서문

필자가 정보 보안 기사를 처음 강의했던 곳은 서울시 인재 개발원이었다. 그때가 2012년 9월이었다. 당시에는 정보 보안 기사가 아닌, 정보 보호 전문가(SIS)였다. 올해가 2019년이니깐 정보 보안 기사를 강의한 세월도 벌써 7년차에 접어 들었다.

그동안 서울시 인재 개발원뿐 아니라, 우정 공무원 교육원• 대구시 공무원 교육원• 경북 교육청• 전북 교육청• 한국 지역 정보 개발원 등에서 정보 보안 기사를 강의했다.

<<2019년 정보 보안 기사 통합본>>은 지난 7년 동안 강의하면서 시험에서 주요하게 다루었던 내용을 중심으로 편집한 일종의 필기• 실기 대비 강의안이다. 그런 만큼 해당 통합본은 정보 보안 기사 시험에 응시하려는 수험자들에게 적합할 수 있다.

정보 보안 기사를 강의한다는 것은 그 어떤 분야를 강의하는 것보다 힘들다. 정보 보안 기사에서 요구하는 5개 과목의 내용을 이해하고, 실습 내용을 조작할 수 있어야 한다. 그러나 이것만으로 끝나는 것이 아니다. 터득한 내용을 출제 경향에 부합하도록 반영하고 이것을 일목요연하게 설명해야 한다. **<<2019년 정보 보안 기사 통합본>>**은 이런 필자의 노력과 시행 착오적인 경험을 최대한 반영했다.

아무쪼록 정보 보안 기사를 준비하는 수험생들에게 유용한 자료로 남아준다면 더할 나위 없이 기쁠 듯하다.

2019년 5월 1일

모의 침투 연구회 오동진(firsblood@naver.com)

雖不足藏之名山 庶無使墁之醬瓿(비록 명산에 비장할 바는 아니오나 간장 항아리 덮개로만은 쓰지 말아 주시옵소서).

김부식(金富軾)의 <<삼국사기(三國史記)>> 서문에서

제1장 정보 보호의 개요

1. 정보 보호의 주요 용어

(1) 자산

1) 개인 또는 조직이 보호해야 할 유• 무형의 가치

2) 위험을 보유한 대상

(2) 취약점

자산 내부에 있는 물리적• 기술적• 관리적 결점

(3) 위협

자산에 손실을 가하는 현실적 사건이나 행위

(4) 위험

1) 위협에 의해 비정상적인 사건이 발생할 수 있는 가능성

2) 자산 * 취약점 * 위협으로 표현

3) 경우에 따라 자산 * 취약점 * 위협 * 정보 보호 대책으로 표현

(5) 노출 계수

자산 가치의 손실을 백분율(%)로 나타낸 수치

(6) 지능형 지속 위협(APT) 공격

1) 특정 대상을 선정해 오랜 시간 동안 지속적으로 침투를 수행하는 방식

2) APT 공격 4단계 과정

침투 > 검색 > 수집 > 유출

3) 사이버 킬 체인(Cyber Kill Chain) 전략으로 방어

(7) 통제

취약점을 억제하기 위한 일련의 제어

1) 예방 통제

방화벽 설치 목적

2) 탐지 통제

IDS 설치 목적

3) 교정 통제

IPS 설치 목적

2. 정보 보호의 정의

(1) 법률적인 정의

정보의 수집• 가공• 저장• 검색• 송신• 수신 중 정보의 훼손• 변조• 유출 등을 방지하기 위해 물리적• 기술적• 관리적 수단 등을 강구하는 개념

(2) 기술적인 정의

정보를 각종 위협으로부터 안전하게 보호하고 정보의 기밀성• 무결성• 가용성 등을 보장하는 개념

3. 정보 보호 정책의 개념

(1) 정보 자산을 보호하기 위한 규약 등을 작성한 문서

1) 정보 보호 문서 중 최상위 등급에 위치

2) 상위 조직의 정책과 방향 등에 부합하는 기본 방향과 근거 등을 제시

3) 정보 보호 조직 구성원의 책임과 역할 등을 규정

4) 실무적인 측면을 고려해 모든 직원들이 숙지할 수 있도록 포괄적이고 일반적인 내용을 최대한 간단하고 명료하게 작성

5) 전략적이고 장기적인 관점에서 수립하고 합병 등과 같은 환경 변화가 생길 때마다 검토

6) 최고 경영진의 승인이 필요

(2) 전반적인 위험에 기반해 정보 자산을 보호하기 위한 일련의 표준• 지침• 절차 등을 의미

1) 표준

조직에서 요구하는 구체적이고 강제적인 사양

2) 지침

표준을 기반으로 유연성을 제공하는 추가적인 권고 사항

3) 절차

정보 보호 정책을 구현하기 위한 단계별 세부 지시 사항

제2장 위험 관리

1. 위험의 종류

(1) 전체 위험

정보 보호 정책 적용 이전의 위험

(2) 잔여 위험

1) 정보 보호 정책 적용 이후의 위험

2) 위험 관리의 대상

2. 위험 관리

(1) 잔여 위험을 수용• 통제할 수 있는 수준으로 유지하기 위한 일련의 과정

(2) 다시 말해, 위험을 인식하고 적절한 비용 범위에서 통제 방안을 선택해 위험을 적절하게 통제하는 일련의 과정

(3) 위험 관리의 5단계 과정

자산 분석 > 위험 분석 > 취약점 분석 > 위험 평가 > 위험 처리

(4) 위험 관리 계획

위험을 예방하고 돌발 상황이 발생했을 때 통제 방안 등을 작성한 일련의 문서

3. 자산 분석

(1) 자산을 적절한 등급으로 분류해 자산 목록을 작성하는 일련의 과정

(2) 자산의 특성을 고려해 사용 용도• 피해 규모 등을 포함해 수행

4. 위험 분석

(1) 위험을 해석하는 과정으로 조직 자산의 취약점을 식별하고 발생 가능한 위험의 내용과 정도 등을 결정하는 일련의 과정

(2) 자산 목록에 기반해 정보 보호 비용을 산출하는 일련의 과정

5. 위험 분석의 접근 방법

(1) 기준선 접근법

1) 소규모 조직에 적합

2) 표준화된 점검 항목(Checklist)에 기반하기 때문에 비용 등을 절약

3) 점검 항목 내용에 따라 과다 비용 또는 보안 공백 등이 발생

(2) 비정형적 접근법

1) 개인의 전문성을 활용

2) 신속하고 저렴

3) 주관성에 의존

(3) 상세 위험 분석 접근법

1) 모든 자산의 가치를 측정하고, 자산의 위험 정도• 취약점 등을 해석해 모든 위험 정도를 결정

2) 정교한 위험 분석이 가능

3) 과도한 비용이 발생

(4) 통합 접근법

1) 고등 위험 영역은 상세 위험 분석 접근법을 수행하고, 기타 영역은 기준선 접근법을 수행하는 통합 방식

2) 비용 등을 효과적으로 사용하며, 고등 위험 영역에 대한 정교한 처리가 가능

3) 고등 위험 영역에 대한 식별 오류가 불필요한 낭비 등을 초래

6. 위험 평가

(1) 조직에서 필요한 정보 보호 요구 사항 등을 분석하기 위해 정보나 정보 처리 기기에 대한 위험의 종류• 영향• 발생 가능성 등을 평가하는 일련의 과정

(2) 산출한 정보 보호 비용에다 우선 순위를 부여해 적절한 대책을 결정하는 일련의 과정

7. 위험 평가의 우선 순위 결정 방식

(1) 정성적 방식

1) 델파이법

전문가를 구성해 위험을 해석하는 방식

2) 시나리오법

일정 조건 아래 위험 발생 가능한 결과 등을 추정하는 방식

3) 순위 결정법

각각의 위험을 상호 비교해 각종 위험 요인의 우선 순위를 도출하는 방식

(2) 정량적 방식

1) 과거 자료 분석법

과거에 발생한 사건은 미래에도 발생할 수 있다는 가정이 필요

2) 수학 공식 접근법

과거 자료 분석법이 곤란한 경우 위험의 발생 빈도를 계산해 분석

3) 확률 분포법

미지의 사건을 통계적인 편차를 이용해 위험을 평가

4) 점수법

위험 발생 요인에다 가중치를 부여해 위험을 측정하는 방식

8. 정량적 방식을 수행하기 위한 계산식

(1) 자산 가치(AV)

(2) 노출 계수(EF)

(3) 단일 손실 예상액(SLE)

자산 가치(AV) * 노출 계수(EF)

(4) 연간 발생률(ARO)

(5) 연간 손실 예상액(ALE)

단일 손실 예상액(SLE) * 연간 발생률(ARO)

9. 정량적 방식을 수행하기 위한 계산식 일례

(1) 자산 가치가 100억원이고, 화재 위험에 대한 노출 계수가 10%이고, 5년에 한 번 정도 화재가 발생하는 경우

1) 단일 손실 예상액 = 자산 가치 100억 * 노출 계수 0.1 = 10억

2) 연간 손실 예상액 = 단일 손실 예상액 10억 * 연간 발생률 0.2 = 2억

(2) 자산 가치가 100억원이고. 화재 위험에 대한 노출 계수가 0.2이고, 20년에 한 번 정도 사고가 발생하는 경우

1) 단일 손실 예상액 = 자산 가치 100억 * 노출 계수 0.2 = 20억

2) 연간 손실 예상액 = 단일 손실 예상액 20억 * 연간 발생률 0.05 = 1억

10. 위험 처리의 종류

잔여 위험을 대상으로 적절하고 정당한 대응 등을 식별• 선정하는 일련의 과정

(1) 위험 수용

사업 목적상 잠재적인 손실 비용을 감수하면서 현재의 위험을 그대로 수용하는 행위

(2) 위험 회피

위험이 있는 사업 등을 포기하는 행위

(3) 위험 감소

방화벽 설치 또는 경비원 고용 등을 통해 위험 수준을 경감시키는 행위

(4) 위험 전이

보험이나 외주 등과 같은 비용 동반을 통해 잠재적인 위험 비용을 제3자에게 전가하는 행위

제3장 재난 대비

1. 사업 연속성 계획(BCP) 개념

(1) 정보 보호 정책의 일부이고, 경영진의 지원이 핵심

(2) 재난이 발생할 경우 최악의 시나리오를 염두에 두고 사업의 연속성을 유지하는 방법을 정의한 문서로 핵심 업무의 재개를 목표로 전사적인 차원에서 수립

(3) 가용성 유지가 관건

2. 사업 영향 분석(BIA) 개념

(1) 재난 발생을 고려해 위험 분석 등을 실시하는데 이 경우 발생 가능한 모든 재해를 고려해 잠재적인 손실을 측정하고 재난을 분류한 뒤 복구 대상의 우선 순위를 부여해 실행 가능한 대안을 개발하는 일련의 과정

(2) 사업 영향 분석(BIA) 접근 5단계 과정

주요 업무 과정의 식별 > 재해 유형과 가능성의 식별 > 재해 시 업무 진행 중단에 따른 손실 평가 > 복구 대상의 우선 순위와 범위 설정 > 주요 업무 진행별 복구 목표 시간 설정

3. 재난 복구 계획(DRP) 개념

(1) 사업 연속성 계획(BCP)의 일부

(2) 재난이 발생할 경우 기술적 측면에서 핵심 장비의 연속성을 유지하도록 정의한 문서

4. 재난 복구 서비스 종류

(1) 미러 사이트

메인 사이트와 동일한 수준의 정보 기술 자원을 실시간 상태에서 동작하는 방식

(2) 콜드 사이트

1) 장소 또는 전산실만을 준비

2) 비용은 저렴하지만 상당한 지연 시간이 발생

(3) 핫 사이트

미러 사이트와 달리 대기 상태에서 동작하는 방식

(4) 웜 사이트

1) 콜드 사이트와 핫 사이트의 중간

2) 중요성이 높은 정보만 부분적으로 보유

(5) 상호 지원 계약

1) 유사한 장비나 환경 등을 가진 두 개 이상의 기업 사이에서 계약을 체결하고, 재난이 발생할 경우 다른 회사의 시설물 일부 또는 전체를 무상으로 사용해 고객에게 안정적인 서비스를 제공할 수 있도록 체결한 계약

2) 설정 관리 또는 운영의 혼합 등으로 보안 문제가 발생할 수 있고, 계약 이행을 위한 강제가 불가능

제4장 디지털 포렌식의 5대 원칙

1. 무결성의 원칙

수집한 증거는 위조• 변조가 없어야 한다.

2. 정당성의 원칙

모든 증거는 적법한 절차를 통해 획득해야 한다.

3. 신속성의 원칙

내부 정보는 휘발성이기 때문에 신속하게 획득해야 한다.

4. 재현성의 원칙

법정에 증거를 제출하기 위해서는 같은 환경에서 같은 결과가 나오도록 재현이 가능해야 한다.

5. 연계 보관성의 원칙

모든 증거는 수집• 이동• 보관• 분석• 제출이라는 일련의 과정이 명확해야 한다.

제5장 정보 보호 표준과 인증

1. 주요 정보 보호 표준

다양한 정보 보호 제품에 대한 객관적인 평가 기준을 제시하기 위해 사용

(1) TCSEC 방식

1) 이른바 오렌지 북

2) 미국 중심

3) 기밀성• 무결성 등을 취급

4) 보안 등급은 최저 D 등급에서 최고 A1 등급까지 7등급으로 구분

(2) ITSEC 방식

1) TCSEC 방식을 참조

2) 영국 중심

3) 기밀성• 무결성• 가용성 등을 취급

4) 보안 등급은 최저 E0 등급에서 최고 E6 등급까지 7등급으로 구분

2. 국제 정보 보호 표준

(1) 국가별 정보 보호 제품의 평가 결과를 상호 인정하며, 정보 보호 시스템에 공통적으로 적용할 수 있는 공통 평가 기준을 개발하고 적용하기 위해 CC(Common Criteria) 방식으로 통합

(2) CC 방식의 구성 요소

1) 공통 평가 기준(Common Criteria)

2) 평가 보증 등급(Evaluation Assurance Level)

3) 보호 프로파일(Protection Profile)

4) 보안 목표 명세서(Security Target)

(3) 보안 등급은 최저 EAL1 등급에서 최고 EAL7 등급까지 7등급으로 구분

3. 국제 정보 보호 관리 체계 인증

(1) 정보의 기밀성• 무결성• 가용성 등을 실현하기 위한 절차와 과정 등을 수립해 문서로 작성하고 지속적으로 관리• 운영하는 제도

(2) 다시 말해, 조직에 적합한 정보 보호를 위해 위험 분석 등과 같은 정보 보호 관리 과정

을 정리하고, 제3자의 인증 기관을 통해 평가받고, 인증 기준에 대한 적합성 여부를 인증받는 제도

(3) BS7799(ISO/IEC 17799)

1995년 발표한 ISMS 표준

(4) PDCA(Plan• Do• Check• Act) 모형을 적용

(5) 11개 통제 분야 제공

4. 국내 정보 보호 관리 체계 인증

(1) 정보 통신망 이용 촉진 및 정보 보호 등에 관한 법률[시행 2017.07.26] 제47조(정보 보호 관리 체계의 인증)에 근거해 한국 인터넷 진흥원에서 2002년부터 KISA-ISMS 시행

(2) 정보 보호 관리 체계 인증 등에 대한 고시(과학 기술 정보 통신부 고시 제2017-7호) 제2조에 따른 정보 보호 관리 과정 수행 절차

정보 보호 정책의 수립과 범위의 설정 > 경영진 조직과 책임의 구성 > 위험 관리 > 정보 보호 정책의 구현 > 사후 관리

(3) 13개 통제 분야 제공

제6-1장 개인 정보 보호법[시행 2017.07.26]

1. 주요 용어[제2조]

(1) 개인 정보

1) 생존하는 개인에 대한 정보

2) 성명• 주민 등록 번호• 영상 등으로 개인을 알아볼 수 있는 정보

3) 해당 정보만으로는 특정한 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합해 알아볼 수 있는 내용까지 포함

(2) 정보 주체

1) 처리되는 정보에 의해 알아볼 수 있는 사람

2) 정보의 주체가 되는 사람

(3) 개인 정보 처리자

업무를 목적으로 개인 정보 파일을 운용하기 위해 스스로 또는 다른 사람을 통해 개인 정보를 처리하는 공공 기관• 법인• 단체• 개인

(4) 영상 정보 처리 기기(CCTV)

일정한 공간에 지속적으로 설치돼 사람 또는 사물의 영상 등을 촬영하거나 이를 유• 무선망을 통해 전송하는 장치

2. 개인 정보 보호 지침[제12조]

(1) 행정 안전부 장관은 개인 정보 처리에 관한 기준• 개인 정보 침해의 유형• 예방 조치 등에 관한 표준 개인 정보 보호 지침(행정 안전부 제2017-1호)을 개인 정보 처리자에게 권장할 수 있다.

(2) 중앙 행정 기관의 장은 표준 개인 정보 보호 지침에 따라 소관 분야의 개인 정보 처리와 관련한 개인 정보 보호 지침을 개인 정보 처리자에게 권장할 수 있다.

(3) 국회• 법원• 헌법 재판소• 중앙 선거 관리 위원회는 해당 기관(그 소속 기관을 포함)의 개인 정보 보호 지침을 시행할 수 있다.

3. 개인 정보의 수집• 이용 동의[제15조]

개인 정보 처리자는 정보 주체의 개인 정보를 수집• 이용하는 경우 다음 사항을 정보 주체에게 고지하고 동의를 받아야 한다.

(1) 개인 정보의 수집• 이용 목적

(2) 수집하는 개인 정보의 항목

(3) 개인 정보의 보유• 이용 기간

(4) 동의를 거부할 권리가 있다는 사실

(5) 동의 거부에 따라 불이익이 있는 경우 그 불이익 내용

4. 개인 정보의 제공[제17• 18조]

개인 정보 처리자는 정보 주체의 개인 정보를 제3자에게 제공하려면 다음 사항을 정보 주체에게 고지하고 동의를 받아야 한다.

(1) 개인 정보를 제공받는 자

(2) 개인 정보를 제공받는 자의 개인 정보의 수집• 이용 목적

(3) 제공하는 개인 정보의 항목

(4) 개인 정보를 제공받는 자의 개인 정보의 보유• 이용 기간

(5) 동의를 거부할 권리가 있다는 사실

(6) 동의 거부에 따라 불이익이 있는 경우 그 불이익 내용

5. CCTV의 설치• 운영 제한[제25조]

(1) 법령에서 구체적으로 허용하는 경우

(2) 범죄의 예방• 수사를 위해 필요한 경우

(3) 시설 안전• 화재 예방을 위해 필요한 경우

(4) 교통 단속을 위해 필요한 경우

(5) 교통 정보의 수집• 분석• 제공을 위해 필요한 경우

6. CCTV의 안내판 설치[제25조]

(1) 설치 목적• 장소

(2) 촬영 범위• 시간

(3) 관리 책임자의 성명• 연락처

(4) 기타 대통령령으로 정하는 사항

7. 개인 정보 보호 책임자의 지정[제31조]

개인 정보 처리자는 개인 정보 처리 업무를 총괄할 개인 정보 보호 책임자를 지정해야 한다.

8. 개인 정보 보호 인증[제32조의 2]

(1) 행정 안전부 장관은 개인 정보 처리자의 개인 정보 보호와 관련한 일련의 조치가 해당 법에 부합하는지 등을 인증할 수 있다.

(2) 인증의 유효 기간은 3년

(3) 행정 안전부 장관은 개인 정보 보호 인증의 실효성 유지를 위해 연 1회 이상 사후 관리를 실시

9. 개인 정보 영향 평가[제33조]

(1) 공공 기관의 장은 대통령령으로 정하는 기준에 해당하는 개인 정보 파일의 운용으로 인해 정보 주체의 개인 정보 침해가 우려되는 경우에는 위험 요인 분석과 개선 사항 도출 평가 등을 수행하고, 그 결과를 행정 안전부 장관에게 제출

(2) 이 경우 공공 기관의 장은 개인 정보 영향 평가를 행정 안전부 장관이 지정하는 기관에 의뢰

(3) 개인 정보 영향 평가를 수행하는 경우에는 다음 사항을 고려

1) 처리하는 개인 정보의 수

2) 개인 정보의 제3자 제공 여부

3) 정보 주체의 권리를 침해할 가능성• 위험 정도

4) 기타 대통령령으로 정한 사항

10. 개인 정보 유출 통지[제34조]

(1) 개인 정보 처리자는 개인 정보 유출을 인지한 경우 즉시 해당 정보 주체에게 다음 사실을 통지해야 한다.

1) 유출된 시점• 경위

2) 유출된 개인 정보의 항목

3) 정보 주체가 조치할 수 있는 방법 등에 관한 정보

4) 피해 발생 신고 등을 접수할 수 있는 담당 부서• 연락처

5) 개인 정보 처리자의 대응 조치• 피해 구제 절차

(2) 개인 정보 처리자는 조치 결과를 즉시 행정 안전부 장관 등에 신고

제6-2장 개인 정보 보호법 시행령[시행 2017.10.19]

1. 개인 정보 처리자의 범위[제15조의 2]

대통령령으로 정하는 개인 정보 처리자란 다음과 같다.

(1) 5만명 이상의 정보 주체에 관하여 민감 정보 또는 고유 식별 정보를 처리하는 자

(2) 100만명 이상의 정보 주체에 관하여 개인 정보를 처리하는 자

2. 민감 정보의 범위[제18조]

대통령령으로 정하는 민감 정보란 유전 정보• 범죄 정보

3. 고유 식별 정보의 범위[제19조]

대통령령으로 정하는 고유 식별 정보란 주민 등록 번호• 외국인 등록 번호• 여권 번호• 운전 면허 번호

4. 개인 정보의 안전성 확보 조치[제30조]

(1) 내부 관리 계획의 수립• 시행

(2) 개인 정보에 대한 접근 통제• 접근 권한의 제한 조치

(3) 암호화 기술의 적용 또는 이에 상응하는 조치

(4) 접속 기록 보관 및 위조• 변조 방지를 위한 조치

(5) 보안 프로그램의 설치• 갱신

(6) 보관 시설의 마련• 잠금 장치의 설치 등 물리적 조치

제6-3장 개인 정보의 안전성 확보 조치 기준[시행 2017.07.26]

1. 주요 용어[제2조]

(1) 개인 정보 처리자

업무를 목적으로 개인 정보를 운용하기 위해 스스로 또는 다른 사람을 통해 개인 정보를 처리하는 공공 기관• 법인• 단체• 개인

(2) 개인 정보 보호 책임자

개인 정보 처리자의 개인 정보 처리 업무를 총괄해 책임지는 자

(3) 개인 정보 취급자

개인 정보 처리자의 지휘• 감독을 받아 개인 정보를 처리하는 임직원• 파견 근로자• 시간제 근로자

(4) 개인 정보 처리 시스템

데이터베이스 시스템 등 개인 정보를 처리할 수 있도록 체계적으로 구성한 시스템

(5) 비밀 번호

정보 주체• 개인 정보 취급자 등이 개인 정보 처리 시스템• 업무용 컴퓨터• 정보 통신망 등에 접속할 때 식별자와 함께 입력해 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보

(6) 바이오 정보

1) 지문 등 개인을 식별할 수 있는 신체적• 행동적 특징에 관한 정보

2) 그로부터 가공되거나 생성된 정보를 포함

(7) 내부망

물리적 망 분리• 접근 통제 시스템 등을 통해 인터넷 구간에서 접근이 통제• 차단되는 구간

(8) 접속 기록

개인 정보 취급자 등이 개인 정보 처리 시스템에 접속한 사실을 알 수 있는 계정• 접속 일시• 접속자 정보• 수행 업무 등을 전자적으로 기록한 것

2. 내부 관리 계획의 수립• 시행(물리적• 기술적• 관리적 조치)[제4조]

(1) 개인 정보 처리자는 내부 의사 결정 절차를 통해 내부 관리 계획을 수립• 시행해야 한다.

1) 개인 정보 보호 책임자의 지정에 관한 사항

2) 개인 정보 보호 책임자와 개인 정보 취급자의 역할• 책임에 관한 사항

3) 개인 정보 취급자 교육 사항

4) 접근 통제 사항

5) 접근 권한 사항

6) 개인 정보의 암호화 조치 사항

7) 접속 기록 보관• 점검 사항

8) 악성 프로그램 등 방지 사항

9) 물리적 안전 조치 사항

10) 개인 정보 보호 조직 구성과 운영 사항

11) 개인 정보 유출 사고 대응 계획 수립• 시행 사항

12) 위험도 분석• 대응 방안 마련 사항

13) 재난• 재해 대비 개인 정보 처리 시스템의 물리적 안전 조치 사항

14) 개인 정보 처리 업무를 위탁하는 경우 수탁자에 대한 관리• 감독 사항

15) 기타 개인 정보 보호를 위해 필요한 사항

(2) 개인 정보 보호 책임자는 연 1회 이상 내부 관리 계획의 이행 실태를 점검• 관리해야 한다.

3. 접근 권한 등에 대한 기록[제5조]

개인 정보 처리자는 개인 정보 처리 시스템에 대한 접근 권한의 부여• 변경• 말소 내역을 기록하고, 해당 기록을 최소 3년간 보관

4. 접근 통제[제6조]

(1) 개인 정보 처리자는 정보 통신망을 통한 불법적인 접근• 침해 사고 방지를 위해 다음 기능을 포함한 조치를 취해야 한다.

1) 개인 정보 처리 시스템에 대한 접속 권한을 IP 주소 등으로 제한해 인가받지 않은 접근을 제한

2) 개인 정보 처리 시스템에 접속한 IP 주소 등을 분석해 불법적인 개인 정보 유출 시도 탐지• 대응

(2) 개인 정보 처리자는 개인 정보 취급자가 정보 통신망을 통해 외부에서 개인 정보 처리 시스템에 접속하려는 경우 가상 사설망(VPN) 또는 전용선 등 안전한 접속 수단을 적용하거나 안전한 인증 수단을 적용해야 한다.

(3) 개인 정보 처리자는 취급 중인 개인 정보가 인터넷 홈 페이지• P2P• 공유 설정• 공개 무선망 이용 등을 통해 열람 권한이 없는 자에게 공개• 유출되지 않도록 개인 정보 처리 시스템• 업무용 컴퓨터• 모바일 기기• 관리용 단말기 등에 접근 통제 조치를 취해야 한다.

(4) 고유 식별 정보를 처리하는 개인 정보 처리자는 인터넷 홈 페이지를 통해 고유 식별 정보가 유출• 변조• 훼손되지 않도록 연 1회 이상 취약점을 점검하고, 필요한 보완 조치를 취해야 한다.

(5) 개인 정보 처리자는 개인 정보 처리 시스템에 대한 불법적인 접근• 침해 사고 방지를 위해 개인 정보 취급자가 일정 시간 이상 업무를 처리하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 해야 한다.

(6) 개인 정보 처리자가 업무용 컴퓨터• 모바일 기기를 이용해 개인 정보를 처리하는 경우에는 업무용 컴퓨터• 모바일 기기의 운영 체제(OS)나 보안 프로그램 등에서 제공하는 접근 통제 기능을 이용할 수 있다.

(7) 개인 정보 처리자는 업무용 모바일 기기의 분실• 도난 등으로 개인 정보가 유출되지 않도록 해당 모바일 기기에 비밀 번호 설정 등의 보호 조치를 취해야 한다.

5. 접속 기록의 점검과 보관[제8조]

(1) 개인 정보 처리자는 개인 정보의 유출• 변조• 훼손 등에 대응하기 위해 개인 정보 처리 시스템의 접속 기록 등을 6개월에 1회 이상 점검

(2) 개인 정보 처리자는 개인 정보 취급자가 개인 정보 처리 시스템 접속 기록을 6개월 이상 보관• 관리

제7-1장 정보 통신망 이용 촉진 및 정보 보호 등에 관한 법률[시행 2017.07.26]

1. 주요 용어[제2조]

(1) 정보 통신망

전기 통신 설비• 컴퓨터 이용 기술 등을 활용해 정보를 수집• 가공• 저장• 검색• 송신• 수신하는 정보 통신 체계

(2) 정보 통신 서비스

전기 통신 서비스와 이를 이용해 정보를 제공 또는 매개하는 서비스

(3) 정보 통신 서비스 제공자

1) 전기 통신 사업자

2) 영리를 목적으로 전기 통신 사업자의 전기 통신 서비스를 이용해 정보를 제공 또는 매개하는 자

(4) 이용자

정보 통신 서비스 제공자가 제공하는 정보 통신 서비스를 이용하는 자

(5) 개인 정보

1) 생존하는 개인에 대한 정보

2) 성명• 주민 등록 번호 등으로 특정한 개인을 알아볼 수 있는 부호• 문자• 음성• 음향• 영상 등의 정보

3) 해당 정보만으로는 특정한 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합해 알아볼 수 있는 내용까지 포함

(6) 침해 사고

컴퓨터 바이러스• 논리 폭탄• 메일 폭탄• 서비스 거부• 고출력 전자기파 등의 방법으로 정보 통신망 또는 관련 정보 시스템을 공격해 발생한 사태

2. 개인 정보의 수집• 이용 동의[제22조]

정보 통신 서비스 제공자는 이용자의 개인 정보를 수집• 이용하는 경우 다음 사항을 이용자에게 고지하고 동의를 받아야 한다.

