Security

Security of a system is defined by:

- Desired properties
- An adversary with specific abilities ← "bad actors"

Threats & Attacks

Eavesdropping:
Interception of information

Alteration:
Unauthorized modification of Data.

Denial-of-service:
Interruption of data service.

Masquerading:
Impersonating data

Correlation/traceback:
Using multiple data sources to find more information about User.

The CIA

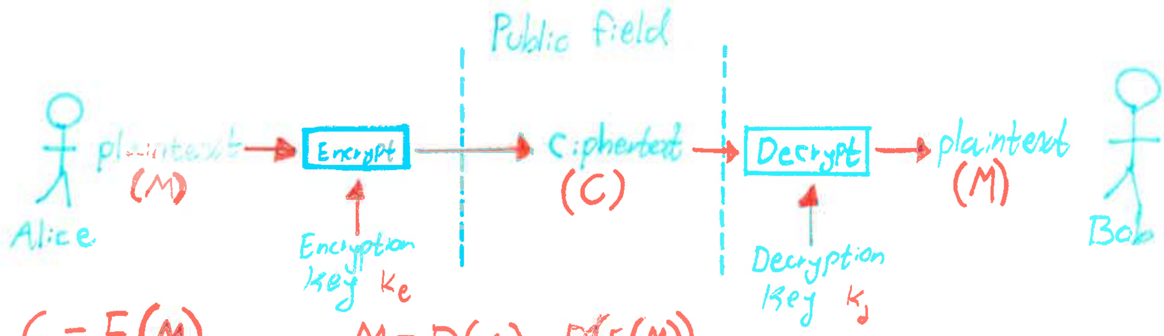
Confidentiallity:
Protection of data from those who may not see it, while giving it to those who may.
↳ cryptography, Access control, Authentication, Authorization, Physical security.
(Authentication → have, Know, is)

Integrity:
Data is valid, not corrupt/manipulated.
↳ Backups, checksums, Hamming codes

Availability:
Data can be accessed and modified by Authorized personel
↳ Physical protection, Redundancies

Cryptographic Concepts

Encryption established communication
Safe from eavesdroppers.



$C = E(M)$ ↳ Cypher

$M = D(C) = D(E(M))$ ↳ Decryption

If $k_e = k_d$ then the encryption is symetric, and the key is called a shared key. $\binom{n}{2}$ keys needed.

If k_e is private & k_d is public it is a public-key cryptography

Digital signatures can sign a message M that is public since. $(2n)$ only the person who can create a cypher C which decrypts to M with the public key k_d is Alice

Lecture 2

Caesar Cipher

Julius Caesar 100-44 BC

Each letter is shifted up by 3 letters A->D, B->E...

$$C_i = E(M_i) = (M_i + 3) \bmod 26$$

$$M_i = D(C_i) = (C_i - 3) \bmod 26$$

Types Of Attacks

Attackers have access to:

Collection of ciphers
↳ ciphertext only attack

Collection of cipher-plaintext pairs:
↳ Known plaintext attack

Chosen plaintext and its cipher:
↳ chosen plaintext attack

Chosen ciphertext and its plain:
↳ Chosen ciphertext attack

Vigenère Cipher

Uses a message & a key to scramble a text.

M = "Attackatdawn"

K = "Lemon"

M' = {0, 19, 19, 0, 2 ..... }

K' = {11, 4, 12, 14 ..... }

$C' = (K' + M') \bmod 26$

C = "LXFOPV ..... "

decrypt:

$M = (C' - K') \bmod 26$

Stream Cipher

Message is converted to a stream that is XOR with the LCG from a shared key.

S = S[0], S[1] ....

M = M[0], M[1] ....

$C[i] = M[i] \oplus S[i]$

Substitution Cipher

Each letter is uniquely substituted by another letter.

$26! \approx 4 \times 10^{26}$ possibilities.

A B C ....
⇕ ⇕ ⇕
N O P ....

Brute force

Try $D_k(C)$ for all keys k. If there are enough possible ks, Brute Force is unfeasable.

Frequency Analysis

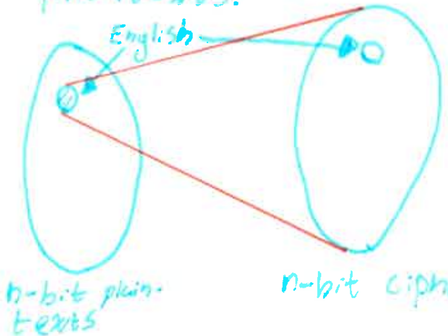
Since the appearance of letters in the english Alphabet is not uniform. Substitution ciphers can be easily cracked.

a - 8%, b - 1.7%, c - 2.2%, d - 5%, e - 12%, f - 2%, g - 2%, h - 6.6%, i - 6%

Works on doubles and tripplets.

Encrypting English

English makes up a small percentage of all plaintexts.



One-Time Pads

Type of substitution that is considered "unbreakable". Encrypts plaintext of len n by using n randomly generated keys.

Pseudo Random Number Generator: (PRNG)

Used to generate n keys. Of uniform distribution. Independent numbers, long periods.

