보안 알고리즘과 VPN 장비의 이해

서울시 인재 개발원

2022.3.2-3.4

강사 소개

서울에서 출생해 인천 대학교(구 인천 전문 대학) 일어과와 경희 사이버 대학교 정보 통신 학과를 졸업하고 한국 외국어 대학교 교육 대학원에서 **전산 교육학 석사**를 취득했다.

약 9년 동안 한국 통신(KT) 등에서 근무하며 다양한 행정 처리와 정보 기술 환경 등을 경험했다. 사무 처리와 관련해 한자 능력 2급 등을 취득했고 정보 기술과 관련해 **정보 처리 산업 기사/정보 보안 산업 기사**와 CCNA/CCNP 등과 같은 자격증을 취득했다. 또한 **교원 2급 자격증과 직업 능력 개발 훈련 교사 3급 자격증** 등을 취득했다.

지난 2004년부터 현재까지 국가 공무원 인재 개발원과 서울시 인재 개발원 등에서 **정보 보안 기사 자격증과 모의 침투 분야 등을 강의 중**이다. 지난 2016년 경찰 인재 개발원(구 경찰 교육원)에서 우수 외래 강사로 감사장을 받았다. 사이버 보안 중 다양한 모의 침투 운영 체제와 사회 공학 등에 특히 관심이 많다.

강의가 없을 때에는 문학• 사학• 철학 등에 대한 책을 읽거나 국가 정보학 등과 같은 책을 읽는다. 페이스북에서 **모의 침투 연구회(www.facebook.com/groups/metasploits)**와 **사이버 안보 연구회(www.facebook.com/groups/koreancyberwar)** 등을 개설해 활동 중이다.

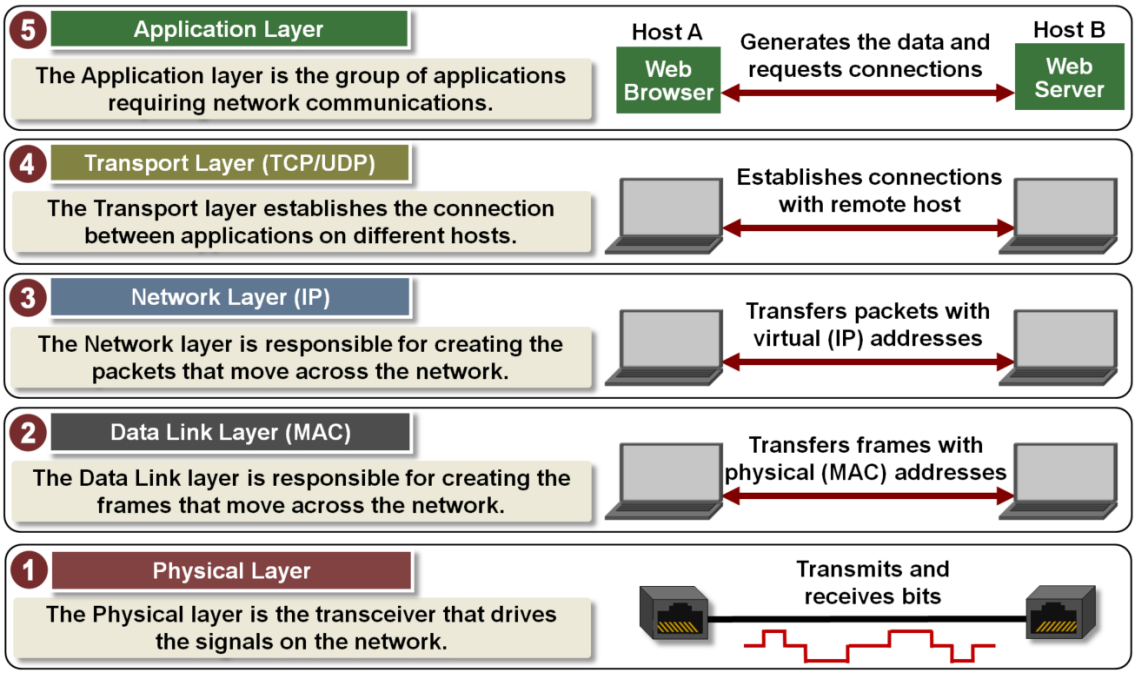
2015년부터 2019년까지 **에이콘 출판사**를 통한 저서로는 **<<해킹 입문자를 위한 TCP/IP 이론과 보안>>• <<칼리 리눅스 입문자를 위한 메타스플로잇 중심의 모의 침투>>• <<백박스 리눅스를 활용한 모의 침투>>• <<해커의 언어 파이썬 3 입문>>• <<소켓 개발 입문자를 위한 백박스 기반의 파이썬 2.7>>** 등이 있고, 공저로는 **<<데비안 리눅스 활용과 보안>>• <<우분투 리눅스 기반의 IDS/IPS 설치와 운영>>• <<모의 침투 입문자를 위한 파이썬 3 활용>>** 등이 있다.

雖不足藏之名山 庶無使墁之醬瓿[비록 명산에 비장할 바는 아니오나 간장 항아리 덮개로는 사용하지 말아 주시옵소서.]

김부식(金富軾)의 <<삼국사기(三國史記)>> 서문 편에서

제1장 TCP/IP 방식의 동작

편지지	편지 봉투



1. 응용 계층

UDP 페이로드

메시지(message) 생성

2. 전송 계층

UDP 페이로드	UDP 헤더

데이터그램(datagram) 또는 세그먼트(segment) 생성

3. 네트워크 계층

UDP 페이로드	UDP 헤더	IP 헤더

패킷(packet) 생성

4. 데이터 링크 계층

UDP 페이로드	UDP 헤더	IP 헤더	이더넷 헤더

프레임(frame) 생성

5. 물리 계층

비트(bit) 생성

제2장 보안 알고리즘의 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

3) 터널

암호문이 통과하는 구간

(2) 암호화• 복호화• 열쇠

1) 암호화

평문을 암호문으로 처리하며 송신자가 주체

2) 복호화

암호문을 평문으로 처리하며 수신자가 주체

3) 열쇠

암호화• 복호화를 위한 해독문

(3) 대칭• 비대칭• 하이브리드 구조

1) 대칭 구조

암호화• 복호화 시 사용하는 열쇠가 동일한 경우

2) 비대칭 구조

암호화• 복호화 시 사용하는 열쇠가 상이한 경우

3) 하이브리드 구조

대칭• 비대칭 구조를 혼용한 방식으로 SSH• SSL 등에서 사용

(4) 선형과 비선형

1) 선형

단일한 입력으로 단일한 출력

2) 비선형

단일한 입력으로 다양한 출력

2. 암호문의 종류

(1) 전치(Transposition) 방식

행렬과 역행렬의 관계처럼 철자의 위치를 재배치하는 방식

(2) 치환(Substitution) 방식

특정 문자를 다른 문자로 대치하는 방식

(3) 스테가노그래피 방식

1) 정보 내용의 존재 자체를 은폐하는 방식으로 일종의 트로이 목마 기법

2) 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 블럭마다 확산을 위한 전치 방식• 혼돈을 위한 치환 방식을 동시에 적용해 16회 등과 같이 반복적으로 암호화

