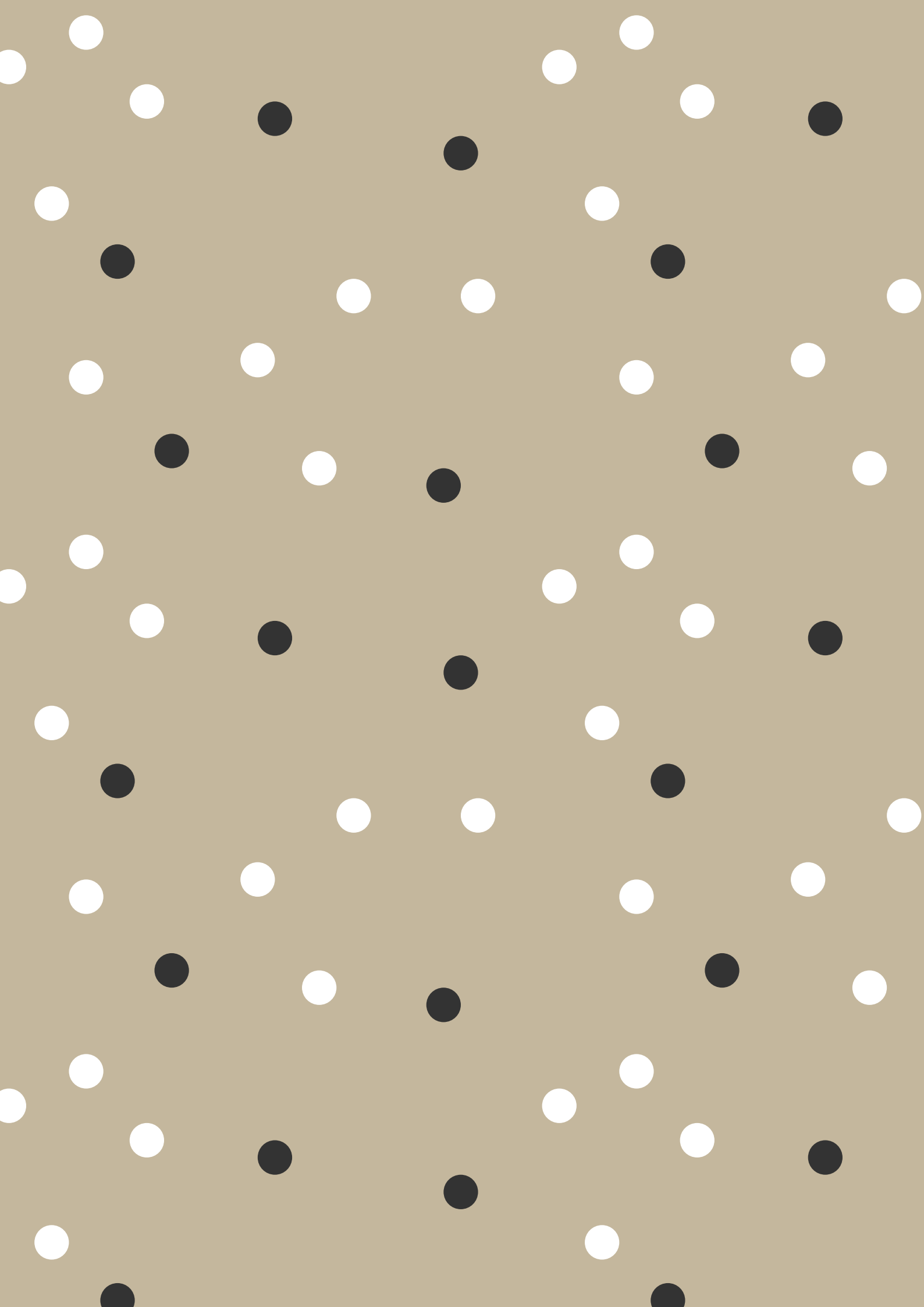


UNIT-3

PASSIVE INFORFMATION GATHERING

DUMPSTER DIVING

- Low tech attacker that needs to know not more than the address of the victim.
- What can be found may vary, but a large no. of news stories indicate that there is a significant amount of info available.

WARDRIVING

- The act of finding & marking locations of wireless networks.
- Prime targets of the attacker.
- The wireless networks are visible due to poor security policies.
- Even when encryption is used, some organizations don't physically secure their wireless access points.

