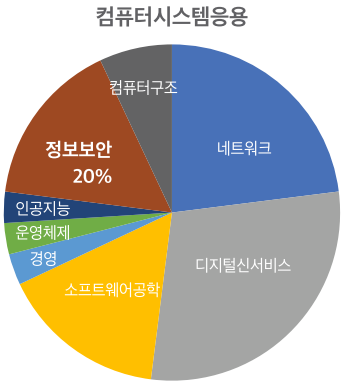
되게 보안시스템을 운영할 수 있으며 관리가 매우 용이하다. 각각의 큰 섹션을 기준으로 세부 과목들을 학습하고 또 관련 기술요소들을 정리하는 방향으로 학습하면 될 것이다.



보안 과목의 출제 비중

가장 최근 117회 기출문제를 통해 정보관리 종목과 컴퓨터시스템응용 종목에서의 보안 문제 출제 비중을 보면 다음과 같다.





보안 과목은 정보관리 종목 및 컴퓨터시스템응용 종목 모두 출제 비율이 비슷하다. 117회 시험에서 정보관리 종목에서는 5문제가 컴퓨터시스템응용 종목에서는 6문제가 출제되었다. 컴퓨터시스템응용 종목에서 좀 더 비중이 높은 것으로 보이지만 실제로 출제되는 문항 수의 비율은 거의 비슷하다 볼 수 있다. 그만큼 보안 과목은 중요하다. 시험뿐만 아니라 이 글의 서두에서도 언급했다시피 트렌드에 따른 모든 기술에 언급되는 것이 보안이기 때문이다.

기출문제를 통한 실전 보안 문제

117회 기출문제를 통해 보안 과목 출제 경향을 알아보자.

[정보관리 117회]

회차	교시	문제
117회	1	1. HMAC(Hash-based Message Authentication Code)
		3. 양자암호통신
	3	5. CCTV 통합 관제센터의 폐쇄회로화면(CCTV) 개인영상정보 보호방안에 대하여 설명하시오.
	4	5. 디지털 포렌식의 증거수집기술과 증거분석기술에 대하여 설명하시오.

[컴퓨터시스템응용 117회]

회차	교시	문제
117회	1	2. 양자정보통신에서 양자(Quantum)의 특성
		12. IPsec
	2	6. 메시지 인증 기법과 디지털 서명 기법에 대하여 설명하고 공통점과 차이점에 대하여 설명하시오.
	3	5. IP 터널링 기술에 대하여 설명하시오.
		6. SSL(Secure Sokets Layer) 프로토콜에 대하여 설명하시오.
	4	1. 2018년 5월 25일부터 시행된 EU(유럽연합)의 개인정보보호 법령인 개인정보보호규정(GDPR: General Data Protection Regulation)에 대해 우리기업도 대응해야할 필요성이 있다. 아래 사항에 대하여 설명하시오. 가. 2018년 5월에 시행된 GDPR 관련 주요 변경 사항 나. GDPR의 주요 골자 다. EU GDPR과 한국 개인정보보호법 비교 라. 우리기업의 준비사항

보안 과목 어떻게 준비해야 할까?

[출제 경향]

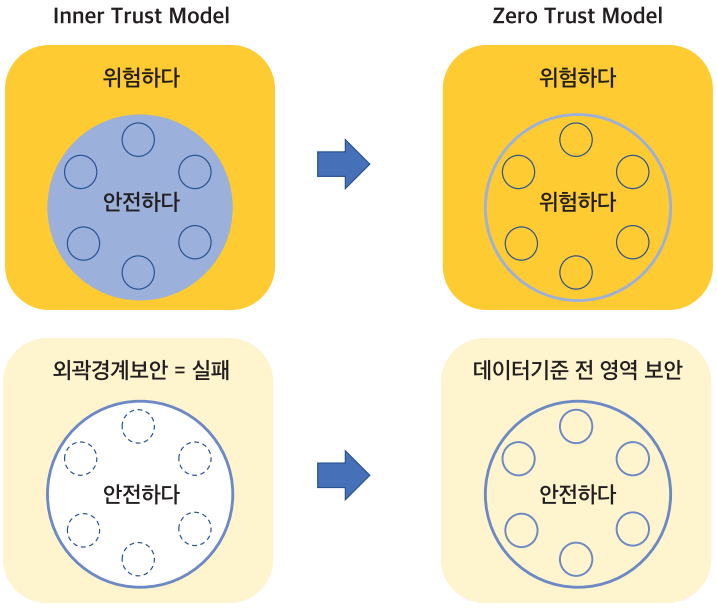
- 보안에 대한 관심이 높아지면서 보안 분야의 출제 비중이 높아지고 있다.
- 보안 분야는 디지털 서비스의 새로운 기술이 발표되면 관련하여 보안 기술, 문제점 및 이슈, 해결방안에 대한 문제가 비슷한 시기에 출제된다.
- 신기술 관련하여 법 제도가 새로 생기거나 개선되고 가이드라인들이 발표됨에 따라 관련 문제들이 출제되고 있다.
- 보안 관련 사고나 이슈가 도출된 토픽, APT, 랜섬웨어 등과 관련된 기반 기술들이 출제되고 있다.
- 암호, 알고리즘 등 기본 토픽에 대한 내용도 꾸준히 출제되고 있다.