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

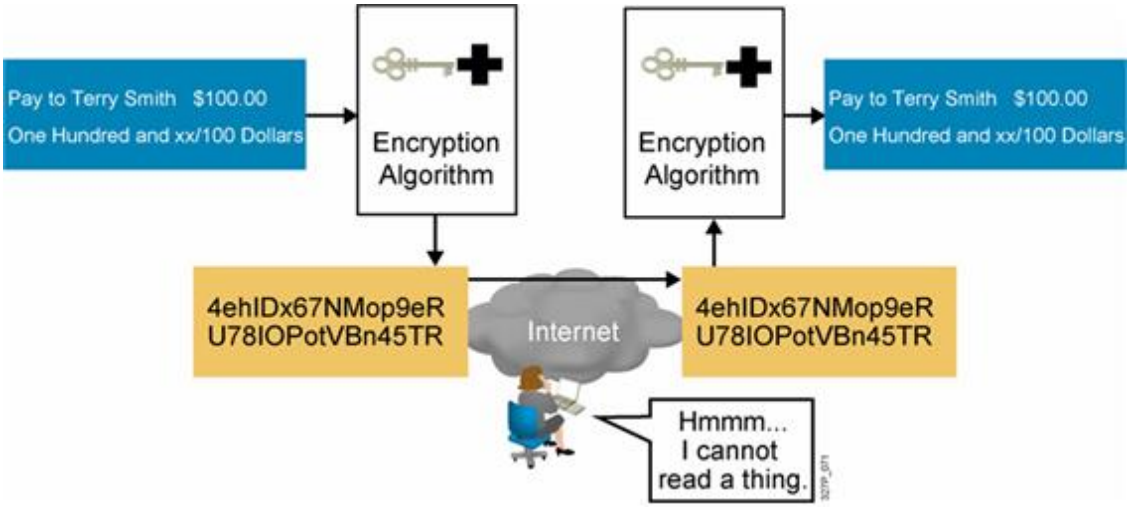
4. 사이버 보안의 구성 요소

가상 공간에서는 송신자와 수신자의 대면이 없다는 가정이 필요

(1) 기밀성(Confidentiality)

1) 쌍방간에 주고받는 실제 정보의 비밀성을 보장하는 개념

2) 각종 VPN 기법 등을 통해 기밀성을 구현



(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) 요약 함수 또는 전자 서명 등을 통해 무결성을 구현

(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 구현

(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 구현

(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 구현

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

제3-1장 대칭적 기밀성 알고리즘

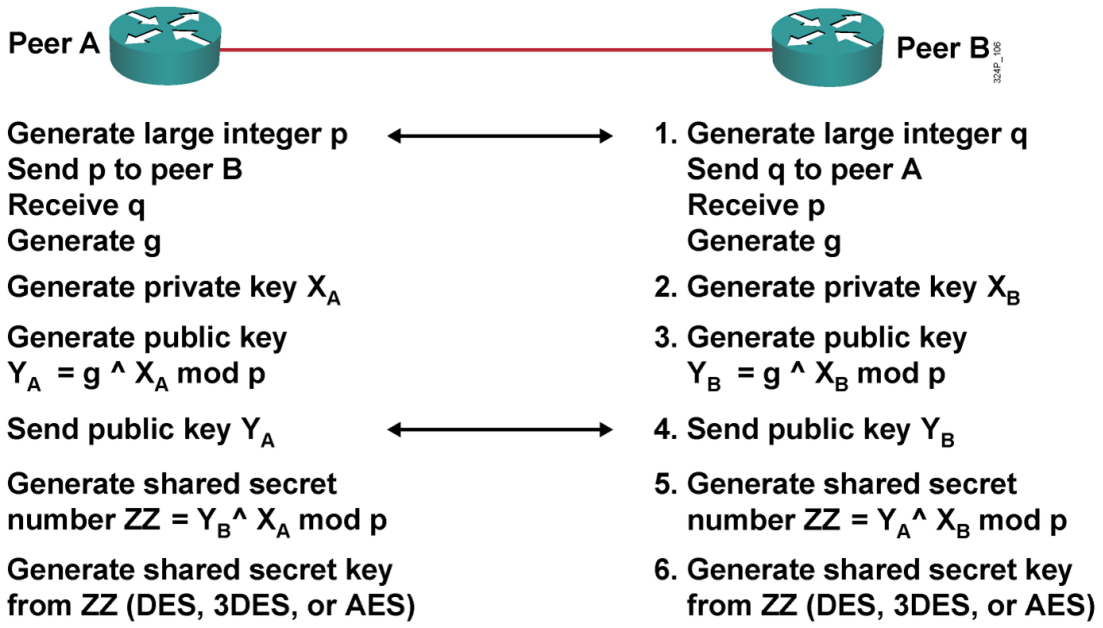
1. 대칭 구조 방식에 기반한 기밀성 알고리즘의 이해

(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) 파이스텔 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) 파이스텔 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) 파이스텔 구조와 SPN 구조의 중간 방식이고, 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

(7) 기타

RC2• RC5• RC6• Blowfish• Twofish• SEAL• HIGHT• LEA• Crypton• FEAL• MISTY 등

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

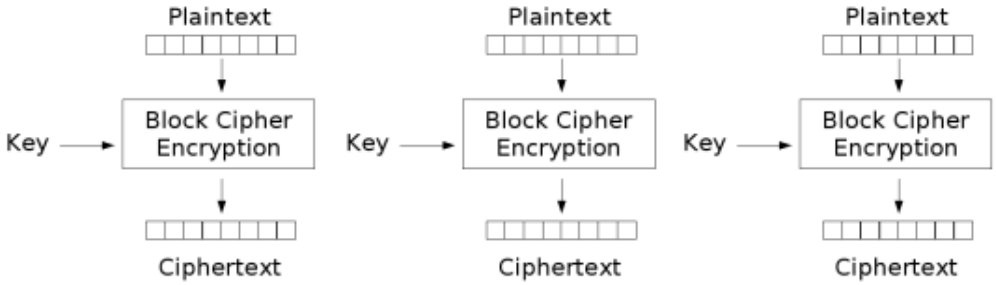
(3) 전수 공격

일종의 암호문 단독 공격

제3-2장 대칭 구조 방식에서 블록 암호의 운영 모드

1. 운영 모드의 종류

(1) ECB 모드



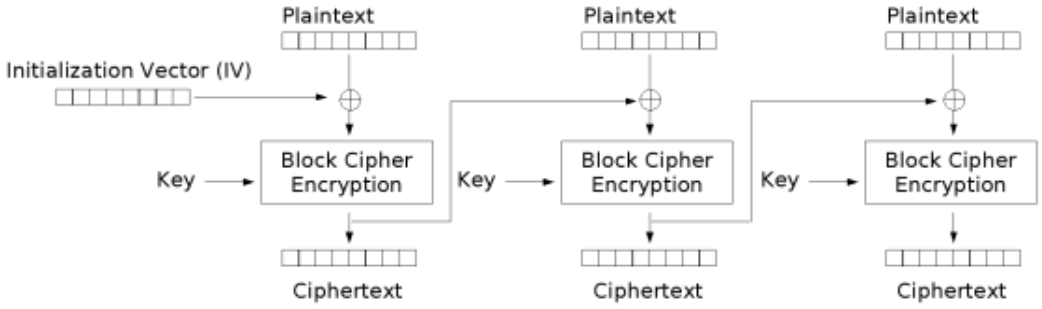
Electronic Codebook (ECB) mode encryption

