협성대학교 소프트웨어공학과

정보보호

〈정보 보안 개론〉 9, 10, 11, 13 장 내용 정리

이시헌

2025-6-16

9장 정리 시작. (보안 시스템. 11주차.)

1. **인증 시스템**

= 인증하려는 주체를 식별하고 이에 대한 인증 서비스를 제공하는 시스템.

A. 인증 수단

i. 알고 있는 것: ID, PW 등…

ii. 자신의 모습: 지문, 홍채 등…

iii. 가지고 있는 것: OTP, 스마트키, 공인인증서, 신분증 등…

iv. 위치하는 곳: 사용자 IP, 콜백 등… (보조 수단)

2. SSO

= Single Sign On

= 모든 인증을 하나의 시스템에서 수행하는, 기본적인 인증 시스템.

= 인증용 서버가, 복수의 다른 서버의 인증을 대신 처리. (p.395)

A. 예시:

i. 물리적 서버로 SSO 구현: MS Kerberos

ii. 서비스 기반으로 SSO 구현: MS Passport

3. **방화벽**

= 신뢰하는 내부 네트워크와, 신뢰하지 않는 외부 네트워크 사이를 지나는 패킷을, 미리 정한 규칙에 따라 차단하거나 통과시키는 하드웨어 또는 소프트웨어.

A. 접근 제어 방식

i. 패킷 필터링: 패킷 헤더를 분석한다. (3, 4 Layer 에서 동작.)

ii. 프록시: 트래픽 전체를 분석한다. (7 Layer 에서 동작.)

B. 접근 제어 명령 <- 룰셋 설정. 외부, 내부의 IP와 Port 기술.

C. 로깅과 감사 추적 기능 제공

D. 인증 기능 제공

i. 메시지 인증 <- VPN과 같은 신뢰할 수 있는 통신선으로 메시지를 전송하여, 신뢰성을 보장하며 메시지 인증 기능 제공 가능.

ii. 사용자 인증 <- PW, OTP 등을 이용한 인증 기능 제공 가능.

iii. 클라이언트 인증 <- 특정 호스트가 정당한지 검사 가능.

E. 데이터 암호화 가능 <- 보통 VPN의 기능으로 실현.

F. 방화벽의 한계: 바이러스의 차단이 근본적으로 불가능(파일로 감염되기 때문)하고, 대부분의 웜 또한 막기 어렵다. (정상 서비스 포트로 웜이 감염되기 때문) 그리하여 전체 해킹 공격의 30%정도만 방어 가능.

4. 침입 탐지 시스템

= Intrusion Detection System, IDS

= 네트워크를 통한 공격을 탐지하는 장비.

= 내부 네트워크에 대한 해킹이나 악성코드 활동을 탐지하는 장비.

(즉, 정상 경로로 들어오는 공격을 탐지해야 한다.)

= 데이터 수집 + 데이터 필터링 + 침입 탐지 + 책임 추적 및 대응.

A. 동작 위치에 따른 분류

i. 호스트 기반. (HIDS)

= 윈도우나 유닉스 등의 운영체제에 부가적으로 설치 및 운용.

ii. 네트워크 기반. (NIDS)

= 네트워크에 설치된 독립적인 시스템. (일반적으로 'IDS'는 이것.)

B. 침입 탐지 기법

i. 오용 탐지 기법

= 이미 발견된 공격 패턴을 미리 입력해두고 탐지 수행.

ii. 이상 탐지 기법

= 정상 상태를 급격히 벗어나는 경우, 확률이 낮은 일이 발생한 경우를 탐지 수행.

C. HIDS의 설치 고려

i. 일반적으로 HIDS는 유지 관리 비용이 너무 많이 든다.

ii. 그리하여 일반적으로, 웹 서버와 같이 사업 유지에 꼭 필요한 경우만 설치한다.

D. NIDS의 설치 위치

i. 일반적으로 라우터 뒤에 위치한 방화벽의 바로 뒤에 설치하는 것이 좋다. 도식으로 정리하면 다음과 같다.

ii. 내부 네트워크 - NDIS - 방화벽 - 라우터 - 외부 네트워크

5. 책임 추적 및 대응

A. 과거에는 탐지 결과(침입)를 알려주는 수동적인 시스템인 경우가 많았다. 그러나 최근에는 능동적으로 침입자의 공격을 역추적하여, 침입자의 시스템이나 네트워크를 사용하지 못하게 하는 기능이 많이 추가되고 있다. (대응 기능이 추가되는 경우가 많아졌다.)