(1) 개인 정보의 수집• 이용 목적

(2) 수집하는 개인 정보의 항목

(3) 개인 정보의 보유• 이용 기간

3. 개인 정보의 제3자 제공 동의[제24조의 2]

정보 통신 서비스 제공자는 이용자의 개인 정보를 제3자에게 제공하려면 다음 사항을 이용자에게 고지하고 동의를 받아야 한다.

(1) 개인 정보를 제공받는 자

(2) 개인 정보를 제공받는 자의 개인 정보의 수집• 이용 목적

(3) 제공하는 개인 정보의 항목

(4) 개인 정보를 제공받는 자의 개인 정보의 보유• 이용 기간

4. 주민 등록 번호의 사용 제한[제23조의 2]

정보 통신 서비스 제공자는 다음 사항을 제외하고는 이용자의 주민 등록 번호를 수집• 이용할 수 없다.

(1) 본인 확인 기관으로 지정받은 경우

(2) 법령에서 이용자의 주민 등록 번호 수집• 이용을 허용하는 경우

(3) 영업상 목적을 위해 이용자의 주민 등록 번호 수집• 이용이 불가피한 정보 통신 서비스 제공자로서 방송 통신 위원회가 고시하는 경우

5. 개인 정보 보호 책임자의 지정[제27조]

(1) 정보 통신 서비스 제공자는 이용자의 개인 정보를 보호하고, 개인 정보와 관련해 이용자의 고충을 처리하기 위해 개인 정보 보호 책임자를 지정해야 한다.

(2) 개인 정보 보호 책임자가 없는 경우에는 사업주 또는 대표자가 개인 정보 보호 책임자의 역할을 수행

6. 정보 보호 최고 책임자의 지정[제45조의 3]

(1) 정보 통신 서비스 제공자는 정보 통신 시스템 등에 대한 보안과 정보의 안전한 관리를 위해 임원급의 정보 보호 최고 책임자를 지정할 수 있다.

(2) 대통령령으로 정하는 기준에 해당하는 정보 통신 서비스 제공자의 경우 정보 보호 최고 책임자를 지정하고, 과학 기술 정보 통신부 장관에게 신고해야 한다.

7. 개인 정보의 보호 조치[제28조]

(1) 정보 통신 서비스 제공자는 개인 정보를 취급할 때 개인 정보의 분실• 도난• 누출• 변조• 훼손 등을 방지하기 위해 대통령령으로 정하는 기준에 따라 다음과 같은 물리적• 기술적• 관리적 조치를 취해야 한다.

1) 내부 관리 계획의 수립• 시행

2) 접근 통제 장치의 설치• 운영

3) 접속 기록의 위조• 변조 방지를 위한 조치

4) 암호화 기술 등을 이용한 조치

5) 백신 소프트웨어의 설치• 운영 등

6) 기타 개인 정보의 안전성 확보를 위해 필요한 보호 조치

(2) 정보 통신 서비스 제공자는 이용자의 개인 정보를 취급하는 자를 최소한으로 제한해야 한다.

8. 개인 정보 유출 통지[제27조의 3]

(1) 정보 통신 서비스 제공자는 개인 정보의 유출을 인지한 경우 즉시 해당 이용자에게 다음 사실을 통지해야 한다.

1) 유출된 시점

2) 유출된 개인 정보의 항목

3) 이용자의 대응 조치

4) 이용자가 연락할 수 있는 부서와 연락처

5) 정보 통신 서비스 제공자의 대응 조치

(2) 정보 통신 서비스 제공자는 통지와 조치 결과 등을 즉시 방송 통신 위원회 또는 한국 인터넷 진흥원 등에 신고해야 한다.

9. 법정 대리인의 권리[제31조]

정보 통신 서비스 제공자는 만 14세 미만의 아동으로부터 개인 정보 수집• 이용• 제공 등 동의를 받으려면 그 법정 대리인의 동의를 받아야 한다.

10. 정보 통신망의 안정성 확보[제45조]

(1) 과학 기술 정보 통신부 장관은 보호 조치의 구체적 내용을 정한 정보 보호 조치에 관한 지침을 고시하고 정보 통신 서비스 제공자에게 권고할 수 있다.

(2) 정보 보호 지침에는 다음 내용을 포함해야 한다.

1) 정당한 권한이 없는 자가 정보 통신망에 접근• 침입하는 것을 방지하거나 대응하기 위한 정보 보호 시스템의 설치• 운영 등 물리적• 기술적 보호 조치

2) 정보의 불법 유출• 위조• 변조• 삭제 등을 방지하기 위한 기술적 보호 조치

3) 정보 통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 물리적• 기술적 보호 조치

4) 정보 통신망의 안정과 정보 보호를 위한 인력• 조직• 경비의 확보• 관련 계획 수립 등

관리적 보호 조치

11. 정보 보호 관리 체계(ISMS)의 인증[제47조]

(1) 과학 기술 정보 통신부 장관은 정보 통신망의 안정성• 신뢰성 확보를 위해 물리적• 기술적• 관리적 보호 조치를 포함한 종합 관리 체계를 수립• 운영하는 자에 대한 기준 여부를 인증할 수 있다.

(2) ISMS 인증의 유효 기간은 3년

(3) 한국 인터넷 진흥원• ISMS 인증 기관• 심사 기관 등은 ISMS의 실효성 제고를 위해 연 1회 이상 사후 관리를 실시하고, 그 결과를 과학 기술 정보 통신부 장관에게 통보해야 한다.

12. 개인 정보 보호 관리 체계(PIMS)의 인증[제47조의 3]

(1) 방송 통신 위원회는 정보 통신망에서 개인 정보 보호 활동을 체계적이고 지속적으로 수행하기 위해 필요한 물리적• 기술적• 관리적 보호 조치를 포함한 종합 관리 체계를 수립• 운영하는 자에 대한 기준 여부를 인증할 수 있다.

(2) 방송 통신 위원회는 PIMS 인증을 위해 물리적• 기술적• 관리적 보호 대책을 포함한 인증 기준 등 기타 필요한 사항을 고시할 수 있다.

제7-2장 정보 통신망 이용 촉진 및 정보 보호 등에 관한 법률 시행령[시행 2018.05.28]

1. 본인 확인 기관의 지정 절차[제9조의 4]

본인 확인 기관으로 지정받으려는 자는 본인 확인 기관 지정 신청서(전자 문서 신청서 포함)에 다음 서류(전자 문서를 포함)를 첨부해 방송 통신 위원회에 제출

(1) 조직• 인력• 설비 등의 현황을 기재한 사업 계획서

(2) 심사 사항별 세부 심사 기준을 충족했다고 증명할 수 있는 서류

(3) 법인의 정관• 단체의 규약(법인• 단체인 경우에만 해당)

(4) 기타 본인 확인 업무 수행의 전문성과 재무 구조의 건전성 등을 확인하기 위해 필요한 서류로서 방송 통신 위원회가 정해 고시하는 서류

2. 개인 정보 보호 책임자의 자격 요건[제13조]

개인 정보 보호 책임자는 임원 또는 개인 정보와 관련해 이용자의 고충 처리를 담당하는 부서의 장에 있어야 한다.

3. 개인 정보의 보호 조치[제15조]

(1) 정보 통신 서비스 제공자는 개인 정보의 안전한 처리를 위해 다음 내용을 포함하는 내부 관리 계획을 수립• 시행

1) 개인 정보 보호 조직의 구성• 운영에 관한 사항

2) 정보 통신 서비스 제공자의 지휘• 감독을 받아 이용자의 개인 정보를 처리하는 자의 교육에 관한 사항

3) 보호 조치를 이행하기 위해 필요한 세부 사항

(2) 정보 통신 서비스 제공자는 개인 정보에 대한 불법적인 접근을 차단하기 위해 다음 사항을 조치해야 한다.

1) 개인 정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템 접근 권한의 부여• 변경• 말소 등에 관한 기준의 수립• 시행

2) 개인 정보 처리 시스템에 대한 침입 탐지 시스템• 침입 차단 시스템의 설치• 운영

3) 개인 정보 처리 시스템에 접속하는 개인 정보 취급자의 컴퓨터 등에 대한 외부망 차단

4) 비밀 번호의 생성 방법• 변경 주기 등의 기준 설정과 운영

5) 기타 개인 정보의 접근 통제에 필요한 조치

(3) 정보 통신 서비스 제공자는 접속 기록의 위조• 변조 방지를 위해 다음 사항을 조치해야 한다.

1) 개인 정보 취급자가 개인 정보 처리 시스템에 접속해 개인 정보를 처리한 경우 접속 일시• 처리 내역 등의 저장• 이의 확인• 감독

2) 개인 정보 처리 시스템의 접속 기록을 별도 저장 장치에 백업 보관

(4) 정보 통신 서비스 제공자는 개인 정보가 안전하게 저장• 전송될 수 있도록 다음 사항을 조치해야 한다.

1) 비밀 번호의 일방향 암호화 저장

2) 주민 등록 번호• 계좌 정보• 바이오 정보 등 방송 통신 위원회가 고시하는 정보의 암호화 저장

3) 정보 통신망을 통해 이용자의 개인 정보• 인증 정보를 송신• 수신하는 경우 보안 서버 구축 등의 조치

4) 기타 암호화 기술을 이용한 보안 조치

제7-3장 개인 정보의 기술적• 관리적 보호 조치 기준[시행 2015.05.19]

1. 주요 용어[제2조]

(1) 개인 정보 보호 책임자

정보 통신 서비스 제공자의 사업장에서 이용자의 개인 정보 보호 업무를 총괄하거나 업무 처리를 최종 결정하는 임직원

(2) 개인 정보 취급자

정보 통신 서비스 제공자의 사업장에서 이용자의 개인 정보를 수집• 보관• 처리• 이용• 제공• 관리• 파기 등의 업무를 수행하는 자

(3) 내부 관리 계획

정보 통신 서비스 제공자가 개인 정보 보호 조직의 구성• 개인 정보 취급자의 교육• 개인 정보 보호 조치 등을 규정한 계획

(4) 개인 정보 처리 시스템

개인 정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템

(5) 바이오 정보

1) 지문 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보

2) 그로부터 가공되거나 생성된 정보를 포함

(6) 보안 서버

정보 통신망에서 송신• 수신하는 정보를 암호화해 전송하는 웹 서버

(7) 인증 정보

개인 정보 처리 시스템 또는 정보 통신망을 관리하는 시스템 등이 요구한 식별자의 신원을 검증하는데 사용하는 정보

2. 내부 관리 계획의 수립• 시행[제3조]

(1) 정보 통신 서비스 제공자는 다음 사항을 정해 개인 정보 보호 조직을 구성• 운영해야 한다.

1) 개인 정보 보호 책임자의 자격 요건• 지정에 관한 사항

2) 개인 정보 보호 책임자와 개인 정보 취급자의 역할• 책임에 관한 사항

3) 개인 정보 내부 관리 계획의 수립• 승인에 관한 사항

4) 개인 정보의 기술적• 관리적 보호 조치 이행 여부에 대한 내부 점검 사항

5) 개인 정보 처리 업무를 위탁하는 경우 수탁자에 대한 관리• 감독 사항

6) 개인 정보의 분실• 도난• 누출• 변조• 훼손 등이 발생한 경우 대응 절차와 방법에 관한 사항

7) 기타 개인 정보 보호를 위해 필요한 사항

(2) 정보 통신 서비스 제공자는 다음 사항을 정해 개인 정보 보호 책임자와 개인 정보 취급자를 대상으로 필요한 교육을 정기적으로 실시해야 한다.

1) 교육 목적과 대상

2) 교육 내용

3) 교육 일정과 방법

3. 접근 통제[제4조]

(1) 정보 통신 서비스 제공자는 개인 정보 처리 시스템의 접근 권한을 개인 정보 보호 책임자 또는 개인 정보 취급자에게만 부여

(2) 정보 통신 서비스 제공자는 개인 정보 취급자를 대상으로 비밀 번호 작성 규칙 등을 수립하고 이를 적용• 운용해야 한다.

1) 영문• 숫자• 특수 문자 중 두 종류 이상을 조합해 최소 10자리 이상의 길이로 구성하거나 세 종류 이상을 조합해 최소 8자리 이상의 길이로 구성

2) 연속적인 숫자• 생일• 전화 번호 등 추측하기 쉬운 개인 정보 또는 계정과 비슷한 비밀번호는 사용하지 않는 것을 권고

3) 비밀 번호에 유효 기간을 설정해 6개월에 1회 이상 변경

4. 접근 권한 등에 대한 기록[제4조]

정보 통신 서비스 제공자는 개인 정보 처리 시스템에 대한 접근 권한의 부여• 변경• 말소 내역을 기록하고, 해당 기록을 최소 5년간 보관

5. 접속 기록의 점검과 보관[제5조]

(1) 정보 통신 서비스 제공자는 개인 정보의 유출• 변조• 훼손 등에 대응하기 위해 개인 정보 처리 시스템의 접속 기록 등을 1개월에 1회 이상 점검

(2) 정보 통신 서비스 제공자는 개인 정보 취급자가 개인 정보 처리 시스템 접속 기록을 6개월 이상 보관• 관리

(3) 기간 통신 사업자의 경우에는 보존• 관리해야 할 최소 기간은 2년

6. 개인 정보의 암호화[제6조]

(1) 정보 통신 서비스 제공자는 비밀 번호가 복호화되지 않도록 일방향 암호화해 저장

(2) 정보 통신 서비스 제공자는 주민 등록 번호• 외국인 등록 번호• 여권 번호• 운전 면허 번호• 신용 카드 번호• 계좌 번호• 바이오 정보 등에 대해 안전한 암호 알고리즘으로 암호화해 저장한다.

(3) 정보 통신 서비스 제공자는 정보 통신망을 통해 이용자의 개인 정보• 인증 정보 등을 송신• 수신할 때에는 안전한 보안 서버 구축 등의 조치를 통해 이를 암호화하고 보안 서버는 다음 사항 중 하나의 기능이 있어야 한다.

1) 웹 서버에 SSL(Secure Socket Layer) 인증서를 설치한 뒤 전송 정보를 암호화해 송신• 수신하는 기능

2) 웹 서버에 암호화 응용 프로그램을 설치한 뒤 전송 정보를 암호화해 송신• 수신하는 기능

제8장 정보 통신 기반 보호법[시행 2017.07.26]

1. 주요 용어[제2조]

(1) 정보 통신 기반 시설

1) 국가 안전 보장• 행정• 국방• 치안• 금융• 통신• 운송• 에너지 등의 업무와 관련한 전자적 제어• 관리 시스템

2) 정보 통신망 이용 촉진 및 정보 보호 등에 관한 법률 제2조에서 정한 정보 통신망

(2) 전자적 침해 행위

정보 통신 기반 시설을 대상으로 해킹• 컴퓨터 바이러스• 논리 폭탄• 메일 폭탄• 서비스 거부• 고출력 전자기파 등에 의해 정보 통신 기반 시설을 공격하는 행위

(3) 침해 사고

전자적 침해 행위로 인해 발생한 사태

2. 주요 정보 통신 기반 시설의 지정[제8조]

중앙 행정 기관의 장은 소관 분야의 정보 통신 기반 시설 중 다음 사항을 고려해 전자적 침해 행위로부터 보호가 필요한 정보 통신 기반 시설을 주요 정보 통신 기반 시설로 지정할 수 있다.

(1) 당해 정보 통신 기반 시설을 관리하는 기관이 수행하는 업무의 국가 사회적 중요성

(2) 기관이 수행하는 업무의 정보 통신 기반 시설에 대한 의존도

(3) 다른 정보 통신 기반 시설과의 상호 연계성

(4) 침해 사고가 발생할 경우 국가 안전 보장과 경제 사회에 미치는 피해 규모와 범위

(5) 침해 사고의 발생 가능성 또는 복구의 용이성

3. 정보 공유 분석 센터(ISAC)[제16조]

금융• 통신 등 분야별 정보 통신 기반 시설을 보호하기 위해 ISAC를 구축• 운영

(1) 취약점과 대응 방안 정보 제공

(2) 침해 사고가 발생한 경우 실시간 경보• 분석 체계 운영

제9장 클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률[시행 2017.7.26]

1. 주요 용어[제2조]

(1) 클라우드 컴퓨팅

집적• 공유된 정보 통신 기기• 정보 통신 설비• 소프트웨어 등 정보 통신 자원을 이용자의 요구나 수요 변화에 따라 정보 통신망을 통해 신축적으로 이용할 수 있도록 하는 정보 처리 체계

(2) 클라우드 컴퓨팅 기술

클라우드 컴퓨팅의 구축 및 이용에 관한 정보 통신 기술

(3) 클라우드 컴퓨팅 서비스

클라우드 컴퓨팅을 활용해 상용(商用)으로 타인에게 정보 통신 자원을 제공하는 서비스

2. 다른 법률과의 관계[제4조]

(1) 해당 법은 클라우드 컴퓨팅의 발전과 이용 촉진 및 이용자 보호에 관해 다른 법률에 우선해 적용

(2) 개인 정보 보호에 관하여는 개인 정보 보호법• 정보 통신망 이용 촉진 및 정보 보호 등에 관한 법률 등 관련 법률에서 정하는 바에 따른다

3. 기본 계획 및 시행 계획의 수립[제5조]

과학 기술 정보 통신부 장관은 클라우드 컴퓨팅의 발전과 이용 촉진 및 이용자 보호와 관련된 중앙 행정 기관의 클라우드 컴퓨팅 관련 계획과 시책 등을 종합해 3년마다 기본 계획을 수립

4. 클라우드 컴퓨팅 사업의 수요 예보[제13조]

국가 기관 등의 장은 연 1회 이상 소관 기관의 클라우드 컴퓨팅 사업의 수요 정보를 과학 기술 정보 통신부 장관에게 제출

4. 이용자 정보의 보호[제27조]

클라우드 컴퓨팅 서비스 제공자는 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 이외의 용도로 이용할 경우 다음 사항을 정보 주체에게 고지하고 동의를 받아야 한다.

(1) 이용자 정보를 제공 받는 자

(2) 이용자 정보의 이용 목적

(3) 이용 또는 제공하는 이용자 정보의 항목

(4) 이용자 정보의 보유 및 이용 기간

(5) 동의를 거부할 권리가 있다는 사실

(6) 동의 거부에 따라 불이익이 있는 경우 그 불이익 내용

제10장 전자 정부법[시행 2017.10.24]

1. 전자 정부 기본 계획의 수립[제5조]

중앙 사무 관장 기관의 장은 전자 정부의 구현·운영 및 발전을 위하여 5년마다 행정 기관 등의 기관별 계획을 종합해 전자 정부 기본 계획을 수립

2. 정보 주체의 사전 동의[제42조]

이용 기관이 공동 이용 센터를 통해 개인 정보가 포함된 행정 정보를 공동 이용할 때에는 정보 주체가 다음 사항을 알 수 있도록 정보 주체의 사전 동의가 필요

(1) 공동 이용의 목적

(2) 공동 이용 대상 행정 정보 및 이용 범위

(3) 공동 이용 대상 이용 기관의 명칭

3. 한국 지역 정보 개발원의 설립[제72조]

둘 이상의 지방 자치 단체는 소관 정보화 사업을 공동으로 추진하기 위해 한국 지역 정보 개발원을 설립

제11장 위치 정보의 보호 및 이용 등에 관한 법률[시행 2018.10.18]

제12장 신용 정보의 이용 및 보호의 관한 법률[시행 2018.8.14]

제1장 암호의 기초

1. 기본 용어

(1) 평문과 암호문

1) 평문

누구나 이해할 수 있거나 접근할 수 있는 정보 형태

2) 암호문

누구나 이해할 수 없거나 접근할 수 없는 정보 형태

(2) 암호화• 복호화의 주체

1) 암호화의 주체는 송신자 또는 출발지

2) 복호화의 주체는 수신자 또는 목적지

(3) 선형과 비선형

1) 선형

단일한 입력으로 단일한 출력

2) 비선형

단일한 입력으로 다양한 출력

2. 암호문의 종류

(1) 전치(Transposition) 방식

행렬과 역행렬의 관계처럼 평문의 위치를 재배치하는 방식

(2) 치환(Substitution) 방식

특정 문자를 다른 문자로 대치하는 방식

(3) 스테가노그래피 방식

정보 내용의 존재 자체를 은폐하는 방식으로 위조 지폐 식별 등을 위한 워터마크• 구매자를 추적하기 위한 핑거프린트 등과 같은 전자 저작권 관리(DRM)에 영향

3. 암호 기법의 분류

(1) 블록 암호 기법

1) 평문을 64 비트• 128 비트 등과 같이 일정한 크기의 블럭 단위로 구분한 뒤 각각의 블

럭마다 확산을 위한 전치 방식• 혼돈을 위한 치환 방식을 동시에 적용해 16회 등과 같이 반복적으로 적용

2) 확산이란 평문과 암호문의 관계를 은폐하는 개념이고, 혼돈은 암호문과 열쇠의 관계를 은폐하는 개념

3) 주로 소프트웨어 기법을 통해 구현하며, DES와 AES 등과 같은 암호 알고리즘에서 사용

(2) 스트림 암호 기법

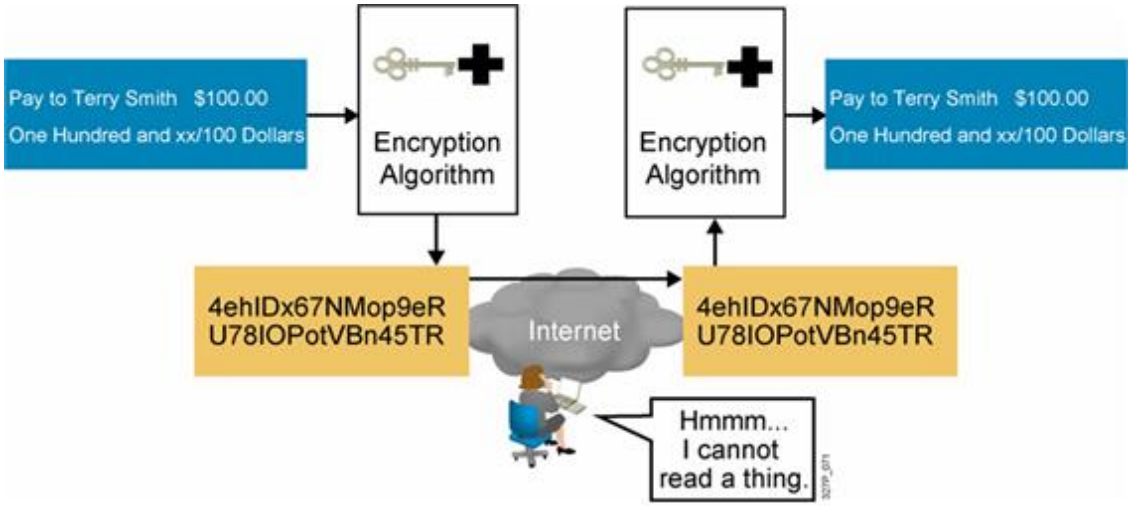
1) 평문과 열쇠를 XOR 연산해 암호문을 생성

2) 주로 선형 귀환 이동 레지스터(LFSR) 등과 같은 하드웨어 기법을 통해 구현

4. 사이버 보안의 구성 요소

가상 공간에서는 송신자와 수신자의 대면이 없다는 가정이 필요

(1) 기밀성(Confidentiality)



1) 쌍방간에 주고받는 실제 정보의 비밀성을 보장하는 개념

2) 소극적인 공격 등이 위협 요소

3) 각종 VPN 기법 등을 통해 기밀성을 유지

(2) 무결성(Integrity)

1) 쌍방간에 주고받는 실제 정보의 정확성을 보장하는 개념

2) 다시 말해, 상호간에 사용하는 열쇠의 유출 유무를 검증해 정보의 훼손• 변조• 유출 등을 방지하는 개념

3) 적극적인 공격 등이 위협 요소

4) 요약 함수 또는 전자 서명 등을 통해 무결성을 유지

(3) 인증(Authentication)

1) 송신자와 수신자 사이의 확신성을 보장하는 개념

2) 인증 정보 또는 생체 인식 등에 기반하며, 접근 통제의 적용 대상

3) HMAC 기법 또는 전자 서명 등을 통해 인증을 유지

(4) 가용성(Availability)

1) 정당한 사용자가 필요할 때마다 즉각적으로 정보에 접근해 사용하는 개념

2) DDoS 공격 또는 자연 재해 등이 위협 요소

3) 사업 연속성 계획(BCP)• 재난 복구 계획(DRP) 등을 통해 가용성을 유지

(5) 부인 방지(Non-Repudiation)

1) 송신자가 정보를 전송했는데 수신자가 이를 부인하는 일 등을 방지하는 개념

2) 다시 말해, 특정 행위나 사건 등을 증명해 나중에 그러한 부분을 부인할 수 없게 하는 일종의 공증과 같은 개념

3) 전자 서명 등을 통해 부인 방지를 유지

5. 암호 해독의 분류

(1) 암호문 단독 공격

송신자와 수신자 사이에서 오직 암호문만으로 열쇠를 획득하는 방법

(2) 기지 평문 공격

ECB 운영 모드와 같이 송신자와 수신자 사이에서 일부 알려진 평문과 암호문의 관계에 기반해 열쇠를 획득하는 방법

(3) 선택 평문 공격

암호화를 수행하는 송신측에서 열쇠를 획득하는 방법

(4) 선택 암호문 공격

복호화를 수행하는 수신측에서 열쇠를 획득하는 방법

제2장 대칭적 기밀성 알고리즘

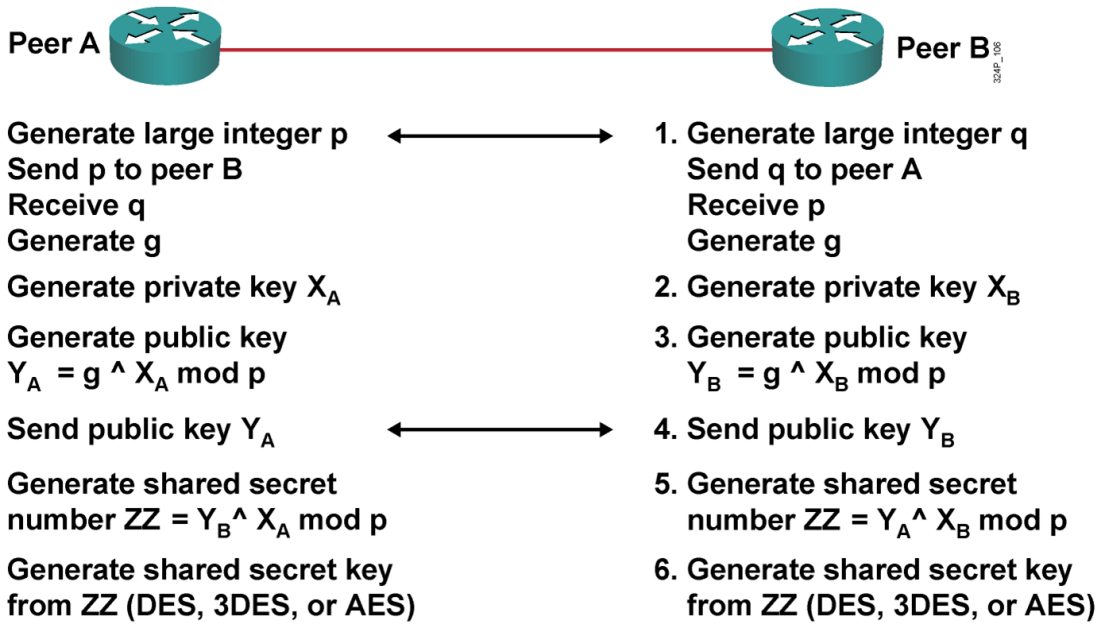
1. 대칭 구조 방식에 기반한 기밀성 알고리즘의 이해

(1) 암호화• 복호화에 비밀 열쇠 또는 사전 공유 열쇠를 대칭적으로 사용하는 블록 기반의 암호 구조이기 때문에 N 명의 사용자가 상호간에 사용하는 열쇠의 갯수는 N(N-1)/2 개에 해당