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



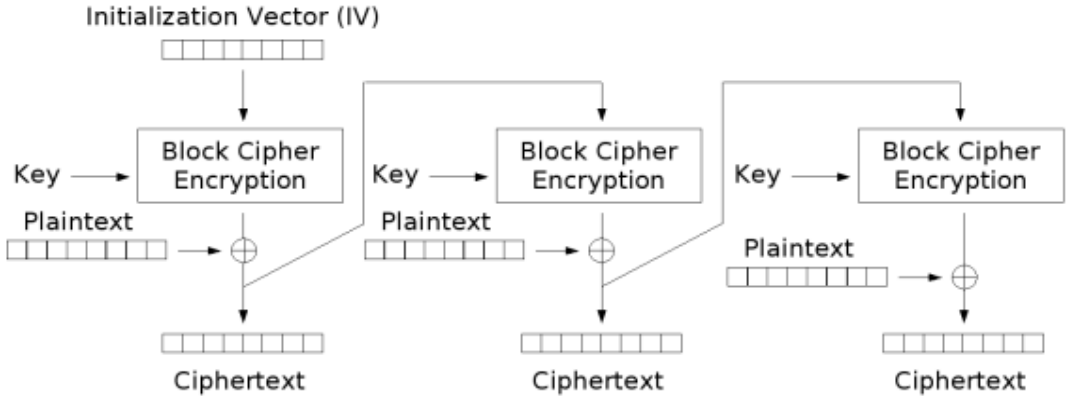
Cipher Block Chaining (CBC) mode encryption

1) 초기 벡터는 송신자와 수신자 사이에 미리 공유

2) SSH VPN 방식과 커버로스 방식 등에서 사용

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

(3) CFB 모드

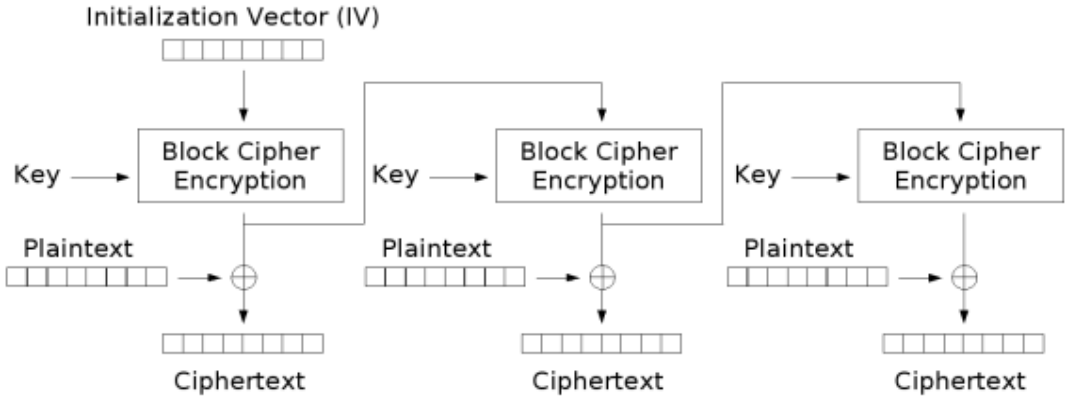


Cipher Feedback (CFB) mode encryption

1) 스트림 암호 방식과 호환

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

(4) OFB 모드



Output Feedback (OFB) mode encryption

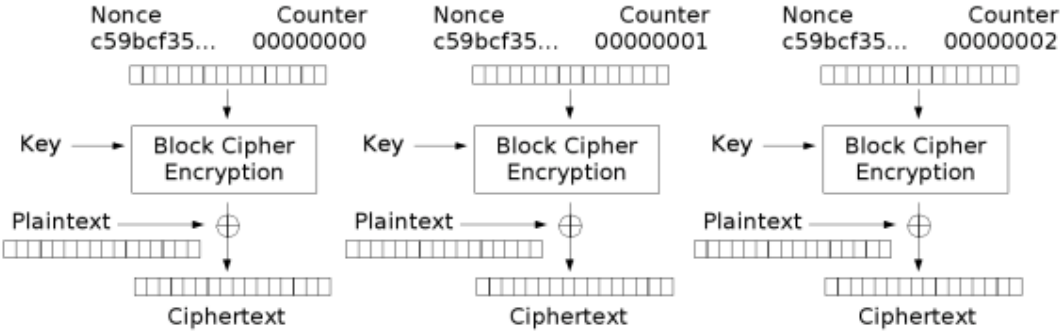
1) 스트림 암호 방식과 호환

2) 오류 전파 속성을 완전히 제거

(5) CTR 모드

1) 스트림 암호 방식과 호환

2) 64 비트 블록마다 카운터를 가진 난수를 생성



Counter (CTR) mode encryption

3) 오류 전파 속성을 완전히 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

1) X.509 형식의 공인 인증서 등을 저장하는 일종의 데이터베이스 서버

2) X.500 방식과 이를 간략화한 LDAP 방식 등을 사용

3. 공인 인증서 발급 시 구성 내용

전자 서명법 제15조에서 규정

(1) 가입자의 이름(법인의 경우에는 명칭을 말한다)

(2) 가입자의 전자 서명 검증 정보

(3) 가입자와 공인 인증 기관이 이용하는 전자 서명 방식

(4) 공인 인증서의 일련 번호

(5) 공인 인증서의 유효 기간

(6) 공인 인증 기관의 명칭 등 공인 인증 기관임을 확인할 수 있는 정보

(7) 공인 인증서의 이용 범위 또는 용도를 제한하는 경우 이에 관한 사항

(8) 가입자가 제3자를 위한 대리권 등을 갖는 경우 또는 직업상 자격 등의 표시를 요청한 경우 이에 관한 사항

(9) 공인 인증서임을 나타내는 표시

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

제5장 하이브리드 방식에 기반한 기밀성 알고리즘

1. SSH VPN 경우

(1) 인증 정보는 비대칭 구조 방식으로 암호화

(2) 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 개념을 적용

(2) 클라이언트의 비밀 열쇠를 서버의 공개 열쇠를 이용해 암호화

제6장 무결성 구현을 위한 전자 서명

1. 전자 서명의 개념

(1) 비대칭 구조 방식에서만 사용 가능

(2) 송신자는 자신이 서명한 부분(무결성 영역)을 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

