Notes

01/23/2023

nat nat network bridge adapater

wireshark:

```
select any adapter
spur traffic to capture packets
```

ip addr: look up ipaddress

02/06/23

review fiestiel model

how many bits in a block of block encryption des

symmetric encryption: work with the same key.

every entity needs to keep the symmetric key safe.

symmetric encryption is not good for rauthentication

man in the middle attack

block traffic

professor and student connection is being intercepted

prof/student enc/dec eachothers messages

02/15/23

next week thursday class is not held

instead use lockdown browser to do test

sign and encrypt

```
sign: encrypt with private key dec with public key
encrypt the message to ensure confidentiality
sign the encrypted text to provide authentication
```

key exchange vulnerabilite:

1. man in the middle attack

mim: active attack

```
blocking comms from a to b
intercept from a to b
```

authentication:

```
you hold private key
others confirm with public key

so, encrypt with private / decrypt with public key
```

store private key

```
use symmetric encryption to store it
password managers: will need acces to private key
    at that time, it will decrypt it to gain access
```

passwords about authentication

hydra specifically designed attack authentication

```
defeating and by-passing authentication

username password relation is authentication
```

private public key pair can be used for authentication

MFA:

```
something you know
something you are
something you have
something you do
```

A and B:

```
symmetric encryption
```

Kerberos:

```
key exhange that uses a centralized trusted server to provide encrypted
connections for key exchange

relies on symmetric encryption
```

02/27/23

network access control (auth, access control)

control to access to resources based on a policy for authenticated user

- authenticating another user
- what are they allowed todo
- enforcement mechanism (access control)

authentication: verify genuine user (private key encryption public key decryption, signing, no ideal way).

mitm against key exchange: biggest problem for encryption (authentication)

Health of a system: how secure is the network

not just authenticating users, policy enforcement

```
some systems are inherently less secure (more compromised) than others
```

DHCP: dynamic host config protocol

```
grants ip addresses
```

vlan server: divide enterprise network into logical segments

EAP: framework for authentication

```
extensible authentication protocol: plug/unplug different modules
```

PSK: Pre shared key: symmetric encryption

```
no key exchcange, before the key exchange problem

means username:password
```

IKE: Internet Key exchange

```
public keys sent over a network
```

authenticatio serves: radius servers, remote access dial in user services

```
good place to put EAP
```

802.1X along with EAP: provides access control

EAPOL:

```
how
```

cloud computing evironment

```
the internet: a server on the otherside of an unsecure connection
```

types of authentication does eap support

digital digests: md5

access control by its self is about authenticated users

last

03/01/2023

access control requires:

- authentication
- policy
- enforcement method/mechanism

firewalls are an enforcement mechanism

- application that blocks/allow/ filters network traffic

mac address trival to forge, therefore should not be used for authentication

03/06/23

automatic confidentiality:

- automatically encrypt packets before sending
- work for any application so app does not need to modify this network protocol
- transparent to end user

TLS: Transport Level Security

Please Review the TLS handshake. PLEASE PLEASE Review the TLS handshake

4 phases:

1. client hello, server hello

2. server sends

    1. vertificate
    2. server key exchange
    3. certificate request
    4. server hello done

3. user sends

    1. certificate
    2. client key exchange
    3. certificate verify

4. client sends

    1. change cipher spec
    2. finished

    server sends

Heartbeat protocol: part of TLS

keep connections open

checks if server and client can still communicate

```
what if send a couple bytes, but request more from server

should be: send max to what ever was sent
```

heartbleed: exploiting the heartbeat protocol and make it reveal something more than it should

dont really need to review ssh handshake, mostly TLS

03/08/23

secure copy:

```
cop files over untrusted entwork
gives confidentiality
```

consider all networks are untrusted

key exchange is always the big problem

why don't we just do all key transfers through ssh if its so good at encrypting packets and has key management built in?

```
in order to get the keys for ssh connection, key exchange problem
```

port numbers are universally preconfigured.

root account that does not have a password.

```
sudo allows us to run commands as root
```

goal of RSA:

```
public and private parts
public key is freely distributed without risk
```

possible some mitm attack

```
first key exhcange is the most dangerous one because keyexcahnges only happen once
at the start of a new connection
```

once public key is on remote the host, innoculated against mitm

TLS adds encrypt before decrypt after for applications that dont do that

```
http + SSL/TLS = https
```

ssh port forwarding: mechanism in ssh for tunneling application ports from the client to server or vice versa

- adds encryption to apps that dont

local forwarding: listens for redirects

opening backdoors

```
opens additional routes not designed by the router
```

Imagine a place and a time where the only true software existed on linux and unix systems

03/13/23 Tuesday

tls provides confidentiality

tls authentication?

```
authentication is really hard
```

ssh authentication

```
public keys and private keys
```

EAP: Extensive Authentication Protocol

```
framework for authentication
```

802.11i:

```
port based network access control
```

03/15/23 Thursday

802.1x and arp:

802.11i

```
wifi
provides all security service categories

provides asymmetric and symmetric encryption

gives security
```

prevent mitm attacks:

```
trusted third party sign keys
but how to get them the key?
    still and issue.
```

wired vs wireless

```
very similar
wired: closer proximity because you need to physically touch the wire
wireless: radio connection can be used at a farther distance
```

nmap:

```
GOAL: discover open ports and hosts connected to the network

open ports
but more importantly
what devices are on the network

it can do both wired and wireless
    it dosent matter the network connection
```

iptables:

```
help to prevent nmap scans
firewall rules
```

wireless networks

- encrypt all packets for hosts not authenticated on the network

  listen to the packets from a wireless network means that all them would be encrypted

- how to decrypt packets

  easy way: know the password for the wifi network

  to decrypt, simply login into the network

  if you dont kno it, then bruteforce it

wifi security

- none
- WEP
- WPA/WPA2

Kali and bridged mode is not the same since it does not communicate directly with the wifi card

```
try and find an usb wifi device with an external antenna
```

```
new wireless device to config it

now the vm has direct wireless access

for wireless scanning: need promiscious access to the device
```

03/20/23 Tuesday

authentication is hard. why?

```
proving who you are

mitm works at attacking authentication by spoofing.
```

DNS

maps domain names to ip addresses

authentication: how to ensure that ip address mapping is correct and not sending you to a bad version of it hosted somewhere else

dns cache poisoning

email

MIME without authentication

```
we want to add security : S/MIME
```

dns needs authentication : nightmare without

send some mail message

what parts that are added dns to make DNSSEC

03/22/23 Thursday

DNS is a third party service

DNS exploitation

```
take stolen data through firewalls
```

nslookup

ipchicken.com, then ssh in