[학습 방향]

- 최근 대두되고 있는 신기술 학습 시 보안관점도 함께 학습하라.
- 보안사고, 보안트렌드와 이슈 및 문제점과 이를 해결하기 위한 법제도, 가이드라인, 기반보안기술 등에 대한 학습이 필요하다
  - 정보공학회지, 전자신문, 디지털타임즈, 주간기술동향, KISA 자료, 정보보호학회지 등
- 암호화 알고리즘, SW 취약점, PKI 등에 기본토픽을 정확히 학습하여야 기반 기술들에 대한 대응이 가능하니 기본에 충실할 것!

보안에 대한 방송기술인들의 이해와 접근 방식

기술사 시험이 아니더라도 우리 방송기술인들이 이것만은 알고 있었으면 한다. 적어도 방송기술인들 만큼은 보안에 대해 일반인들보다는 조금 더 깊은 이해를 바탕으로 했으면 하는 바람으로 적어본다. 서두에도 적었지만 최근 "아무도 믿지 마라!", '제로 트러스트(Zero Trust)' 보안론이 제시되고 있다. 제로 트러스트. 시스템 외부와 내부를 따로 나누지 않고 모든 곳이 위험하다고 전제하고, 적절한 인증 절차 없이는 그 누구도 믿어서는 안 되며, 누구든 시스템에 접근하려면 권한을 부여하기 전에 재차 신원을 확인해야 한다는, 어찌 보면 원래 그랬어야 했던 당연한 이야기가 새삼스럽게 요란한 것 같기도 하다. 하지만 이렇듯 깔끔하게 용어 하나로 딱 정리되니 그 계몽적 집중 효과는 기대해 볼 만하겠다. "같은 직원끼리 뭐 절차를 이렇게 복잡하게 해?" "우리가 한두 해 같이 일하나요?" 사실 보안사고의 대부분은 내부자를 통해 일어난다는 점이다. 주로 거론되는 '제로 트러스트' 방법론은 보안을 바라보는 관점과 정책에 집중된다. 시스템 전체를 한꺼번에 지켜야 할 하나의 큰 덩어리로 보지 않고 모든 부분을 '미세-분할(micro-segmentation)' 요소로 나누고, 각 요소에 대해 '과립형 경계 시행(granular perimeter enforcement)' 방식으로 보안을 적용해야 한다는 '제로 트러스트' 모형은 보안의 관점과 정책 문제다.



데이터 접근은 엄격히 제한하되, 사용자 편의성은 낮아지지 않아야 한다. 절차가 너무 복잡하면 효율이 급격히 저하된다. 그에 따라 불편이 핑계인 편법이 만연하게 되는데, 이를 단지 개인의 보안 의식 부족 탓으로만 모는 지적은 결국 쓸데없는 헛된 말로 그치고 마는 게 현실이다. 인간은 뭐든 조금이라도 불편하면 무조건 편한 방법을 찾기 마련이니까. 필자가 이렇게 제로 트러스트 모델에 대해 자세히 말하는 까닭은 우리가 방송제작 및 송출 그리고 유통과 관련하여 전 영역의 IT 시스템화를 하고 있음에도 불구하고 아직도 보안에 대한 의식은 매우 낮기 때문이다. 이번 글을 통해 보안에 대해 전체적으로 다양한 관점에서 볼 수 있는 시야를 갖기를 바라며 또 방송 IT 현장에서 적용할 수 있는 제로 트러스트 기반의 보안참조모델을 만들 수 있는 역량 있는 기술사가 방송기술인 중에 배출되길 희망해본다. **[마인드맵 첨부]**

다음 호에서는 경영정보 과목에 대해 알아보겠다. 종목별 경영정보 과목의 출제 비중과 실전에서 어떤 문제들이 출제되며 또, 고득점을 위해서는 어떤 형식으로 답안을 기술해야 하는지에 대해 알아보도록 하겠다.