(2) 통신하기 전 송신자• 수신자 사이에 열쇠의 전달 또는 공유 등과 같은 이른바 비밀 열쇠의 분배 문제가 발생

2. DH 알고리즘의 이해

(1) 1976년 이산 대수 문제에 따라 비밀 열쇠의 분배 문제를 해결하기 위해 송신자• 수신자 사이에 한 쌍의 공개 열쇠• 개인 열쇠를 각각 생성하고 공개 열쇠를 상호 교환한 뒤 상호 호환 가능한 비밀 열쇠를 생성하는 방식



1) 앨리스와 밥은 두 개의 소수 p = 23과 g = 7을 사용하기로 합의

2) 앨리스는 임의의 정수 a = 3을 고른 뒤 밥에게 x = g^a mod p 값을 전송

x = 7^3 mod 23 = 21

3) 밥은 임의의 정수 b = 2를 고른 뒤 앨리스에게 y = g^b mod p 값을 전송

y = 7^2 mod 23 = 3

4) 앨리스는 밥에게서 받은 y 값을 바탕으로 s = y^a mod p 값을 계산

s = 3^3 mod 23 = 4

5) 밥은 앨리스에게서 받은 x 값을 바탕으로 s = x^b mod p 값을 계산

s = 21^2 mod 23 = 4

6) 앨리스와 밥은 이제 비밀 열쇠 s = 4 값을 공유

(2) DH 알고리즘 종류에는 사용하는 열쇠의 길이에 따라 DH1 방식• DH2 방식• DH5 방식 등으로 구분

(3) DH 알고리즘에서 사용하는 공개 열쇠• 개인 열쇠는 비밀 열쇠를 생성하기 위한 용도로만 사용

3. 대칭 구조 방식에 기반한 기밀성 알고리즘의 종류

(1) DES 방식

1) 64 비트 블록 단위로 P 박스에 기반한 전치 방식• S 박스에 기반한 치환 방식을 혼용해 16회 암호화

2) 비밀 열쇠의 크기는 64 비트이지만 실제 크기는 56 비트

3) 페이스텔 기반 구조

암호화• 복호화 과정이 동일

(2) AES 방식

1) 128 비트 블록 단위로 암호화

2) 비밀 열쇠의 크기는 128 비트(AES-128)• 192 비트(AES-192)• 256 비트(AES-256)로 구성하기 때문에 라운드 횟수도 이에 따라 가변적

3) SPN 기반 구조

암호화• 복호화 과정이 상이

(3) SEED 방식

1) 일종의 한국형 DES 방식

2) 128 비트 블록 단위로 16회 암호화

3) 128 비트 크기의 비밀 열쇠를 이용

4) SPN 기반 구조

(4) ARIA 방식

1) 일종의 한국형 AES 방식으로 블록 단위와 열쇠의 크기가 AES 방식과 동일

2) SPN 기반 구조

(5) IDEA 방식

1) 128 비트의 비밀 열쇠를 이용해 64 비트 블록 단위로 8회 암호화

2) SPN 구조이고, PGP VPN 기법 등에서 사용

(6) RC4 방식

1) 스트림 암호 기법

2) 40 비트 크기의 비밀 열쇠 기반으로 WEP 방식 등에서 사용하는 스트림 암호

4. 위협 요소

(1) 차분 공격

일종의 선택 평문 공격으로 입력 값의 변화에 따라 출력 값의 변화를 이용하는 공격

(2) 선형 공격

일종의 기지 평문 공격으로 비선형 구조를 선형 구조로 변형하는 공격

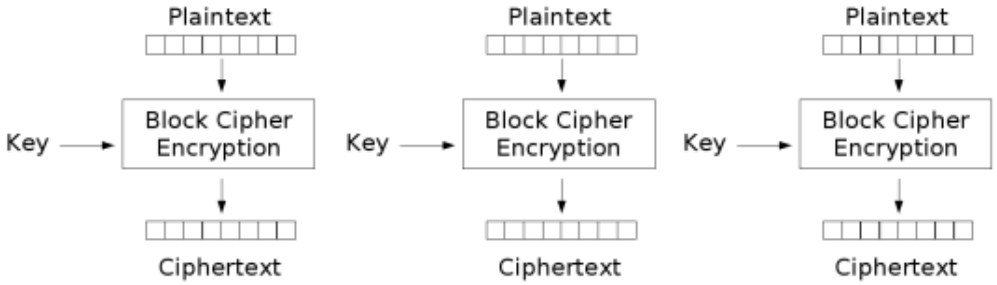
(3) 전수 공격

일종의 암호문 단독 공격

제3장 대칭 구조 방식에서 블록 암호의 운영 모드

1. 운영 모드의 종류

(1) ECB 모드



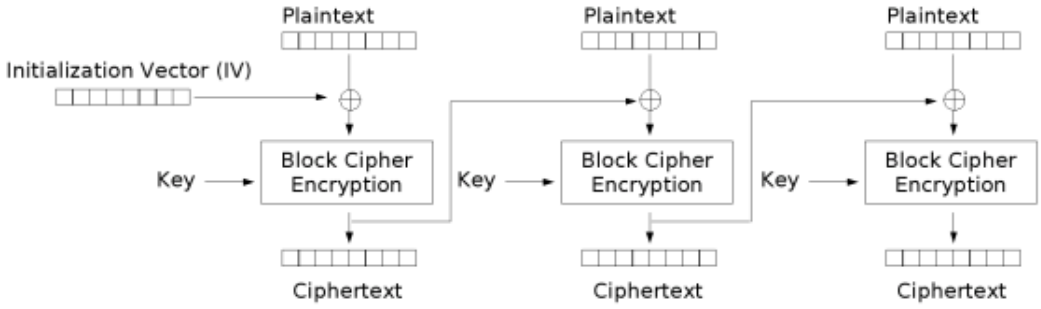
Electronic Codebook (ECB) mode encryption

1) 64 비트 블록 단위의 평문과 암호문이 각각 일대일 관계를 형성하기 때문에 평문과 암호문이 동일

2) 데이터베이스 분야 등에서 사용

3) 보안에 취약

(2) CBC 모드



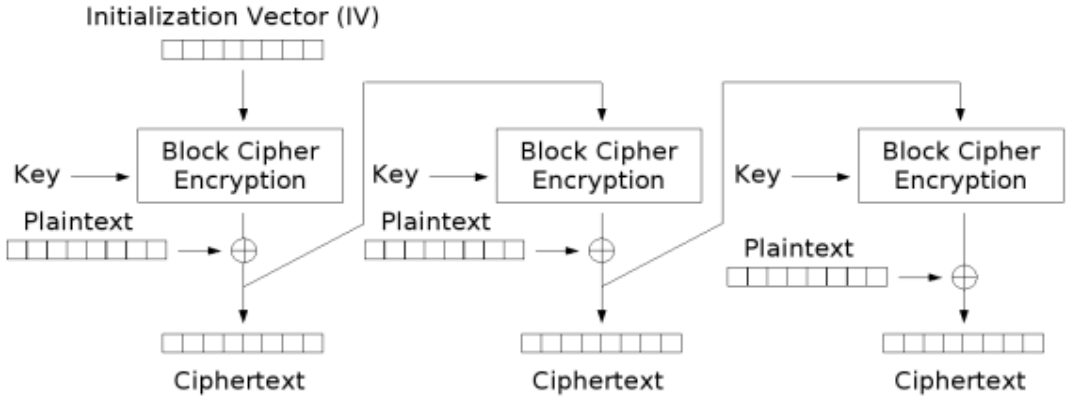
Cipher Block Chaining (CBC) mode encryption

1) 초기 벡터는 송신자와 수신자 사이에 미리 공유

2) IPSec VPN 방식과 커버로스 방식 등에서 사용

3) 평문 안의 비트에서 발생한 오류는 다음 블록의 암호문에 영향을 줌

(3) CFB 모드

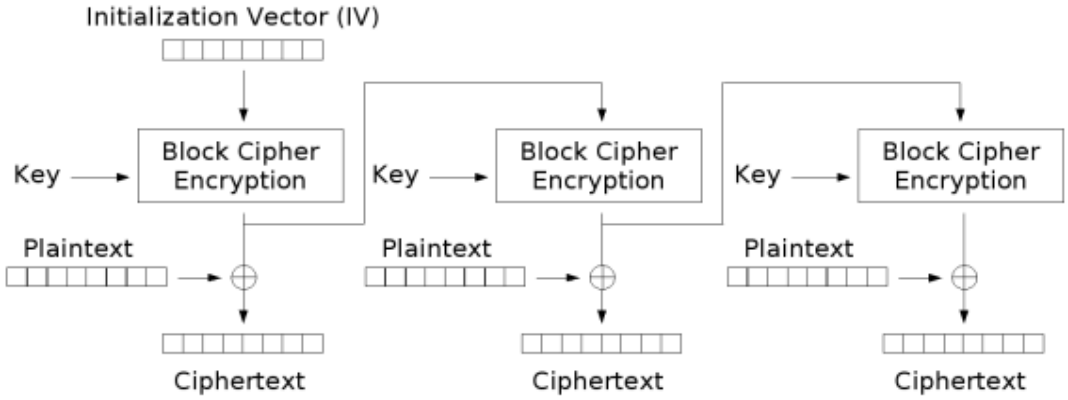


Cipher Feedback (CFB) mode encryption

1) 스트림 암호 방식과 호환

2) 복호화 과정에서는 영향을 주지 않지만 암호화 과정에서는 여전히 영향을 줌

(4) OFB 모드



Output Feedback (OFB) mode encryption

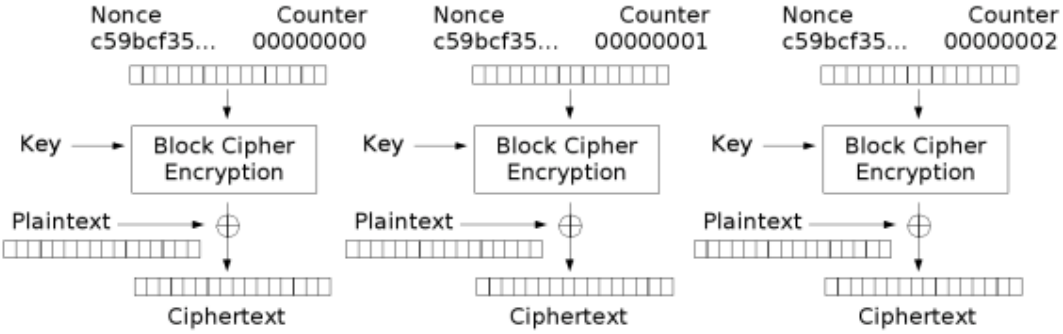
1) 스트림 암호 방식과 호환

2) CBC 모드• CFB 모드의 오류 전파 속성을 제거

(5) CTR 모드

1) 스트림 암호 방식과 호환

2) 64 비트 블록마다 카운터를 가진 난수를 생성



Counter (CTR) mode encryption

3) CBC 모드• CFB 모드의 오류 전파 속성을 제거

2. 비대칭 구조 방식에는 블록 운영 모드가 없다.

제4장 비대칭적 기밀성 알고리즘

1. 비대칭 구조 방식에 기반한 기밀성 알고리즘의 이해

(1) 암호화• 복호화에 한 쌍의 공개 열쇠• 개인 열쇠를 사용하는 구조

1) 송신자는 수신자의 공개 열쇠를 이용해 암호화

2) 수신자는 수신자 자신의 개인 열쇠를 이용해 복호화

3) 비대칭 구조 방식에서는 DH 알고리즘을 통해 생성한 비밀 열쇠가 불필요

4) 비대칭 구조 방식에서는 N 명의 사용자가 있다면 2N 개의 열쇠가 필요

(2) 대칭 구조 방식의 종류보다 열쇠의 길이가 상대적으로 길기 때문에 처리 속도 지연이 크다

(3) 비대칭 구조 방식에서는 이른바 공개 열쇠의 신뢰 문제가 발생하기 때문에 PKI 구조가 필요

2. PKI 구조의 이해

비대칭 구조 방식에 기반한 기밀성을 광범위하게 활용하기 위한 기술적• 조직적• 법률적 트리 형태의 기반 시설

(1) 인증 기관

1) 과학 기술 정보 통신부 장관이 지정한 인증 기관은 계층 구조를 형성하면서 공인 인증서를 발급

2) 공인 인증서 폐기 목록(CRL) 등을 관리

3) OCSP 방식을 통해 실시간으로 공인 인증서 상태를 확인

(2) 등록 기관

사용자와 인증 기관 사이에서 중간 대행자 역할을 수행하거나 인증 기관 역할을 대행

(3) 디렉토리 서비스 서버

X.509 형식의 공인 인증서 등을 저장하는 일종의 데이터베이스 서버로 X.500 방식과 이를 간략화한 LDAP 방식 등을 사용

3. 공인 인증서 발급 시 구성 내용

전자 서명법 제15조에서 규정

4. 비대칭 구조 방식에 기반한 기밀성 알고리즘의 종류

(1) RSA 방식

1) 비대칭 구조 방식에서 사실상 표준

2) 1978년 소인수 분해 문제에 기반해 개발

3) 기밀성뿐 아니라 무결성• 인증• 부인 방지까지 확장해 사용 가능

(2) 로빈 방식

소인수 분해 문제에 기반해 구현

(3) 엘가말 방식

이산 대수 문제에 기반해 구현

(4) 타원 곡선 암호(ECC) 방식

1) 이산 대수 문제에 기반해 구현

2) RSA 방식보다 짧은 열쇠를 이용해 높은 보안성을 구현

3) 전자 상거래 환경 등에 적합

5. 위협 요소

(1) 무차별 대입 공격

(2) 중간자 개입 공격

1) 공개 열쇠를 이용하는 DH 알고리즘과 RSA 알고리즘 등에서 가장 위협적인 요소

2) PKI 방식의 공개 열쇠와 전자 서명 등을 적용한 국대국(Station To Station) 프로토콜 사용

6. 하이브리드 방식에 기반한 기밀성 알고리즘의 종류

(1) SSH VPN 경우

원격 접속에 필요한 인증 정보는 비대칭 구조 방식으로 암호화하고, 실제 정보는 대칭 구조 방식으로 암호화

```
Router(config)#hostname keysco

keysco(config)#ip domain-name cisco.com #열쇠 생성 시 사용할 문자열 정보 설정

keysco(config)#crypto key generate rsa
The name for the keys will be: cisco.cisco.com
Choose the size of the key modulus in the range of 360 to 2048
for your General Purpose Keys.
Choosing a key modulus greater than 512
```

```
may take a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

keysco(config)#username cisco secret 1234
keysco(config)#enable secret 1234

keysco(config)#line vty 0 4
keysco(config-line)#login local
keysco(config-line)#transport input ssh

keysco(config)#ip ssh version 2
keysco(config)#ip ssh time-out 30
keysco(config)#ip ssh authentication-retries 3
```

(2) SSL/TLS VPN 경우

1) 열쇠 분배 센터(KDC)의 개념

2) 비밀 열쇠를 공개 열쇠로 암호화해 전송하는 전자 봉투 기법을 사용

제5장 무결성 구현을 위한 전자 서명

1. 전자 서명의 개념

(1) 비대칭 구조 방식에서만 사용 가능

(2) 송신자는 자신이 서명한 부분을 자신의 개인 열쇠로 암호화

(3) 전자 서명을 통해 무결성• 인증• 부인 방지를 동시에 만족

2. 전자 서명의 종류

(1) RSA 방식• 로빈 방식• 엘가말 방식과 전자 서명 전용인 DSS 방식 등

(2) 국내 표준인 KCDSA 방식• ECKCDSA 방식

KCDSA 방식은 이산 대수 문제에 기반해 엘가말 방식을 개선한 방식으로 DSS 방식과도 유사

3. 이중 전자 서명

(1) 전자 상거래 등에서 거래자의 익명성을 보장하기 위해 구매자의 지불 정보와 주문 정보를 각각 상점과 은행에 은닉하기 위한 방식

(2) 주문 정보의 요약본과 지불 정보의 요약본을 합해 전체 요약본을 구한 뒤 고객의 개인 열쇠로 암호화

(3) 사용자의 주문 정보는 상점의 공개 열쇠로 암호화하고, 지불 정보는 은행의 공개 열쇠로 암호화

제6장 무결성 구현을 위한 요약 함수

1. 요약 함수의 개념

(1) 대칭• 비대칭 구조 방식에서 무결성 구현

(2) 가변적인 원본을 고정적인 요약본으로 처리하는 일종의 메시지 무결성 코드

(3) 요약본을 다시 원본으로 복원할 수 없는 일방향성

1) 역상 저항성

주어진 임의의 출력 y 값에 대해 y = h(x)를 만족하는 입력 x 값을 구할 수 없다는 속성

2) 충돌 저항성

h(x) = h(x')와 같은 식을 만족하는 임의의 두 입력 x 값과 x' 값을 구할 수 없다는 속성

3) 요약 함수로 사용하는 경우 리눅스 계열에서는 솔트(salt) 방식을 이용해 충돌 저항성을 구현

```
root@xubuntu:~# cat /etc/shadow | egrep "root"

root:$6$hIhzqnvs$XxCI4aXM8Dp/...eLkbB0:17164:0:99999:7:::
```

(4) 요약 함수는 기본적으로 512 비트 블럭 단위로 처리

2. 리눅스 운영 체제에 기반한 요약 함수의 종류

(1) 128 비트 크기의 요약본을 출력하는 MD5 방식

(2) 160 비트 크기의 요약본을 출력하는 SHA-1 방식

(3) SHA-256 방식• SHA-512 방식 등을 SHA-2 방식이라고 통칭

(4) 160 비트 크기의 요약본을 출력하는 한국형 HAS-160 방식

3. HMAC(Hash-based Message Authentication Code) 개념

(1) 요약 함수에서는 무결성만을 지원하기 때문에 인증 기능을 동시에 만족할 수 있는 기법이 필요

(2) HMAC 방식이란 원본과 비밀 열쇠를 결합해 요약 함수로 처리하는 기법으로 무결성과 인증을 동시에 검증

(3) 부인 방지 기능은 불가능

4. 위협 요소

(1) 레인보우 테이블(Rainbow Table)은 요약 함수를 사용해 변환 가능한 모든 요약본을 저

장한 일종의 데이터베이스

Password	MD5 Hash
123456	e10adc3949ba59abbe56e057f20f883e
password	5f4dcc3b5aa765d61d8327deb882cf99
12345	827ccb0eea8a706c4c34a16891f84e7b
12345678	25d55ad283aa400af464c76d713c07ad
qwerty	d8578edf8458ce06fbc5bb76a58c5ca4
123456789	25f9e794323b453885f5181f1b624d0b
1234	81dc9bdb52d04dc20036dbd8313ed055
baseball	276f8db0b86edaa7fc805516c852c889
dragon	8621ffdbc5698829397d97767ac13db3
football	37b4e2d82900d5e94b8da524fbeb33c0

(2) 레인보우 테이블을 통해 요약본에서 원본을 검색

```
root@kali:~# cat /etc/shadow | egrep "root"

root:$6$/4PVlupz$:

root@kali:~# unshadow /etc/passwd /etc/shadow > /tmp/password.txt

root@kali:~# john --format=crypt /tmp/password.txt

Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
1234             (root)
1g 0:00:00:01 DONE (2017-02-02 10:55) 0.7299g/s 70.07p/s 70.07c/s 70.07C/s
123456..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

제7장 접근 통제 보안 모형

1. 강제적 접근 통제(MAC)

(1) 관리자가 중앙 집권적으로 다단계 보안 등급을 설정해 접근 권한을 부여하는 방식

(2) 일례로 방화벽 등에서 사용

2. 임의적 접근 통제(DAC)

(1) 정보의 소유자가 정보의 보안 수준 등을 결정

(2) 일례로 리눅스 계열 등에서 접근 권한을 부여하는 방식

3. 역할 기반 접근 통제(RBAC)

(1) 사용자의 역할 또는 직능에 따라 구현한 방식

(2) 관리자는 주체에게 구체적인 역할을 부여한 뒤 해당 역할의 접근 권한을 집합적으로 부여하기 때문에 인사 이동이 빈번한 조직 등에 적합한 방식

(3) 일례로 리눅스 계열 등에서 계정이 속한 그룹에 접근 권한을 부여

제8장 다양한 보안 모형

1. 벨 라파둘라 모형

(1) 특징

기밀성을 강조한 방식으로 강제적 접근 통제의 이론적 토대

(2) 접근 권한

1) 자기보다 상위 수준의 문서는 읽을 수 없고, 자기보다 하위 수준의 문서는 읽을 수 있음

2) 자기보다 상위 수준의 문서에는 쓸 수 있고, 자기보다 하위 수준의 문서에는 쓸 수 없음

2. 비바 모형

(1) 특징

벨 라파둘라 모형의 단점인 무결성을 보장하기 위한 모형

(2) 접근 권한

1) 자기보다 상위 수준의 문서는 읽을 수 있고, 자기보다 하위 수준의 문서는 읽을 수 없음

2) 자기보다 상위 수준의 문서에는 쓸 수 없고, 자기보다 하위 수준의 문서에는 쓸 수 있음

3. 클락• 윌슨 모형

비바 모형의 확장판으로 사용자가 직접 객체에 접근할 수 없고, 해당 소프트웨어를 통해서만 접근 가능

제9장 사용자 인증

1. 지식 기반 인증(Something You Know)

계정/비밀 번호

2. 소유 기반 인증(Something You Have)

스마트 카드• 토큰

3. 인체 기반 인증(Something You Are)

생체 인증 시스템의 정확성 측정 기준

(1) 잘못된 허용 비율(FAR)

성대 모사 등에 의한 우회

(2) 잘못된 거부 비율(FRR)

감기 등에 의한 거부

제10장 다양한 인증 방식

1. 영 지식 증명의 개념

비밀 번호 전송이 없어도 상호 인증이 가능한 기법

2. 커버로스 방식의 인증 과정

(1) DES 방식 등과 같은 대칭 구조 방식 기반의 대표적인 통합 인증 체계(SSO) 시스템

(2) 사용자는 커버로스 서버에 이미 등록한 계정과 비번 등을 입력

(3) 티켓 승인 서버는 비밀 열쇠로 암호화한 티켓을 사용자에게 전송

(4) 사용자는 비밀 열쇠로 전송받은 티켓을 복호화

(5) 이후 사용자는 티켓만으로 해당 서버로 접속

(6) 티켓의 유효 시간은 통상 8시간 정도

제1장 리눅스 운영 체제의 구성

1. 커널의 이해

(1) 운영 체제의 핵심

(2) 주 기억 장치에 상주하면서 가장 하위 수준에서 하드웨어 전반을 관리

2. 이중 공간과 시스템 호출의 이해

(1) 이중 공간

운영 체제를 보호하기 위해 사용자 영역과 커널 영역으로 구분한 공간

(2) 시스템 호출

사용자 영역에서 커널 영역의 함수를 호출하는 경우

3. 프로세스와 데몬의 이해

(1) 프로세스

주 기억 장치에서 현재 동작 중인 프로그램

(2) 데몬

외부로부터 접속을 기다리는 프로세스

1) 독립형 방식

해당 데몬이 항시 접속 대기 상태를 유지하는 방식

```
root@xubuntu:~# cat /etc/vsftpd.conf

listen=YES #독립형 방식 사용 설정

이하 내용 생략
```

2) 수퍼 데몬 방식

수퍼 데몬이 항시 접속 대기 상태를 유지하다 접속 요청이 발생할 경우 수퍼 데몬이 해당 데몬을 활성 상태로 전환시키는 방식

```
root@xubuntu:~# cat /etc/vsftpd.conf

listen=NO #수퍼 데몬 방식 사용 설정

이하 내용 생략
```

4. TCP Wrapper 도구

수퍼 데몬 방식에서 사용 가능한 방화벽

(1) 구성 내역

```
root@xubuntu:~# cat /etc/xinetd.conf

service ftp
{
 flags           = REUSE #주소 재사용 활성화
 disable         = no #수퍼 데몬 방식 사용
 log_on_failure  += USERID #접속 실패한 ID 기록
 wait            = no #다중 쓰레드 지원
 user            = root #사용 권한
 socket_type     = stream #TCP 방식
 only_from       = 192.168.10.0/24 #특정 IP 주소 또는 IP 대역만 접근 허용
 no_access       = 192.168.10.201 #특정 IP 주소 또는 IP 대역만 접근 차단
 access_times    = 09-18 #접근 허용 시간대 설정(24시 기준)
 instances       = 5 #동시에 서비스할 수 있는 서버의 최대 개수 지정
 per_source      = 10 #동일한 출발지 IP 주소로부터 최대 서비스 연결 개수를 10으로 제한
 cps             = 20 5 #초당 연결 개수를 20으로 제한하고 이를 초과 시 5초간 일시 중지
한 뒤 다시 서비스를 개시
 server          = /usr/sbin/vsftpd vsftpd
#server          = /usr/sbin/tcpd vsftpd #TCP Wrapper 도구 적용 설정
}
includedir /etc/xinetd.d
```

(2) 접속 허용[우선 적용]

```
root@xubuntu:~# cat /etc/hosts.allow

ALL:LOCAL
in.ftpd:192.168.10.0/255.255.255.0
httpd:ALL
```

(3) 접속 차단

```
root@xubuntu:~# cat /etc/hosts.deny

ALL:ALL
```

5. 쉘(Shell)의 이해

(1) 사용자와 운영 체제 사이에서 대화할 수 있는 일종의 명령어 해석기

(2) 커널과 달리 보조 기억 장치에서 교체 가능

(3) 2014년 쉘 쇼크(Shell Shock) 취약점(cve-2014-6271) 발견

원격에서 악성 코드가 실행 가능한 취약점으로서 아래와 같이 확인

```
root@metasploitable:~# env x='() { :;}; echo vulnerable' bash -c "echo cve-2014-6271"

vulnerable #취약점이 있는 경우 해당 문자열 출력
cve-2014-6271 #취약점 여부와 무관하게 해당 문자열 출력
```

제2장 리눅스 운영 체제의 자원 관리

1. 접근 권한의 이해

(1) 파일 단위

1) R은 파일의 내용을 볼 수 있다는 의미

2) W는 파일을 생성• 수정할 수 있다는 의미

3) X는 파일의 내용을 실행할 수 있다는 의미

(2) 디렉토리 단위

1) R은 디렉토리 목록을 볼 수 있다는 의미

2) W는 디렉토리에서 파일 또는 디렉토리를 생성• 수정할 수 있다는 의미

3) X는 디렉토리로 진입할 수 있다는 의미

2. 사용자 마스크 이해

(1) 파일이나 디렉토리 등을 생성할 때 기본적인 접근 권한을 설정하는 초기 값

(2) umask 명령어로 확인 가능

```
odj@xubuntu:~$ umask

0002
```

(3) 파일과 디렉토리 생성 시 기본 접근 권한 예시

1) 파일을 생성하면 기본 접근 권한은 0666 - 0022 = 0644

2) 디렉토리를 생성하면 기본 접근 권한은 0777 - 0022 = 0755

3. SetUID 이해

(1) 임의의 정보를 실행하는 동안 해당 정보의 소유자 권한으로 실행하는 기능으로서 일시적인 공유에 해당

(2) 비록 일반 사용자일지라도 SetUID로 설정된 관리자 정보를 실행시키는 동안 일반 사용자의 권한은 권리자 권한으로 상승

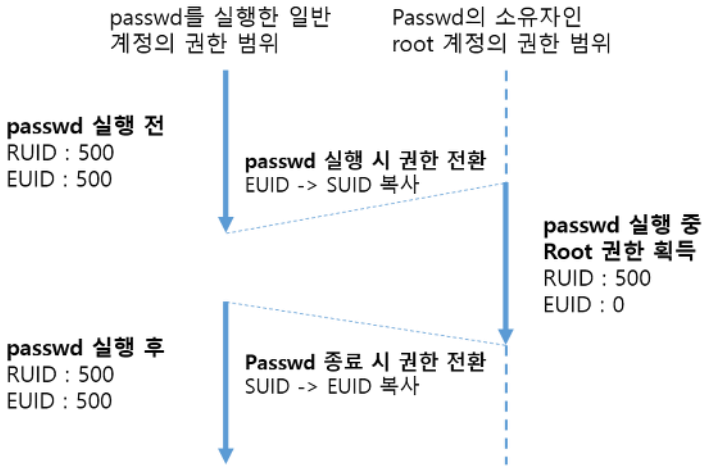
1) 비번을 변경하는 명령어

```
odj@xubuntu:~$ ls -l /usr/bin/passwd

-rwsr-xr-x 1 root root 62024  1월 26  2018 /usr/bin/passwd
```

2) 비번을 저장하는 영역

```
odj@xubuntu:~$ ls -l /etc/shadow

-rw-r----- 1 root shadow 1523 11월  11 11:57 /etc/shadow
```

(3) 다양한 UID 이해



1) RUID(RealUserID)

프로세스의 실제 소유자(접속할 때 사용한 계정의 UID를 의미)로서 프로세스를 시작하는 사용자를 결정하는데 사용

```
odj@xubuntu:~$ id
uid=1000(odj) gid=1000(odj) 그룹들=1000(odj)

odj@xubuntu:~$ who am i #RUID
odj         pts/0           2019-03-19 08:25 (192.168.10.1)

odj@xubuntu:~$ whoami #EUID
odj
```

2) EUID(EffectiveUserID)

일반적으로 실제 사용자(RUID)와 유효 사용자(EUID)는 동일하지만, EUID는 SetUID 권한이 설정된 실행 프로세스에 의해 변경되기 때문에 EUID에는 일시적으로 다른 계정의 UID가 저장

```
odj@xubuntu:~$ su root
암호:

root@xubuntu:/home/odj# id
uid=0(root) gid=0(root) 그룹들=0(root)

root@xubuntu:/home/odj# who am i #RUID
```

```
odj      pts/0        2019-03-19 08:25 (192.168.10.1)

root@xubuntu:/home/odj# whoami #EUID
root
```

3) SUID(SavedsetUserID)

원래의 EUID를 저장할 때 사용

4. 스티키 비트 이해

(1) 모든 일반 사용자가 자유롭게 정보를 생성할 수 있는 영구적인 공유 영역

```
root@xubuntu:~# ls -lF / | grep tmp

drwxrwxrwt  11 root root  4096  4월 30 10:39 tmp/
```

(2) 정보의 소유자 또는 관리자만이 해당 정보를 삭제

5. chattr 명령어의 이해

정보의 소유자일지라도 읽기 전용으로만 사용할 수 있고, 관리자 계정조차 해당 정보를 변경할 수 없다.