B. 이처럼 능동적인 침입 탐지 기능을 많이 탑재한 경우를 특별히, IPS라 한다. (Intrusion Prevention System)

6. 침입 방지 시스템 (IPS, Intrusion Prevention System)

= 침입 탐지 시스템 + 방화벽

= 침입을 실시간으로 탐지하고, 방화벽으로 차단하는 능동적인 시스템.

A. 등장 배경

i. 최근 취약점이 발표된 당일에 공격이 이뤄지는, 제로데이 공격이 많다. 그리하여 운영자가 웜이나 바이러스에 대한 차단 프로그램을 모두 업데이트 했더라도, 방화벽과 침임 탐지 시스템으로는 방어가 불가능하다.

ii. 그리하여 침입 탐지 시스템의 실시간 이상 감지를 강화하고, 방화벽에 룰셋을 추가할 수 있도록 하는 것으로 침입을 차단하는 시스템이 등장한 것이다.

B. 침입 탐지 방법들

i. 패킷을 모두 검사하여, 공격 패턴이 있는지 확인. (전통적인 방법.)

ii. 가상 머신을 사용하여 패킷을 직접 실행해 보고, 악성 코드 감염 증상을 보이는지 시험. (패킷에 대한 검사 없이, 가상머신으로 넘겨보는 것.)

C. 설치 위치

i. 일반적으로 방화벽 바로 뒤에 설치한다. NIDS와 동일한 위치 권장.

ii. 최근에는 방화벽 없이 IPS만 설치하기도 한다. 그리고 이 시스템을, 고성능을 위해 하드웨어 칩으로 만들어 설치하기도 한다. (ASIC, Application Specific integrated Circuit. 예: Viruswall)

7. VPN (Virtual Private Network)

= 일반 회선의 일부를, 가상의 사설망으로 분리하는 기술.

= 임대 회선의 대체 기술이다. (논리적으로 임대 회선을 구현. 임대 회선: 인터넷과 같은 그물이 아닌, 단순히 두 지점을 연결하는 통신선.)

A. VPN 장비와 클라이언트(나) 사이의 통신을 암호화 하여, 마치 별도의 통신선으로 연결된 것 같은 효과를 내는 것이 핵심이다. 이때 VPN 장비는 클라이언트를 대신하여 여러 일을 수행할 수 있다.

B. VPN으로 할 수 있는 일

i. 지역 IP 우회:
VPN 장비는 IP를 할당받는다. 이때 클라이언트는 VPN 장비에 접속하여, 해당 장비가 있는 지역의 IP를 사용할 수 있다. (예: 해외에서 국내 온라인 게임 접속 등.)

ii. 접근이 제한된 보안 서버로의 접속:
회사 내부의 특정 보안 영역에 연결된 VPN 장비가 있다고 하자. 이런 장비가 있다면, 어디서든 VPN을 통해 암호화된 통신선을 얻어서, 회사의 보안 영역에 접속할 수 있다.

iii. 원격의 두 지점을 하나의 내부 네트워크로 연결:
두 개의 사설 네트워크 사이에, 2개의 VPN 장비가 있다고 하자. 각 사설 네트워크는 VPN으로 만들어진 통신선에 의해, 마치 하나의 네트워크인 것 처럼 동작할 수 있다.

8. VLAN

= 특정 네트워크 내부에서, 논리적으로 작은 여러 네트워크를 구성하여 독립적으로 작동하도록 구분하는 기술.

A. 구현 방식

i. 하나의 스위치 내부에서:
포트 단위로 스위치가 네트워크를 구분하여, 패킷의 전송가능 여부를 판단한다.

ii. 두 개 이상의 스위치에서:
각 네트워크에 부여된 포트로의 통신을, 다른 스위치로 보내는 '트렁크(trunk) 포트'를 사용하여, 가상의 네트워크를 구현.

9. NAC (Network Access Control)

= 스위치에서 MAC 주소를 기반으로 접근제어를 수행하는 것을 지칭.

= IP 기반의 접근제어 시스템의 발전형태.

= 인가된 MAC 주소만 접근을 허가하도록 하는 것이 기본 동작 방식.

A. 구체적인 구현 방식은 교재의 p.417~419 를 참고할 것.

10. **보안 운영체제**

= 보안 커널(보안기능이 통합된 커널)로 제작된 OS.