참고문헌

KPC 기술사회 네이버 카페 자료실(https://cafe.naver.com/81th) / https://www.zdnet.co.kr/view/?no=20190610114522

보안위협

정보화 역기능(유비쿼터스 5대 위협) : 감(Little Sister)/사/바/개/사
정보보안 공격 : 정보수집→침입→공격전이

응용 취약

Buffer Overflow : SUID 권한 프로그램 공격
-유형 : Local(루트권한)/Remote(RPC, FTPD)
Zero day Attack
XSS(Cross Site Script)
-유형 : 반향식(CSRF/요청변조), 저장(서버동작)
SQL Injection
-유형 : Authentication Bypass(or '1'='1'), OS Call, Query Manipulation
Drive By Download
-유형 : Plug-In API, 브라우저(스크립트)
trap door : 은닉 프로그램/모듈 진입 통로

악성 프로그램

바이러스 : 자기증식, 복제, 은닉, 기생
-유형 : Appended(Head, Head/Tail), Mixed
트로이목마
-특징 : 정상 프로그램 가장
-기술 : Server, Client, Plug-in, Port 점령
Worm : 독자, Poly/Meta-morphic
-Stuxnet : 사이버미사일, 산업시설 공격 원
Spy-ware : 정상행위 방지
Ransom-ware : 암호화/기능제한, 금품요구
Bot : Bot Master 명령을 기다리는 좀비PC
Roolkit : 침입사실 은폐, 차후 침입 지원 P
Auto Program : 게임을 스스로 플레이
-Out of Game : 패킷분석, 소스분석
-In Game : 메모리분석, 그래픽분석

네트워크 취약

Sniffing : 동일 서브넷 도청
-Promiscuous
Session Hijacking(Man in the Middle)
Replay Attack
-절차 : Sniffing→메시지변경→전송
Pharming
-방법 : 도메인 탈취, 호스트 파일 변경
Spoofing
-유형 : IP(B/NB)/ARP(arp cache)/DNS/email
DoS(Denial of Service)
-Mail Bomb, BO, Tear Drop, Ping Of Death Syn Flooding, UDP Storming, Smurfing
DDoS
-구성 : Bot Net, Command&Control Server
-Bandwidth/PPS Consuming, Httpd Flooding
-대응 : DNS Black, Sink Hole(ITU-T X.1205)
-변형 : DRDoS, CC, HTTP Pipeline, PDoS

기타

사회공학 : 인간관계 상호신뢰 바탕
-Phishing(MIM/Key Logger/Screen Grab/XSS)
-Whaling(유명인, 기관단체의 특정인물 타겟)
Flaming(언어 일탈, 비대면/표현자유/광범위)
PW : exhaustive/Dictionary/시스템File(PWSalt)
Salami Attack : 금액여분 누적, 이체
Ever Cookie(악성쿠키 분산저장)
Tempest Attack(키보드-본체 전자기파 검출)

OWASP
-기준 : 위험평가 방식(알려진 정도, 탐지용이, 공격용이, 기술영향)
-10대위협 : 인X취객C보안U불감
사이버 경보수준 : 심각(R)→경계(O)→주의(Y)→관심(B)

⇩파악

보안분석

Honey-Pot
-Server : Data Control, Data Capture, Data Collection
-Client : Low Interactive(정적), High Interactive(동적)
NMS
RPD(Realtime, Preactive, Image Spam 처리)
-Bulk(1toN), SPAN(NtoN), Virus

기업 인증

ISO 27000
-1(BS7799 P2, '99)→ISO27001('05)
-2(BS7799 P1, '95)→ISO17799('00)→27002('07)
-0(규직/용어), 1(요구/규격), 2(실행지침), 3(RM), 4(메트릭/측정), 5(실행가이드), 6(DRS)
-통제영역 : 정/조/분/인/물/접/사/연/개/운+ 준
ISMS
-관리과정 : 정책/범위/위험/구현/사후
-보호대책 : 정/조/분/인/물/접/사/연/개/운+ 훈/모/외/암/거
-문서화 : 요건, 통제, 운영기록의 통제
e-Privacy(i-Safe, 한국정보통신산업협회)