```
root@xubuntu:/tmp# touch odj.txt

root@xubuntu:/tmp# file odj.txt
odj.txt: empty

root@xubuntu:/tmp# lsattr odj.txt
--------------e--- odj.txt

root@xubuntu:/tmp# chattr +i odj.txt

root@xubuntu:/tmp# rm -f odj.txt

rm: 'odj.txt'를 지울 수 없음: 명령을 허용하지 않음

root@xubuntu:/tmp# chattr -i odj.txt

root@xubuntu:/tmp# rm -f odj.txt
root@xubuntu:/tmp#
```

제3장 리눅스 운영 체제의 find 명령어 사용법

```
root@xubuntu:~# stat index.html
File: index.html
Size: 1203            Blocks: 8          IO Block: 4096   일반 파일
Device: 801h/2049d    Inode: 1591579     Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)

Access: 2018-05-06 13:45:26.670290363 +0900
Change: 2018-05-19 09:11:43.527926686 +0900
Modify: 2018-05-19 09:11:43.527926686 +0900

Birth: -
```

1. 전체 정보를 대상으로 해당 정보에 접근한 마지막 시간(10일 미만)을 검색

```
root@xubuntu:~# find / -type f -user root -atime -10 > /tmp/atime.txt &
```

2. 전체 정보를 대상으로 해당 정보의 속성을 변경한 마지막 시간(10일 초과)을 검색

```
root@xubuntu:~# find / -type f -user root -ctime +10 > /tmp/ctime.txt &
```

3. 전체 정보를 대상으로 해당 정보의 내용을 수정한 마지막 시간(정확히 10일)을 검색

```
root@xubuntu:~# find / -type f -user root -mtime 10 > /tmp/mtime.txt &
```

4. SetUID만 설정한 파일을 검색

```
root@xubuntu:~# find / -type f -user root -perm 4000 > /tmp/setuid.txt &
```

5. SetUID를 포함한 파일을 검색

```
root@xubuntu:~# find / -type f -user root -perm -4000 > /tmp/setuid.txt &
```

제4장 리눅스 운영 체제의 로그 관리

1. 시스템 로그 설정

```
root@xubuntu:~# cat /etc/rsyslog.conf
module(load="imuxsock") #provides support for local system logging
module(load="imklog") #provides kernel logging support
$KLogPermitNonKernelFacility on

이하 내용 생략

$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
$RepeatedMsgReduction on
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog
$WorkDirectory /var/spool/rsyslog
$IncludeConfig /etc/rsyslog.d/*.conf

root@xubuntu:~# service rsyslog restart
```

(1) 기본 형식 facility.priority logfile-location

facility 데몬과 관련해 priority 우선 순위에 해당하는 상황이 발생하면 logfile-location 위치에 데몬 기록을 남기라는 형식

(2) 메시지 우선 순위(낮은 순서에서 높은 순서)

```
debug > info > notice > warning > err > crit > alert > emerg
```

2. 주요 시스템 로그 확인

(1) who 명령어를 입력하면 utmp에서 현재 로그인한 사용자들에 대한 상태 정보를 출력

```
root     pts/0        2018-10-17 21:11 (:0.0)
root     pts/1        2018-10-17 21:13 (192.168.10.1)
```

(2) last 명령어를 입력하면 wtmp에서 사용자들이 로그인 또는 로그아웃한 정보를 출력

```
root     pts/0        python-pc.local  Sun Apr 30 09:57    still logged in
odj      tty7         :0               Sun Apr 30 09:56    still logged in
reboot   system boot  3.2.0-4-686-pae  Sun Apr 30 09:56 - 11:11  (01:14)
root     pts/0        python-pc.local  Sat Apr 29 18:29 - down    (01:42)
odj      tty7         :0               Sat Apr 29 18:26 - down    (01:45)
reboot   system boot  3.2.0-4-686-pae  Sat Apr 29 18:25 - 20:11  (01:45)
```

```
root     pts/0        python-pc.local  Wed Apr 26 21:08 - down    (00:04)
odj      tty7         :0               Wed Apr 26 21:06 - down    (00:06)
reboot   system boot  3.2.0-4-686-pae  Wed Apr 26 21:06 - 21:12   (00:06)
root     pts/0        python-pc.local  Mon Apr 24 20:01 - down    (00:18)
odj      tty7         :0               Mon Apr 24 19:59 - down    (00:19)
reboot   system boot  3.2.0-4-686-pae  Mon Apr 24 19:59 - 20:19   (00:19)
root     pts/0        python-pc.local  Mon Apr 24 19:32 - down    (00:24)

wtmp begins Mon Apr 24 19:32:22 2017
```

(3) lastb 명령어를 입력하면 btmp에서 5번 이상 접속 실패한 정보를 출력

```
btmp begins Sat Apr 22 10:07:54 2017
```

(4) lastlog 명령어를 입력하면 lastlog에서 각 사용자의 최근 로그인 시간과 접근한 소스 호스트에 대한 정보를 출력

```
Username         Port     From             Latest
root             pts/1    192.168.10.1     Wed Oct 17 21:13:03 -0400 2018
daemon                                     **Never logged in**
bin                                        **Never logged in**

이하 내용 생략

msfadmin         tty1                      Sun Nov 16 01:38:25 -0500 2014

이하 내용 생략
```

(5) dmesg 명령어를 입력하면 dmesg에서 운영 체제 시작 시 출력한 제반 정보를 출력

```
이하 내용 생략

[    38.462211] Bluetooth: Core ver 2.21
[    38.462242] NET: Registered protocol family 31
[    38.462245] Bluetooth: HCI device and connection manager initialized

이하 내용 생략
```

(6) lastcomm 명령어 등을 입력하면 acct/pacct에서 사용자가 로그인한 뒤부터 로그아웃할 때까지 입력한 명령과 시간 등의 정보를 출력(유닉스 운영 체제)

제5장 유닉스• 리눅스 운영 체제의 기타 보안 설정

1. 관리자 계정의 원격 접속 차단 설정

AIX 운영 체제	HP-UX 운영 체제	솔라리스 운영 체제	주분투 운영 체제
/etc/security/**user**	/etc/**securetty**	/etc/default/**login**	/etc/**pam.d/login**

2. 비밀 번호의 최소 길이 정책 등 설정

AIX 운영 체제	HP-UX 운영 체제	솔라리스 운영 체제	주분투 운영 체제
/etc/security/**user**	/etc/default/**security**	/etc/default/**passwd**	/etc/**login.defs**

```
root@xubuntu:~# cat /etc/login.defs

이하 내용 생략

PASS_MAX_DAYS 99999
PASS_MIN_DAYS 0
PASS_WARN_AGE 7

이하 내용 생략

ENCRYPT_METHOD SHA512

이하 내용 생략
```

3. 작업 지정

(1) cron 서비스

고정적인 작업을 설정

```
root@xubuntu:~# crontab -e
```

```
root@xubuntu:~# crontab -l

#*(분) *(시간) *(일) *(월) *(요일)

#매분 test.sh 실행
* * * * * /home/script/test.sh

#매주 금요일 오전 5시 45분에 test.sh 실행
45 5 * * 5 /home/script/test.sh

#매일 매 시간 0분• 20분• 40분에 test.sh 실행
0,20,40 * * * * /home/script/test.sh

#매일 1시간 0분부터 30분까지 매분 test.sh 실행
0-30 1 * * * /home/script/test.sh
```

```
#매 10분 test.sh 실행
*/10 * * * * /home/script/test.sh
```

```
root@xubuntu:~# crontab -r
```

(2) at 서비스

일시적인 작업을 설정

제6-1장 메모리 영역과 주요 레지스터

1. 32 비트 4G 기반의 메모리 구조

(1) 코드 영역

실행 소스 코드 할당

(2) 데이터 영역

전역 변수와 정적 변수 적재

(3) 힙 영역

사용자가 할당한 동적 변수 적재

(4) 스택 영역

1) 지역 변수와 매개 변수 적재

2) 함수의 복귀 주소 적재

2. 레지스터 종류

(1) ESP : 스택 영역의 상단 위치를 저장하는데 사용

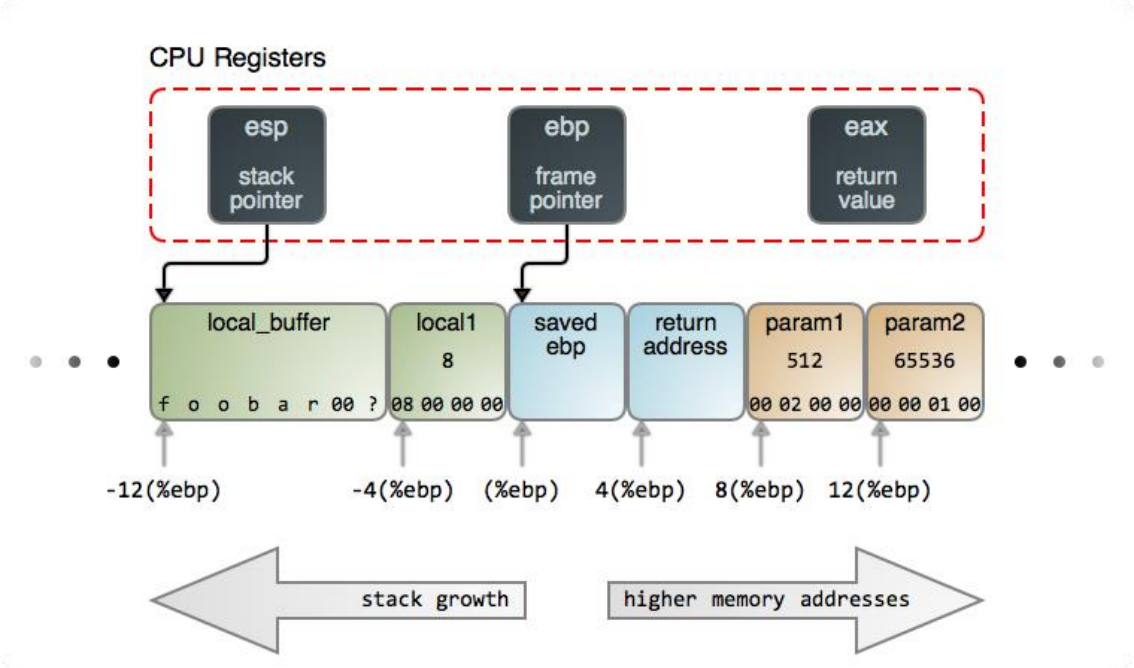
(2) EBP : 스택 영역의 하단 위치를 저장하는데 사용

(3) EIP : 다음에 실행할 명령어 위치를 저장하는데 사용

3. 스택 영역의 주요 용어

(1) 스택 프레임(Stack Frame)

단일 함수가 생성하는 스택 영역



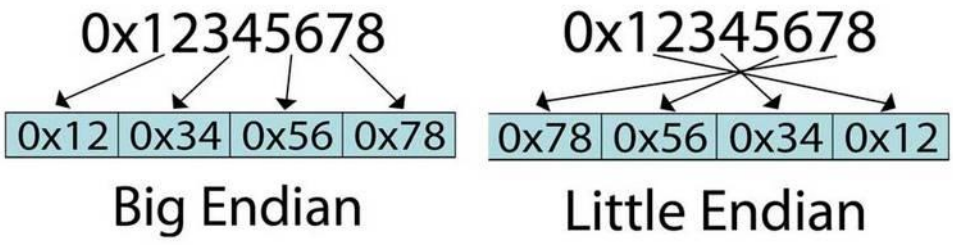
(2) 스택 포인터(Stack Pointer)

스택 영역의 ESP 주소를 저장

(3) 프레임 포인터(Frame Pointer) 또는 스택 프레임 포인터(Stack Frame Pointer)

이전 함수의 EBP 주소를 저장

4. 엔디언(Endian) 방식 또는 바이트 순서(Byte Order)



(1) 빅 엔디언 방식

스팍 계열의 CPU 등에서 사용하는 방식

(2) 리틀 엔디언 방식

인텔 계열의 CPU 등에서 사용하는 방식

제6-2장 주요 시스템 해킹 기법

1. 버퍼 오버플로우(Buffer Overflow) 기법

(1) 지정한 버퍼 용량을 초과한 데이터는 인접 영역에 위치한 데이터를 덮어 쓰면서 프로세스의 흐름 제어를 변경

(2) 버퍼 오버플로우 기법을 이용해 복귀 주소 영역에 공격자가 의도했던 함수의 시작 번지를 덮어 쓴 뒤 해당 함수를 실행

(3) 커널 차원에서 수행하는 버퍼 오버플로우 방지 기법

1) DEP 기법

```
root@xubuntu:~# cat /proc/self/maps | grep stack
bff04000-bff25000 rw-p 00000000 00:00 0          [stack]
```

2) 주소 공간 임의 추출(ASLR) 기법

```
root@xubuntu:~# cat /proc/self/maps | grep stack
bfad6000-bfaf7000 rw-p 00000000 00:00 0          [stack]
root@xubuntu:~# cat /proc/self/maps | grep stack
bfcbc000-bfcdd000 rw-p 00000000 00:00 0          [stack]
root@xubuntu:~# cat /proc/self/maps | grep stack
bf7f7000-bf818000 rw-p 00000000 00:00 0          [stack]

root@xubuntu:~# echo 0 > /proc/sys/kernel/randomize_va_space #ASLR 기법 중지

root@xubuntu:~# cat /proc/self/maps | grep stack
bffdf000-c0000000 rw-p 00000000 00:00 0          [stack]
root@xubuntu:~# cat /proc/self/maps | grep stack
bffdf000-c0000000 rw-p 00000000 00:00 0          [stack]
root@xubuntu:~# cat /proc/self/maps | grep stack
bffdf000-c0000000 rw-p 00000000 00:00 0          [stack]

root@xubuntu:~# echo 2 > /proc/sys/kernel/randomize_va_space #ASLR 기법 사용

root@xubuntu:~# cat /proc/self/maps | grep stack
bf8d2000-bf8f3000 rw-p 00000000 00:00 0          [stack]
root@xubuntu:~# cat /proc/self/maps | grep stack
bf9d9000-bf9fa000 rw-p 00000000 00:00 0          [stack]
root@xubuntu:~# cat /proc/self/maps | grep stack
bff04000-bff25000 rw-p 00000000 00:00 0          [stack]
```

3) 스택 가드(Stack Guard) 기법 또는 카나리(Canary) 기법

```
Buffer          SFP          Canary          RET
```

SFP 구간(이전 함수의 EBP 주소를 저장한 영역)과 RET(해당 함수의 복귀 주소를 저장한 영역) 구간 사이에 임의의 난수인 카나리 값을 추가해 BoF 발생 시 카나리 값의 변화를 통

해 BoF 발생을 감지하는 기법

4) 스택 방패(Stack Shield) 기법

RET 구간에서 복귀 주소를 생성할 때 복귀 주소 사본도 같이 생성해 함수 복귀 시 복귀 주소 사본을 참조하는 기법

2. 형식 문자열(Format String) 기법

(1) C 언어에서 사용하는 %s 등과 같은 형식 문자열 설정 오류 때문에 메모리 번지 주소가 드러나면서 생기는 취약점

(2) 동적 포맷 스트링이 아닌 정적 포맷 스트링 사용

```
char* input_string;
scanf("%s",input_string)
printf(input_string); #dynamic string formatting
printf("%s",input_string); #static string formatting
```

3. 경쟁 상태(Race Condition) 기법

(1) 두 개 이상의 프로세스가 동시에 돌아갈 경우 이 두 개의 프로세스들은 서로 CPU를 선점하기 위해 자원 경쟁이 발생

(2) 두 개의 프로세스는 정상 프로세스와 공격 프로세스이고, 정상 프로세스에는 SetUID를 임시로 생성

(3) 공격자는 임시로 생성하는 SetUID에 심볼릭 링크를 설정해 정상 프로세스가 생성하는 임시 정보를 공격 프로세스가 생성한 심볼릭 링크에 연결해 관리자 권한으로 상승

(4) 커널 차원에서 심볼릭 링크의 생성을 검사해 권리자 계정에서 실행한 명령어 등이 일반 소유자의 정보로 이어지는 심볼릭 링크 실행을 차단

(5) 리눅스 로컬 권한 상승(DirtyCow) 취약점(cve-2016-5195)도 경쟁 상태 기법의 변형

리눅스 커널 2.6.11 이후 버전에서 발견

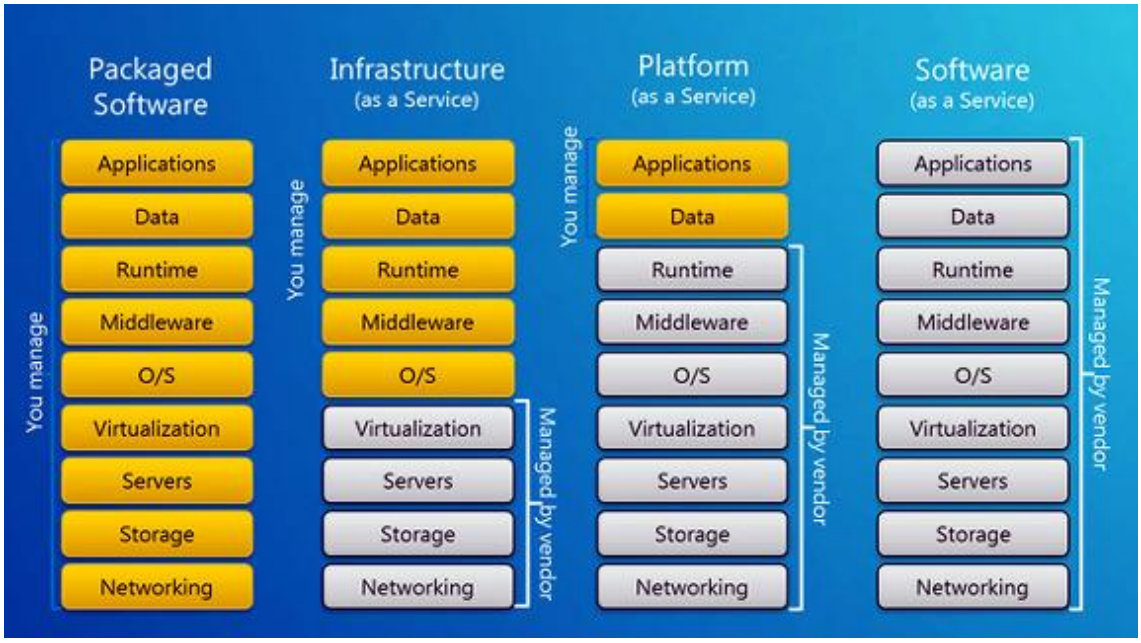
사이버 공격자들이 더티카우(DirtyCow)라는 버그를 다시 익스플로잇하기 시작했다. 이를 통해 드루팔 웹 서버(Drupal Web Server)에 백도어를 심고 있다고 한다.

어떻게 해서든 결국 공격자가 원하는 건 루트 권한이다. 성공하면 공격자에게 새로운 서비스를 설치할 권한이 생긴다. 공격자는 이를 활용해 SSH를 설치하고 자기들이 원하는 대로 설정한다.

아비탈은 "더티카우는 2년 전에 발견된 버그인데, 아직도 바이러스토탈(VirusTotal) 기준으로 탐지율 0을 기록하고 있다"며 "관리자들은 호스트 시스템에 대한 패치를 다시 한 번 점검해야 한다"고 권고한다.

2018년 11월 20일 보안 뉴스 기사 중에서

제7장 클라우드 컴퓨팅 서비스 종류



1. IaaS(infrastructure as a Service)

하부의 인프라 부분만 제공

2. PaaS(Platform as a Service)

소프트웨어를 개발할 때 필요한 플랫폼을 제공

3. SaaS(Software as a Serviece)

최상위 계층에 해당하는 서비스

제1장 네트워크 공격 유형

1. 프린팅(배너 그래빙) 공격

```
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-116-generic i686)

Last login: Mon May 21 14:48:12 2018 from 192.168.10.1
root@xubuntu:~#
```

2. 스니핑 공격

무작위(promiscous) 모드란 프레임 헤더의 목적지 MAC 주소와 LAN 카드의 MAC 주소를 비교한 뒤 두 개의 주소가 상이하더라도 LAN 카드가 해당 프레임을 수신하는 동작

```
root@xubuntu:~# ifconfig eth0 promisc
root@xubuntu:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:91:39:80
          inet addr:192.168.10.215  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe91:3980/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:1578 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1593 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:317233 (317.2 KB)  TX bytes:184616 (184.6 KB)
          Interrupt:18 Base address:0x2000

root@xubuntu:~# ifconfig eth0 -promisc
root@xubuntu:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:91:39:80
          inet addr:192.168.10.215  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe91:3980/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1603 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1623 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:320009 (320.0 KB)  TX bytes:190124 (190.1 KB)
          Interrupt:18 Base address:0x2000
```

3. 스캐닝 공격

(1) TCP Full Open 스캔 방식

```
root@xubuntu:~# nmap 127.0.0.1 -p 22 --reason -sT

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:37 KST
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response (0.00095s latency).

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

1) 해당 포트가 열린 경우에는 ACK + SYN 응답

2) 해당 포트가 닫힌 경우에는 ACK + RST 응답

(2) TCP Half Open 스캔 방식

```
root@xubuntu:~# nmap 127.0.0.1 -p 22 --reason -sS

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:38 KST
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response (0.000057s latency).

PORT    STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
```

1) 해당 포트가 열린 경우에는 ACK + SYN 응답

2) 해당 포트가 닫힌 경우에는 ACK + RST 응답

(3) FIN 스캔 방식

```
root@xubuntu:~# nmap 127.0.0.1 -p 22 --reason -sF

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:39 KST
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response.

PORT    STATE          SERVICE REASON
22/tcp open|filtered ssh     no-response

Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
```

1) SYN 신호를 차단한 방화벽 등을 통과하기 위한 기법

2) 해당 포트가 열린 경우에는 무응답

3) 해당 포트가 닫힌 경우에는 ACK + RST 응답

(4) X-mas 스캔 방식

```
root@xubuntu:~# nmap 127.0.0.1 -p 22 --reason -sX

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:39 KST
Nmap scan report for localhost (127.0.0.1)
```

```
Host is up, received localhost-response.

PORT     STATE           SERVICE REASON
22/tcp open|filtered ssh       no-response

Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds
```

1) SYN 신호를 차단한 방화벽 등을 통과하기 위한 기법

2) 해당 포트가 열린 경우에는 무응답

3) 해당 포트가 닫힌 경우에는 ACK + RST 응답

(5) Null 스캔 방식

```
root@xubuntu:~# nmap 127.0.0.1 -p 22 --reason -sN

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:40 KST
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response.

PORT     STATE           SERVICE REASON
22/tcp open|filtered ssh       no-response

Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
```

1) SYN 신호를 차단한 방화벽 등을 통과하기 위한 기법

2) 해당 포트가 열린 경우에는 무응답

3) 해당 포트가 닫힌 경우에는 ACK + RST 응답

4. 스푸핑 공격

(1) ARP 스푸핑 공격

(2) IP 스푸핑 공격

(3) DNS 스푸핑 공격

5. 플러딩 공격

(1) 랜드 공격

(2) 티얼드롭 공격

(3) 죽음의 핑 공격

(4) ICMP 스머프 공격

(5) TCP SYN 공격

(6) TCP 본크• 보잉크 공격

(7) HTTP GET 플러딩 공격

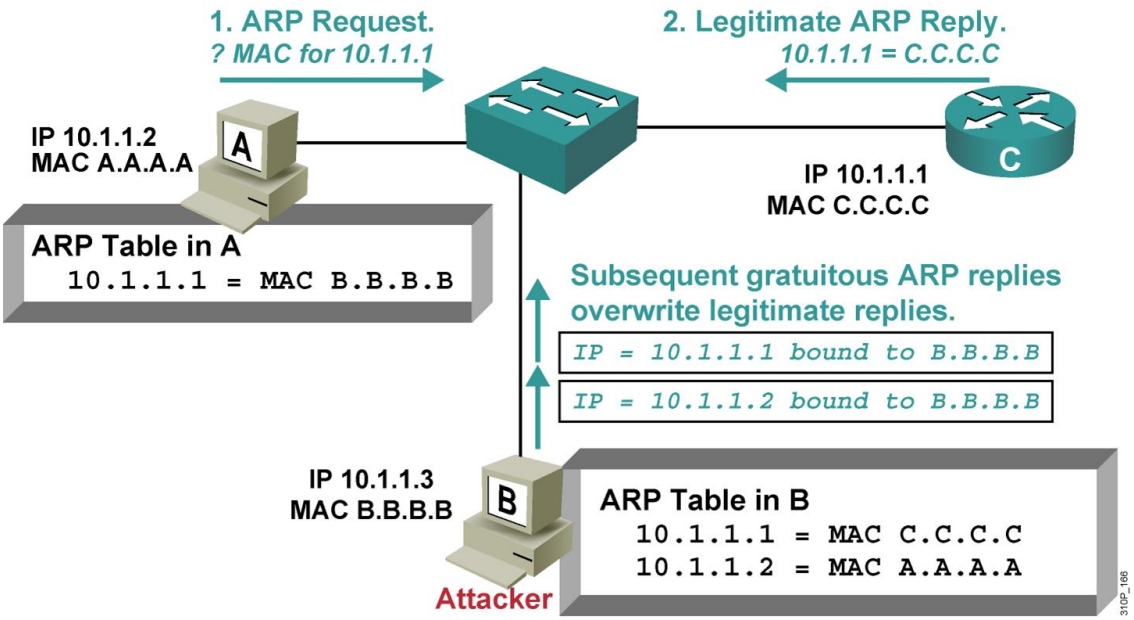
(8) 슬로우 로리스 공격

(9) 러디 공격

제2장 TCP/IP 방식의 계층별 취약점에 기반한 공격 유형

1. 데이터 링크 계층에서 ARP 스푸핑 공격

(1) 동일한 LAN 영역에서 라우터 MAC 주소 등을 조작하는 기법으로 각종 스니핑 공격을 위한 전제로 수행하는 대표적인 중간자 개입(MITM) 공격