제7장 무결성 구현을 위한 요약 함수

1. 요약 함수의 개념

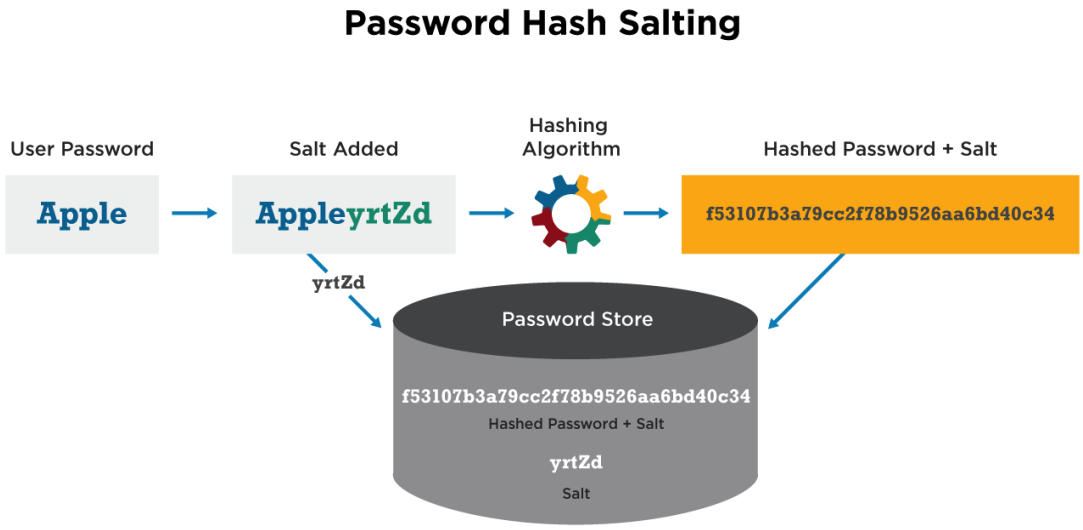
(1) 대칭• 비대칭 구조 방식에서 무결성 구현

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

(3) 요약본을 다시 원본으로 복원할 수 없는 일방향성(역상 저항성)

(4) 충돌 저항성

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




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

root:$6$hIhzqnvs$...:17164:0:99999:7:::
```

(5) 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

```
조작이 없는 경우

root@kali:/tmp# sha256sum /tmp/putty.exe
```

```
abcc2a2d828b1624459cf8c4d2ccdfdcde62c8d1ab51e438db200ab3c5c8cd17
/tmp/putty.exe

root@kali:/tmp# sha256sum /tmp/putty.exe
abcc2a2d828b1624459cf8c4d2ccdfdcde62c8d1ab51e438db200ab3c5c8cd17
/tmp/putty.exe

조작이 있는 경우

root@kali:/tmp# sha256sum /tmp/putty.exe
abcc2a2d828b1624459cf8c4d2ccdfdcde62c8d1ab51e438db200ab3c5c8cd17
/tmp/putty.exe

root@kali:/tmp# sha256sum /tmp/putty.exe
2754e79645d4a26829a25ebf3c2fcc9c8de37f609f11a3e26a6690b2865e8b58
/tmp/putty.exe
```

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

3. 윈도우즈 운영 체제에 기반한 요약 함수의 종류

LM• NTLM• NTLM2

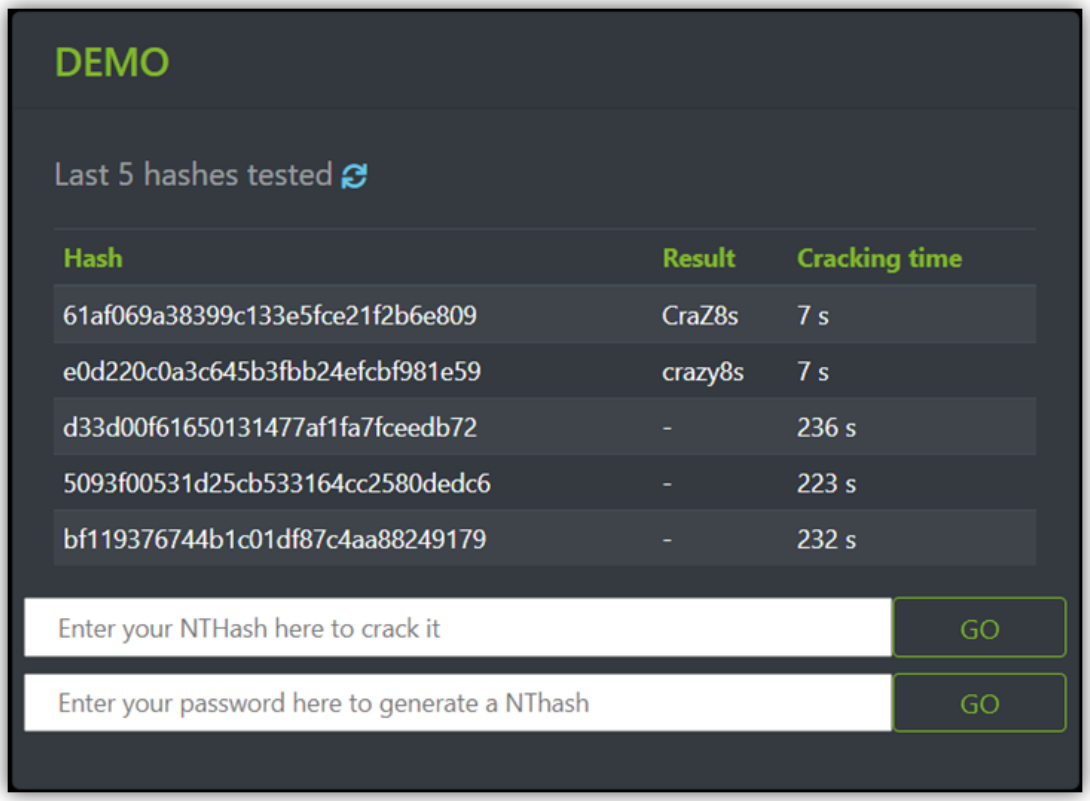
```
C:₩Windows₩System32₩config₩SAM
```

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

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

(2) 부인 방지 기능은 불가능

5. 위협 요소



(1) 레인보우 테이블(Rainbow Table)은 요약 함수를 사용해 변환 가능한 모든 요약본을 저장한 일종의 데이터베이스

(2) 레인보우 테이블을 통해 요약본에서 원본을 검색