  Attackers can reset or reprogram such devices.

WARDIALING

- Act of automatically scanning telephone no:s using a modem usually dialing every no. in a local area.
- The goal is to find a system that may have a modem connected.
- Modems are a low-cost network-access alternative if network connectivity is lost.
- Many of these modems have weak authentication, or none at all.

USING GOOGLE TO MINE SENSITIVE INFORMATION / GOOGLE HACKING

→ Google offers the attacker the ability to gather sensitive info. that shouldn't be available to outsiders.

- By using the following operators you can use google to uncover sensitive information that shouldn't be revealed.

Filetype

Directs Google to only search wlin the text of a particular filetype.

eg: filetype:xls

Link

" " to check wlin hyperlinks for a term.

eg: link: www.domain.com

Inurl

Directs Google to search for a term wlin the specified url of the document.

eg: inurl: search-text

Intitle

" " " search for a term wlin the title of a doc.

eg: intitle: "Index of..."

EXPLORING DOMAIN OWNERSHIP

- Domain Ownership — something an attacker might want to know & an owner might want to disguise.
- IANA (Internet Assigned Numbers Authority) is reponsible for preserving the coordinating functions of the global Internet & also manages domain names & addresses.

WHOIS

→ These databases can be used to query info. an organization entered while registering their domain.

→ ICANN (Internet Corporation for Assigned Names & Numbers) regulations require all domain holders to submit WHOIS info..

contd.

ICMP

- It gives TCP/IP a way to handle errors.
- Any network device using TCP/IP can send, recieve & process ICMP messages.
- For ICMP to work efficiently, it must be governed by certain rules, like — to ensure ICMP messages don't flood the network, they are given no special priority.
- ICMP msgs cannot be sent in response to other ICMP msgs.
- " " " to multicast or broadcast traffic, nor from traffic that is from an invalid address

PING

→ Most common type of ICMP msg.
→ Identifies active machines — sends an echo request to a system & waits for the target to send an echo reply back.
→ If the target device is unreachable, a request timeout is returned.
→ To ping a large no. of hosts, a ping sweep is performed.

DRAWBACKS OF PING

- Only identifies if a system is active & not which services are running on it.
- Many network admins have blocked ping & don't allow it to pass the border device.
- If ping is used from the command line, only 1 system at a time is pinged.

contd.

→ A non-security-minded person may give out too much info while registering, whereas a security-savy individual may script a well-spoofed entry to misguide attackers.
→ RIRs (Regional Internet Registries) are tasked with overseeing the regional distribution of IP addresses wlin a geographical region. This is a way to uncover initial domain info.
→ DNS resolves known domain names to unknown IP addresses.
→ After determining domain ownership, IP address & domain names, the next step is to identify what software the web server is running. (Apache, IIS, Sun One)
→ The best way to determine web server location is to use traceroute command.
It determines the path to a domain by incrementing the TTL field of the IP header.

DETECTING LIVE SYSTEMS

- ICMP
- Wardriving
- Port Scanning
- OS Fingerprinting

TCP/IP PROTOCOL STACK

FTP	SMTP	SNMP	TELNET	HTTP	DNS	TFTP	BOOTP	Process layer
TCP Connection-oriented				UDP Connectionless-oriented				Host-to-host layer
IP								Internet layer
ARP	RARP	ICMP	EGP	OSPF				
LAN/WAN Ethernet, token ring, ATM								Network access layer

① THE NETWORK ACCESS LAYER

- is at the bottom of the TCP/IP stack.
- Responsible for physical delivery of IP packets via frames.
- Ethernet - most commonly used LAN frame type.
- Ethernet frames are addressed w/ MAC addresses.
- The destination of a MAC address can be unicast/multicast/broadcast, whereas the source can only be unicast

② THE INTERNET LAYER

- Contains 2 important protocols - IP & ICMP.
- IP is a routable protocol whose job is delivery.
- IP can also dictate a specific path using source routing & is responsible for data fragmentation.
- ARP resolves known IP addr. to unknown MAC addresses.
- ARP attacks play a role in a variety of man-in-the middle attacks, spoofing, & session-hijack attacks.

③ THE HOST-TO-HOST LAYER

→ Protocols in this layer - TCP, UDP

→ TCP:

- Enables 2 hosts to establish a connection & exchange data reliably.