(2) IP 주소와 MAC 주소를 고정하는 방식으로 방어

```
C:₩>arp -s 192.168.10.2 08-5d-dd-92-81-9b
```

2. 네트워크 계층에서 공격 유형

(1) IP 스푸핑 공격

1) TCP 연결 하이재킹 공격 과정에서 등장

2) 출발지의 IP 주소를 제거하거나 조작하여 상대방으로 하여금 자신을 은폐하는 기법으로 일종의 NAT 기법

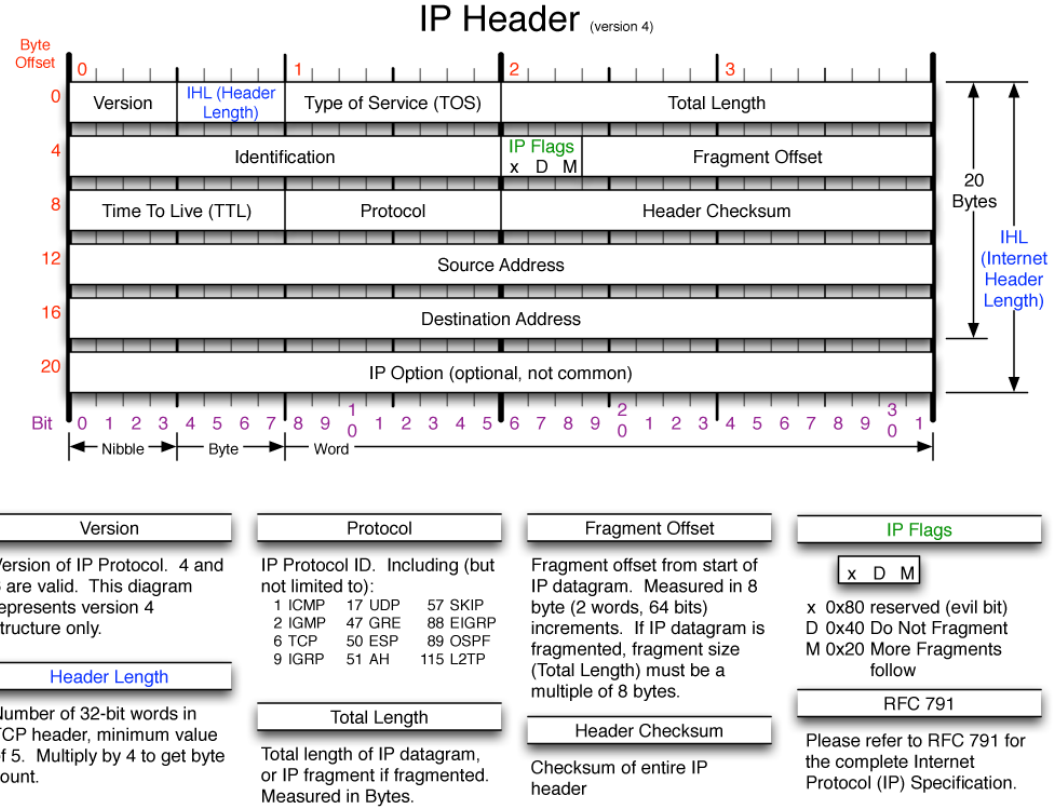
3) 방화벽 설정을 통해 방어

(2) 랜드 공격

1) IP 스푸핑 공격의 변형으로 출발지 IP 주소와 목적지 IP 주소를 동일하게 설정하는 일종의 플러딩 공격

2) 들어오는 패킷 헤더에서 출발지 IP 주소와 목적지 IP 주소가 동일하면 차단

(3) 티얼드롭 공격



1) 패킷 분할이 발생할 때 IP 헤더의 오프셋 항목을 조작해 수신자로 하여금 정상적인 재조립 과정을 방해하는 일종의 플러딩 공격

ID 항목	플래그 항목(D 비트)	플래그 항목(M 비트)	플래그먼트 오프셋
0	1	0	0

ID 항목	플래그 항목(D 비트)	플래그 항목(M 비트)	플래그먼트 오프셋
1234	0	1	0
1234	0	1	1,500
1234	0	1	3,000/1500
1234	0	0	4,500

2) 운영 체제 차원에서 차단

(4) ICMP 플러딩 공격 또는 죽음의 핑 공격

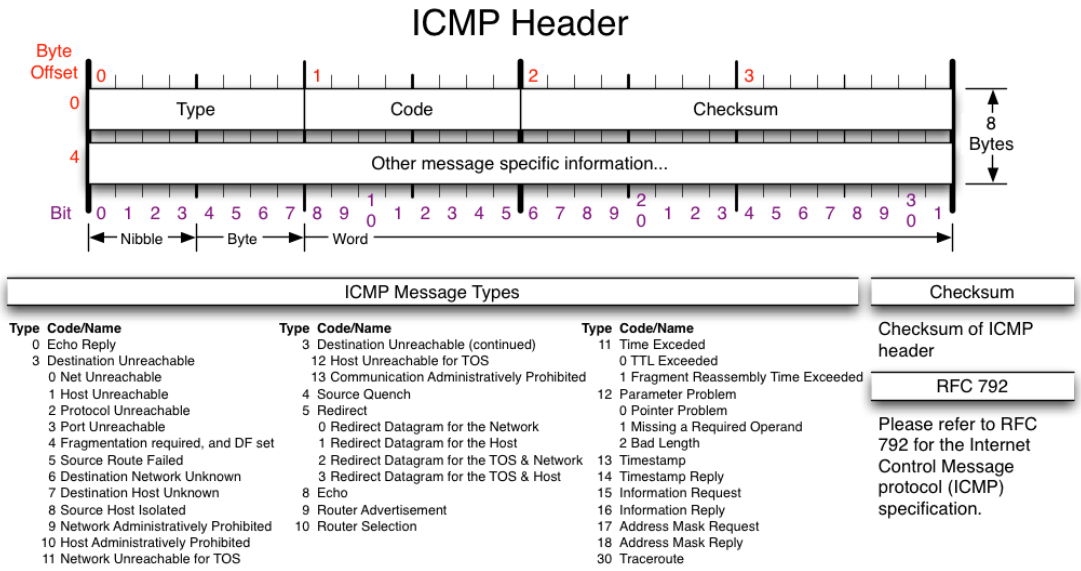
1) 65,535 바이트 크기 이상의 ICMP 요청을 연속적으로 전송하는 플러딩 공격

```
root@backbox:~# hping3 192.168.10.215 -a 192.168.10.215 --icmp --flood -d 65000 &

root@backbox:~# tcpdump -e icmp[icmptype] == 8
```

2) ICMP 기능 중지 등으로 방어

```
root@xubuntu:~# echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all

root@xubuntu:~# tcpdump -e icmp[icmptype] == 0
```

3) 방화벽 설정을 통해 방어



(5) ICMP 스머프 공격

```
root@xubuntu:~# echo 0 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
root@xubuntu:~# ping 192.168.10.255 -b
```

1) IP 스푸핑 공격의 변형으로 출발지 IP 주소 항목에 공격 대상자의 IP 주소로 설정하고, 목적지 IP 주소 항목에 브로드캐스트 IP 주소 255를 포함하도록 설정해 ICMP 요청을 전송하는 일종의 플러딩 공격

```
root@backbox:~# hping3 192.168.10.255 -a 192.168.10.215 --icmp --flood -d 65000 &

root@backbox:~# tcpdump -e icmp[icmptype] == 8
```

2) 방화벽 설정을 통해 방어

3. 전송 계층에서 공격 유형

(1) TCP SYN 플러딩 공격

```
root@backbox:~# hping3 192.168.10.215 -a 192.168.10.219 -p 22 -S --flood &

root@backbox:~# tcpdump "tcp[tcpflags] & (tcp-syn) != 0"
```

1) 좀비 시스템 종류에 따라 Syn DDoS 공격과 Syn DRDoS 공격으로 구분

2) 연결 요청에 대한 임계치 설정

```
root@xubuntu:~# sysctl -a | egrep "tcp_max_syn_backlog"

net.ipv4.tcp_max_syn_backlog = 128

이하 내용 생략
```

(2) TCP 본크• 보잉크 공격

1) TCP 헤더의 일련 번호 항목을 조작하여 수신측에서 재조립할 때 과부하를 유발시키는 기법으로 일종의 플러딩 공격

2) 운영 체제 차원에서 차단

4. 응용 계층에서 공격 유형

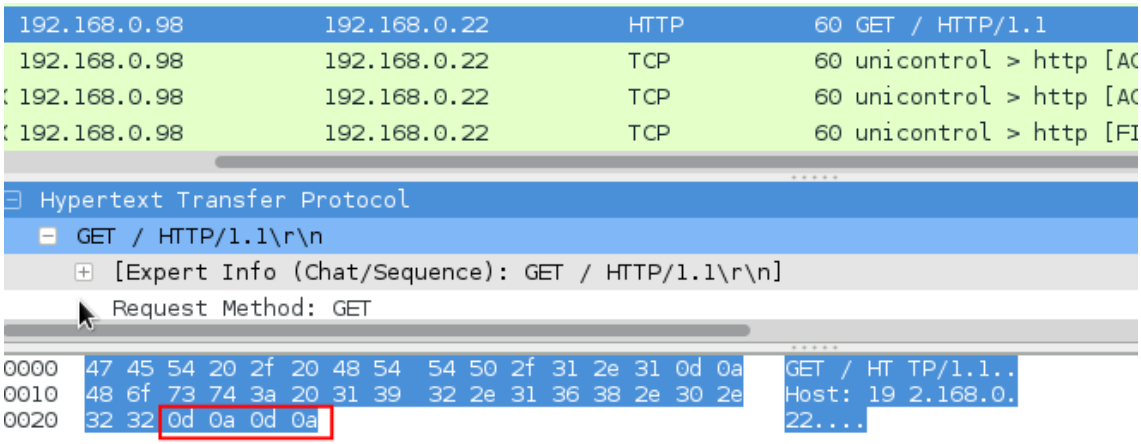
(1) HTTP GET 플러딩 공격

	Time	Source	Destination	Protocol	Info
4	0.000583	169.146.166.37	213.153.205.182	HTTP	GET / HTTP/1.0
5	0.002280	213.153.205.182	169.146.166.37	HTTP	HTTP/1.1 200 OK (text/html)
11	0.201695	56.95.172.130	213.153.205.182	HTTP	GET / HTTP/1.0
12	0.206368	213.153.205.182	56.95.172.130	HTTP	HTTP/1.1 200 OK (text/html)
18	0.402112	168.217.142.0	213.153.205.182	HTTP	GET / HTTP/1.0
19	0.403480	213.153.205.182	168.217.142.0	HTTP	HTTP/1.1 200 OK (text/html)
25	0.602584	199.148.145.6	213.153.205.182	HTTP	GET / HTTP/1.0
26	0.606367	213.153.205.182	199.148.145.6	HTTP	HTTP/1.1 200 OK (text/html)
32	0.804373	162.216.154.125	213.153.205.182	HTTP	GET / HTTP/1.0
33	0.809453	213.153.205.182	162.216.154.125	HTTP	HTTP/1.1 200 OK (text/html)
39	1.004762	205.182.177.239	213.153.205.182	HTTP	GET / HTTP/1.0
40	1.007915	213.153.205.182	205.182.177.239	HTTP	HTTP/1.1 200 OK (text/html)
46	1.204983	164.192.24.244	213.153.205.182	HTTP	GET / HTTP/1.0
47	1.207573	213.153.205.182	164.192.24.244	HTTP	HTTP/1.1 200 OK (text/html)
53	1.406715	39.163.133.234	213.153.205.182	HTTP	GET / HTTP/1.0
55	1.408858	213.153.205.182	39.163.133.234	HTTP	HTTP/1.1 200 OK (text/html)
62	1.607263	197.59.89.173	213.153.205.182	HTTP	GET / HTTP/1.0
64	1.608710	213.153.205.182	197.59.89.173	HTTP	HTTP/1.1 200 OK (text/html)
71	1.808347	189.246.11.232	213.153.205.182	HTTP	GET / HTTP/1.0
73	1.809737	213.153.205.182	189.246.11.232	HTTP	HTTP/1.1 200 OK (text/html)
80	2.008932	119.204.77.25	213.153.205.182	HTTP	GET / HTTP/1.0
82	2.010315	213.153.205.182	119.204.77.25	HTTP	HTTP/1.1 200 OK (text/html)
89	2.209195	108.198.119.75	213.153.205.182	HTTP	GET / HTTP/1.0
90	2.210959	213.153.205.182	108.198.119.75	HTTP	HTTP/1.1 200 OK (text/html)
96	2.409461	179.217.244.130	213.153.205.182	HTTP	GET / HTTP/1.0
97	2.410698	213.153.205.182	179.217.244.130	HTTP	HTTP/1.1 200 OK (text/html)
107	2.609894	140.245.134.208	213.153.205.182	HTTP	GET / HTTP/1.0
108	2.611252	213.153.205.182	140.245.134.208	HTTP	HTTP/1.1 200 OK (text/html)
114	2.811219	80.8.97.20	213.153.205.182	HTTP	GET / HTTP/1.0
115	2.813127	213.153.205.182	80.8.97.20	HTTP	HTTP/1.1 200 OK (text/html)
121	3.010681	9.152.57.149	213.153.205.182	HTTP	GET / HTTP/1.0
122	3.012027	213.153.205.182	9.152.57.149	HTTP	HTTP/1.1 200 OK (text/html)
128	3.212046	163.135.22.148	213.153.205.182	HTTP	GET / HTTP/1.0

1) 서버에게 반복적으로 기본 페이지를 요청

2) 타임아웃에 기반한 임계치 설정을 통해 방어

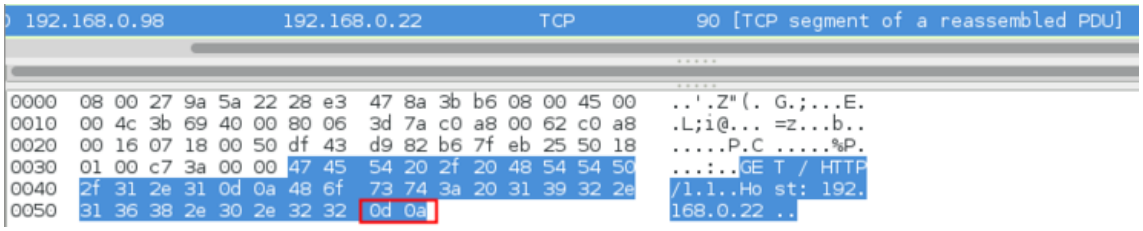
(2) 슬로우 로리스(Slow Loris) 공격



1) 웹 서버 접근 과정에서 명확한 캐리지 값 ₩r₩n₩r₩n(0d0a0d0a)을 입력해야 응답을 제공

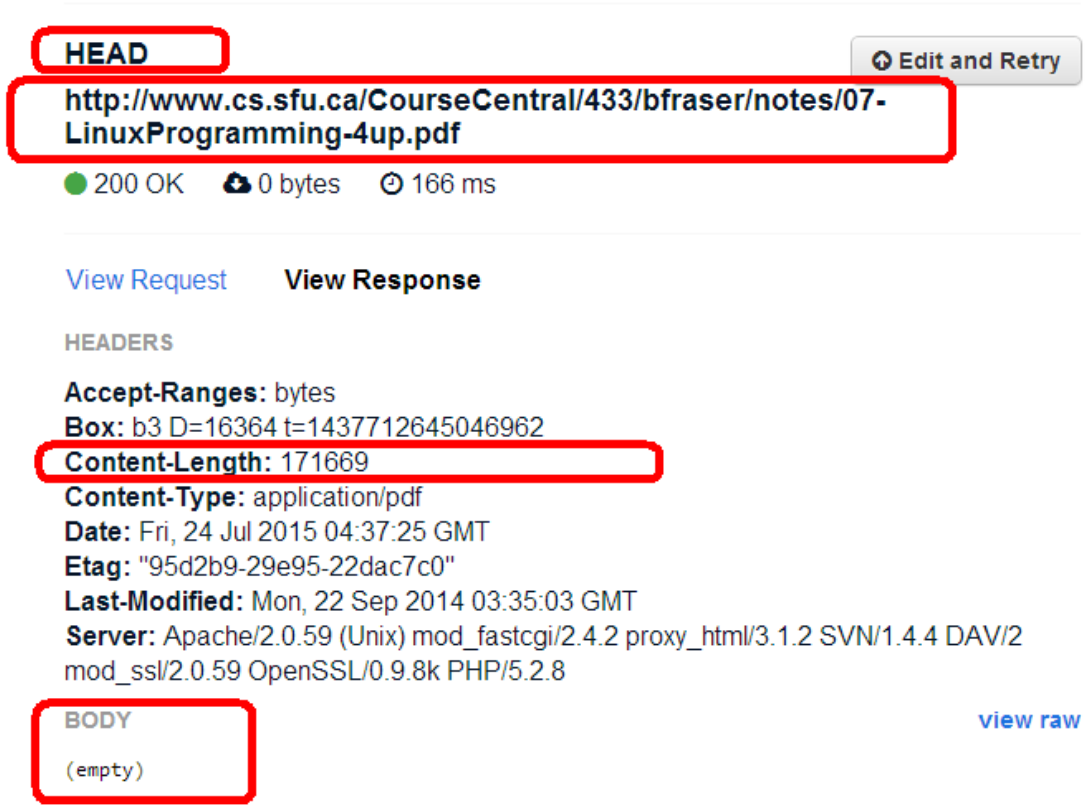
2) HTTP 헤더와 HTTP 바디 사이의 경계를 ₩r₩n(0d0a) 등과 같이 애매하게 설정해 반복적으로 전송하면 서버가 헤더 정보를 완전히 수신할 때까지 연결을 유지

```
root@backbox:~# slowhttptest -H -g -o slowloris -c 4000 -r 100 -i 10 -t GET -p 3 -x 3 -u http://192.168.10.215
```



3) 타임아웃에 기반한 임계치 설정을 통해 방어

(3) 러디(Rudy) 공격



1) content-length 항목에 기반해 서버로 대량의 데이터를 전송할 때 장시간 동안 분할 전송

```
root@backbox:~# slowhttptest -B -g -o rudy -c 4000 -r 200 -i 100 -t GET -s 4096 -x 3 -u http://192.168.10.215
```

2) 타임아웃에 기반한 임계치 설정을 통해 방어

제3-1장 VPN 종류

1. 응용 계층 기반의 VPN

(1) SSH VPN 방식

1) TELNET 방식을 대체한 방식

2) SSHv1과 SSHv2가 있는데 상호 호환 불가

(2) PGP VPN 방식

1) SMTP 방식에 적용하는 방식

2) 기밀성• 무결성• 인증• 송신 부인 방지 등을 지원

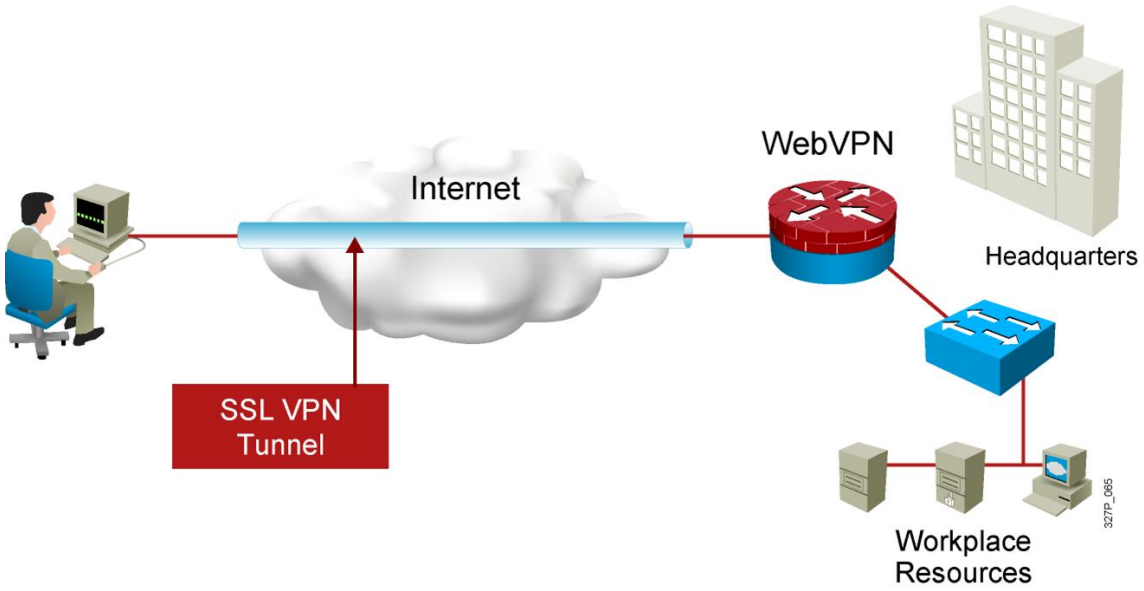
3) IDEA 방식에 기반한 전자 봉투 사용

(3) SET VPN 방식

1) SSL/TLS 방식을 전자 상거래 환경에 최적화시킨 방식

2) 전자 봉투와 이중 전자 서명 방식 사용

2. 전송 계층 기반의 VPN

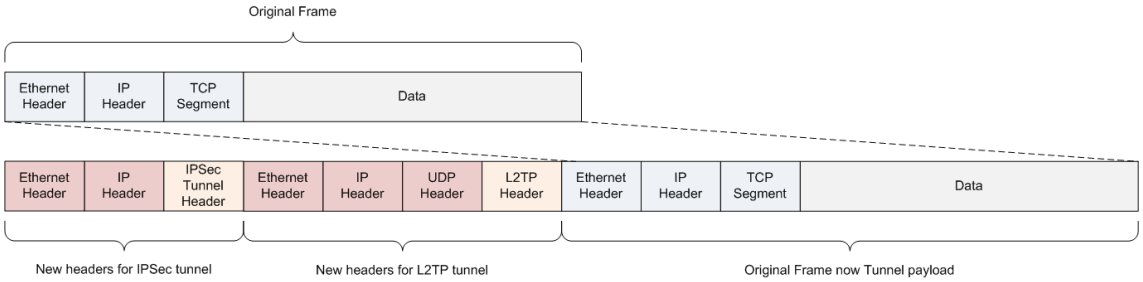


SSL/TLS VPN 방식

3. 네트워크 계층 기반의 VPN

IPSec VPN 방식

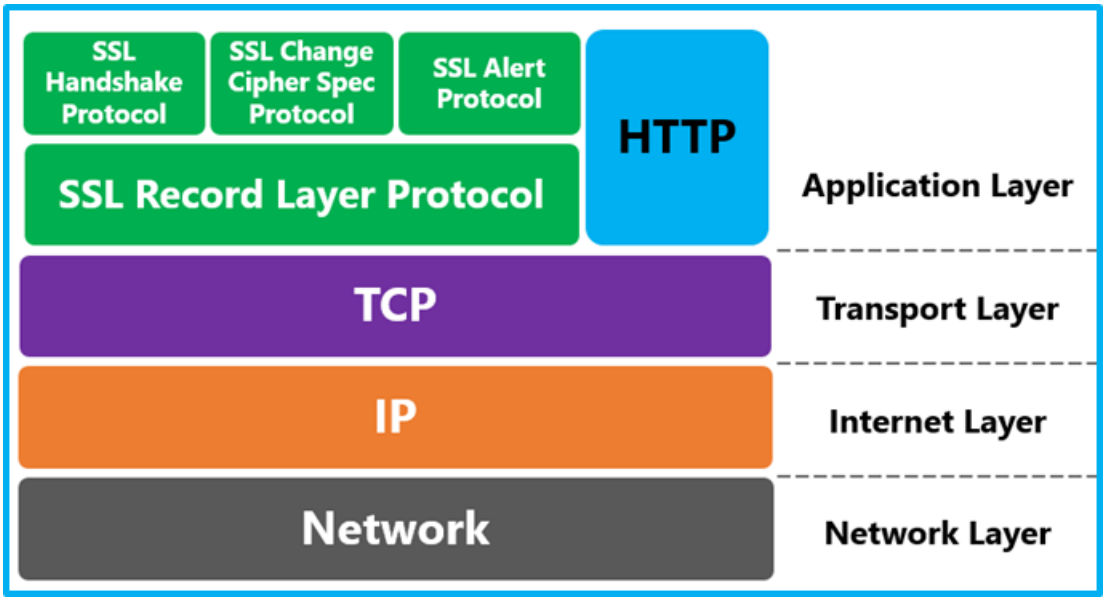
4. 데이터 링크 계층 기반의 VPN



L2F VPN• L2TP VPN• PPTP VPN 등

제3-2장 SSL/TLS VPN 구성과 동작

1. SSL/TLS 방식의 계층적 구조



(1) SSL 핸드쉐이크 프로토콜

1) DES 또는 RC4 방식 등에 기반해 임시 비밀 열쇠를 생성

2) 서버와 클라이언트 상호 간의 인증 기능을 수행

(2) SSL 암호 변경 사양 프로토콜

일련의 보안 매개 변수를 주고받으면서 보안 협상을 수행

(3) SSL 경고 프로토콜

상대방에게 오류 통보 기능을 수행

(4) SSL 레코드 계층 프로토콜

압축화• 암호화 기능을 수행

2. SSL/TLS 방식의 기능과 내부 처리 과정

(1) 기밀성• 무결성• 인증 기능 등을 제공

(2) 단편화 > 압축화 > 해쉬 첨부 > 암호화 > SSL 레코드 헤더 추가

3. SSL/TLS 방식의 동작

전자 봉투 생성 과정

(1) 초기 협상 단계

클라이언트와 서버 사이에서 클라이언트 헬로• 서버 헬로 신호 교환

(2) 서버 인증 단계

서버에서 공인 열쇠를 클라이언트에게 전송

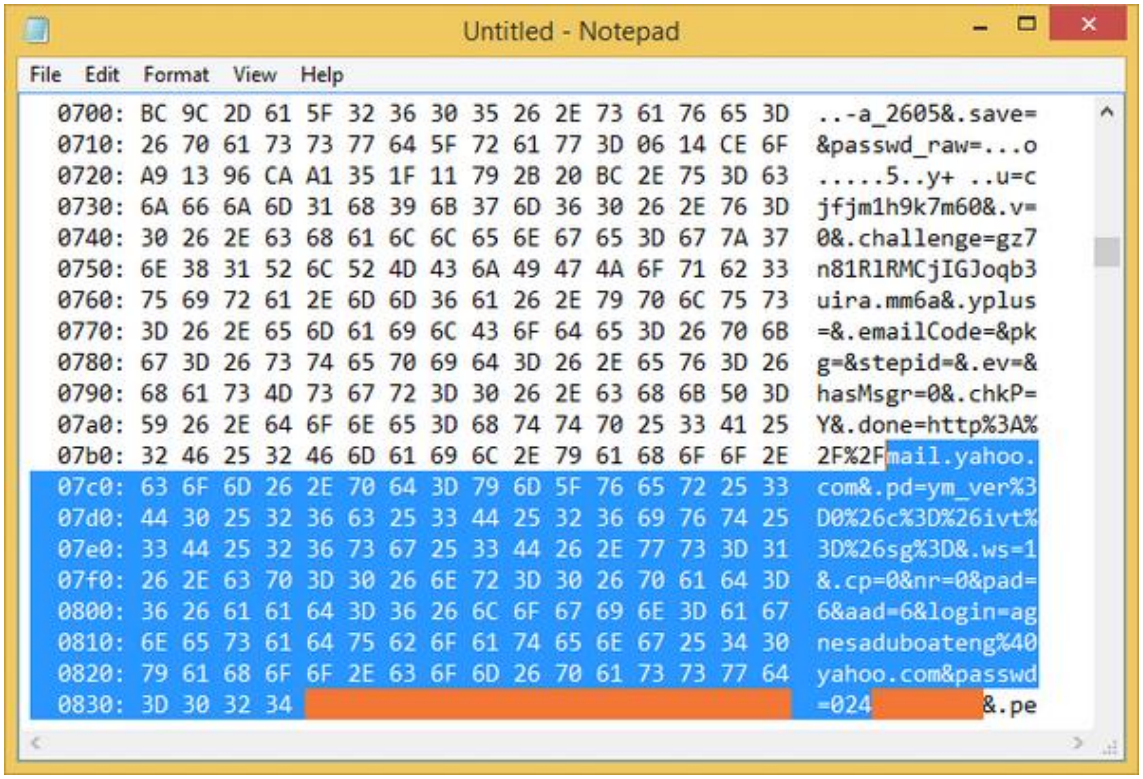
(3) 클라이언트 인증 단계

핸드쉐이크 프로토콜에서 생성한 임시 비밀 열쇠를 공인 인증서에 담긴 공개 열쇠로 암호화해 전송하고, 암호 변경 사양 프로토콜에서 다음 단계에서 사용할 일련의 보안 매개 변수를 서버에게 전송