```
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
```

제8장 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

제9장 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

제10장 사용자 인증의 종류

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

제11장 통합 인증 체계(SSO) 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 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

제12장 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. WPA3 방식

(1) 기밀성

AES 방식에 기반한 GCMP-256 알고리즘을 사용

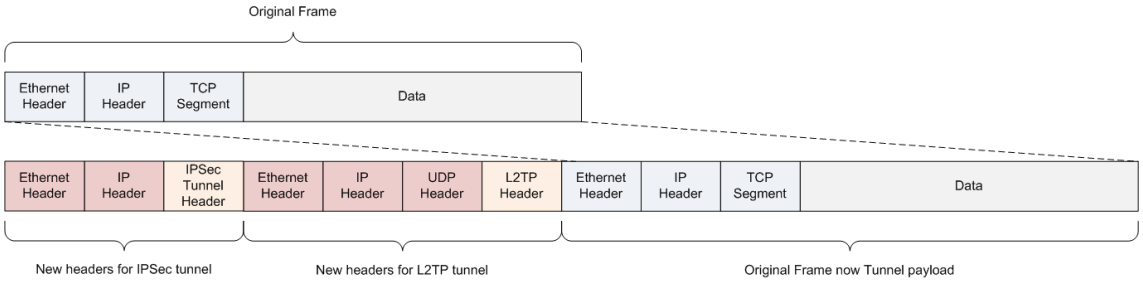
(2) 무결성

MIC 방식 기반

(3) 인증

SAE 방식

제13장 VPN 계층별 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

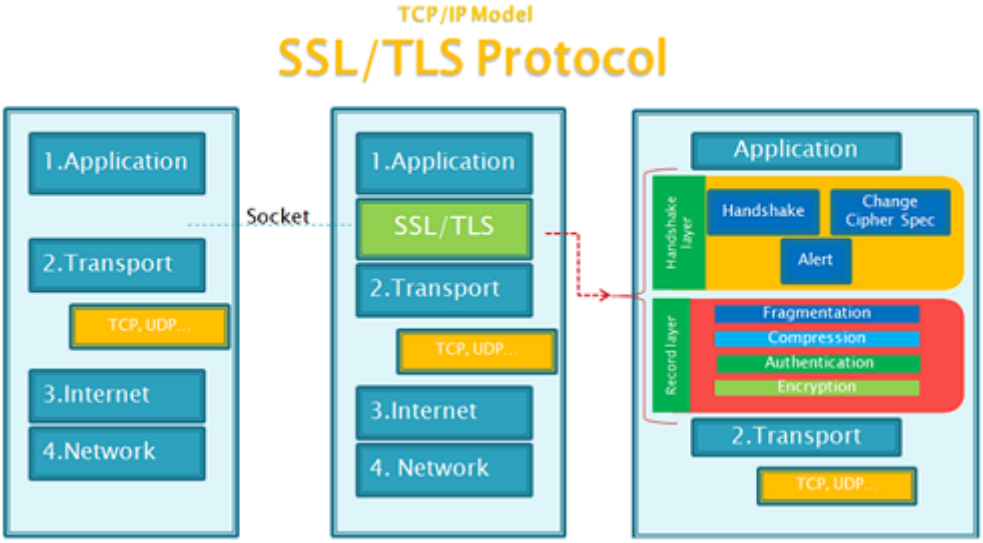
IPSec VPN 방식

4. 데이터 링크 계층 기반의 VPN

L2F VPN(시스코)• PPTP VPN(마이크로소프트)• L2TP VPN(시스코와 마이크로소프트) 등

제14장 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

단편화 > 압축화 > 해쉬 첨부 > 암호화 > SSL 레코드 헤더 추가

2. 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 공개 열쇠를 클라이언트에게 전송

(3) 클라이언트 인증 단계

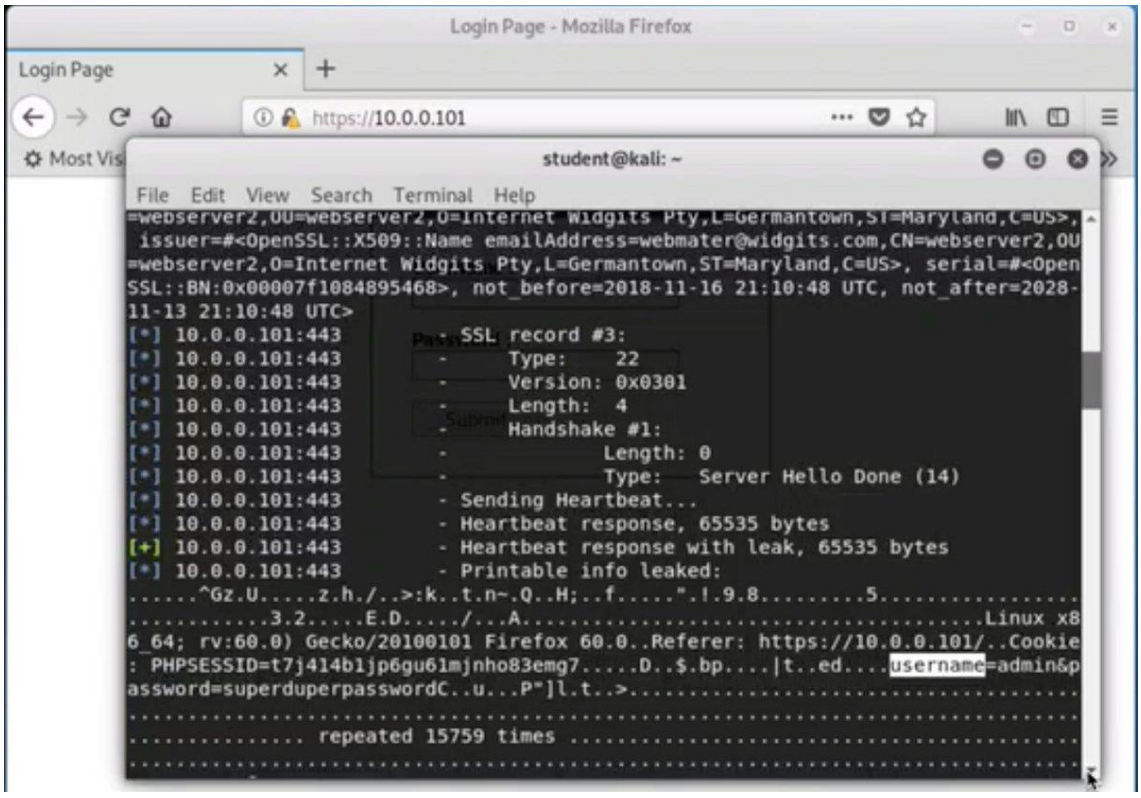
핸드쉐이크 프로토콜에서 생성한 임시 비밀 열쇠를 공인 인증서에 담긴 공개 열쇠로 암호화해 전송하고, 암호 변경 사양 프로토콜에서 다음 단계에서 사용할 일련의 보안 매개 변수를 서버에게 전송

(4) 종료 단계

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

3. SSL/TLS 방식의 취약점

(1) OpenSSL 하트블리드(HeartBleed) 공격

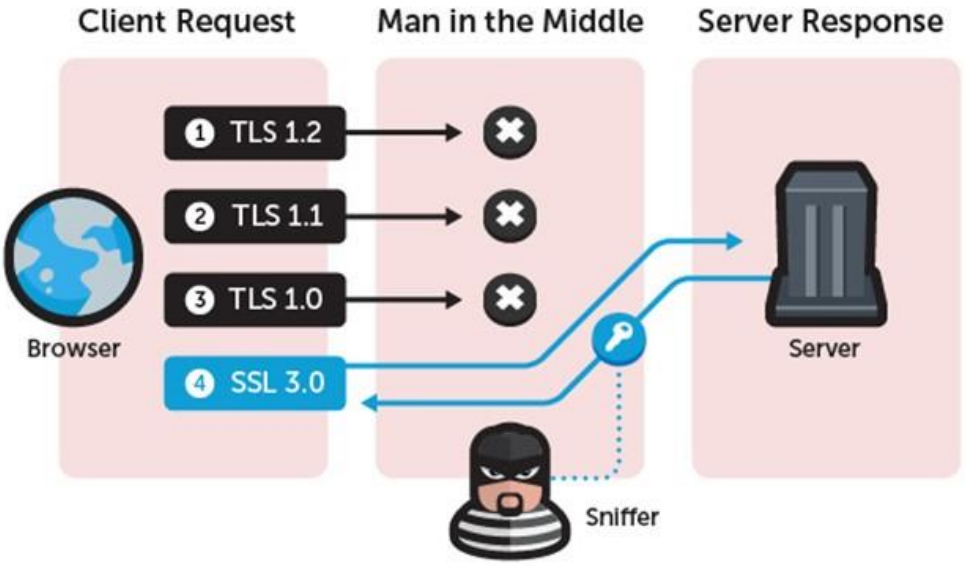


1) 2014년 OpenSSL 1.0.1-1.0.1f 버전과 1.0.2-beta 버전 등에서 발견한 일종의 버퍼 오버플로우 기법으로서 인증 정보가 노출되는 취약점

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

(2) SSLv3 POODLE 공격

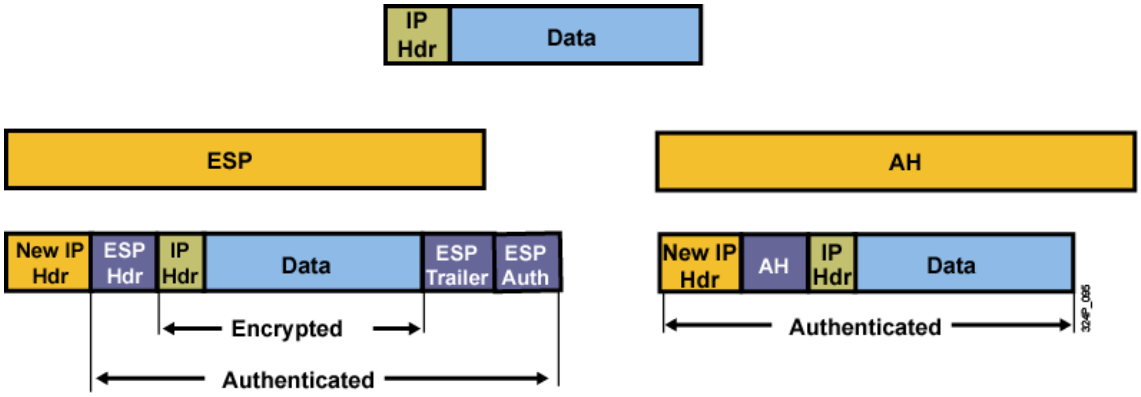
1) 구형인 SSLv3 방식은 CBC 모드로 동작하기 때문에 웹 브라우저에서 SSLv3 방식을 사용하는 공격 대상자를 대상으로 ARP 스푸핑 공격을 가한 뒤 공격 대상자와 서버 사이에 SSLv3 방식으로 강제 연결되도록 유도



2) SSLv3 방식의 동작 중지

제15장 IPSec VPN 구성과 동작

1. IPSec 방식의 종류[터널 모드의 경우]