개인정보 인증

BS 10012(DPA 대응, '00)
-Scope/Concept/Plan/Do/Check/Act
PIMS(3개분야, 119 통제항목)
-관리과정 : 정책/범위/위험/구현/사후
-보호대책 : 정/조/분/교/인/침/기/물/감
PIA(Privacy Impact Assessment)
-사전분석(필요성검토, 주체선정, 계획수립)
-관리현황분석(자료수집/흐름분석/개선안도출)
-결과정리(개선계획수립, 보고서 작성)

CC(TCSEC+ITSEC) : CCRA(CAP, CCP)
-구성 : 소개/일반, 보안기능요구, 보증요구사항, EAL(부/기/구/시/설/준/검/정)

정보보안 산업/지침

보안산업 : 정보보안, 물리보안, 융합보안
Smart phone 안전수칙(방통위)
-의다/신사/불메/비변/무선/이상/검사/백신/변경/최신
SNS 개인정보 보호수칙
-사업자 : 공개설정 최소화, 온라인 행태정보 보호, 미성년 보호, OPEN API 개인정보 관리
-사용자 : 신중한 정보공개, 모르는 타인과 친구맺기 자제, 위치/이동경로 노출 주의

Authorization

생체인식(보편성, 영구성, 독특성, 획득성, 저항성, 수용성)
-유형 : 생체(지문/얼굴/망막/홍채/정맥), 행동(음성/서명)
-성능 : FAR, FRR, CER, 등록/검색 시간
-카드 : Store On Card, Match On Card, Sensor On Card
-표준화 : ITU-T X.1086(보호 가이드), X.bhsm(바이오인증FW), X.tif(원격의료 FW)
음성인식
-목적 : 음성분석, 음소분석, 단어인식, 문장해석, 의미추출
-화자 : 화자종속, 화자독립, 화자적응
-기술 : 끝점검출, 특징추출, 잡음처리, 채널보상, 탐색

Open ID(ID 2.0)
-구성 : Relying Partner, Open ID 서버, User Agent, Identify
OTP
-OPT 인증서버, Secret, Seed, Function, OTP 생성매체
-OTP 서버구성 : 단일, 중앙집중, 확장중앙집중, 크로스도메인
-OPT 생성매체 : 비동기, 동기(시간, 이벤트)
SSO : Delegation, Propagation
Mobile ID
-유형 : ID/PW, 지불수단, 인증수단, 전자신분증, 개인정보
-기술 : 보안(Life, 인/접, RF), 기반(추/익/협), 응용(P, 인증)
Smart Wallet

Access Control

DAC(Discretionary) : CL, ACL
MAC(Mandatory) : CBP(부서타겟 허가), MLP(Clearance 부여)
RBAC(Role Base) : 핵심, 계층, 제약
Access Control 원칙
-최소권한, 명허않금, 명금않허, RM, 권한분리
Access Control Model
-Bell-Lapadula(기), Biba(무), C&W(금융), Access Matrix
Access Control 개발절차(OM-AM)
-모델 : Objective, Model, Architecture, Mechanism
-절차 : 요분→기존모델적용평가→수정/활용→구조수립→기술정의

EAM : 통합 접근제어 관리
-구성 : SSO, PMI, 보안정책, 디렉토리
-기능 : 사용자인증, 접근통제, 개인화속성, 관리위임, 모니터링
IAM
-3A 지원 : Authentication, Authorization, Management
-프로비저닝, AC, 정책관리, 통합저장, 워크플로어, 감사, 보고
PMI
-X.509 V4에서 FW 소개, ITUG PKIX WG, ITU-T-SG8 주관
-요소 : SOA, AA, PH, PV, AC → 구성 : GM, CM, DM, RM

Cryptography

스트림 : 실시간, bit/byte 단위(RC4, SEAL)
블록단위 : 고속, 대량

대칭키	비대칭키
DES(64, 56, 16)	**DH**(이산대수)
3DES(64, 168, 48)	**RSA**(소인수분해)
AES(128, 128/192/256, 10/12/14)	**DSA**(이산대수)
IDEA(64, 128, 8)	**KCDSA**(HAS 160, 이대)
SEED(128, 128, 16)	**ECC**(타원곡선)
HIGHT(64, 8비트, S-Box 제거)	**EC-KCDSA**(타원, 무선)