(4) 종료 단계

일련의 SSL/TLS 통신을 진행한 뒤 TCP 방식에 따라 순차적으로 연결 종료

5. OpenSSL 하트블리드(HeartBleed) 공격

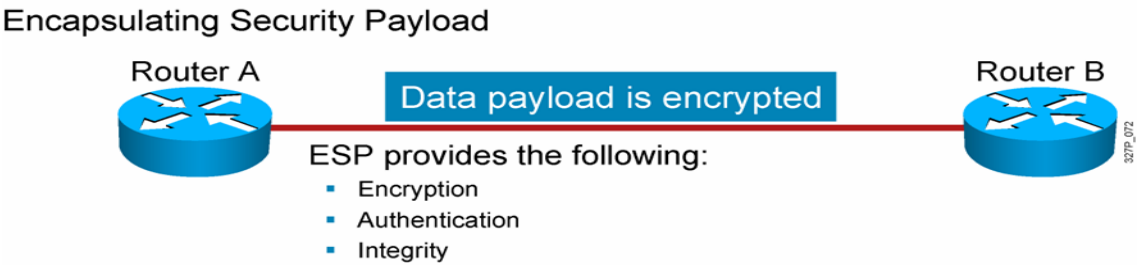


(1) 2014년 OpenSSL 1.0.1-1.0.1f 버전과 1.0.2-beta 버전 등에서 발견한 일종의 버퍼 오버플로우 기법으로서 인증 정보가 노출되는 취약점

(2) 침투 발견 시 비밀 번호 재설정• 해당 버전 업데이트• 공인 인증서 재발급

제3-3장 IPSec VPN 구성과 동작

1. IPSec 방식의 종류



(1) AH 방식은 암호화 패킷을 대상으로 무결성• 인증 기능 등을 부여한 방식

(2) ESP 방식은 암호화 패킷을 대상으로 기밀성• 무결성• 인증 기능 등을 부여한 방식

2. 보안 협상 절차

평문 상태의 패킷을 대상으로 암호화를 수행하기 위한 일련의 보안 정책을 협상하는 IKE 1단계 절차와 IPSec 방식의 종류를 협상하기 위한 IKE 2단계 절차로 구성

(1) IKE 1단계 절차

기본 설정인 6단계의 메인 모드로 동작하거나 3단계의 축약 모드로 동작

(2) IKE 2단계 절차

3단계의 퀵 모드로 동작

3. IKE• ISAKMP 개념

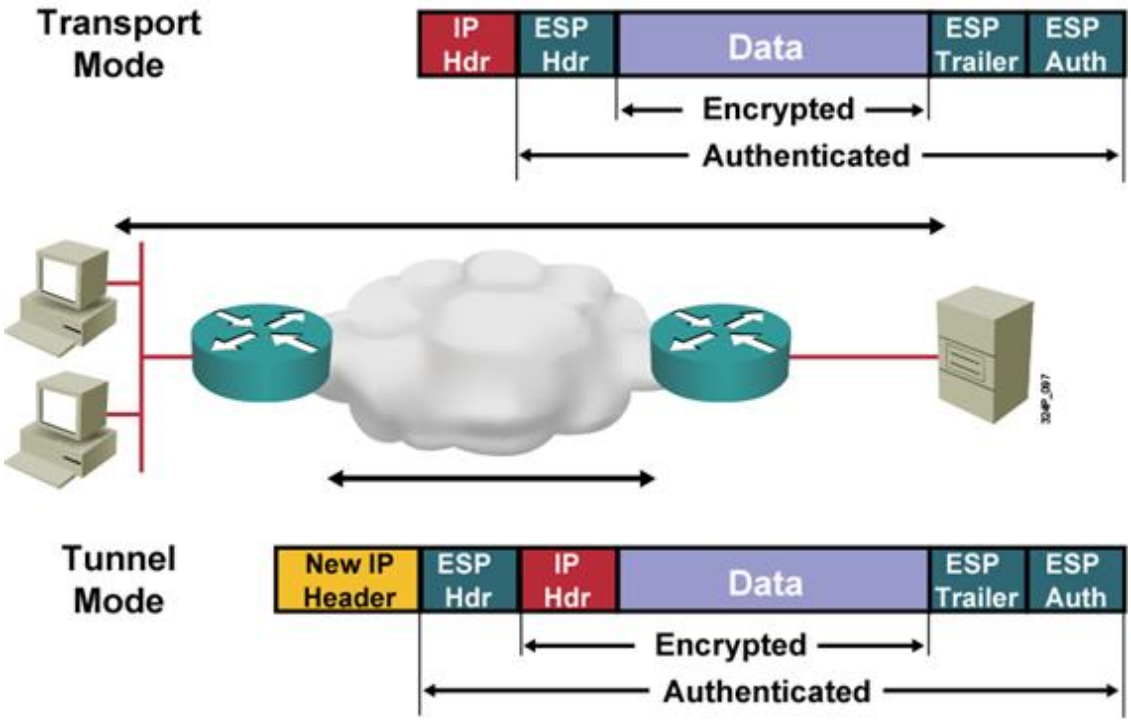
(1) 보안 협상이 가능하도록 지원하는 프로토콜

(2) IKE 방식은 구체적인 절차를 명시한 프로토콜이고, ISAKMP 방식은 전체적인 절차를 명시한 프로토콜

(3) 2010년 현재 IKE 2.0 방식에서 ISAKMP 방식을 흡수• 통합

4. ESP 방식에 기반한 IPSec VPN 전송 유형

터널 구간의 차이와 ESP 헤더의 삽입 위치의 차이에 따라 전송 모드와 터널 모드로 구분



(1) 전송 모드

1) 일종의 종단간 VPN 기법으로 암호화• 복호화의 주체가 각각 송신자와 수신자

2) 동일한 LAN 영역에서도 암호문으로 송신• 수신하기 때문에 높은 보안성을 유지

3) 사용자가 직접 IPSec VPN 작업을 수행

(2) 터널 모드

1) 일종의 링크 VPN 기법으로 암호화• 복호화의 주체가 라우터 또는 VPN 장비

2) 사용자에게 IPSec VPN 투명성을 제공

3) 송신자• 수신자와 해당 장비 사이에서 평문으로 송신• 수신

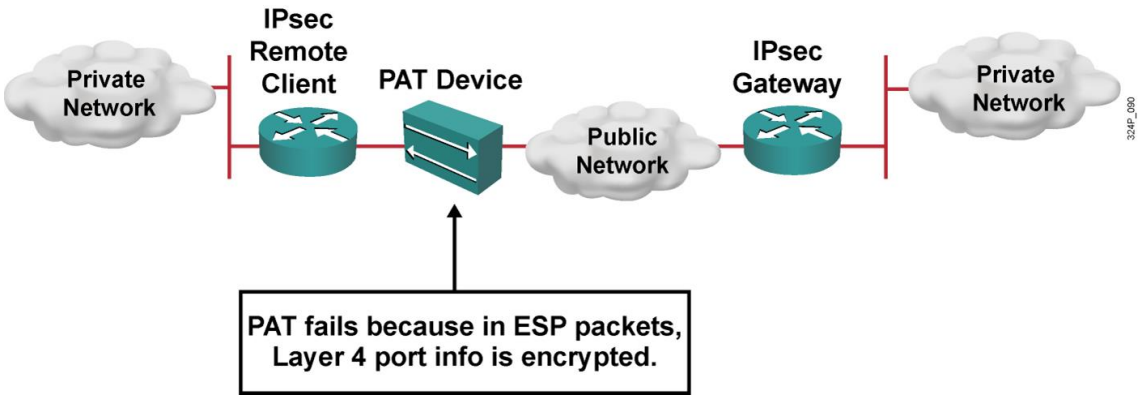
5. IPSec VPN 구성 일례

```
crypto isakmp policy 20
encryption des
group 2
hash md5
authentication pre-share
lifetime 60
exit #IKE 1단계 절차 설정 종료
crypto isakmp key 1234 address 192.168.34.4
crypto IPSec transform-set secrpass esp-3des esp-md5-hmac
```

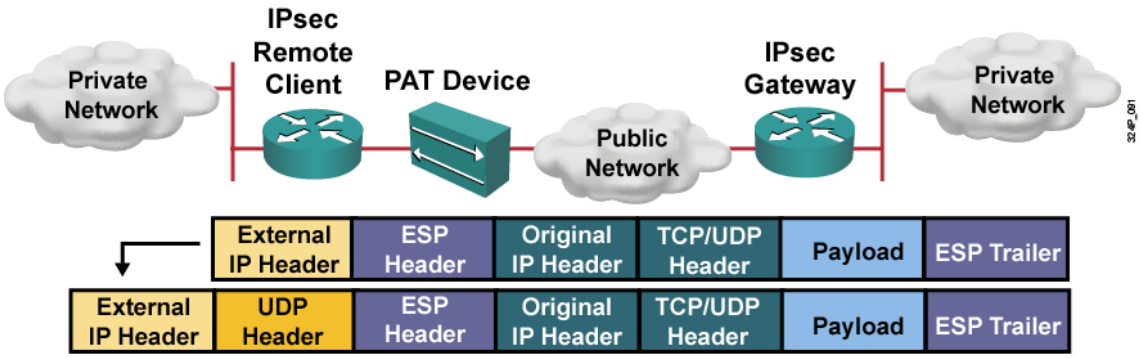
exit #IKE 2단계 절차 설정 종료

6. IPSec VPN 환경에서 PAT 방식의 처리 문제

(1) 문제점

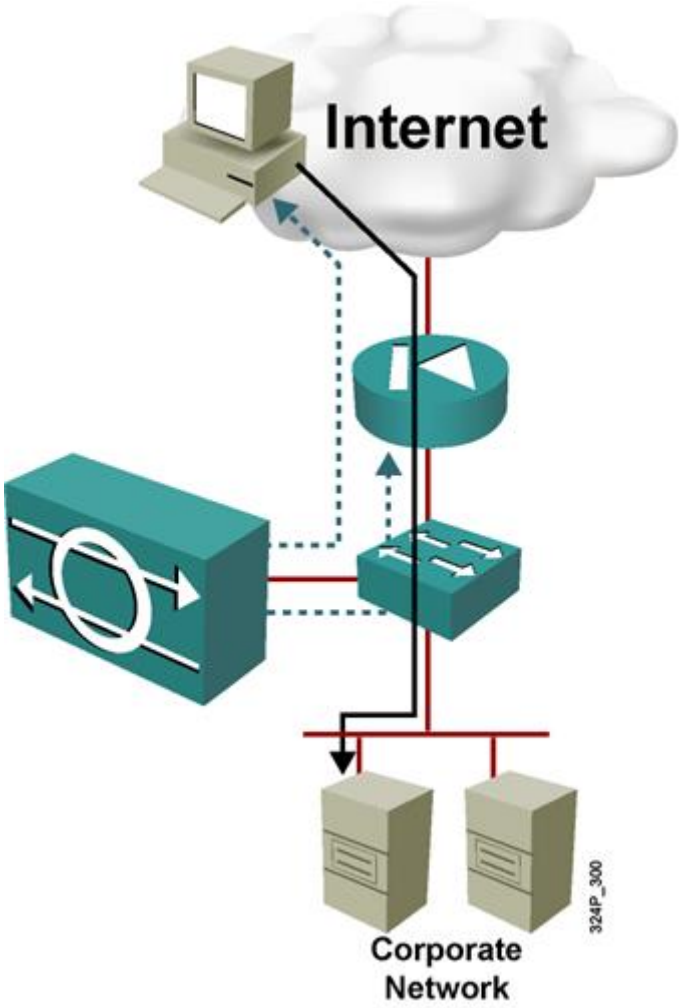


(2) 해결책



제4장 침입 탐지 장비(Intrusion Detection Systems)의 이해

1. IDS의 기능



일정한 탐지 규칙에 따라 기존의 공격 유형을 탐지

2. 탐지 방법의 종류

(1) 서명 기반의 탐지

지식 기반으로 침입 유형 등을 사전에 등록해 탐지

(2) 정책 기반의 탐지

행위 기반으로 접속 경로 등을 사전에 등록해 탐지

(3) 이상 기반의 탐지

정량적• 통계적 분석에 기반해 일정한 시간 동안 발생한 트래픽 유형을 관찰하면서 임계치를 초과하면 경보를 발생

(4) 유인 기반의 탐지

유인 서버에 추적 소프트웨어를 설치해 실제 서버를 보호하거나 공격자의 활동을 감시

3. IDS의 종류

(1) 네트워크 기반의 IDS

1) LAN 영역 전체를 탐지하는데 유리

2) 자신에게 향하는 패킷이나 암호화 패킷 등은 탐지 곤란

(2) 호스트 기반의 IDS

1) 내부 공격을 탐지하는데 유리

2) 호스트 단위만 탐지

4. 탐지 오류

(1) 오탐(False Positive)

행위 기반에서 정상적인 유형을 악의적인 유형으로 오판

(2) 미탐(False Negative)

서명 기반에서 악의적인 유형을 정상적인 유형으로 오판

제5장 스노트 사용 일례

이하의 내용은 관리자 계정을 이용해 주분투 16.04 환경에서 작성

1. ICMP 요청 탐지 설정

```
cat > /etc/snort/rules/local.rules

alert icmp any any -> any any (sid:1000001;)
```

(1) 동작(action) 유형

alert• log• pass• activate• dynamic• drop• reject• sdrop 등 총 8개

(2) sid 의미

1) 99 이하

시스템 내부에서 사용

2) 100부터 1,000,000 이하

외부에서 배포하는 탐지 규칙에서 사용

3) 1,000,001 이상

사용자가 local.rules에서 임의로 사용할 때 사용

2. 죽음의 핑 공격 탐지 설정

```
cat > /etc/snort/rules/local.rules

alert icmp any any -> any any (msg:"PingOfDeath";threshold:type both,track by_src,count 10,seconds 2;sid:1000001;)
alert icmp any any -> any any (msg:"PingOfDeath";threshold:type both,track by_src,count 10,seconds 2;dsize:>5000;sid:1000002;)
```

(1) msg 의미

이벤트 발생 시 설정한 문자열을 제목으로 출력

(2) threshold:type 의미

1) threshold:type threshold 경우

패킷의 갯수에 기반해 10개의 패킷을 단위로 경고창을 출력[패킷이 20개라면 두 번 출력]

2) threshold:type both 경우

시간 간격에 기반해 매 2초 간격으로 10개의 패킷까지만 경고창을 출력[패킷이 20개라도

한 번 출력]

3) threshold:type limit 경우

패킷의 갯수와 시간 간격에 기반해 매 2초 간격으로 경고창을 10번 출력

Category	Option	Description
IP condition	track by_src	Source IP base
	track by_dst	Destination IP base
Log type	threshold:type threshold	Number of packet
	threshold:type limit	Number of packet /Time period
	threshold:type both	Time period
Number of packet	count 10000	
Time period	seconds 2	

(3) track 의미

1) track by_src 경우

출발지 IP 주소에 기반해 추적

2) track by_dst 경우

목적지 IP 주소에 기반해 추적

(4) dsize 의미

패킷의 크기 설정

3. IP 스푸핑 공격 탐지 설정

```
cat > /etc/snort/rules/local.rules

alert icmp 10.0.0.0/8 any -> any any (sid:1000001;)
alert icmp 172.16.0.0/16 any -> any any (sid:1000002;)
```

4. 랜드 공격 탐지 설정

```
cat > /etc/snort/rules/local.rules

alert icmp any any -> any any (sid:1000001;)
alert icmp any any -> any any (sameip;sid:1000002;)
```

5. 각종 포트 스캔 탐지 설정

```
cat > /etc/snort/rules/local.rules

alert tcp any any -> 192.168.10.215 22 (flags:S;sid:1000001;)
alert tcp any any -> 192.168.10.215 22 (flags:F;sid:1000002;)
alert tcp any any -> 192.168.10.215 22 (flags:UPF;sid:1000003;)
alert tcp any any -> 192.168.10.215 22 (flags:!UAPRSF;sid:1000004;)
```

6. SYN 플러딩 공격 탐지 설정

```
cat > /etc/snort/rules/local.rules

alert tcp any any -> any any (flags:S;threshold:type both,track by_src,count 10,seconds 2;sid:1000001;)
```

7. 무차별 대입 공격 탐지 설정

```
cat > /etc/snort/rules/local.rules

alert tcp any any -> any 21 (threshold:type both,track by_src,count 10,seconds 2;sid:1000001;)
```

8. FTP 계정별 접속 탐지 설정

```
cat > /etc/snort/rules/local.rules

alert tcp any any -> any 21 (content:"user root";nocase;sid:1000001;)
```

(1) content 의미

페이로드에서 검색할 문자열 또는 헥사 코드 설정

(2) nocase 의미

대• 소문자 구분 무시

9. SSH 접속 탐지 설정

```
cat > /etc/snort/rules/local.rules

alert tcp any any -> any 22 (content:"SSH";nocase;offset:9;depth:5;sid:1000001;)
```

검색 시간을 줄이기 위한 좌표 지정

응용 계층의 페이로드에서 123456789ABCDEFGHIJK 내용이 있는 경우

(1) content:"567";offset:3;depth:5;

3 바이트에서 5 바이트까지 검색한 뒤(56789) 해당 문자열을 추출(567)

(2) content:"123";depth:5;content:"ABC";nocase;distance:5;within:5;

0 바이트에서 5 바이트까지 검색한 뒤(123456) 해당 문자열을 추출(123)하고, 해당 문자열(123)에서 5 바이트 통과한 해당 위치(9ABCDEFGHIJK)에서 5 바이트까지 검색해(ABCDE) 해당 문자열을 추출(ABC)

10. HTTP GET 플러딩 공격 탐지 설정

```
cat > /etc/snort/rules/local.rules

alert tcp any any -> any 80 (content:"GET / HTTP/1.";nocase;threshold:type both,track by_src,count 10,seconds 2;sid:1000001;)
```

11. 슬로우 로리스 공격 탐지 설정

```
cat /etc/snort/rules/local.rules

alert tcp any any -> any 80 (flow:to_server,established;pcre:"/[^₩x0d₩x0a]₩x0d₩x0a$/";threshold: type both ,track by_src,count 10,seconds 2;sid:1000001;)
```

(1) flow 의미

1) 서버와 클라이언트의 흐름을 제어하는 용도로 사용

2) flow:to_server,established

스노트 서버로 향하는 패킷을 대상으로 3단계 연결 설정 이후의 패킷만을 제어하겠다는 의미

(2) pcre 의미

펄 호환 정규 표현식(Perl Compatible Regular Expressions)을 의미

제6-1장 방화벽(Firewall)의 이해

1. 방화벽의 기능

외부망과 내부망 사이에서 일정한 차단 규칙에 따라 특정 패킷을 차단• 허용하는 소프트웨어 설정 또는 하드웨어 장비

2. 방화벽의 접근 제어 기법

(1) ACL 방식

OSI 참조 모형의 3계층• 4계층에 기반해 필터링 기능을 수행

(2) ALG 방식

프록시 방화벽이라고도 부르며, OSI 참조 모형의 7계층에 기반해 필터링 기능을 수행하기 때문에 웹 방화벽(Web Application Firewall)처럼 특정 응용 계층의 프로토콜만을 지원해 과부하 해소

(3) 상태 추적(SPF) 방식

1) OSI 참조 모형의 3계층• 4계층• 5계층에 기반해 리턴 패킷 여부를 검사하는데, 상태 추적 테이블을 통해 전체 통신 과정을 추적

2) UDP 방식 등은 TCP 플래그와 같은 기능이 없어서 추적이 불가능하기 때문에 타임아웃을 설정해 사용

3. 방화벽 설치와 배치

(1) 패킷 필터링 기능을 수행하는 라우터를 스크리닝 라우터라고 함

(2) 하드웨어 방식으로 구현한 방화벽을 베스천 호스트라고 함

(3) 두 개의 NIC 장치로 내부망과 외부망을 연결하는 베스천 호스트를 듀얼 홈드 게이트웨이라고 함

(4) 스크리닝 라우터와 듀얼 홈드 게이트웨이를 결합한 구조를 스크리닝 호스트 게이트웨이라고 함

(5) DMZ 지역에서 듀얼 홈드 게이트웨이 등을 운영하는 구조를 스크린드 서브넷 게이트웨이라고 함

제6-2장 ACL 기반의 방화벽 설정

1. ACL 설정 시 고려 사항

(1) 와일드카드 마스크 개념

(2) 순차적인 실행 구조

(3) 방화벽을 기준으로 방향 설정

2. 표준 ACL 방식

(1) 출발지 IP 주소 또는 IP 대역에 기반해 필터링 기능을 수행

(2) IOS 기준으로 사용 가능한 ACL 식별 번호는 1-99 또는 1300-1999

(3) 구성 일례

```
access-list 10 permit 192.168.10.1 0.0.0.0
access-list 10 deny 192.168.10.0 0.0.0.255
access-list 10 permit ip
```

3. 확장 ACL 방식

(1) 모든 IP 주소와 포트 번호 등에 기반해 필터링 기능을 수행

(2) IOS 기준으로 사용 가능한 ACL 식별 번호는 100-199 또는 2000-2699

(3) 구성 일례

```
access-list 100 deny tcp 172.16.10.0 0.0.0.255 any eq 23
access-list 100 deny tcp 192.168.10.0 0.0.0.255 any eq 25
access-list 100 permit tcp any any
access-list 100 permit udp any any
```

4. 기타 TCP/IP 기반 공격에 대한 ACL 방어 설정

(1) IP 스푸핑 공격 방어

```
R2(config)#access-list 150 deny ip 10.2.1.0 0.0.0.255 any log
R2(config)#access-list 150 deny ip 127.0.0.0 0.255.255.255 any log
R2(config)#access-list 150 deny ip 0.0.0.0 0.255.255.255 any log
R2(config)#access-list 150 deny ip 172.16.0.0 0.15.255.255 any log
R2(config)#access-list 150 deny ip 192.168.0.0 0.0.255.255 any log
R2(config)#access-list 150 deny ip 224.0.0.0 15.255.255.255 any log
R2(config)#access-list 150 deny ip host 255.255.255.255 any log
R2(config)#access-list 150 permit ip any 10.2.1.0 0.0.0.255
R2(config)#interface e0/0
R2(config-if)#ip access-group 150 in
R2(config-if)#exit
```

(2) ICMP 플러딩 공격 방어

```
R2(config)#access-list 112 deny icmp any any echo log
R2(config)#access-list 112 deny icmp any any redirect log
R2(config)#access-list 112 deny icmp any any mask-request log
R2(config)#access-list 112 permit icmp any 10.2.1.0 0.0.0.255
R2(config)#interface e0/0
R2(config-if)#ip access-group 112 in
R2(config-if)#end
```

(3) ICMP 스머프 공격 방어

```
R2(config)#access-list 111 deny ip any host 10.2.1.255 log
R2(config)#access-list 111 permit ip any 10.2.1.0 0.0.0.255 log
R2(config)#access-list 112 deny ip any host 10.1.1.255 log
R2(config)#access-list 112 permit ip any 10.1.1.0 0.0.0.255 log
R2(config)#interface e0/0
R2(config-if)#ip access-group 111 in
R2(config-if)#end
R2(config)#interface e0/1
R2(config-if)#ip access-group 112 in
R2(config-if)#end
```

제7-1장 IPTables 이해

이하의 내용은 관리자 계정을 이용해 주분투 16.04 환경에서 작성

1. IPTables 시작

2001년 1월 리눅스 2.4 커널부터 제공

2. IPTables 기능

(1) 3• 4 계층 기반의 방화벽

(2) 상태 추적 기능

(3) NAT 기능

3. IPTables 구성

Filter 테이블• NAT 테이블• Mangle 테이블• Raw 테이블로 구성

4. 주요 용어

(1) INPUT 체인

방화벽을 목적지로 설정해 이동하는 경로

(2) OUTPUT 체인

방화벽을 출발지로 설정해 이동하는 경로

(3) FORWARD 체인

방화벽을 통과 또는 경유해 이동하는 경로

5. IPTables 위치

```
ls -l /sbin | grep iptables
```

6. 기본 명령어

```
iptables --help
```

```
iptables --version
```

```
iptables --flush
```

```
iptables --list
```

제7-2장 IPTables 사용 일례

이하의 내용은 관리자 계정을 이용해 주분투 16.04 환경에서 작성

1. ICMP 요청 차단 설정

```
iptables --append INPUT --protocol icmp --icmp-type echo-request -j LOG
iptables --append INPUT --protocol icmp --icmp-type echo-request -j REJECT
```

(1) --append INPUT 명령어는 들어오는 패킷을 대상으로 적용하겠다는 의미

(2) --protocol icmp 명령어는 ICMP 방식을 대상으로 적용하겠다는 의미

(3) --icmp-type echo-request 명령어는 ICMP 요청을 대상으로 적용하겠다는 의미

(4) -j LOG 명령어는 조건에 부합하면 로그를 기록하겠다는 의미

(5) -j REJECT 명령어는 조건에 부합하면 ICMP 오류 응답을 통해 거부하겠다는 의미

2. ICMP 요청 차단 추가 설정

```
iptables --append INPUT --source 192.168.10.219 --protocol icmp --icmp-type echo-request -j LOG
iptables --append INPUT --source 192.168.10.219 --protocol icmp --icmp-type echo-request -j DROP
```

--source 192.168.10.220 명령어는 출발지 IP 주소가 192.168.10.220번인 경우 적용하겠다는 의미

3. ICMP 요청 차단 추가 설정

```
iptables --append INPUT --protocol icmp --icmp-type echo-request --match length --length 1024: -j LOG
iptables --append INPUT --protocol icmp --icmp-type echo-request -j LOG
iptables --append INPUT --protocol icmp --icmp-type echo-request --match length --length 1024: -j REJECT
iptables --append INPUT --protocol icmp --icmp-type echo-request -j ACCEPT
```

--match length --length 1024: 명령어는 패킷의 길이가 1024 바이트 이상을 대상으로 정책을 적용하겠다는 의미

4. 랜드 공격 차단 설정

```
iptables --append INPUT --source 192.168.10.215 --protocol icmp --icmp-type echo-request -j LOG
iptables --append INPUT --source 192.168.10.215 --protocol icmp --icmp-type echo-request -j REJECT
```

5. TCP 오픈 스캔과 TCP 할프 오픈 스캔 차단 설정

```
iptables --append INPUT --protocol tcp --tcp-flag ALL SYN -j LOG
iptables --append INPUT --protocol tcp --tcp-flag ALL SYN -j REJECT
```

--tcp-flag ALL SYN 명령어는 SYN 플래그를 설정한 세그먼트를 대상으로 적용하겠다는 의미

6. 기타 스캔 차단 설정

```
iptables --append INPUT --protocol tcp --tcp-flag ALL FIN -j REJECT
iptables --append INPUT --protocol tcp --tcp-flag ALL FIN -j REJECT
iptables --append INPUT --protocol tcp --tcp-flag ALL URG,PSH,FIN -j REJECT
iptables --append INPUT --protocol tcp --tcp-flag ALL NONE -j REJECT
iptables --append INPUT --protocol tcp --tcp-flag ALL NONE -j REJECT
```

(1) --tcp-flag ALL FIN 명령어는 FIN 플래그를 설정한 세그먼트를 대상으로 적용하겠다는 의미

(2) --tcp-flag ALL URG,PSH,FIN 명령어는 URG• PSH• FIN 플래그를 동시에 설정한 세그먼트를 대상으로 적용하겠다는 의미

7. SSH 접속 차단 설정

```
iptables --append INPUT --source 192.168.10.219 --protocol tcp --destination-port 22 -j LOG
iptables --append INPUT --source 192.168.10.219 --protocol tcp --destination-port 22 -j REJECT
```

--destination-port 22 명령어는 목적지 포트 번호가 22번인 경우 적용하겠다는 의미

8. SSH 무차별 대입 공격 차단 설정

```
iptables --append INPUT --source 192.168.10.219 --protocol tcp --destination-port 22 --match state --state NEW --match recent --set
iptables --append INPUT --source 192.168.10.219 --protocol tcp --destination-port 22 --match state --state NEW --match recent --update --seconds 1 --hitcount 2 -j REJECT
```