A. 시스템의 모든 프로세스를 검사하여, 보안 정책에 위반되는지를 검사한다. (항상 일정량 CPU를 점유한다.)

11. **백신**

= 바이러스, 웜, 등을 탐지하는 SW.

12. **PC 방화벽**

= 운영체제 수준에 설치되어 있는 방화벽.

13. **스팸 필터 솔루션**

= 메일 서버 앞단에 위치하며, 특정 메일을 차단.

= 메일 헤더, 제목, 본문, 첨부파일에서 특정 패턴을 찾아 필터링 수행.

14. DRM

= 문서 암호화 기술.

A. 작동 방식:

문서의 저장 시점에, DRM 모듈을 통해 암호화 하여 보조기억장치에 저장되도록 하는 DRM커널을 운영체제에 삽입한 것.

B. DRM 모듈로 동작하는 하드디스크는 도난 당하더라도 보안상 위험이 적다.

C. 일반적으로 인증서 기반으로 동작한다. 관리자는 권한이 설정된 인증서를 발급하고, 조직 구성원은 그 인증서를 통해 문서에 접근한다.

15. DLP

= Data Leak Prevention

A. 정보 유출을 막는 솔루션을 통칭하는 용어.

B. 구체적인 방식들:

i. 업무용 기기의 USB, CD 등의 매체 사용 차단.

ii. 업무용 기기의 통신 인터페이스 제거. (인터넷, 블루투스 등)

iii. 업무용 기기의 클라우드 서버 통신 차단.

9장 정리 끝. (11주차)

10장 정리 시작. (IoT 보안과 AI 보안. 12주차.)

1. IoT

= Internet of Things

= 사물에 인터넷이 연결되는 것.

A. IoT 제품이 갖는 주된 취약점

i. 인증 메커니즘 부재.

ii. 접근 통제 부재.

B. IoT 제품은, 개발 단계에서 충분한 보안성이 적용되었는지 검증해야만 한다. 악용 가능성이 높기 때문.

2. AI 기술 개요

A. 머신러닝: 정답 제공. 분류 및 회귀 문제 해결.

i. 지도학습

◆ 선형 회귀

◆ 로지스틱 회귀

◆ 서포트 벡터 머신

◆ 결정 트리 & 랜덤 포레스트

◆ 신경망

ii. 비지도학습: 정답 제공 없음. 스스로 데이터를 특징으로 군집화. 군집화 및 차원 축소 문제 해결.

◆ 군집

A. K-평균

B. 계층 군집 분석

C. 기댓값 최대화

◆ 시각화 및 차원 축소

A. 주성분 분석

B. 커널 PCA

C. 지역적 선형 임베딩

D. t-SNE

iii. 강화학습: 보상 최대화 정책을 수립하며 행동.

◆ 시행착오 및 지연보상

3. AI 취약점 유형

A. 데이터 변조 공격 (회피 공격)

= AI가 잘못된 판단을 하도록 유도하는 방식의 공격.

=> 변조 사례를 함께 학습시켜서 차단 가능.

B. 악의적 데이터 주입 공격 (중독 공격)

= 악의적 데이터를 AI에 넣어서 학습시키는 공격.

=> 부정적 데이터에 대한 사전 학습으로 대응 가능.

=> 답변 우회가 가능하도록 프로그램을 설계하여 대응 가능.

C. 데이터 추출 공격 (전도 공격)

= 인공지능에 사용된 데이터를 추출하는 공격. (학습에 사용된 민감한 데이터 추출)

=> 질의 횟수 제한으로, 학습 데이터 추론을 방해 가능.

4. AI를 이용한 보안

A. 스팸 메일 탐지 가능

i. 나이브 베이즈 분류기 기반 + BERT 등의 언어모델.

B. 네트워크 침입 탐지 가능

i. 네트워크 트래픽 패턴을 정상/비정상으로 학습시켜, 비정상 트래픽 탐지.

C. 악성 코드 탐지 가능

i. 악성코드의 일반적 특징을 학습시켜 탐지.

D. CCTV 영상의 위험 요인 탐지 가능

i. CCTV영상의 실시간 AI 처리 수행. (불, 폭력 등을 탐지)

10장 정리 끝.

11장 정리 시작. (침해 대응과 디지털 포렌식)

1. 침해 대응 절차

A. 사전 대응

i. 침해 대응 체계 구축.

(CERT 구성으로 시작.)