PKI : PAA/PCA(최상위), CA, RA, Directory(계층/NW/Hybrid)
-인증서 검증 : CRL, OCSP(유효/취소/Unknown), SCVP
-기술 : 공개키, 인증서(X.509), Hash, 전자서명, 대칭키, 암호화
WPKI : 인증서+URL Link, Short Live, ECC, OCSP 인증서 검증
Digital Signature : 기밀성, 무결성, 부인봉쇄, 인증
Dual Signature(Blind Signature) : SET에서 활용
-주문, 지불정보 분리/접근으로 사용자 추적 불가능
Fair Blind Signature : 법원 명령시 익명성 추적 가능
KMI : Key Escrow, 암호/인증서 관리, 자발/강제 키 복구
HASH : SNEFRU, N-NASH, MD4/MD5(128bit), SHA(160bit)
Directory Service(W/Y/G/W)
-구성(DUA/DSA/DAP/DSP/DIB), 프로토콜(X.500(X.500/509)), LDAP)

⇩방법

보안 목표

Ubiquitous Security
-U-Security : 소/인/네
-U-Clean : 건/이/환
-U-Trust : 이/콘/디/서
-U-Privacy : 개/위/의/R
정보보호 목표
-기/무/가/부/인
3D 보안
-정책, 사람, 집행을 통합관리

⇩방법

기업정보보호

SRM(Security Risk Management)
-대상 : 인력, 인프라, 정보, 서비스, 환경(Compliance)
E-Discovery : DAS
DLP : 기업정보 유출 방지
-기능 : 정보분류, 정책/흐름관리, 증거확보, 취약보완
ERM
-구성 : RMS, XrML, IRM Client, 암호화
PMS
-구성 : Distribution Server, Agent, DB, Manager, Test Center

개인정보보호

OECD 개인정보보호원칙
-수/정/이/안/목/공/개/책
개인정보 보호기법
-C : Ad-Broker, 백신/Filer, 쿠키 메니저, Personal FW, Re-Mailer, Trace Remover, Anonymizer(LPWA/Crowds/Onion Routing/Tazan)
-S : VPN, FW
-C/S : PGP, P3P
P3P(Platform for Privacy Preference) : 자기통제권
I-PIN(Internet Personal Identification Number)

보안정책

정부노력 : 개인정보보호법, 국제협력추진
인증제도, 체제정비(조직/강령)
좀비 PC방지법
-설치/제한/삭제/점검/장려
개인정보보호법
-설치/기준/고유/영상/평가/통지/권리/신고
Computer Forensics
-원칙 : 무/정/신/재/연
-수집 : 이미징/덤프/무결성입증
-분석 : 타/삭/비/이/슬/암/덤

목표 ⇨ 대상 ⇦ 정책

⇩적용 ⇩적용

네트워크 보안

인터넷 보안

응용	**S-HTTP** : 전자서명, 암호화, 메시지 인증 **ALS** : S-HTTP + TLS, 부분암호화, 전자서명 가능 **S/MIME** : SMTP 확장 **PEM** : 중앙집중키 **PGP** : 분산공개키
L4	**SSL/TLS** : HSP, CCP, AP, RP **WTLS** **SET** : X.509 V3, 신용카드, 이중서명
L3	**IPSec** : AH, ESP, IKE, SA

VPN : MPLS(RFC2547), IPSec(RFC2401), SSL(TLS)
Tunneling
-프로토콜 : L2(PPTP, L2F, L2TP), L3(IPSec)
Secure OS
-구성요소 : 참조모니터, SKDB
FW : BH, DHG, SR, SHG, SSG, GW/Proxy Server
- Packet Filtering, Application GW(WAF), Stateful Inspection
IDS : 유형(HOST/NW 기반), 분석(Misuse/Anomaly/Reputation)
IPS : Activer, Pro-active
UTM : 다기능 통합 보안관리 시스템
ESM
-유형(Hybrid, Interoperation(OPSEC), Broker 연동)
무선네트워크 보안
-공격 : Packet Sniffing, MITM, Evil Twin, War Driving, Dictionary Attack
-보호 : 물리적, SSID, MAC, WEP, WPA(PSK/EAP), mVPN
-사용자인증 : IEEE 802.1X, 802.1aa, EAP, AAA
-무선정보보호 : IEEE 802.11i, 802.1aa
-핸드오프/로밍 : IEEE 802.11f, 802.11k
AAA(Authentication, Authorization, Accounting)
-유무선 인터넷, VoIP 인증/연가/과금 서비스/서버/FW 중심
-RADIUS(비번만), TACACS+(패킷전체 암호화), DIAMETER(P2P)