Linear Congruental Generator:

$x_{i+1} = (a x_i + b) \bmod m \quad a \in [1, m-1] \quad b \in [0, m-1]$ if b = 0 then a can be 0

Generates periods of up to $\phi(m)$ when a is a primitive root

→ Order of a is p-1

→ $\phi(m) = m - 1$ if $m \in$ Primes

Order of a O(a) in $\mathbb{Z}_p$ is the minimum x such that

$a^x \bmod p = 1$

$x = O(a)$

if

$x = p - 1$

then

a is a primitive element in $\mathbb{Z}_p$

in general $O(a) \mid p-1$

Example:

$\mathbb{Z}_7$ p-1 divisors = 6, 3, 2

for all a < 7

$2^2 = 4$

$2^3 = 8 = 1$

$3^2 = 6$

$3^3 = 27 = 6$

$3^6 = 2^3 = 1$

$4^2 = 16 = 2$

$4^3 = 64 = 1$

$5^2 = 25 = 4$

$5^3 = 125 = 6$

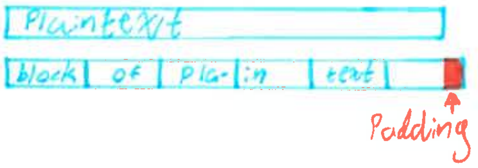
$5^6 = \dots = 1$

$6^2 = 36 = 1$

Lecture 3

Block Cipher

Plaintext is stored and converted into blocks to be encrypted

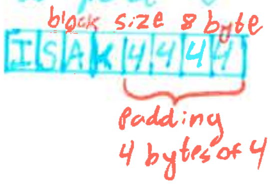


Padding

The padding cant be all zeros. (insecure)

PKCS5:

↳ Pad with sequence of number of bytes left to pad



If the message fills blocks completly witout padding. A final block is added with Just padding.

Hill Cipher

Lester Hill 1929

Block cipher n length

The key K is a $n \times n$ invertable matrix

Message is encoded as an n sized vector

Encryption:

$$C = K \cdot M \mod 26$$

Decryption

$$M = D \cdot C$$

Where $D = K^{-1} \mod 26$

To find D

1. $K \Rightarrow K^{-1}$
2. $d = \det(K)$
3. find $d^{-1} \mod 26$ (Not $\frac{1}{d}$ but d^{-1})
4. $\left(\underbrace{d \cdot d^{-1}}_{=1 \mod 26} \cdot K^{-1}\right) \mod 26$
5. Result from 4 is D

$$K = \begin{pmatrix} 1 & 0 & 11 \\ 11 & 16 & 24 \\ 7 & 17 & 1 \end{pmatrix} \quad K^{-1} = \frac{1}{443}\begin{pmatrix} -392 & 187 & 176 \\ 157 & -76 & 97 \\ 75 & -17 & 16 \end{pmatrix}$$

$d = 443 \qquad d^{-1} \mod 26 = 23$

$$d \cdot d^{-1} \cdot K^{-1} = \begin{pmatrix} -9016 & 4301 & -4048 \\ 3611 & -1748 & -2231 \\ 1725 & -391 & 368 \end{pmatrix} \mod 26$$

$$\Rightarrow D = \begin{pmatrix} 6 & 11 & 8 \\ 23 & 20 & 21 \\ 9 & 25 & 4 \end{pmatrix}$$

Transposition Cipher

Message is shuffeled according to a permutation (π) and decoded with (π^{-1})

$$C = \pi M$$

$$M = \pi^{-1} C$$

$M =$ CATANDHOUND

$\pi = (1,6,11,9,8)(4,7,5)$

$\Rightarrow C =$ OATNHCAUDND

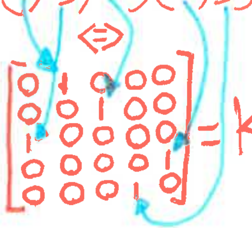
$\pi^{-1} = (1,8,9,11,6)(4,5,7)$

$\Rightarrow C \cdot \pi^{-1} = M$

Can also be encoded as a Hill Cipher

$(1,3,2)(4,5)$

⇕



$= K \qquad D = K^T$

Both Hill and Transposition ciphers are weak to known plaintext attacks since they are linear.

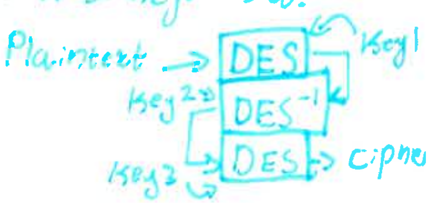
Data Encryption Standard

DES 1975–2005

Block encryption with 2^{64} symbols.

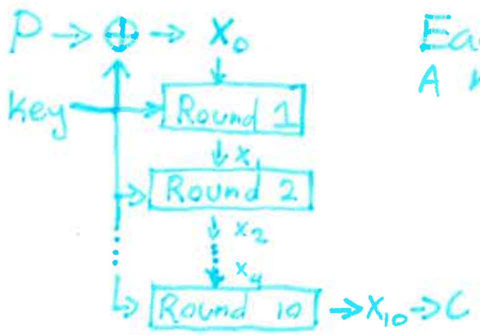
56 bit key (brute force is possible)

1999 3× keys used.



Advanced Encryption Standard (AES)

1997 NIST called for new encryption standard
128 bit blocks, 128, 192 or 256 bit Keys
Using 10, 12 or 14 rounds
Plaintext (P) is first xor with the Key



Each X is A matrix.

Each Round does the following:

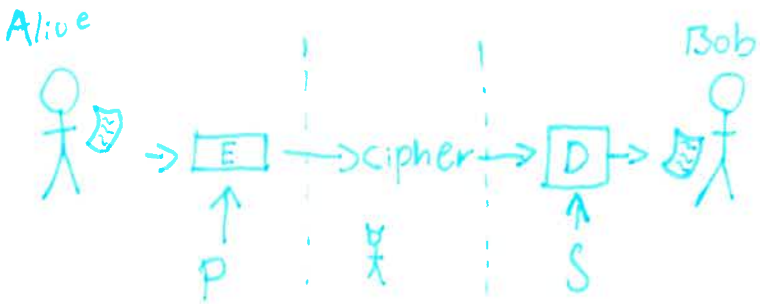
1. S-box substitution
2. Shift rows
3. Mix colums
4. AddRoundKey (xor with Key derived from original Key and round number)

Lecture 4

Public key Encryption

Instead of using a shared Key, A pair of keys are used. One secret (S) key and one public key (P). Public key is used to encrypt messages and secret is used to decrypt messages.