(1) AH 방식은 무결성• 인증 기능만을 지원

(2) ESP 방식은 무결성• 인증 기능은 물론, 기밀성을 선택적으로 지원

2. ESP 방식에 기반한 보안 협상 절차

IKEv1

20	54.472115	10.0.0.1	10.0.0.9	ISAKMP	186 Identity Protection (Main Mode)
21	54.652126	10.0.0.9	10.0.0.1	ISAKMP	146 Identity Protection (Main Mode)
22	54.762132	10.0.0.1	10.0.0.9	ISAKMP	410 Identity Protection (Main Mode)
23	54.923141	10.0.0.9	10.0.0.1	ISAKMP	410 Identity Protection (Main Mode)
24	55.056149	10.0.0.1	10.0.0.9	ISAKMP	146 Identity Protection (Main Mode)
25	55.177156	10.0.0.9	10.0.0.1	ISAKMP	114 Identity Protection (Main Mode)
26	55.247160	10.0.0.1	10.0.0.9	ISAKMP	210 Quick Mode
27	55.357166	10.0.0.9	10.0.0.1	ISAKMP	210 Quick Mode
28	55.437171	10.0.0.1	10.0.0.9	ISAKMP	106 Quick Mode

IKEv2 single CHILD_SA - any to any

36	127.973143	10.0.0.1	10.0.0.2	ISAKMP	634 IKE_SA_INIT MID=00 Initiator Request
37	128.530653	10.0.0.2	10.0.0.1	ISAKMP	634 IKE_SA_INIT MID=00 Responder Response
38	129.044279	10.0.0.1	10.0.0.2	ISAKMP	370 IKE_AUTH MID=01 Initiator Request
39	129.197867	10.0.0.2	10.0.0.1	ISAKMP	338 IKE_AUTH MID=01 Responder Response

IKEv2 multiple CHILD_SAs

6	20.853572	10.0.0.1	10.0.0.2	ISAKMP	634 IKE_SA_INIT MID=00 Initiator Request
8	21.433008	10.0.0.2	10.0.0.1	ISAKMP	634 IKE_SA_INIT MID=00 Responder Response
11	22.006451	10.0.0.1	10.0.0.2	ISAKMP	370 IKE_AUTH MID=01 Initiator Request
12	22.156825	10.0.0.2	10.0.0.1	ISAKMP	338 IKE_AUTH MID=01 Responder Response
28	58.769138	10.0.0.2	10.0.0.1	ISAKMP	674 CREATE_CHILD_SA MID=00 Responder Request
29	59.310712	10.0.0.1	10.0.0.2	ISAKMP	642 CREATE_CHILD_SA MID=00 Initiator Response

(1) IKE 1단계 절차

1) 6단계의 메인 모드로 동작하거나 3단계의 축약 모드로 동작

2) VPN 장비 상호간 인증 절차로서 선택적 기능(생략 시 no crypto isakmp enable 명령어 이용)