(1) --match state --state NEW 명령어는 TCP 3단계 연결 수립부터 정책을 적용하겠다는 의미

(2) --match recent --set 명령어는 출발지 IP 주소 등을 동적으로 반영해 정책을 적용하겠다는 의미

(3) --match recent --update 명령어는 새로운 출발지 IP 주소 등을 동적으로 추가해 정책을 적용하겠다는 의미

제8장 기타 보안 장비

1. 보안 통합 장비(Unified Threat Management)

2. ESM과 SIEM

보안 장비들의 이벤트를 취합• 상호 연관 분석함으로서 실시간 보안 위협을 파악하고 대응하는 시스템

(1) ESM(Enterprise Security Management)

DBMS에 기반해 단기 이벤트 위주 분석에 초점

1) 에이전트 포트

보안 장비에 탑재하며 에이전트 포트가 수집한 정보를 매니저 포트로 전송

2) 매니저 포트

에이전트 포트를 통제하며, 에이전트 포트에서 수신한 정보를 분석하고 저장한 뒤 콘솔 포트로 전송

3) 콘솔 포트

수신한 정보에 대해 시각적 전달• 상황 판단 기능 등을 설정하도록 지휘• 통제

(2) SIEM(Security Information & Event Management)

1) 인덱싱에 기반해 빅 데이터 수준의 장기간 심층 분석에 초점

2) 로그 수집• 분류• 변환• 분석

(3) 상호 연관 분석

여러 보안 장비에서 발생하는 이벤트 패턴 간에 연관성을 분석해 보안 위협에 대한 보다 정확한 판단력과 대응력 등을 향상

3. PacketFence• FreeNAC 등은 대표적인 오픈 소스 방식의 NAC 도구

4. KISA의 Castle• ATRONIX의 WebKnight• TrustWave의 ModSecurity 등은 대표적인 오픈 소스 기반의 웹 방화벽

제9장 무선 LAN 보안 알고리즘의 이해와 종류

1. WEP 방식

(1) 기밀성

RC4 방식에 기반해 40 비트의 상호 인증 열쇠 값과 24 비트의 초기 벡터 값을 XOR 연산으로 통합해 기밀성을 구현

(2) 무결성

CRC-32 방식 기반

(3) 인증성

고정적인 공유 열쇠 값 사용

2. WPA 방식

(1) 기밀성

RC4 방식에 기반해 ECB 모드가 아닌 CBC 모드를 적용한 TKIP 방식을 사용

(2) 무결성

MIC 방식 기반

(3) 인증성

고정적인 공유 열쇠 값을 사용하는 WPA-PSK 방식과 인증 서버를 사용하는 WPA-EAP 방식

3. WPA2 방식

(1) 기밀성

AES 방식에 기반한 CCMP 알고리즘을 사용

(2) 무결성

MIC 방식 기반

(3) 인증성

고정적인 공유 열쇠 값을 사용하는 WPA-PSK 방식과 인증 서버를 사용하는 WPA-EAP 방식

4. 무선 공유기 보안 설정

(1) 비번 기반 인증

(2) MAC 주소 기반 인증

(3) SSID 전파 중지 설정

(4) IEEE 802.1x 기반 인증

제1장 FTP 서비스 보안

1. TCP 방식에 기반해 포트 번호 20번과 21번 사용

2. 20번 또는 1,024번 이상 포트 번호는 데이터 연결에 사용하고, 21번 포트는 제어 연결에 사용

3. 제어 연결은 전체 FTP 연결 동안 접속 상태를 유지하지만, 데이터 연결은 데이터를 전송할 때마다 연결과 해제를 반복

4. 연결 모드 종류

클라이언트 측에서 연결 모드를 변경

(1) 능동 모드

기본 설정

1) 클라이언트 측에서 1,024번 이상의 임시 포트 번호를 이용해 서버 측 21번 포트 번호로 제어 채널을 생성

2) 클라이언트 측에서는 PORT 명령어를 전송한 뒤 데이터 전송에 사용할 새로운 1,024번 이상의 임시 포트 번호와 IP 주소도 서버 측에게 전달

3) 서버 측에서는 20번 포트 번호를 이용해 클라이언트 측의 새로운 1,024번 이상의 임시 포트 번호로 데이터 채널을 생성

4) 서버 측에서는 20번 포트 번호를 이용해 클라이언트 측의 새로운 1,024번 이상의 임시 포트 번호로 데이터 전송

(2) 수동 모드

데이터 채널에 대한 방화벽 우회 목적

1) 클라이언트 측에서 1,024번 이상의 임시 포트 번호를 이용해 서버 측 21번 포트 번호로 제어 채널을 생성

2) 클라이언트 측에서 서버 측으로 PASV 명령어를 전송

3) 서버 측에서는 데이터 전송에 사용할 1,024번 이상의 임시 포트 번호를 설정해 클라이언트 측에게 전달

4) 클라이언트 측에서는 서버 측 1,024번 이상의 임시 포트 번호로 데이터 채널을 생성

5) 서버 측에서는 1,024번 이상의 임시 포트 번호를 이용해 클라이언트 측 1,024번 이상의 임시 포트 번호로 데이터 전송

5. FTP 서비스 위협 요소

(1) FTP 서비스는 평문 구조이기 때문에 SFTP 서비스 사용을 권장

(2) 익명 FTP 서버 설정 오류에 따른 취약점

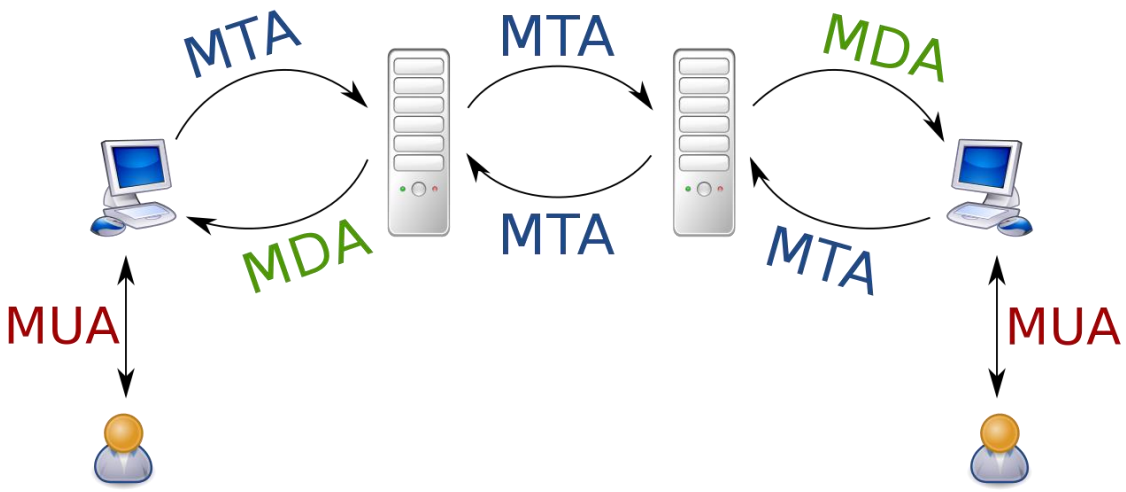
(3) FTP 바운스 공격

1) PORT 명령어의 속성을 악용

2) 다시 말해, 익명 FTP 서버를 경유해 공격 대상자를 공격

제2장 SMTP 서비스 보안

1. 구성 요소



(1) 메일 전달 에이전트 MDA

메일의 헤더와 바디 등을 생성하고 주기적으로 스풀에서 메일 도착 여부를 검사

(2) 메일 전송 에이전트 MTA

실제 메일 전송을 수행

(3) 메일 사용자 에이전트 MUA

Outlook Express 등과 같이 사용자에게 메일을 보여 주기 위한 소프트웨어

2. PEM 방식

구현의 복잡성

3. PGP 방식

(1) 필 짐머만(Phil Zimmermann)이 개발

(2) PKI 기반의 인증 기관이 없다.

(3) 기존 시스템과 호환이 곤란

4. S/MINE 방식

전자 봉투에 기반

(1) 기밀성

3DES 방식 등에 기반

(2) 무결성

RSA 방식 또는 DSS 방식에 기반한 전자 서명

(3) 인증

제3장 DNS 서비스 보안

1. TCP/UDP 방식에 기반해 포트 번호 53번 사용

2. 윈도우즈 운영 체제에서 DNS 처리 과정

(1) 로컬 디스크의 C:₩Windows₩System32₩drivers₩etc₩hosts에서 대응 IP 주소 검색

(2) 로컬 메모리의 DNS 캐시 테이블에서 IP 주소 검색

ipconfig/displaydns 명령어 또는 ipconfig/flushdns 명령어로 확인

(3) 로컬 DNS 서버에게 IP 주소 질의

3. DNS 질의 확인

```
root@xubuntu:~# cat /etc/hosts

127.0.0.1       localhost
127.0.1.1       debian
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

root@xubuntu:~# cat /etc/host.conf

multi on
order hosts,bind

root@xubuntu:~# cat /etc/resolv.conf

domain localdomain
search localdomain
nameserver 192.168.10.215
nameserver 8.8.8.8
```

4. DNS 서비스 위협 요소

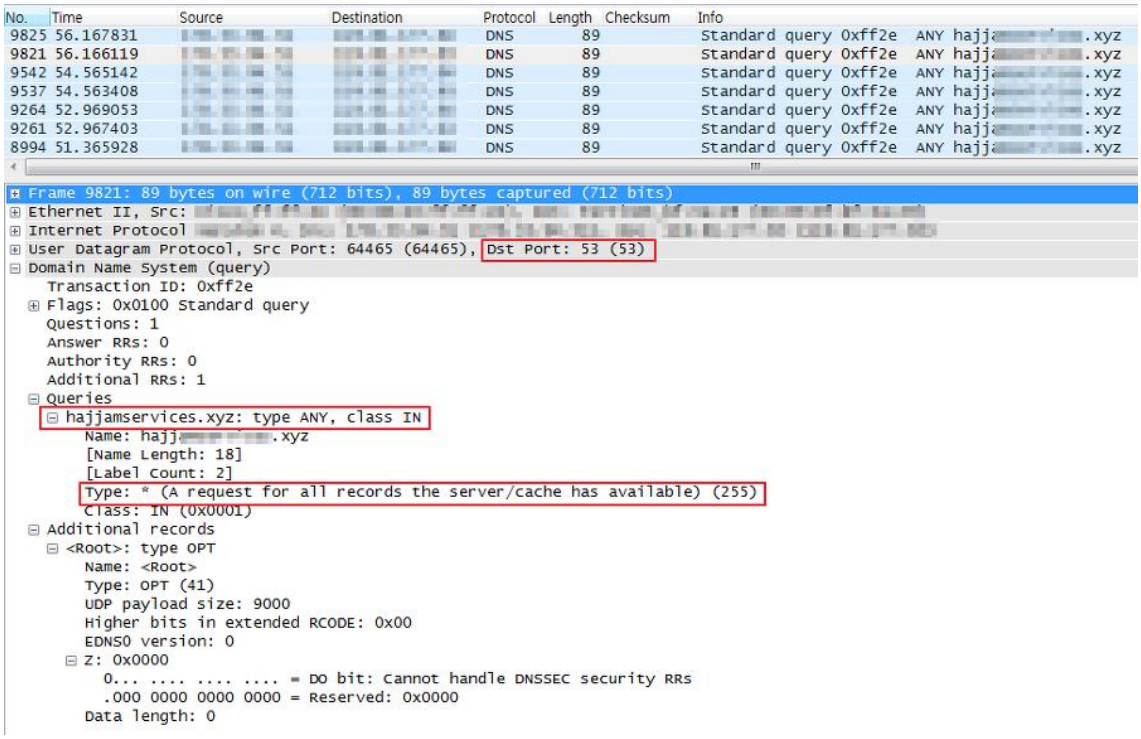
(1) DNS 증폭(DNS Amplification) 공격

1) 출발지의 주소를 공격 대상자의 주소로 설정하는 IP 스푸핑 기법을 적용해 질의하는 일종의 플러딩 공격

2) DNS 서버는 출발지 주소에 기반해 공격자가 질의한 요청을 공격 대상자에게 응답

3) 질의문의 유형을 A 유형 또는 CNAME 유형 등이 아닌 Any 유형으로 설정해 응답 크기를 증가시킴으로서 공격 대상자에게 과부하 유발

4) 내부 IP에서 요청한 DNS 질의에 대해서만 응답하도록 설정을 권고



(2) DNS 스푸핑(DNS Spoofing) 공격

(3) 리소스 레코드 정보 노출

```
root@backbox:~# dig @192.168.10.215 public.go.kr axfr

; <<>> DiG 9.10.3-P4-Debian <<>> @192.168.10.215 public.go.kr axfr
; (1 server found)
;; global options: +cmd
public.go.kr.                86400   IN      SOA     public.go.kr. root.public.go.kr. 1
10800 3600 432000 86400
public.go.kr.                86400   IN      NS      ns.public.go.kr.
public.go.kr.                86400   IN      MX      10 public.go.kr.
public.go.kr.                86400   IN      A       192.168.10.215
ftp.public.go.kr.            86400   IN      A       192.168.10.215
mail.public.go.kr.           86400   IN      CNAME   smtp.public.go.kr.
ns.public.go.kr.             86400   IN      A       192.168.10.215
smtp.public.go.kr.           86400   IN      A       192.168.10.215
ssh.public.go.kr.            86400   IN      A       192.168.10.215
telnet.public.go.kr.         86400   IN      A       192.168.10.215
www.public.go.kr.            86400   IN      A       192.168.10.215
public.go.kr.                86400   IN      SOA     public.go.kr. root.public.go.kr. 1
10800 3600 432000 86400
;; Query time: 1 msec
;; SERVER: 192.168.10.215#53(192.168.10.215)
;; WHEN: Mon May 01 10:00:48 KST 2017
;; XFR size: 12 records (messages 1, bytes 295)
```

```
root@backbox:~# dig @192.168.10.215 private.go.kr axfr

; <<>> DiG 9.10.3-P4-Debian <<>> @192.168.10.215 private.go.kr axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.

root@xubuntu:~# cat /etc/bind/named.conf.local

zone "public.go.kr" {type master;file "/etc/bind/public.go.kr.zone";allow-transfer {any;};};
zone "private.go.kr" {type master;file "/etc/bind/private.go.kr.zone";allow-transfer {localhost;};};
```

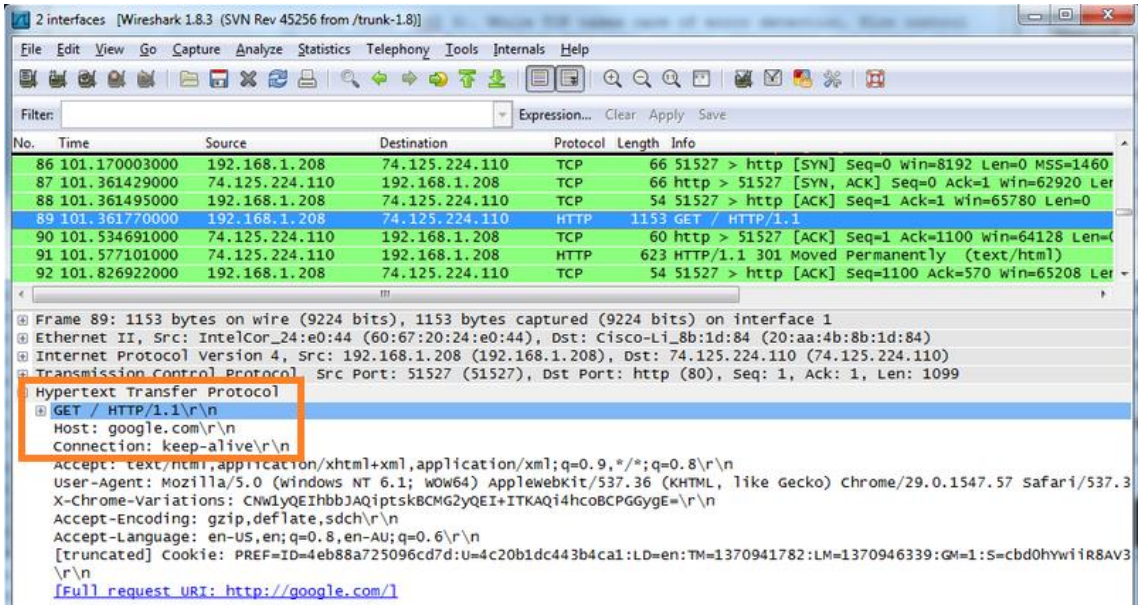
5. 사이트 차단 정책

(1) 서버 IP 차단 방식

(2) DNS 차단 방식

ISP 업체가 제공하는 DNS 서버에서 도메인 네임에 해당하는 IP 주소를 질의하는 요청이 들어오면 실제 해당 IP 주소 대신 차단 사이트(warning.or.kr)의 IP 주소를 알려주는 방식

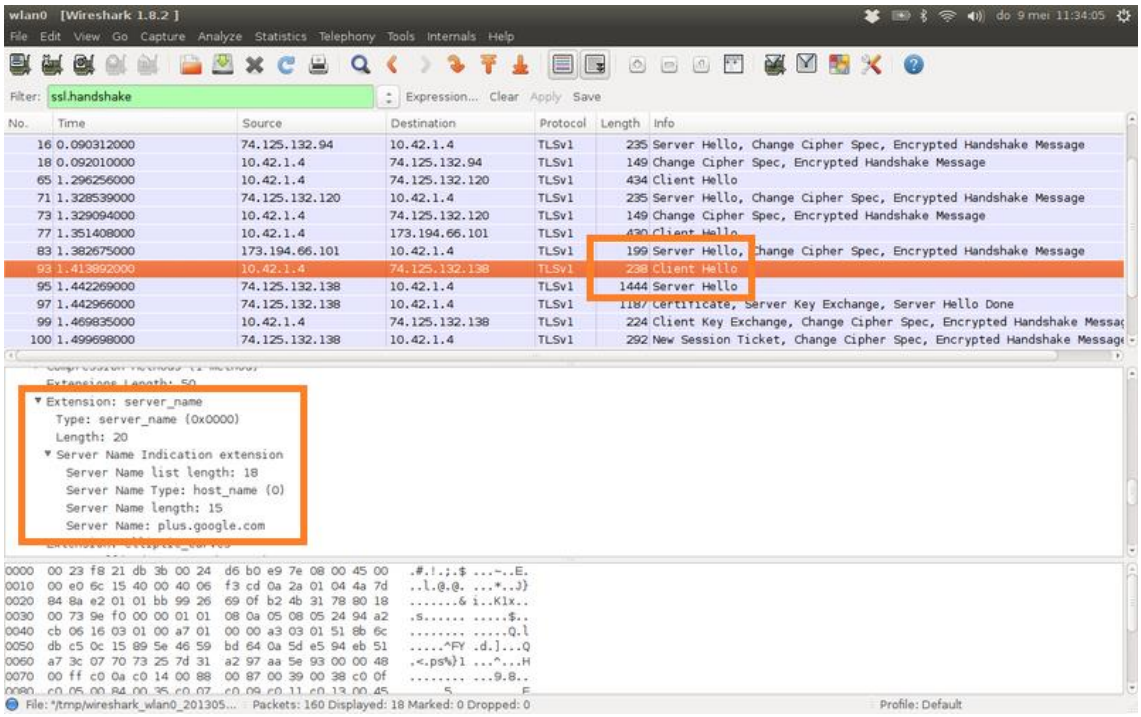
(3) HTTP 헤더의 호스트 정보를 이용한 차단 방식



(4) SNI(Server Name Indication) 차단 방식

1) 암호화가 본격적으로 개시되기 직전에 순간적으로 Extension: server_name 항목에 호스트 이름이 표시되는 순간을 포착해 차단

2) ESNI(Encrypted SNI) 기술을 통해 우회


wlan0 [Wireshark 1.8.2]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ssl.handshake
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
16 0.090312000 74.125.132.94 10.42.1.4 TLSv1 235 Server Hello, Change Cipher Spec, Encrypted Handshake Message
18 0.092010000 10.42.1.4 74.125.132.94 TLSv1 149 Change Cipher Spec, Encrypted Handshake Message
65 1.296256000 10.42.1.4 74.125.132.120 TLSv1 434 Client Hello
71 1.328539000 74.125.132.120 10.42.1.4 TLSv1 235 Server Hello, Change Cipher Spec, Encrypted Handshake Message
73 1.329094000 10.42.1.4 74.125.132.120 TLSv1 149 Change Cipher Spec, Encrypted Handshake Message
77 1.351408000 10.42.1.4 173.194.66.101 TLSv1 430 Client Hello
83 1.382675000 173.194.66.101 10.42.1.4 TLSv1 199 Server Hello, Change Cipher Spec, Encrypted Handshake Message
93 1.413892000 10.42.1.4 74.125.132.138 TLSv1 238 Client Hello
95 1.442269000 74.125.132.138 10.42.1.4 TLSv1 1444 Server Hello
97 1.442966000 74.125.132.138 10.42.1.4 TLSv1 1187 Certificate, Server Key Exchange, Server Hello Done
99 1.469835000 10.42.1.4 74.125.132.138 TLSv1 224 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
100 1.499698000 74.125.132.138 10.42.1.4 TLSv1 292 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
Extension: server_name
Type: server_name (0x0000)
Length: 20
Server Name Indication extension
Server Name list length: 18
Server Name Type: host_name (0)
Server Name length: 15
Server Name: plus.google.com
0000 00 23 f8 21 db 3b 00 24 d6 b0 e9 7e 08 00 45 00
0010 00 e0 6c 15 40 00 40 06 f3 cd 0a 2a 01 04 4a 7d
0020 84 8a e2 01 01 bb 99 26 69 0f b2 4b 31 78 80 18
0030 00 73 9e f0 00 00 01 01 08 0a 05 08 05 24 94 a2
0040 cb 06 16 03 01 00 a7 01 00 00 a3 03 01 51 8b 6c
0050 db c5 0c 15 89 5e 46 59 bd 64 0a 5d e5 94 eb 51
0060 a7 3c 07 70 73 25 7d 31 a2 97 aa 5e 93 00 00 48
0070 00 ff c0 0a c0 14 00 88 00 87 00 39 00 38 c0 0f
File: "/tmp/wireshark_wlan0_201305... Packets: 160 Displayed: 18 Marked: 0 Dropped: 0
Profile: Default

제4-1장 HTTP 서비스 보안

1. HTTP 서비스

(1) 웹의 3대 구성 요소 중 하나

(2) TCP 방식에 기반해 포트 번호 80번 사용

(3) 현재 HTTP 1.1 버전 사용

2. 주요한 HTTP 헤더 항목

HTTP 페이로드는 캐리지 값 ₩r₩n₩r₩n(0d0a0d0a)을 통해 HTTP 헤더와 HTTP 바디로 구성되는데, 헤더에는 서버의 바디 처리 방식 정보를 저장

(1) Content-Length 항목

HTTP 바디의 길이 정보를 저장

(2) Cache-Control 항목

```
HTTP 1.0

pragma: no-cache

HTTP 1.1

cache-control: no-cache
```

(3) Set-Cookie 항목

서버 측에서 클라이언트 측으로 보내는 일종의 인증 식별자

(4) Cookie 항목

클라이언트 측에서 서버 측으로 보내는 일종의 인증 식별자

(5) Referer 항목

A 페이지를 경유해 B 페이지로 접속하는 경우 A 페이지 정보를 저장

(6) Location 항목

A 페이지를 경유해 B 페이지로 접속하는 경우 B 페이지 정보를 저장

3. 주요한 HTTP 요청 지시자

(1) GET 지시자

서버의 기본 페이지 요청 시 사용

(2) HEAD 지시자

GET 지시자와 동일한 기능을 수행하지만 응답 헤더만 요청 시 사용

(3) POST 지시자

클라이언트 측에서 계정과 비번 등을 전송하기 위해 사용

(4) PUT 지시자

데이터를 저장하기 위해 사용

(5) DELETE 지시자

데이터를 삭제하기 위해 사용

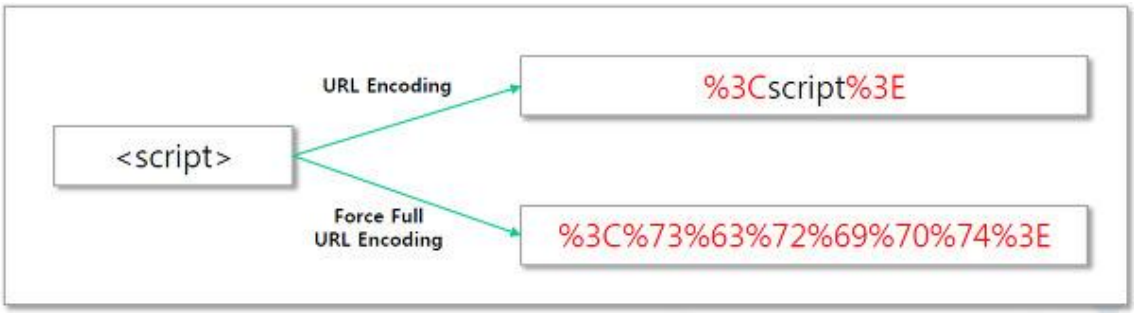
(6) OPTIONS 지시자

서버가 어떠한 지시자를 사용하는가 질의하기 위해 사용

5. URL 인코딩

(1) ASCII 코드에 없는 영어를 제외한 외국어와 ASCII 코드에서 표현하지 않는 특수 문자 등을 표현하기 위해 사용

(2) 해당 문자열의 헥사 값 앞에 % 기호를 붙여 사용



6. 응답 상태 코드

(1) 200번대 성공

(2) 300번대 재지정

(3) 400번대 클라이언트 측 오류

(4) 500번대 서버 측 오류

제4-2장 2017 OWASP TOP 10

1. 삽입

(1) 입력 과정에서 악의적인 명령어 등을 삽입해 인증 처리 등을 무력화

(2) SQL 삽입 공격의 개념과 종류

1) 오류 기반 SQL 삽입 공격

```
root@xubuntu:~# mysql -u root -p

use injectiond;

select * from injectiont where user = 'tiger' and password = '4321';

select * from injectiont where user = 'tiger' and password = '4321' or '10' = '10';

select * from injectiont where user = 'tiger' or '10' = '10';#' and password = '';
```

2) 무차별 SQL 삽입 공격

```
root@backbox:~# sqlmap -D "dvwa" -T "users" --users --passwords --dump-all

Payload: cat=1 AND (SELECT 5477 FROM(SELECT COUNT(*),
CONCAT(0x716a787071,(SELECT (ELT(5477=5477,1))),
0x7162717171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP
BY x)a)

이하 내용 생략
```

SQL 질의문이 참인 경우와 거짓인 경우를 이용해 서버의 반응으로부터 데이터를 추출하는 기법

3) mysql_real_escape_string() 함수 등을 사용해 SQL 삽입 공격 방지

```
[수정 전]

$id = $_POST['id'];
$pw = $_POST['pw'];

$get = "select * from injectiont where user = '$id' and password = '$pw'";

[수정 후]

$id = $_POST['id'];
$pw = $_POST['pw'];

$id = stripslashes($id); #stripslashes() 함수 적용
$pw = stripslashes($pw);
```

```
$id = mysql_real_escape_string($id); #mysql_real_escape_string() 함수 적용
$pw = mysql_real_escape_string($pw);

$get = "select * from injectiont where user = '$id' and password = '$pw'";
```

(3) 명령어 삽입 공격

1) ping 8.8.8.8;cat /etc/passwd 등과 같이 명령어를 삽입

2) 필요 시 허용 가능한 명령어 목록 등을 설정

2. 취약한 인증

쿠키 스푸핑 등과 같이 비정상적인 인증 처리로 비밀 번호 도용 등과 같은 취약점 발생

3. 민감한 데이터 노출

평문 처리 등에 의한 위협

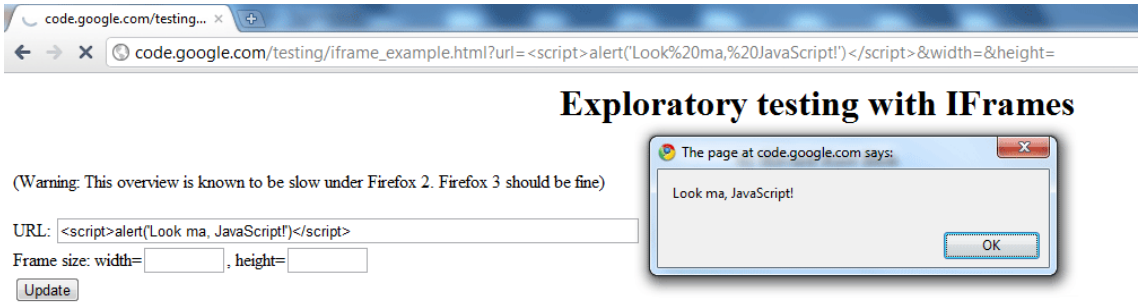
4. XML 외부 개체

5. 취약한 접근 통제

6. 잘못된 보안 설정

7. 크로스 사이트 스크립팅(XSS)