$C = E_P(M) \quad M = D_S(C)$



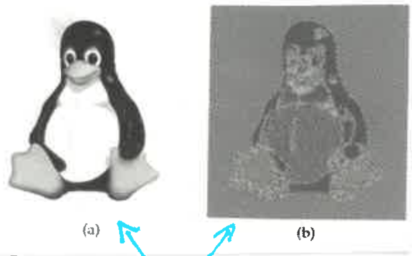
Every participant has a key pair.

Electronic Code Book

Very simple but also bad.
The same encryption is done on each block.

$C[i] = E_k(M[i]) \Leftrightarrow M[i] = D_k(C[i])$

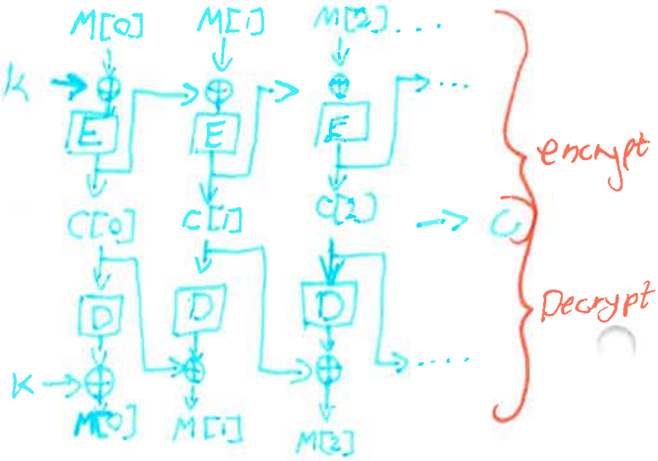
This means repeated info will look the same in the cipher.


(a) (b)

Not good

Cipher Block Chain

First block is xor with Key but next block is xor with previous block. This means entire file is needed to decode.



Maths Recap

Every $\mathbb{Z}^+ > 1$ is the product of primes $n = \prod p_i$

coprime:

a, b coprime $\Leftrightarrow$ $\gcd(a,b) = 1$

Inverse:

$\mathbb{Z}_n \quad a \cdot a^{-1} = 1 \bmod n$

Totient:

$\phi(n)$ = number of coprimes to n

RSA

1977 Ron Rivest, Adi Shamir, Len Adelman
Based on number factorization.

Setup:

$n = p \cdot q \quad p, q \in \mathbb{P}$

set e relative prime to $\phi(n) = (p-1)(q-1)$

set $d = e^{-1}$ in $\mathbb{Z}_{\phi(n)}$

⇒ Public key $= K_E = (n, e)$

Private/secret key $= K_D = d$

Encryption:

$C = M^e \mod n$

Decryption:

$M = C^d \mod n$

Elgamal Cryptosystem

Public key cryptography
based on modular aritmetic

Setup:

Pick prime p
↳ find primitive root g
Pick random $x < p-1$

$y = g^x \mod p$

p, g, y are public x is secret

Encryption:

Pick random $x < p-1$

Compute $S = y^x$ this is the shared secret

Compute $c_1 = g^x$, $c_2 = M \cdot S$

c_1 & c_2 are sent to the other person

Diffie-Hellman Key Exchange

Key exchange Protocol.

Whitfield Diffie & Martin Hellman

Setup:

- Publically agree on modulus: p
- Publically agree on primitive rot of p: g
- Alice & Bob choose their own secret integers a & b.
- Exchange $A = g^a \mod p$, $B = g^b \mod p$
- Both compute $B^a \mod p = S = A^b \mod p$

S is a shared secret known only to Alice & Bob.

This is subseptible to man in the middle attack.

Public | Alice | Bob

$p = 23$
$g = 5$

$a = 4$ $\quad$ $b = 3$

$A = 5^4 \% 23 = 4$
$B = 5^3 \% 23 = 10$

$S = 10^4 \% 23 = 18$ $\quad$ $S = 4^3 \% 23 = 18$

Shared secret

Hash Functions

Maps Plaintext to a fix length value called hash value or digest.

$x = h(P)$

Collision - When two different plain text P & Q have the same digest

$h(P) = x = h(Q)$

h(P) should be O(n)

Message Digest Algorithm (MD5)

Ron Rivest 1991

128 bit hash. ⇒ no longer secure.

Collision can be found in 250 hashes.

Secure Hashing Algorithm (SHA)

SHA-0 & SHA1 1993 160 bit

↳ insecure today

SHA-2 2002

↳ 256 bits / 512 bit

↳ Still secure

SHA-3 2015

↳ very good

Digital Signature

Confidentiality, Integrity.

Signing With Hash

Signing full message is inefficient, sign with digest instead.

Function h(K,M): K-Key M-message

K is shared sender and reciever.

$C = h(K, M)$

Send C and M, reciever compares C with computing of:

$h(K, M) == C$

If true then message is signed.