```
crypto isakmp policy 10 #(선택적) IKE 1단계 절차 설정
encryption des
```

```
group 2
hash md5
authentication pre-share
lifetime 60
exit
crypto isakmp key 4321 address 192.168.34.4 #메인 모드 설정
exit
crypto ipsec transform-set KNHI esp-3des esp-md5-hmac #(필수적) IKE 2단계 절차 설정
exit
```

```
crypto isakmp policy 10 #(선택적) IKE 1단계 절차 설정
encryption des
group 2
hash md5
authentication pre-share
lifetime 60
exit
crypto isakmp peer address 192.168.34.4 #축약 모드 설정
set aggressive-mode password 4321
set aggressive-mode client-endpoint ipv4-address 192.168.23.2
exit
crypto ipsec transform-set KNHI ah-md5-hmac #(필수적) IKE 2단계 절차 설정
exit
```

(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

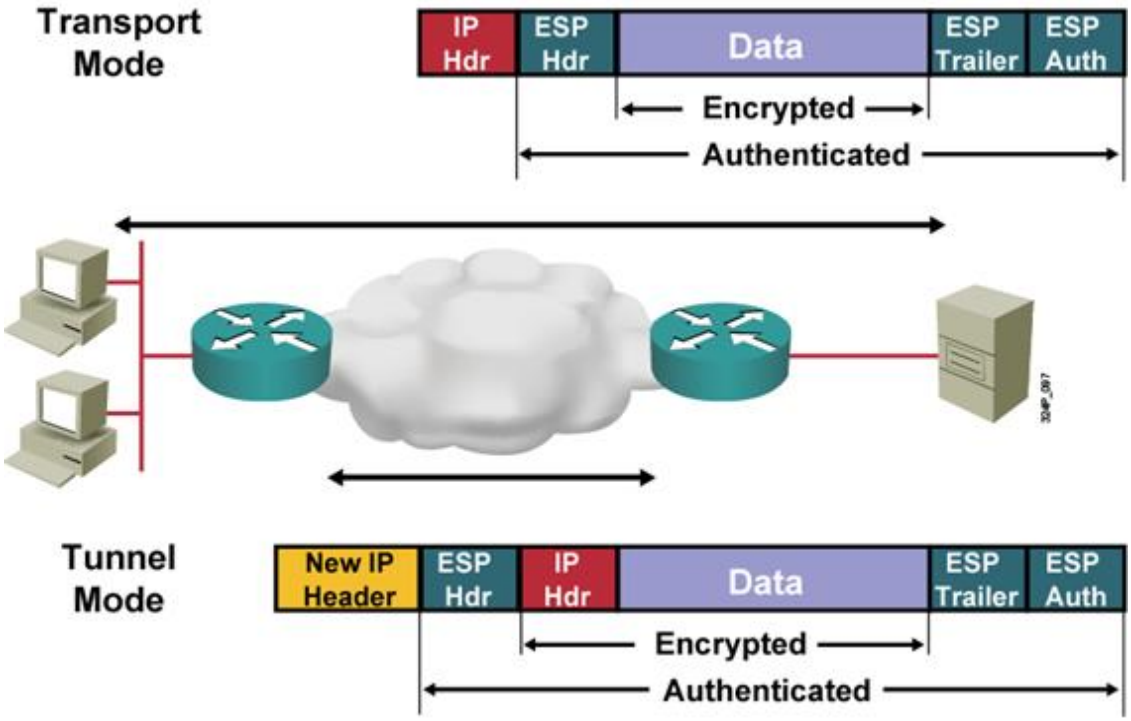
3) 사용자가 직접 IPSec VPN 작업을 수행

(2) 터널 모드

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

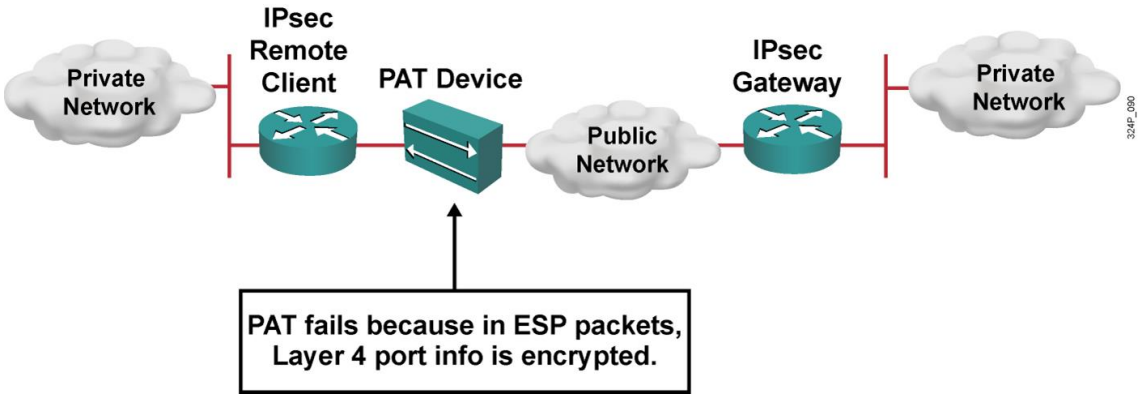
2) 사용자에게 IPSec VPN 투명성을 제공

3) 송신자• 수신자와 해당 장비 사이에서 평문으로 송신• 수신

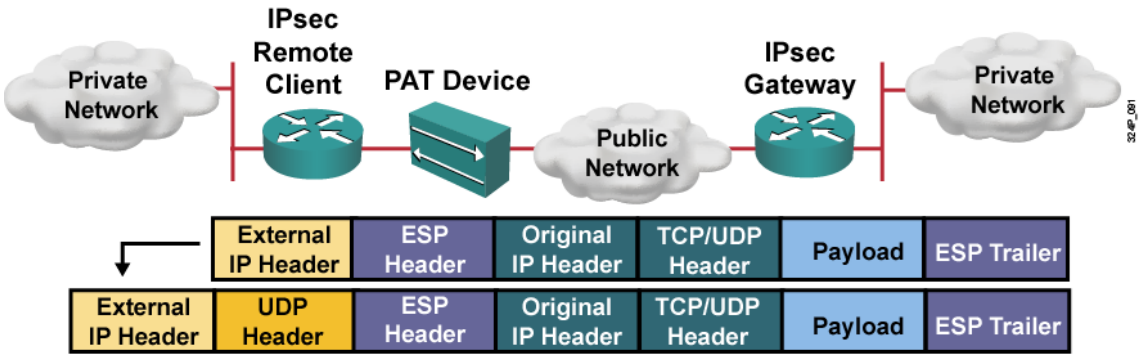


5. IPSec VPN 환경에서 PAT 방식의 처리 문제

(1) 문제점

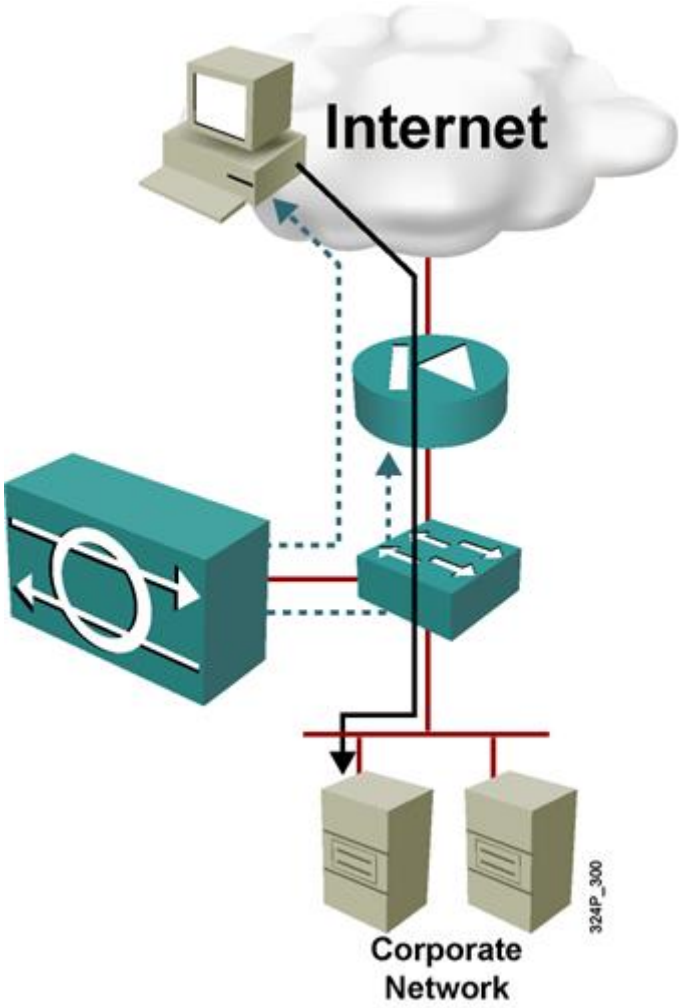


(2) 해결책


Private Network
IPsec Remote Client
PAT Device
Public Network
IPsec Gateway
Private Network
External IP Header
ESP Header
Original IP Header
TCP/UDP Header
Payload
ESP Trailer
External IP Header
UDP Header
ESP Header
Original IP Header
TCP/UDP Header
Payload
ESP Trailer

제16장 침입 탐지 장비의 이해

1. IDS의 기능



일정한 탐지 규칙에 기반해 모니터링 또는 미러링 방식에 따라 기존의 공격 유형을 탐지

2. IDS의 동작 순서

정보 수집 > 정보 가공• 축약 > 분석• 침입 탐지 단계 > 보고• 대응