(1) XSS 공격의 개념



공격 대상자의 웹 브라우저에서 자바스크립트 언어의 실행을 허용하기 때문에 발생하는 공격

(2) XSS 공격의 방어

특수 문자를 strip_tags() 함수 등을 이용해 제거하거나, htmlspecialchars() 함수 등을 이용해 일반 문자로 치환

8. 안전하지 않은 역직렬화

9. 알려진 취약점이 있는 구성 요소 사용

MS-SQL xp_cmdshell 등과 같은 기능 때문에 서버 권한을 획득할 수 있는 취약성

10. 불충분한 로깅 및 모니터링

제4-3장 기타 다양한 웹 공격

1. 디렉토리 리스팅 공격

```
root@xubuntu:~# cat /etc/apache2/apache2.conf | grep Indexes

[수정 전]

<Directory /var/www/html>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>

[수정 후]

<Directory /var/www/html>
        Options FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>
```

(1) 강제 웹 브라우징 공격

```
http://192.168.10.215/dvwa/vulnerabilities/fi/?
page=../../../../../etc/passwd
```

외부 입력 값에서 경로를 변경할 수 없도록 문자열에 대해 필터링

(2) 문자 인코딩(HEX Encoding) 공격

```
http://192.168.10.215/dvwa/vulnerabilities/fi/?
page=%2E%2E%2F/%2E%2E%2F/%2E%2E%2F/%2E%2E%2F/%2E%2E%2F
/etc/passwd
```

1) 보안 장비 등을 우회하기 위해 강제적으로 모든 문자를 URL 인코딩하는 기법

2) urldecode() 함수와 utf8_decode() 함수 등을 이용해 제거

(3) 널 바이트(Null Byte) 삽입 공격

```
http://192.168.10.215/dvwa/vulnerabilities/fi/?
page=%2E%2E%2F/%2E%2E%2F/%2E%2E%2F/%2E%2E%2F/%2E%2E%2F
/etc/passwd%00html
```

1) 보안 장비 등에서는 확장자를 html로 인식하지만 웹 서버의 운영 체제에서는 %00 이후 부분을 무시하고 처리

2) eregi() 함수 등을 이용해 제거

2. 파일 포함 공격

(1) 원격에서 include() 함수나 require() 함수의 인자를 조작해 악의적인 시스템 명령어를 실행하는 기법

(2) php.ini에서 allow_url_fopen 부분을 Off로 설정

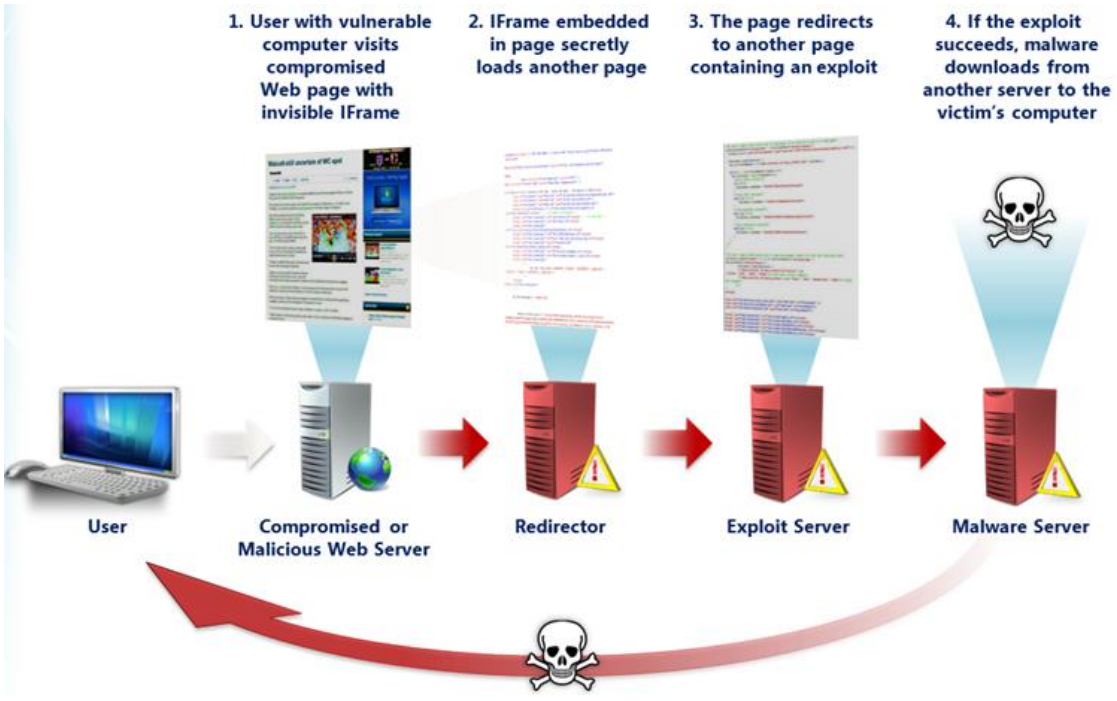
```
root@xubuntu:~# cat /etc/php/7.0/apache2/php.ini | grep allow_url_fopen

allow_url_fopen = On
```

3. 파일 업로드 공격

(1) 웹쉘(Webshell) 등을 이용한 공격

(2) 업로드 파일의 확장자 제한이나 저장 공간의 격리 등 필요

4. 드라이브 바이 다운로드(Drive by Download) 공격



(1) 공격자가 서비스 중인 웹 페이지에 악성 코드를 삽입해 공격 대상자에게 악성 코드를 주입

(2) 유포 사이트 은폐를 목적으로 다단계 경유지를 생성

제5장 NTP 서비스 보안

(1) UDP 123번 기반의 시간 동기화 서비스

```
root@xubuntu:~# apt-get install ntp

root@xubuntu:~# ntpd --help
ntpd - NTP daemon program - Ver. 4.2.8p10 #NTP 증폭 공격 악용 제거 버전

이하 내용 생략

root@xubuntu:~# cat /etc/ntp.conf

이하 내용 생략

root@xubuntu:~# service ntp restart

root@xubuntu:~# ntpq -p

이하 내용 생략

root@xubuntu:~# ntpdc -c monlist 127.0.0.1
127.0.0.1: timed out, nothing received
***Request timed out
```

(2) NTP 증폭 공격

1) NTP 서비스의 monlist 기능을 악용해 중계자가 특정 대상자에게 대량의 트래픽을 전송해 과부하를 유발시키는 기법

2) monlist 기능

NTP 서버에 접속한 시스템 목록을 요청하고 출력하는 기능

3) 대응 방법

4.2.8 버전 이상으로 업데이트를 진행하거나, /etc/ntp.conf 환경 설정의 restrict default 항목에 noquery 내용을 추가해 monlist 기능을 비활성 상태로 전환

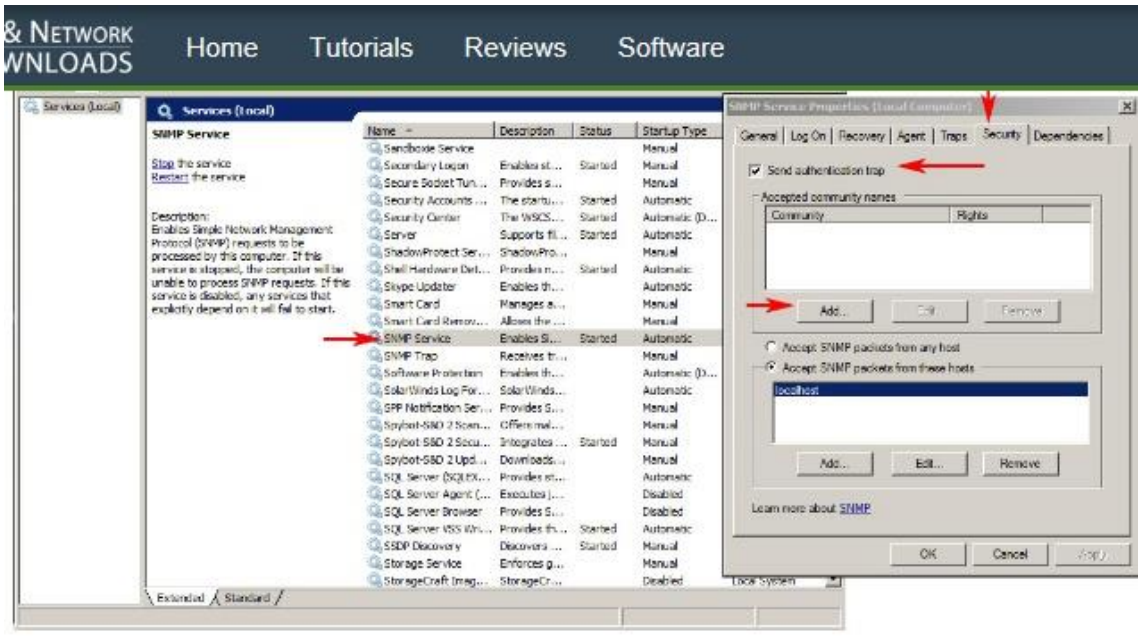
제6장 SNMP 서비스 보안

1. UDP 방식에 기반해 매니저가 폴링 방식에 따라 에이전트의 상태를 감시하고 관리하는 기능을 수행

2. 에이전트(포트 번호 161번 사용)와 매니저 사이에서 주고받는 데이터 집합을 MIB라고 한다.

3. 트랩 방식은 에이전트에서 비동기적인 이벤트가 발생하면 이벤트 리포팅 방식에 따라 포트 번호 162번을 이용해 관리자에게 즉각 전송하는 기능

4. 커뮤니티 스트링(Community String) 개념을 통해 인증 기능을 수행하면서 감시 장비 대상의 범위를 논리적으로 설정



5. SNMP 서비스 위협 요소

(1) 커뮤니티 스트링 부분이 스니핑 공격에 취약

(2) SNMP 증폭 공격

제7장 기타 DB 서비스 취약점

1. 집성(Aggregation)

저수준의 보안 등급에 해당하는 정보를 조합해 고수준의 보안 등급에 해당하는 정보를 획득

2. 추론(Inference)

보안 등급이 없는 정보에 접근한 뒤 기밀 정보를 유추

3. 데이터 디들링(Data Diddling)

처리할 자료를 다른 자료와 바꾸는 일종의 사기 수법

역대 주요 실기 기출 문제 분석

1. SIEM(Security Information & Event Management)은 IDS/IPS 등에서 생성하는 **개별 로그를 수집• 관리**하기 위해 일반적으로 다음과 같은 기능을 제공한다. **[2013년 1회 기사]**

(1) **로그 수집**

관제 대상 시스템에 설치한 에이전트로서 SNMP 또는 시스템 로그(SysLog) 서버에 저장하는 과정

(2) **로그 분류**

이벤트 발생 누적 횟수 등 유사 정보에 기반해 그룹핑한 뒤 한 개의 정보로 취합하는 과정

(3) **로그 변환**

다양한 로그 표현 방식을 단일한 로그 표현 방식으로 변환하는 과정

(4) **로그 분석**

타임스탬프• IP 주소• 이벤트 등으로 구성된 규칙에 기반해 여러 개의 로그 연관성을 분석하는 과정

2. **시스템 로그(SysLog)**는 기밀성• 무결성• 가용성 등 **정보 보호 특성을 고려하지 않고 개발**되었다. 따라서 UDP 방식을 통해 로그를 전송할 때 공격자가 시스템 로그(SysLog) 메시지를 모니터링해 중요 정보를 알아낼 수 있다. 이것 때문에 RFC 3195에서는 다음과 같이 몇 가지 보안 기능을 제공하도록 권고하고 있다. **[2013년 1회 산업 기사]**

(1) 로그 전송의 신뢰성 보장을 위해 연결 지향 프로토콜인 **TCP 방식**을 이용하도록 권고

(2) 시스템 로그(SysLog) 메시지 전송 시 기밀성 보장을 위해 시스템 로그(SysLog) 서버• 로그 수집 대상 서버의 페이로드를 보호할 수 있는 **BEEF 방식**을 이용하도록 권고

3. 다음은 **보안 관제 모니터링 방법**이다. **[2014년 3회 산업 기사]**

(1) **보안 장비 모니터링**

위협 관리 시스템• 침입 탐지 시스템 등 네트워크 상황에 대한 실시간 감시 기능을 이용해 실시간 공격 정보• 네트워크 트래픽 상황 등을 확인

(2) **서버 모니터링**

주요 시스템에 대한 헬스 체크(Health Check) 모니터링 결과를 종합 상황판에 표시해 정기적으로 가용성을 확보

(3) **트래픽 모니터링**

인터넷 주요 기간의 패킷에 대한 흐름 상태를 종합 상황판에 제공해 관리

4. 다음 **Snort PCRE 헤더 중 액션 항목의 옵션 내용**이다. **[2014년 3회 산업 기사]**

(1) alert: 정해진 방식에 따라 alert을 발생시키고 패킷을 기록

(2) log: 패킷의 로그를 남긴다.

(3) pass : 패킷을 무시한다.

(4) activate: alert을 발생시키고 대응하는 dynamic 시그니처를 유효하게 한다.

(5) dynamic: activate에 의해 활성화되면 log와 동일한 동작을 취한다.

(6) **drop** : 패킷 차단 후 로그에 저장

(7) **reject**: TCP 패킷일 때 차단하고 로그를 저장한 뒤 TCP Rest 패킷을 전송하고, UDP 패킷일 때 차단하고 로그를 저장한 뒤 **icmp port unreachable** 내용을 전송

(8) **sdrop** : 패킷을 차단하지만 로그를 남기지 않는다.

5. HTTP **OPTIONS 요청 지시자** 사용 일례 **[2014년 4회 기사]**

```
root@metasploitable:~# telnet 127.0.0.1 80

Trying 127.0.0.1…
Connected to 127.0.0.1.
Escape character is '^]'.
OPTIONS * HTTP/1.0
HTTP/1.1 200 OK
Data: Fri, 06 Feb 2015 17:48:04 GMT
Server: Apache
Content-Length: 0
Allow: GET, HEAD, POST, OPTIONS, TRACE
Connection: close
Content-Type: text/plain; charset=UTF-8
Connection closed by foreign host.
```

6. 다음은 어느 웹 서버(211.168.100.23)에 설치한 침입 탐지 시스템(IDS)에서 탐지한 이벤트 결과를 보여 주고 있다. 이 정보를 기초로 판단하면 이 패킷이 위조된 패킷임을 의미하는 단서가 두 가지 있는데, 각각 무엇인지 기술하시오. **[2014년 4회 산업 기사]**

```
12/29-09:13:32 211.168.38.3:80 -> 211.168.100.23:80
TCP TTL:31 TOS:0X0 ID:39426 LPLEN:20 DGMLEN:44
******SF SEQ:0X63BCECE1 ACK:0X1DB99E53 WIN:0X404 TCPLEN:24"
```

7. 다음은 어떤 WAF(Web Application Firewall)에서 탐지된 이벤트 중 일부이다. 공격자가 수행한 공격명을 쓰시오. **[2015년 5회 기사]**

```
Raw Body: Log=root&pwd=%27+or+1%3D1--&wp-submit="
```

SQL 삽입 공격

8. 다음은 **HTTP 요청과 응답 결과**이다. 질문에 답하시오. **[2015년 5회 기사]**

```
[Request]

Get /home/greet/ HTTP/1.1
Accept : text/html, application/xhtml+ xml. */*
Accept-Language: ko-KR
User-Agent : Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 192.168.19.131
DNT: 1
Proxy-Connection: Keep-Alive

[Response]

HTTP/1.1 200 OK
Date: Fri,
<html>
<head>
<title>Index of /home/greet</title>
</head>

<body>
<h1>Index of /home/greet</h1>
```

(1) 어떤 유형의 공격인가? **디렉토리 인덱싱(리스팅) 취약점**

(2) 공격 대상은 무엇인가? 웹 서버(192.168.19.131)

(3) 공격의 성공 여부와 판단 기준을 서술하시오.

응답 결과에서 /home/greet 디렉토리 파일 목록을 표시

9. 악성 코드의 동적 분석을 위해 SysAnalyzer를 이용해 악성 코드 동작 전후 스냅샷을 찍어본 결과 다음과 같은 시스템 변경 사항이 발견되었다. 각 동작을 설명하시오. **[2015년 5회 기사]**

```
CreateFileA(C:₩windows₩system32₩msnsrv.exe)
CreateFileA(C:₩windows₩system32₩wassa.exe)

msnsrv.exe 및 wassa.exe 파일 생성

KEY : HKLM₩SYSTEM₩CurrentControlSet₩Services₩SharedAccess₩Parameters₩
FirewallPolicy₩StandardProfile₩GloballyOpenPorts₩List
Value : ""9070:TCP""=""9070:TCP:*:Enabled:Agent""

윈도우즈 방화벽에서 TCP 9070번 포트 허용

KEY : HKLM₩Softeware₩Microoft₩Windows₩CureentVersion₩Run
Value : ""wassa.exe""=""c:₩₩windows₩₩system32₩₩wassa.exe""
```

```
wassa.exe를 윈도우즈 시작 시 자동으로 시작하는 시작 프로그램에 등록

KEY : HKLM₩SYSTEM₩CurrentCnotrolSet₩Services₩msnsrv.exe
Value : ""Start""=dword:00000002

msnsrv.exe를 윈도우즈 서비스에 자동 실행으로 등록

KEY : HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVerion₩Explorer₩
Advanced₩Folder₩Hidden₩SHOWALL
Value : ""CheckedValue""=dword:00000000"

윈도우즈 탐색기의 폴더 옵션 > 숨김 파일 및 폴더 옵션을 표시함으로 변경할 수 없게 함
```

10. syslog.conf 내역을 설정해 모든 요소(kern• mail 등)에 대해 정상이지만 주의가 필요한 (normal, but significant condition) 로그에 대해 /var/log/messages 위치에 남기려 한다. [2015년 5회 산업 기사]

```
*.notice /var/log/messages
```

11. VLAN 개념을 설명하고 구성 방식에 따른 종류를 설명하시오. [2015년 5회• 2017년 7회 산업 기사]

(1) VLAN 개념

데이터 링크 계층에서 **브로드캐스트 도메인을 논리적으로 분리**하기 위해 사용하는 기술

(2) VLAN 종류

1) 포트 기반 VLAN : 가장 일반적으로 사용하는 방식

2) 맥 기반 VLAN : 각 호스트들의 맥 주소를 VLAN에 등록하는 방식

3) IP 기반 VLAN : 각 호스트들의 IP 주소를 VLAN에 등록하는 방식

4) 프로토콜 기반 VLAN : 같은 통신 프로토콜로 VLAN을 구성하는 방식

12. 다음은 어떤 리눅스 호스트에서 netstat -rn 명령어를 통해 얻은 라우팅 테이블 정보다. 아래 질문에 적절한 게이트웨이 주소를 쓰시오. [2015년 6회 기사]

```
Destination   Gateway       Genmask           Flags   Iface
10.0.96.100   10.0.160.1    255.255.255.255   UGH     eth0
10.0.64.0     10.0.160.2    255.255.255.0     UG      eth0
10.0.64.0     10.0.160.3    255.255.192.0     UG      eth0
10.0.128.0    10.0.160.4    255.255.192.0     UG      eth0
10.0.160.0    *             255.255.254.0     U       eth0
127.0.0.0     *             255.0.0.0         U       lo
0.0.0.0       10.0.160.5    0.0.0.0           UG      eth0
```

(1) 10.0.96.100 목적지로 ping 명령 수행 시 사용되는 gateway 주소를 쓰시오.

10.0.160.1

(2) 10.0.122.100 목적지로 ping 명령 수행 시 사용되는 gateway 주소를 쓰시오.

10.0.160.3

(3) 10.0.192.100 목적지로 ping 명령 수행 시 사용되는 gateway 주소를 쓰시오.

10.0.160.5

13. 다음은 IPSec VPN를 통해 제공되는 보안 서비스들이다. 나머지 네 가지에 대한 명칭과 의미를 기술하시오. [2015년 6회 기사]

(1) **기밀성**

(2) 제한적 트래픽 흐름에 대한 기밀성

(3) **비연결형 무결성**

(4) **데이터 원천 인증• 송신처 인증**

(5) 접근 제어

(6) **재전송 공격 방지**

14. 다음은 **윈도우즈 감사 정책**을 서술한 것이다. 세부 감사 정책을 기술하시오. [2015년 6회 산업 기사]

(1) **시스템 이벤트 정책**

시스템 시작 또는 종료• 보안 로그에 영향을 미치는 이벤트 등을 감사할지 여부를 결정.

(2) **계정 로그온 이벤트 정책**

도메인 컨트롤러에서 도메인 사용자 계정을 인증할 때마다 감사할지 여부를 결정

(3) **프로세스 추적 정책**

프로세스 생성• 프로세스 종료• 핸들 복제• 간접 개체 액세스 같은 프로세스 관련 이벤트를 감사할지 여부를 검사

15. 윈도우즈 DNS 서버 설정 시 DNS 서버에 관리하는 도메인을 등록하는 **존 설정**과 DNS 서버에 서비스 정보를 입력하는 **리소스 레코드 설정**이 있다. [2016년 7회 기사]

16. 리눅스 시스템 관리자는 **cron 도구**를 이용해 다음과 같은 작업을 수행하려고 한다. 다음 질문에 각각 답하시오. [2016년 8회 기사]

(1) 예약 작업을 확인하기 위한 crontab 명령어를 작성하시오.

crontab -l

(2) sys라는 사용자의 cron 테이블을 생성하기 위한 crontab 명령어를 작성하시오.

crontab -u sys -e

(3) cron 테이블에 ""/bin/rm -rf"" 명령어를 사용해 /home 디렉토리 밑에 있는 모든 디렉토리 및 파일 등을 삭제하기 위한 crontab 명령어를 작성하시오. 단, **매주 일요일 오전 03:00에 동작**하며, 표준 출력은 /dev/null로 보내어 출력되지 않게 하고 **표준 오류는 표준 출력으로 재입력**하도록 등록하시오.

0 3 * * 0 /bin/rm -rf /home/* > /dev/null 2>&1

17. 다음은 TCP 연결 설정 과정에 대한 내용이다. 각각의 빈 칸에 적절한 **일련 번호(Sequence Number)**와 **확인 번호(Acknowledgment Number)**를 작성하시오. **[2016년 8회 기사]**

(1) SYN 플래그 경우 Seq.Num: 37892111 ACK.Num: *

(2) ACK• SYN 플래그 경우 Seq.Num:236548731 ACK.Num: 37892112

(3) ACK 플래그 경우 Seq.Num: 37892112 ACK.Num: 236548732

18. **2014년 4월에 발견**된 오픈 소스 암호화 라이브러리의 취약점으로 **서버에 저장된 중요 메모리 데이터가 노출**되는 심각한 버그가 발견되어 시스템과 소프트웨어에 대한 신속한 취약점 조치가 권고되고 있다. 이를 탐지하기 위한 스노트 룰은 아래와 같다. 다음 질문에 각각 답하시오. **[2016년 8회 기사]**

```
alert tcp any any < > any
[443,465,563,636,695,898,989,990,992,993,994,995,2083,2087,2096,2484,8443,8883,9091]
(content:""|18 03 00|"";depth:3;content:""|01|"";distance:2;within:1;
content:!""|00|"";within:1;sid:1;)
alert tcp any any < > any
[443,465,563,636,695,898,989,990,992,993,994,995,2083,2087,2096,2484,8443,8883,9091]
(content:""|18 03 01|"";depth:3;content:""|01|"";distance:2;within:1;
content:!""|00|"";within:1;sid:2;)
alert tcp any any < > any
[443,465,563,636,695,898,989,990,992,993,994,995,2083,2087,2096,2484,8443,8883,9091]
(content:""|18 03 02|"";depth:3;content:""|01|"";distance:2;within:1;
content:!""|00|"";within:1;sid:3;)
```

(1) 취약점 이름은 무엇인가? **하트블리드(HeartBleed)**

(2) 보안 장비를 이용하지 않고 해당 취약점을 해결할 수 있는 방안을 두 가지를 서술하시오. **비밀 번호 재설정• 해당 버전 업데이트• 공인 인증서 재발급**

19. 리눅스 시스템에서 웹 서버의 로그를 **logrotate 도구**를 이용해 보관하려고 한다. 다음 설명에 적절한 옵션을 기술하시오. **[2016년 8회 산업 기사]**

[보기]

```
# cat httpd

/var/log/httpd/*log {
        weekly #1주일 단위로 로케이션
        rotate 4 #4개의 순환 파일을 사용
        compress #로그 파일을 압축• 보관
        missingok
        notifempty
        sharedscripts
        postrotate
            /bin/kill -HUP 'cat /var/run/httpd/httpd.pid 2>/dev/null' 2> /dev/null
        endscript
}
```

20. 리눅스 서버에서 SSH 원격 접근을 **TCP Wrapper 도구**를 이용해 아래와 같이 제한하고자 한다. 이를 위해 **/etc/hosts.allow** 파일과 **/etc/hosts.deny** 파일에 추가할 내용을 기술하시오. 단, SSH 이외의 서비스에는 영향이 없어야 하며, SSH 데몬은 sshd이다. **[2016년 8회 산업 기사]**

(1) 허용할 IP 주소: 192.168.159.133,10.10.10.0**[/etc/hosts.allow 파일에서 작성]**

in.sshd: 192.168.159.133,10.10.10.0/255.255.255.0[우선 적용]

(2) 허용할 IP 이외의 모든 IP 주소에 대해 SSH 접속 불가**[/etc/hosts.deny 파일에서 작성]**

sshd: ALL

21. 버퍼 오버플로우 공격은 메모리에 할당된 버퍼 크기를 초과하는 양의 데이터를 입력해 이로 인해 프로세스의 흐름이 바뀌게 되는 형태의 공격을 말한다. **[2017년 9회 기사]**

(1) 버퍼 오버플로우 공격은 **스택 영역**에 할당된 버퍼 크기를 초과하는 양의 데이터(실행 가능한 코드)를 입력해 **복귀 주소(Return Address)**를 변경한 뒤 공격자가 원하는 임의의 코드를 실행

(2) 버퍼 오버플로우 공격은 프로그램 실행 시 **힙 영역**에 할당된 버퍼 크기를 초과하는 양의 데이터(실행 가능한 코드)를 입력해 메모리의 데이터와 함수 주소 등을 변경한 뒤 공격자가 원하는 임의의 코드를 실행

22. **IP 단편화(fragmentation)**는 다양한 네트워크 환경에서 IP 패킷의 효율적인 전송을 가능하게 하는 패킷 분할 기법이다. IP 데이터그램을 단편화할 때 tcpdump 내용 중 다음 (1)• (2)• (3)이 의미하는 바를 쓰시오. **[2017년 9회 기사]**

```
[보기]

04:05:493961718 < 10.10.10.1 > 10.10.10.100: (frag 22666:1480@2960+) (ttl 128)
```

(1) 22666

단편화 ID를 의미

(2) 1480

IP 헤더를 제외한 단편화된 크기를 의미

(3) 2960+

단편의 상대 위치(Offset)가 2960이고, 추가 단편(+)이 있다

23. 윈도우즈 레지스트리의 하이브

(1) HKEY_CLASSES_ROOT(HKCR)

파일 연결• OLE 객체 클래스 ID와 같은 등록된 응용 프로그램의 정보를 저장

(2) HKEY_CURRENT_USER(HKCU)

현재 로그인한 사용자의 설정을 저장

(3) HKEY_LOCAL_MACHINE(HKLM)

모든 사용자의 설정을 저장

(4) HKEY_USERS(HKU)

사용 중인 각 사용자 프로파일의 HKEY_CURRENT_USER 키에 일치하는 서브키를 저장

(5) HKEY_CURRENT_CONFIG

실행 시간에 수집한 자료를 저장