Cryptographic Hash Function

Hash functions that are also:

Preimage risistant:

one way.

given x, P is hard to find such that $x = h(P)$

Second preimage resistant:

weak collision resistant

given P, Q is hard to find such that $h(P) = h(Q)$

Collision resistant:

strong collision resistant

Any pair P, Q is hard to find $h(P) = h(Q)$

At least 256 bit hash is needed

Iterative/compression

Iterative:

Works for any length input < SHA, MD5

Compression:

works on fixed length

Signature with RSA

When sending a message the sender includes the message encrypted with the senders secret key. Only the sender can encrypt messages that can be decrypted with the senders public key. ⇒ Message is signed by sender.

Signing With Elgamal

Find random number K invertible in (p-1)

$C = g^K \bmod p$ $D = K^{-1}(m - x \cdot C) \bmod (p-1)$

(C, D) is signed message pair

Signature verified by

$(y^C \cdot C^D == g^m) \bmod p$

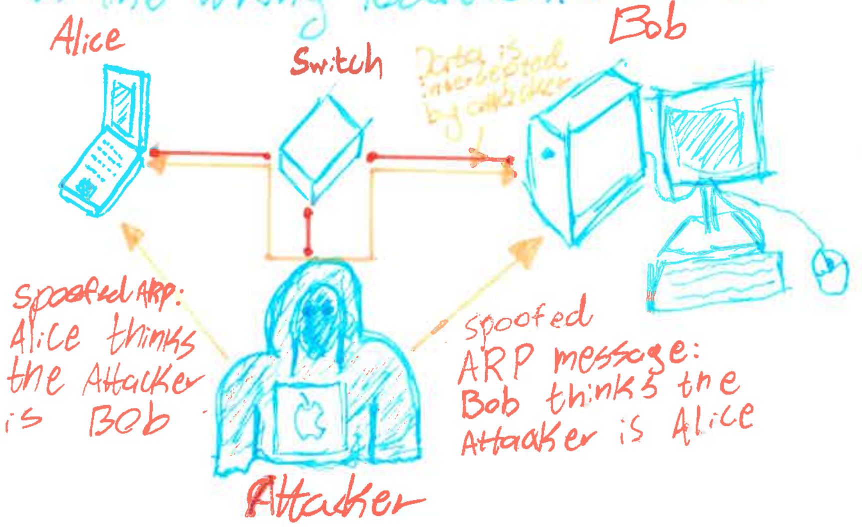
Lecture 6 - Module 2 - Network Security

Link Layer Attack

Mac address:
48 bit numbers unique to device. First 3 octets (3 byte) is IEEE assigned manufacturers
<u>can be spoofed!</u>

Mac address filtering:
Switches can be configured to only to serve specific MAC addresses.
But since MAC Addresses can be spoofed so the links must watch out for duplicates and devices in the wrong location. (interface)

ARP Spoofing:
Matches IP to MAC address.
"Who has <IP1> tell <IP2>
spoofing is when a fake ARP response is sent to trick routers to send data meant for somebody else to the attackers device.



Network Layer Attacks

ICMP: internet control message protocol
↳ Ping: echo requests to get statistics
↳ Traceroute: UDP packets with increasing TTL to discover routes.

IP Vulnerabilities:
↳ Evesdropping
↳ spoofing
↳ Forgery/Man in the middle
↳ denial of service

IP spoofing:
Sending packages to server while Pretending to be somebody else.
Blind spoofing:
Attack from outside subnet. Attacker does not see responses from server.
NON-blind spoofing:
Attacker is on the same subnet and can sniff response packets.

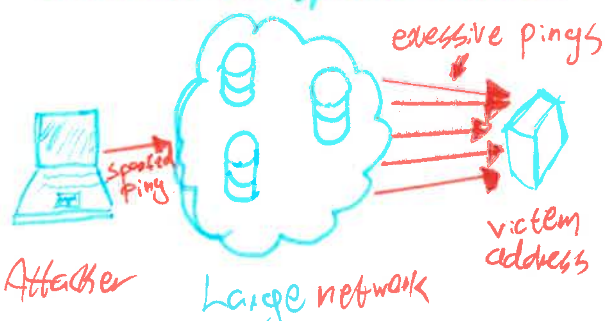
Solution:
↳ Block packets from internal IP when it comes from external interface.
↳ IP traceback: Filtering & tracing Messaging Logging. <u>Probabilistic marking</u>.

ICMP Attack

Ping flooding:
overwhelm weak machine with exessive number of Pings.

Ping of death:
Send fragments off message that reassemble packets to cause buffer overflow and crash operating system

Smurf ping:
ping large network with spoofed source address so that the respons overhelms the spoofed address.



Probabilistic Marking:
Routers randomly invect information into packet headers if it already does not exist. ⇒ routers with high frequency are close to attacker.

Syn flooding

Send multiple spoofed SYN-TCP messages to force server to open many connections not used.

Solved by Syn cookies that are hashes of the first syn. cookies are sent back and the server only creates data structures etc when client responds.

Session Hijacking

On a subnet sniff packets and send message with spoofed IP and stolen sequence number.

Countermeasure:
 IPsec encrypts communication.