- 3-step handshake before data is sent

- 4-step shutdown after data transmission

→ UDP:

- Doesn't perform any of the handshaking that TCP does.
- Less reliable than TCP, but faster.
- Easier to spoof by attackers as it doesn't use sequence & acknowledgement no's.

④ THE APPLICATION LAYER

- is at the top of the stack & is reponsible for application support.
- App"s are mapped by their corresponding port.
- Ports are placed into TCP & UDP packets so that the correct application can be passed to the required protocols below.
- Services may have an assigned port, but may listen on another port.

TCP PORT SCANNING

TCP full connect scan

Most reliable but also most detetable. It is easily logged & detected as a full connection is established.

Open ports reply with a SYN/ACK; closed ports reply with a RST/ACK.

TCP SYN Scan

This scan is called half-open as a full connection is not established.

It was originally designed to evade IDS, but now most detect it.

Open ports "SYN/ACK
Closed " " RST/ACK

TCP FIN Scan

Jumps straight to shutdown.

It sends a FIN packet to the target port. Closed ports should send back an RST.

TCP NULL Scan

Sends a packet w/ no flags set. If the OS has implemented TCP per RFC 793, closed ports will return an RST

TCP ACK Scan

Attempts to determine ACL (Access Control List) rule sets & if stateless inspection is being used. If an ICMP Destination Unreachable, Communication adminis-trative Prohibited msg is returned, the port is considered to be filtered.

TCP XMAS Scan

Has toggled on the FIN, URG & PSH flags. Closed ports should return an RST.

OS FINGERPRINTING

PASSIVE FINGERPRINTING

- The tool doesn't interact with the target system. It monitors network traffic, looking for patterns that are characteristic of known OSs.
- Reconnaissance has provided some basic info about the system - IP addresses, active systems, & open ports.

4 commonly examined items used to fingerprint an OS:

* **IP TTL value** - Different OSs set the TTL to unique values on outbound packets.

ACTIVE FINGERPRINTING

- The tool interacts with the network target by sending several probes & triggers. Analyzing the responses from the target make it possible to guess what OS is in control.

Basic methods used:

* **The FIN probe** - A FIN packet is sent to an open port. While RFC 793 states the required behaviour is not to respond, some OSs (including windows) will respond with a RESET.

* **TCP Window Size** - Diff. OS vendors use different values for initial window size
* **IP DF Option** - Diff. OS vendors handle fragmentation in different ways.
* **IP TOS option** - This field controls the priority of specific packets. Not all OS vendors implement this option in the same way.
* **Bogus Flag probe** - TCP header has only 6 valid flags. This probe sets one of the used flags along with the SYN flag in an initial packet.
* **IPID sampling** - Many systems increment a system-wide IPID value for each packet they send. Others (windows) increment the no. by 256 for each packet.
* **Fragmentation handing** - Diff. OS vendors handle fragmented packets differently.
* **ACK value** - Vendors have diff. implementations for this. Some OSs send back the previous value + 1 ; others send random values.

ENUMERATING SYSTEMS

SNMP

- Simple Network Management Protocol is a popular TCP/IP standard for remote monitoring & management of routers, hosts & other nodes & devices on a network.
- It uses 2 components - manager & agent.

The manager sends & updates requests, & the agent responds to these requests.

SNMP Enumeration

→ Attacker begins by port scanning for port 161 (SNMP).
→ " attempts to connect to SNMP-enabled devices using default community strings or by sniffing community strings.
→ " uses the aquired info to attempt to log in to an enumerated system.
→ " escalates privilege

SNMP Enumeration Countermeasures

- Best defense against it is to turn off SNMP if it's not needed.

ROUTING DEVICES

- They connect networks & use routing protocols to help packets find the best path to a target network.
- Routers & routing protocols are a potential target as they may offer a lot of info that an attacker can use.
- Knowing the network runs RIP means there is no security against route spoofing.

Routing Enumeration Tools

→ One of the best ways to start the routing enumeration process is to use your own browser.
→ Google hacking may help you find vulnerabilities like- usernames, access lists, encrypted passwords & IP addresses of routers.

PASSWORD CRACKING

Calculated hashes

- here, you can use :
  - dictionary - uses a predefined dictionary to look for a match blw the encrypted password & the encrypted dictionary word.
  - hybrid - may use a dictionary or a word list. It prepends & appends characters & nos to the dict. word.
  - brute-force - use random nos & characters.

