컴망 12주차 1차시

암호학 to network

Encryption 방법 :

Symmetric , public

Sym 🡺 shared key 가 필요, 여기서 문제점, sharing .키를 어떻게 만드냐?

음 그 message 주는 방법 중간에 도청 피하는 거

Rsa 구하는거 , DES 쓰는법

진짜 CA 를 못믿겠다 == > block chain 이 나온거임.

Email 을 안전하게 보내는 용도로 사용하기

Email 은 길다 == symmetric 방법

Symm 키 생성

밥의 public 키를 가지고 symm 키를 암호화

Secure email 그림 잘보기

Mail 은 confidential 하게 날아갈 수 있음.

하지만 alice 가 보낸게 맞냐는 확인 하지 못함

Authentication 추가해야됨

* Message 를 hashfunc 을 통해 digest 한 내용을 encryption 해서 alice private 키를 통해 암호화 시켜서 같이 보냄.
* 이렇게 만든 전체적인 메시지를 아까의 작업을 통해 암호화 다시 시키는거임 .

이제 받은 메시지(추가적으로 밥이 해슁 해야됨) 와 alice public 으로 연 메시지 비교

수신측의 입장을 정확히 이해 해야 한다 아마 문제 나올 듯

Secure socket Layer

Transport Layer 와 application Layer 사이에 SSL 이 들어감.

생각해보니까 옛날에 TCP 쪽으로 빠지는거랑 검사 쪽으로 빠지는거 두개 얘기했던거같은데.

API 개념

모든 웹서버 브라우저들에서 지원한다.

TLS ( 법률쪽에서 정한 Security ) == SSL (현실에서 쓰는거) 비슷하다고 보면됨.

3가지 기능 제공

Hand shake 함 .

* Alice 와 밥이 Certificates, private key 사용 🡺 서로 확인.

Key 를 만듬

* Encryption 을 위한 key 와 authentification 을 위한 키를 만듬.
* Message encryption, 출처 확인 (Message authen code) 부착

Data 전송

연결 끊음.

4가지 키를 만듬. ( 방향성을 가지고 있기 때문에 2개 2개 )

4등분해서 key 내용 전달 (MS)

데이터 전체를 대상으로 한번에 encrypt 하는게 아니라 적당하게 끊어서 format 갖춰서 던지.

Record 단위로.

Trudy 가 SSL 에서 할 수 있는 나쁜 짓

23:41초

내용을 캡쳐해서

Replay, reorder 할 수 있음

* MAC 를 계산 할 때 Sequence 번호를 MAC 에 포함 해서 넣기

강제로 TCP 연결을 끊을 수 있음. .

그래서 또 MAC 에 종료 신호(type) 을 넣어서 끊기.1, 도착하고 종료 신호가 와야 됨 .

IP packet 자체를 안전하게 보낸다면? Transport 에서 고민할 필요 없이 전체 가능.

IP 가 blacket coverage ( 모든 것을 커버 하는 것) 이 아니냐

.VPN 서비스를 통해서 보안 제공 .security

VLAN : 하나의 Lan segement 에 있는거 처럼 (Data Link)

VPN 하나의 network 에 있는 것 처럼.

* 하나의 Network 안에 있으면 안전하게 통신 할 수 있음 ( 이건 NETWORK LAYER )

안에 있는거 처럼 보내는 거임. 밖으로 보내야 된다면 ip sec 을 사용한다.

Ip sec == vpn에서 쓰는건가?

IP header, ip sec(secure) head, encrypt data 을 통해

Rsa 같은 규칙이 있다.

AH(암호화는 안시킴, 대신 보낸사람이랑, 변조된지는 확인), ESP (이건 다확인)

Host 가 ipsec 단말 to 단말 host mode

Router 만 가지는 것 tunnel mode

Security association 을 위해 SA Identifier 을 저장

저장되어 있는 DB를 가지고, encrypt type , key ~ 등을 다 알 수 있음 서로의 router 에 저장 되어있기때문, Security parameter index 기준으로 디비를 뒤진다. 이게 SAD 인가?

Head quarter , branch office 그 router server 인가 router 가 연결을 지원해야된다던데..

Router 에는 security asso~ Database 가 있다 .

다양한 곳의 service 를 지원하기 위해

이 데이터그램을 가지고 ,SA 를 적용해야하는지 그냥보내야하는지 결정

* Security Policy
* What to do
* How 는 SAD 에 들어가 있음.

SAD 가 MANUAL 로 등록되서 자동으로 SA 와 Key 정책을 적용할 수 있다면 좋겠지만,

Key..?

어쨋건, handshake 해서 key validation 하는것

무선네트워크

Wep

Wired equivalence protocol

유선 따라잡기.

하나의 key 사용하는게 아니라 key를 변화.

Key stream 을 사용해서 데이터를 변화 ~~ 죽 넘어가서

방화벽 하기 .

Fire wall 에 대해서 수업.

안쪽 네트워크를 보호하자.

외부로부터의 침입을 막아보자.

내부에서 외부로 나가는 것도 차단 할 수 있음.

Prevent DOS 를 하기 위해.

SYN Flooding 같은 공격. Bogus: 가짜, 접속을 통한 공격

Tcp header 에 syn bid 가 있었음. Syn 열면 tcp connection 열자 , handshaking 시작.

Connection 여는데 힘을 다 써버리는 거지.

Resource 다 써서 의 본연의 임무 x

DDOs 는 ?

한 쪽에서만 요청하는게 아니라 여러 좀비 컴으로 공격.

-내부 데이터에 대한 불법 접근 막고

-Authorized access 만 들어 올 수 있도록

3가지 방화벽.

지나가는거 다 뜯어 봄

Allow 된 데이터만 ok 하고 나머지 다 걸러냄. (state 고려)

Application gateways