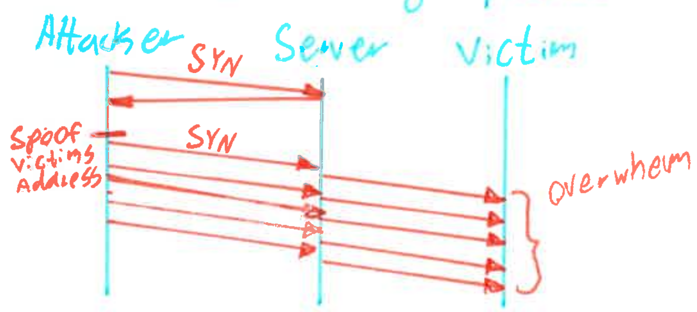
TCP Sequence Prediction (blind injection)

1 Attacker sends SYN to server and takes notes of initial sequence number.

2 Attacker waits and spoofs victims Address.

3 Attacker sends new spoofed SYN to server with the victems IP

4 continue sending requests with



Lecture 7

Intruder

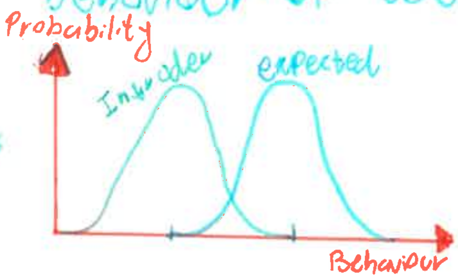
Masquerader:
 Unauthorized user that disguises legitemate user.

Misfeasor:
 Legitemate user using privileges badly.

Clandestine user:
 User with supervisory control that misuses system to avoid detection.

Intrusion Detection

Based on expected vs actual behaviour of user.



Honeypot

Decoy to prevent attacker from critical system.
Can be put anywhere in Network.

Firewalls

Control which packets that go in & out.

Service control:

What type of packets that can flow through.
proxy, server hosting, mail etc.

Direction Control:

Which direction that is allowed, for example TCP can only be started from the inside.

User Control:

Determines which users may do what.

Behavior Control:

Specific filters of content
spam email filters...

Creates choke point, good for monitoring, convinient for NAT, logging etc, IPsec.

Firewall types:

Packet filter:

Inspects every single packet in both direction. Reads IP headers, and sometimes more. uses src and dst headers of IP.

Default discard, Default forward
(whitelist) (blacklist)

Rule set:

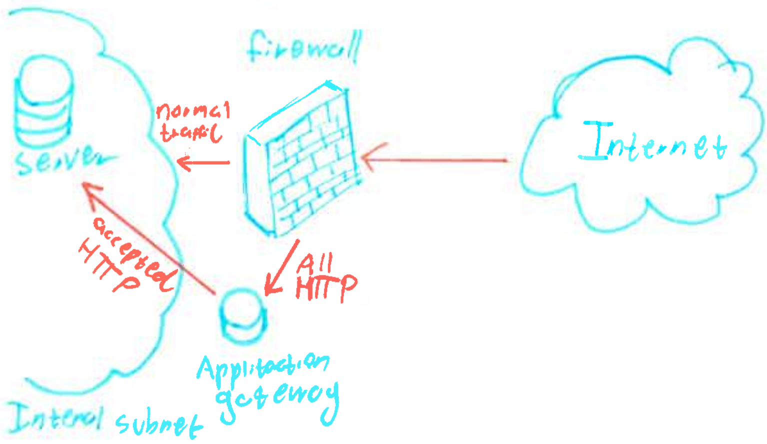
Rule	Direction	src	Dst	Protocol	Port	Action
A	in	external	internal	TCP	25	Premit
B	out	int	ext	TCP	>1023	Premit
C	out	int	ext	TCP	25	premit
D	in	ext	int	TCP	>1023	Premit
E	-	-	-	-	-	Deny

Stateful firewall:

Keeps track of established connections.
eg: A communicates to B. Then for some time B may communicate with A

Application-Level Gateway:

also known as proxy, may require login
works on application level, with specific ports
Advanced filtering.

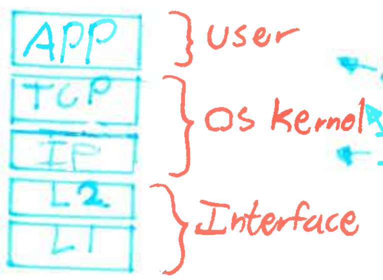


Lecture 8

IPSec

Ip security,

Current Issues:
- ↳ Eavesdropping
- ↳ Packet modification
- ↳ Identity spoofing
- ↳ Denial of service

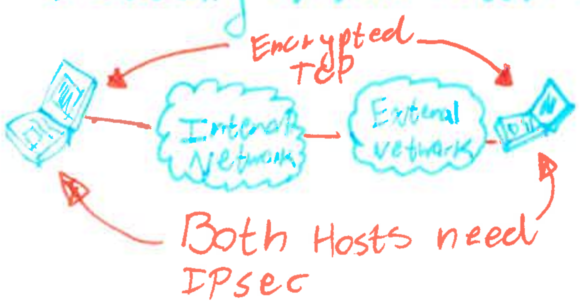


IPsec = AH + ESP + IKE (one or both: AH, ESP)
- AH: Integrity & Authentication
- ESP: confidentiality
- IKE: Key exchange

IPsec Provides:
- ↳ Authentication & integrity
- ↳ confidentiality through encapsulating
- ↳ Access control
- ↳ Replay Security

IPsec Modes:

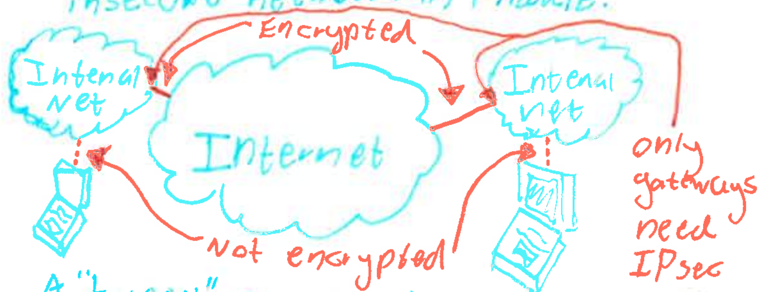
Transport Mode
- ↳ from Host to Host, from Host to Gateway
- ↳ usually within network



Secures payload, leaves IP header

IP header (real dst)	IPsec	TCP/UDP Hdr + Data

Tunnel Mode
- ↳ Gateway to Gateway or Host to Gateway
- ↳ usually between networks with insecure network in middle.