(Computer Emergency Response Team)

(CERT =

시스템 운영 전문가 (시스템 복구 수행) +

대외 언론 및 외부 기관 대응 전문가 (언론, 경찰 등에 대응) +

법률 팀 (사고 대응시의 법률 문제 해결) +

인사팀(권리와 책임 파악))

ii. 위험 등급 설정

- ◆ 1등급 상황: 침입자 공격에 대응 수단이 없는 경우 + 시스템 마비.
- ◆ 2등급 상황: 비인가자의 시스템 접근 및 수정이 발생한 경우.
- ◆ 3등급 상황: 취약점 수집 행위, 불법 접근 시도 등….
- ◆ 등급에 따른 대응:

  1등급 => CERT 팀장에게 즉시 보고 + 시스템 전원 공급 중단 등….

  2, 3등급 => 적절한 대응 시도.

B. 사고 탐지

= 문제 발생 시, 침해 사고가 발생한 것인지 확인하는 단계.

=> 침해 판명 시 미리 지정된 절차를 밟는다.

C. 대응

= 침해 사고로 인한 손상을 최소화하고, 추가 피해를 막기 위한 대응.

i. 단기 대응: 네트워크 연결 해제 등….

ii. 백업 및 증거 확보: 포렌식 절차에 따른 시스템 이미지 획득.

iii. 시스템 복구: 악성 코드 제거, 시스템 계정 및 패스워드 재설정…. 이후 시스템을 다시 네트워크에 연결.

D. 제거 및 복구

= 다른 피해가 있는지 확인 후, 완전한 복구를 시도하는 단계.

E. 후속 조치 및 보고

= 침해 사고 식별과 대응 과정을 문서화 하여 보관 및 보고.

2. (디지털) 포렌식

= (디지털) 증거 수집의 보조 분석을 위한 응용과학 분야.

A. 법적 효력을 지니는 증거
   i. 직접 증거: 요증 사실(증명을 요하는 사실)을 직접적으로 증명하는 증거. (범행 목격자….)
   ii. 간접 증거: 요증 사실을 간접적으로 추측하게 해주는 증거. (지문, 알리바이….)
   iii. 인적 증거: 증인의 증언, 감정인의 진술, 전문가의 의견 등….
   iv. 물적 증거: 범행에 사용한 흉기, 사람의 신체 등.

B. 디지털 포렌식으로 얻은 증거: 간접 증거.

C. 증거 개시 제도: 증거를 미리 준비하여, 정식 재판이 진행되기 전에 공개하는 것. 미리 제시하지 않은 증거는 법정에서 원칙적을 사용 불가.

3. 디지털 포렌식의 기본 원칙

A. 정당성의 원칙: 적법한 절차를 거쳐서 증거를 얻어야만 한다. (정보 제공 동의 필수.)

B. 재현의 원칙: 증거는 정제과정을 거쳐 복원될 수 있는데, 이 정제 과정이 재현될 수 있어야 함.

C. 신속성의 원칙: 휘발성 데이터를 빠르게 얻어내야 한다.

D. 연계 보관성의 원칙: 증거물의 이동과정이 명확하고 투명하게 기록되어야 함.

E. 무결성의 원칙: 증거가 위조, 변조되지 않았음을, 모든 연계 보관 과정에서 계속 검증해야 한다.

4. 포렌식 수행 절차

A. 수사 준비: 장비 확보, 피의자 또는 수사 대상에게 접근.

B. 증거물 획득: 증거 획득인 + 감독 + 인증인(검토책임자) 의 참관 하에 증거 수집.

C. 보관 및 이송: 연계 보관성을 준수하며 보관 및 이송되어야 한다. 변경되는 책임자와 증거의 위치 등을 모두 로깅해야 한다.

D. 분석 및 조사: 원본은 보존하고, 복사본을 분석 및 조사해야 한다. (최량 증거 원칙으로, 법정에는 항상 원본을 제출해야 함.)

E. 보고서 작성: 모든 과정을 기록해야 한다. 무결성 관련 정보를 모두 로깅해야 한다.

5. 디지털 포렌식의 증거 수집 분류

A. 네트워크 증거 수집

〈= 네트워크 자체는 데이터를 저장하지 않으므로, 네트워크 관련 보안 솔루션에서 정보를 수집해야 한다.

i. 침입탐지 시스템 이용. (라우터의 모든 로그 수집.)
ii. 네트워크 로그 서버 이용.
iii. 스니퍼 운용. (패킷 탐지.)