3. IDS의 탐지 오류

(1) 오탐(False Positive)

정상적인 유형을 악의적인 유형으로 오판

(2) 미탐(False Negative)

악의적인 유형을 정상적인 유형으로 오판

4. IDS의 탐지 방법

(1) 오용 탐지

1) 지식 기반 탐지• 패턴 기반 탐지• 서명 기반 탐지라고도 함

2) 전문가 시스템(Expert System)을 이용하고 침입 유형 등을 사전에 등록해 탐지

3) 미탐 비율이 높은 편

(2) 이상 탐지

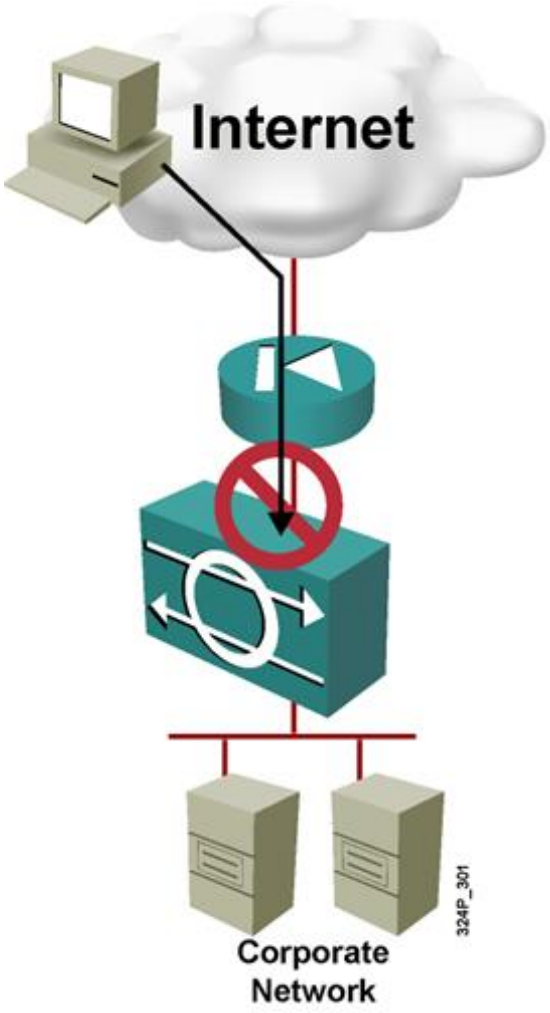
1) 행위 기반 탐지라고도 함

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

3) 오탐 비율이 높은 편

제17장 침입 방지 장비의 이해

1. IPS의 기능



IDS가 탐지하면 게이트웨이 방식 또는 인라인 방식에 따라 침입을 방지

2. IDS/IPS의 종류

(1) 네트워크 기반의 IDS/IPS

1) LAN 영역 전체를 탐지하는데 유리

2) 자신에게 향하는 패킷이나 암호화 패킷 등은 탐지 곤란

(2) 호스트 기반의 IDS/IPS

1) 내부 공격을 탐지하는데 유리

2) 호스트 단위만 탐지

제18장 침입 차단 장치(방화벽)의 이해

1. 방화벽의 기능

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

(2) 일반적으로 침입 차단 장치• 침입 탐지 장치• 침입 방지 장치 순서대로 배열[상황에 따라 다양하게 배열 가능]

2. 방화벽의 접근 제어 기법

(1) ACL 방식

TCP/IP 네트워크 계층• 전송 계층에 기반해 필터링 기능을 수행

(2) ALG 방식

프록시 방화벽이라고도 부르며, TCP/IP 응용 계층에 기반해 필터링 기능을 수행하기 때문에 웹 방화벽(Web Application Firewall)처럼 특정 응용 계층의 프로토콜만을 지원해 과부하 해소

(3) 상태 추적(SPF) 방식

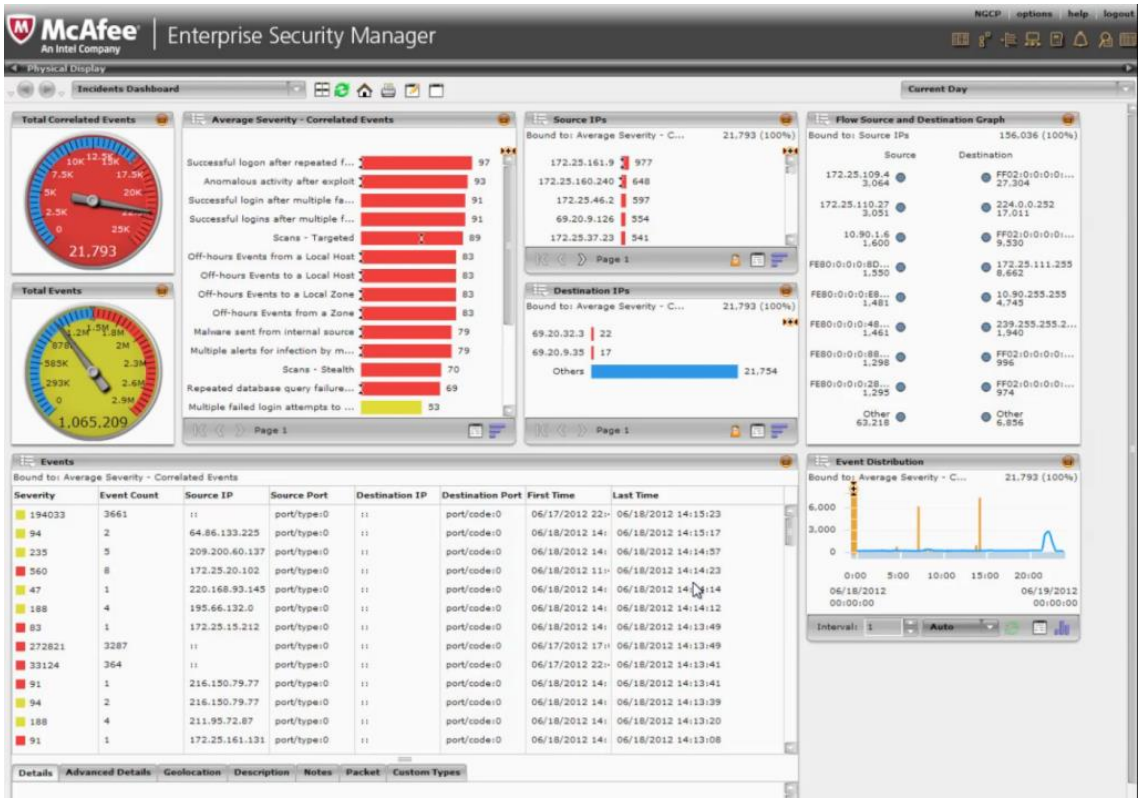
1) 상태 추적 테이블을 통해 리턴 패킷 여부를 검사

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

제19장 기타 보안 장비

1. UTM(Unified Threat Management)

2. ESM(Enterprise Security Management)



보안 장비들에서 발생하는 각종 이벤트를 취합한 뒤 상호 연관 분석해 다양한 실시간 보안 위협을 파악하고 대응하는 시스템

(1) 에이전트 포트

각종 보안 장비에서 수집한 정보를 매니저 포트로 전송

(2) 매니저 포트

에이전트 포트를 통제하면서 수집한 정보를 분석하고 저장한 뒤 콘솔 포트로 전송

(3) 콘솔 포트

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