A "tunnel" is created between both nets where all packets are encapsulated

Encapsulates IP header & Data

IP Hdr (gateway)	IPsec Hdr	IP Hdr real dst	TCP/UDP + Data

Security Association (SA)
- ↳ Determine how packets are processed (Algorithms, keys, protocol, etc)
- ↳ Identified by:

SPI: Secure parameter Index.
Flag: Protocol identifier ESP/AH
dst IP Addr: Destination Host
- ↳ Each IPsec implementation keeps track of each SA.
- ↳ this is sent as tuple

{SPI, IP addr, Flag}

Authentication Header (AH)

Next header TCP	Payload length	reserved
Security parameter Index (SPI)		
Sequence number		
Integrity check value (ICV) HMAC of IP header, AH, Payload		

- SPI → Security parameter Index (SPI)
- Anti Replay → Sequence number
- authenticity and integrity → Integrity check value (ICV)

Encapsulated Security Payload (ESP)

- ↳ Confidentiality
- ↳ goes through firewalls
- ↳ transport/Tunnel mode
- ↳ VPN
- ↳ Firewall must be before tunnel

Original IP Head	ESP Header	TCP/UDP segment	ESP Trailer	ESP Auth

Encrypted (TCP/UDP segment – ESP Trailer)

Authenticated (ESP Header – ESP Trailer)

New IP Header	ESP	Original IP Hdr,	Packet TCP/UDP...	ESP trailer	ESP Auth

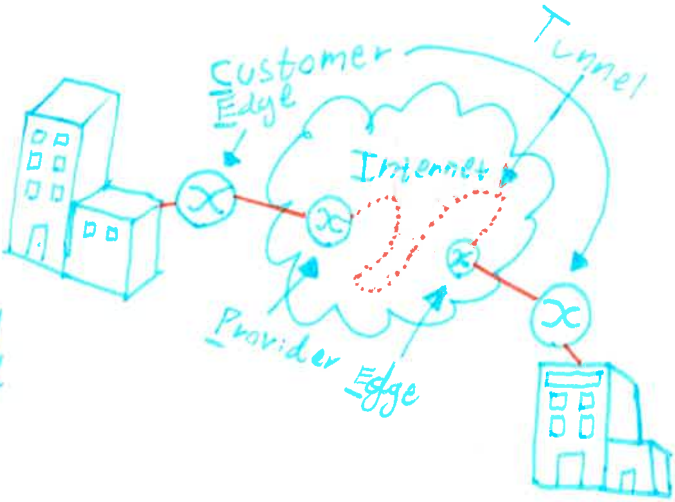
Authenticated (ESP – ESP trailer)

Encrypted (Original IP Hdr – ESP trailer)

Problem with NAT & tunnels

Host to public gateway won't work

↳ Private address must be in original IP header



Virtual Private Network (VPN)

Extention of networks.

Data arrives at CE, Encapsulated by PE & sent over tunnel. Decapsulated at other PE and sent to CE

Customer: | Header | Data |

Provider packet: | Tunnel Hdr | (encapsulated) |

Different protocols:

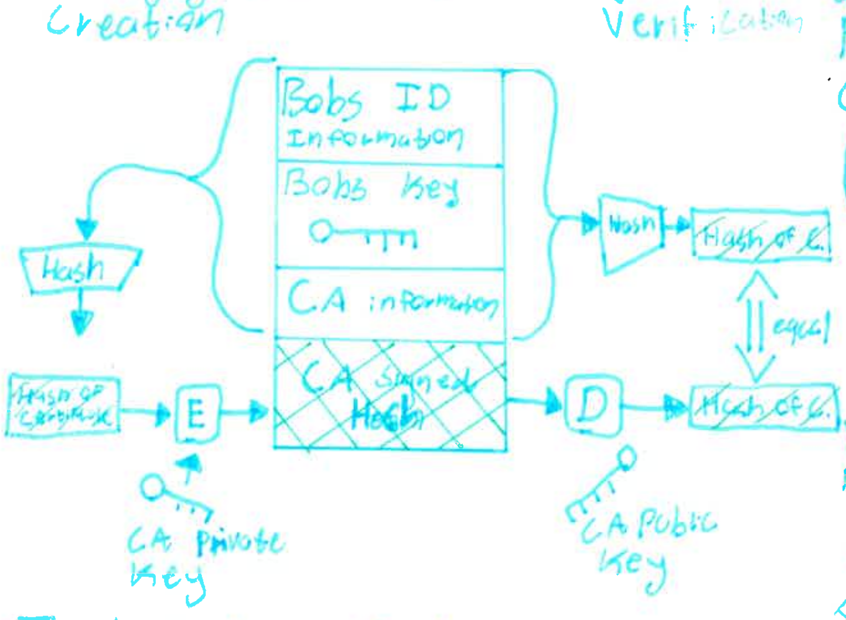
- IP, GRE, MLPS, IPsec ....

IPsec VPN is sometimes used as false marketing to describe secure VPN that uses a different protocol

Lecture 9

Public Key Authentication

Verifying owners of public keys.