B. 시스템 증거 수집

〈= 법원에 제출되는 정보의 대부분은 시스템에서 수집되는 증거이다. 증거 수집이 쉽다.

i. 활성 데이터 수집. (확인한 증거를 캡처, 영상 등으로 증거한다.)
ii. 시스템 로그 분석.
iii. 저장 장치 분석.

C. 데이터 및 응용 프로그램 증거 수집

i. 이메일 분석. (이메일의 내용을 분석한다.)
ii. 인터넷 분석. (쿠키 등을 분석한다.)

11장 정리 끝.

13장 정리 시작. (보안 관리)

1. 정보 보안 거버넌스 (Security Governance)

= 조직 보안 달성을 위한 구성원 간의 지배 구조.

A. 구현이 어렵다. 어려운 이유:

i. 조직 구성이 어렵다. 최고보안책임자(CSO)를 CTO 밑에? 옆에? 보안조직은 중앙집중으로? 분상형으로?

ii. 성과 측정이 어렵다. 사고가 일어나지 않는 이상, 성과 측정이 어렵다.

iii. 조직이 무관심하다. 경영진의 무관심, 조직 구성원의 무관심이 보안 거버넌스 형성의 장애물.

B. 구현 요건 (효율적이고 효과적인 정보 보안 거버넌스의 다섯 요건):

i. 전략적 연계: 비즈니스, IT기술, 정보보안의 셋이 서로 연계되어야 한다.

ii. 위험 관리: 지속적인 위험 관리 체계 수립 필요.

iii. 자원 관리: 적절한 정보보안 아웃소싱 필요.

iv. 성과 관리: 비즈니스 측면을 고려한, 성과 평가 체계 운용 필요.

v. 가치 전달: 구성원들에게 정보보안의 중요성과 가치를 교육해야 한다.

2. 보안 프레임워크

= 조직의 보안 체계. (ISMS)

= 조직 구성원이 전문가가 아니어도 보안이 유지되도록 하는 보안 시스템.

A. 국제 표준 인증: ISO 27001

B. 영국 표준에서는 ISMS를 PDCA 모델을 기반으로 발전시킬 수 있다고 했다.

C. PDCA

i. Plan: 전반적인 보안 정책 수립.

ii. Do: 계획을 실제 업무에 적용.

iii. Check: 모니터링 단계. (얼마나 잘 적용 및 운영되는지 확인.)

iv. Act: 조치. (정상 운영이 안 될 때, 원인을 분석하고 개선.)

D. 한국 표준: K-ISMS

3. **보안 조직**

A. 보안 조직에 적절한 권한과 책임이 부여되어야, 보안성 향상이라는 목표 달성을 위한 보안 업무를 수행할 수 있다.

B. 보안조직의 배치는, CEO 직속의 별도 조직으로!

C. 보안조직의 구성원들:

i. 정보 보안 책임자 (CSO): 예산 확보.

ii. 정보 보안 관리자: 보안 업무 기획 및 점검.

iii. 정보 보안 담당자: 보안 실무 수행.

iv. 각 부서 및 팀별 정보 보안 담당자: 일일 보안 점검 수행.

D. 보안 조직의 규모와 형태 <= 상황에 맞게, 다양한 요소를 고려하여 결정해야 한다.

4. **보안 정책과 절차**

= 지켜져야 할 정책 + 권유해야 할 정책 + 목적이 있는 정책.

= 조직의 비즈니스 목표와 운영 목표에 부합하고 법규나 규정에 어긋나지 않으면서 보안을 달성할 수 있는 정책과 절차.

5. **접근 제어 모델**

= 기밀성과 무결성 확보를 위한 체계화된 접근 제어 모델.

A. 주요 모델들

i. 임의적 모델: 데이터 소유자가 권한을 설정한다.

ii. 강제적 모델: 중앙에서 정보를 수집 및 분류한다.

iii. RBAC: 사람이 아닌 직책에 권한을 부여한다.

6. **내부 통제**

= 기업의 구성원들이 지속적으로 실행하는 일련의 통제 과정.

A. 목적: 효과적이고 효율적인 업무 운영….

B. 내부 통제의 중요한 개념 둘.

i. 최소 권한: 필요한 만큼만 권한을 부여해야 한다.

ii. 직무분리: 하나의 업무 절차를 두 사람 이상이 수행하도록 업무를 분리해야 한다.

7. **보안 인증**

= SW or System 에 대한 품질 표시 마크.

A. TCSEC, ITSEC, CC ….

8. **개인 정보 보호**

= 개인을 알아볼 수 있는 정보를 보호하는 것.

13장 정리 끝.