디지털콘텐츠 보안

디지털콘텐츠 보호
-소극적 : 법적자각 유도(CCL, Watermarking, Finger-Printing)
-적극적 : 사용제어, 접근제어, 복제방지(CPRM/DTCP/HDCP)
CCL
-구성 : 저작권표시/비영리/변경금지/동일조건변경허락
-확장 : CC0, CC+, Science Commons
DRM : 콘텐츠 보호, 인증/과금, 생명주기 관리
-Packager(RMI), 클리어링하우스, TRM(Temper Register Module)
-EDRM : 기업의 중요자산 보호(Commercial DRM과 비교)
CAS : ECM(CW, 수신조건), EMM(수신자격), Smart Card, STP
XCAS(eXchangeable CAS, Downloadable CAS)
Watermarking
-특징 : 비인지/위조방지/강인성/연약성
-방법 : Spatial Domain, Transform Domain(DCT/DFT)
Finger-Printing(Dual Watermarking) : Robust, Fragile
-공격 : Filtering, Copy, Mosaic, Template Attack
Steganography : 멀티미디어에 정보를 은닉, 비밀메시지 전송
URN : DOI(P/S), UCI(접/개/한)
INDECS : Entity, Parties, Creation, Relation
-스키마 : Abstract, Creation, Commerce, Legal View
XrML : Grant, Principle, Right, Resource, Condition
Tamper-Proofing : 부정조작에 대한 방어기술
-Tampering 감지, 콘텐츠 사용 불가
ICOP : 고인식, 변형에 강인, 특징점(DNA, 고유벡터) 인식

이메일 보안

Spam(대량/일방/목적성)
-전송 : Open Relay, Open Proxy, 악성코드, 메일서버
-차단 : TM → SMTP 단계 차단 → 콘텐츠 단계 차단
-대응 : SPF(Sender Policy FW, 메일서버 DNS 등록)
-정책 : OPT-Out(사후거부), OPT-In(사전승인), 메일등급제
VoIP Spam
-유형 : Call(Invite M), IM(Subject 헤더), Presence(Subscribe M)
-대응 : BL/WL/CB/RB/SIP URL인증

서비스 보안

Web Services 보안
-FW : P/P/S/T/C/F
-표준 : W3C(XML암호화/전자서명/XKMS), OASIS(SAML/XACML)
-XML 전자서명(Enveloping/Enveloped/Detached)
-SAML : 구성(Assertions, Protocol, Binding, Profile)
DB 보안
-사전 : 인증(ID/PW), 접근제어(EAM/IAM)
-접근 : 암호화(API/Filter/Hybrid), 가상View, 허가규칙(DCL)
추론제어(튜플수제한, 연속질의방지, 고의오류삽입, 분할)
-사후 : 흐름제어(디지털/인쇄물 전달 방지), 감사
Virtualization
-위협 : VMM 설계, 통합서버, 물리매체 복합경로, 관리프로그램
-대응 : VMM AC/내부통신 접근 강화, SW 취약 제거, 솔루션
Cloud Computing
-ENSIA 위협요소 : 운상/내침/고실/보위/인손/데위/데식/악사
-대응 : 이동체형 토큰, 속성 AC, 중재자, 다단계 키 구조
Mobile
-물리 : Chipping, Nano Machine, EMP, RF Jamming
-논리 : 바이러스/웜, 메시지폭탄, 논리폭탄, 해킹
-통신 : Sniffing, MITM, DDoS
-대응 : MTM, 원격보안관리, 앱스토어 보안, 모바일 결재
Smart Sign : ActiveX 대체
-원리 : URL Protocol Handler, PKCS#7 호환, smartsign://
RFID
-위협 : Tag, Tag-Reader(도청/접근), Reader-Local(도청, 해킹)
-대응 : Kill, Faraday Cage, Smart RFID, Blocker, Active Jamming
Smart Card
-부채널공격 : Invasive(Micro-probing), non-Invasive(고장이용, 전력분석, 타이밍 분석)
-대응 : 마스킹, 무작위성, 블라인딩
SNS
-공격 : Phishing, Short URL, 악성, ID 도용, 2차정보, 스토킹
-대응 : 기술(필터링/스파이더링 제한), 정책, 사업자, 이용자
전자여권 : 비접촉 IC칩 내장, 보안우수, 심사의 정확/신속성
-보안 : PA, AA, BAC, EAC TA, EAC CA, BD

해결 ⇨ 내재 ⇦