Included in Certificate:

- Owner Information & key
- serial number
- CA information
- Validity period
- hashes

Certificate Authority (CA)

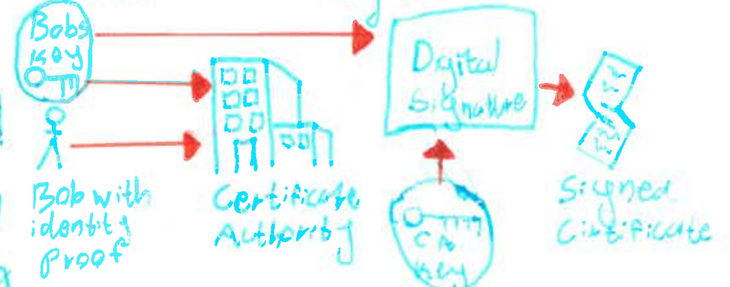
Multiple CA exist.
Use Hierarchies (oligarcy)
Roots CA keys are preinstalled and publically known.

Digicert ← Root CA
- Terena
  - KHT

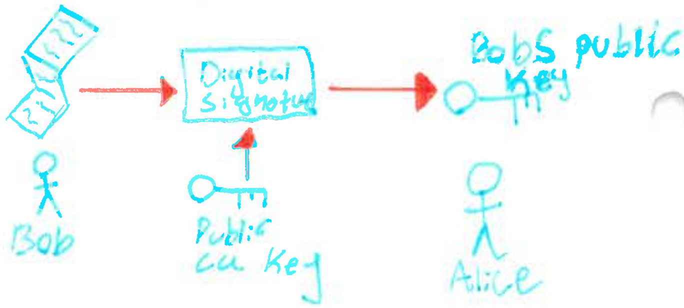
Certificates can be given by:
- Alice
- Database
- DNS
- LDAP

Cirtificate

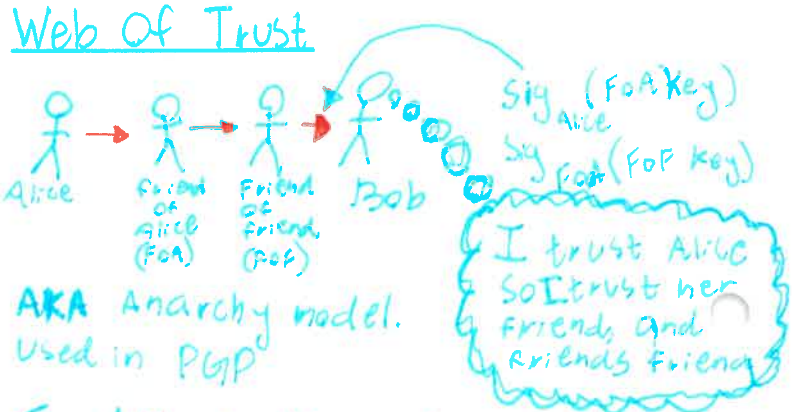
Document including user information and public key signed by a third party. (issuer / certificate authority)
Can be verified by issuer



Validation:



Web Of Trust



AKA Anarchy model.
Used in PGP

Certificate Revocation

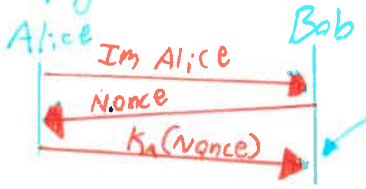
- key leeked, did not pay CA, CA compromized

User is responsible to look up if a certificate is still valid.

Check database online.

Identifying Owner of Key

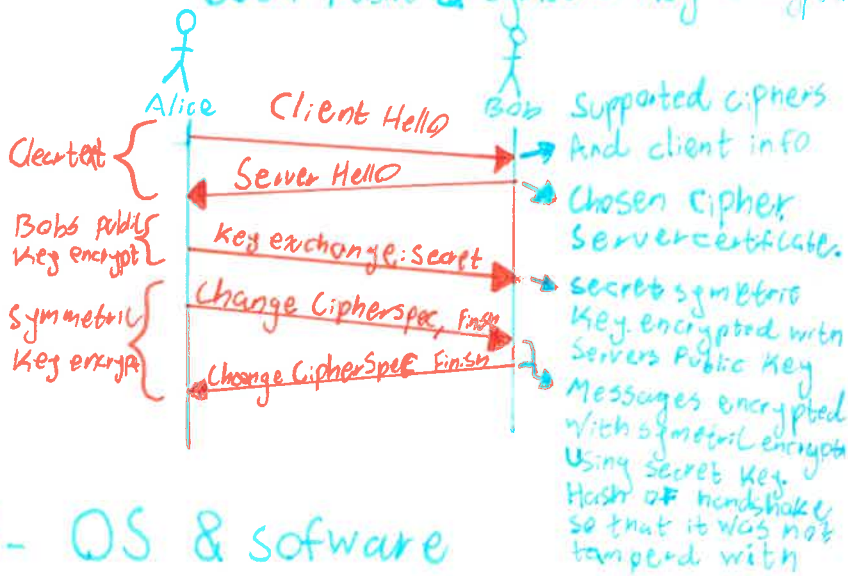
How do we know it is Alice and not somebody with a copy of her certificate & messages?



only Alice can encrypt Nonce, so her identity is verified.

Secure Socket Layer

↳ Also known as TLS
↳ Runs on TCP
↳ Both public & symetric key encryption



Lecture 10 - Module 3 - OS & sofware

Authentication

What you know
↳ passwords
↳ secret keys

What you have
↳ Tokens

What you are
↳ Biometrics.

NIST Password Guidelines

↳ Don't require special characters.
↳ Allow long passwords
↳ check for popular passwords
↳ don't require periodic changes
↳ allow copy paste

Passwords

In unix pass words are salted and then hashed and stored. The actual passwords are not stored, And Hashes are unique even if two people use the same passwords. Stored in safe place (etc/shadow)

Password Salt

Random unpredictable number that is added to the password before it is hashed.

Hash = H(S+Password)

In Unix it is stored as two bytes before the hash. XbAadofdA...

Xb = Salt; AadofdA... = H(S+Password)

Password stretching

↳ Instead of being hashed once it is instead hashed many times.
↳ 5000 times for unix.

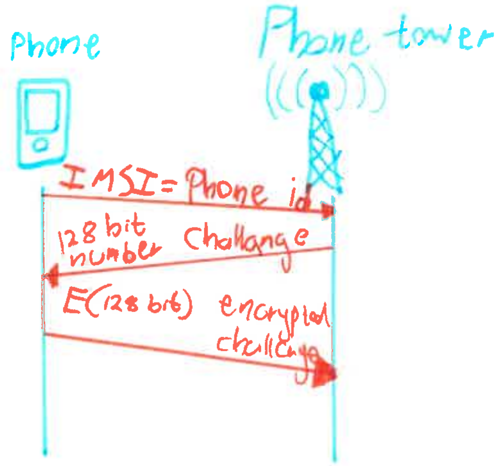
What you have:

Smart Card

SL Access Card
Intergrated circuit with memory and processor.

SIM Card

Subscriber Identity Module.
18 digit hardware identifier.
128 bit secret key
Pin to unlock.



What you are:

Biometrics

Universality - Most people should have

Distinctiveness - Is unique

Permanence - Is nonchangeing

Collectability - Easy to collect.

Passports

↳ contains a lot of biometrics.

Multifactor Authentication:
two or more types of authentication

Lecture 11 File System Security.

Access Control List

Each object is stored with a file detaled with who may use it.

etc/Passwd
↓
root: r w
Mike: r
roberto: r
⋮

etc/global
↓
root: r w
Mike: r w
roberto: rw
⋮

Windows File Access

Closed policy with negative auth. and Deny priority.

File access based on ACL

Linux File Access

Closed policy - default deny.

Each file needs premissions of its super folders.

↳ folders need exec premission to be opened

Inode is a datastructure of file information linked to directories. Several Directories can point to the same Inode

↳ Refcount keeps track on how many times Inode is Used.

Symbolic Links.

Another name for same file (Shortcuts)
↳ becomes "stale" if original is removed.

Each file is owned by a User who is Part of a group.

-rwx rwx rwx
owner group others.

drw- r-- r--
owner group other
(d →) file is a directory

-rwsr-xr-x
(s →) execute file as file owner to elevate premissions.

File system Root

root is the top directory of a File system.

↳ chroot limits program to a different directory instead of the root directory is safer.

Extended ACL

Give aditional specific user right to file.

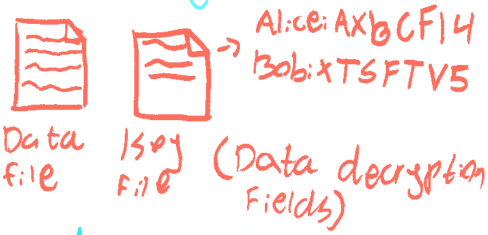
-rwx------+ → Extended ACL tag.

↳ user:person2:r-

Sharing Encrypted Files

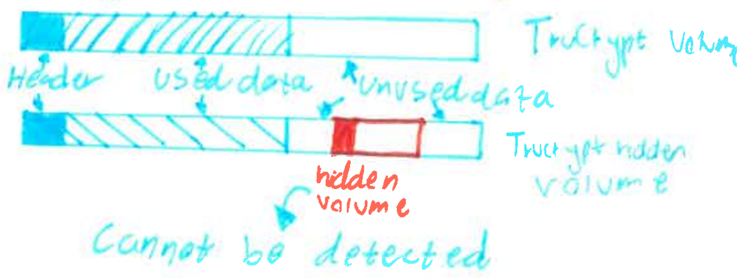
Sharing single symetric key is not safe, storing many copies with public key cryptography is bad.

Instead Encrypted files are stored with a file with a symetric ke encrypted with each users public key.



Plausable deniability

Deny precence of encrypted data



Lecture 12 - Software Security

Exploit - An input that takes advantage of bug/glitch/vulnerability.

Attack - Unintended behaviour of software that gives adventage to an attacker.

Common Weaknesses:

- Improper input sanetazion
- out of bounds write
- improper input validation
- out of bounds read
- Memory buffer missmanagement.

Input Validation

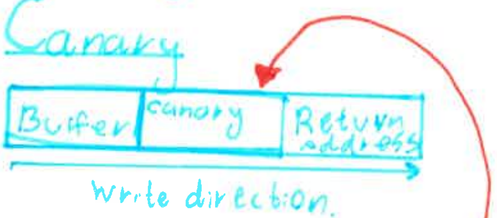
Reject code that could execute other code.
↳ shell, SQL etc...

Stack smashing

Vunerability of C. Cause program to overrwrite parts of the stack to cause damage s.a. return address.

Requires precise knowledge of system memory knowleddge.

Canary



Compiler inserts a canary that is just a few random bytes. If the buffer overflows the canary will be edited and the overflow is detected.

Malware

Any malicious software.

Virus - Human assisted propagation

Worm - Self propagating

Rootkit - Modifies OS to stay hidden

Trojan - Secret code inside other App.

Backdoor - Exploit inside program to give access left intentionally.

Logic Bomb - An action that will cause damage unless attacker is paid

Virus Phases

Dormant - Doing nothing

Propagating - Infecting new files

Triggering - Triggers action

Action - Performs Malicious action.

Zero Day Attack

First time vunerability is discovered by an Attacker.