Precomputed hashes

- They make use of time-memory tradeoff.
  It is implemented using a rainbow table
  ↓
  It works by precomputing all possible passwords in advance. After that task is completed, the passwords & their corresponding encrypted values are stored in a file called the rainbow table.

PASSWORD CREATION

PASSWORD CRACKING = or ≠

Routing Enumeration Counter-measures

- Higher-end switches - Allow for more control & advanced features that provide greater security.
- Dynamic ARP inspection - To prevent man-in-the middle attacks.
- Anti sniffing - detecting bogus ARP traffic
- Promiscuous mode detection - detecting NICs that are listening to traffic other than their own.
- Signatures added to IDS - An IDS can be used to detect signatures of router enumeration & router attacks

BUFFER OVERFLOWS

- For this attack to work, the target system has to have 2 vulnerabilities — a lack of boundary testing in the code, & a machine that executes the code in the data or stack segment.
- Buffer overflows occur when a program puts more data into a buffer than what it can hold.
- when a program is executed, some specific amt. of memory is assigned to each variable & these variables are stored in logical order in a stack.
- A typical program can have many subroutines. When a subroutine is finished, a return pointer must tell the program how to return control back to the main program.
- For the attacker to do anything more than crash the program, he must be able to tweak the pointer.

contd.

The buffer will need to be loaded with the attacker's code. The attacker must also overwrite the location of the return pointer

UNIT- 4

METASPLOIT

- 1st open source tool of its kind
- Development platform for security tools & exploits.
- Metasploit is an attack platform.

Basic approach:

→ Selecting the exploit module to be executed.
→ Choosing the configuration options for the exploit options.
→ Selecting the payload & specifying the payload options to be entered.
→ Launching the exploit & waiting for a response.

Metasploit has 3 ways that it can be controlled:

① **Metasploit web**-
- The **msfweb** interface is a standalone web server that allows the user to run Metasploit through a web browser.
- Metasploit offers 3 primary options: Exploits, Payloads, Sessions.

② **Metasploit console** - (**msfconsole**)
- More powerful way to use Metasploit as it gives the user a much more granular control over the delivery of an exploit.

③ **Metasploit command-line interface**-
- The diff. b/w the msfconsole & msfcli is that **msfcli** doesn't have access to the underlying OS. This means that it is most useful when no interactivity is required or msfcli is being run as a piece of a script for use w/ another program.

VIRUS

3 basic **ways** that **viruses** propagate throughout the computer world:
- Master boot record infection - is the original form of attack. Works by attacking the master boot record of the floppy disk or hard drive.
- File infection - This newer form of virus relies on the user to execute the file. (social Eng.)
- Macro infection - Most modern type of virus. They exploit scripting services installed on the computer.

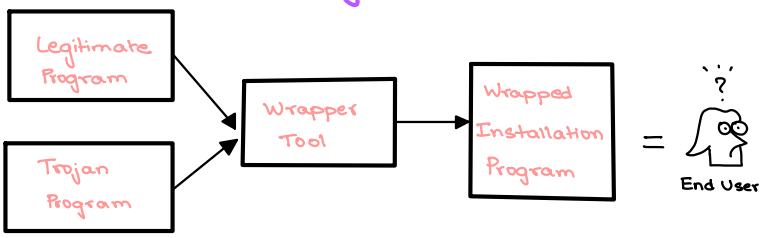
→ Some viruses spread quickly in a computer & infect any file they are capable of infecting. This virus is called **fast infection**
→ **Sparse infection** means that the virus takes its time infecting other files or spreading its damage. This technique helps the virus avoid detection.
→ Some viruses forgo a life of living in files & load themselves into RAM. They're called **RAM resident**. This is the only way boot sector viruses can spread.
→ A **multipartite virus** can use more than 1 propagation method.
→ **Polymorphic viruses** can change their signature everytime they replicate & infect a new file. Components of this virus — an encrypted virus body, a decryption routine, & a mutation engine.

TROJANS

* They are programs that pretend to do one thing but, when loaded, actually perform another, more malicious act.
* Before a Trojan program can act, it must trick the user into downloading it or performing some type of action.
* The Trojan may be configured to do things such as, log keystrokes, add the user's system to a botnet, or even give the attacker full access to the victim's computer

WRAPPERS

- Program used to combine 2 or more executables into a single packaged program.
- They are also referred to as binders, packagers, & EXE binders.



DDoS ATTACKS

- DDoS attacks make computer systems inaccessible by flooding servers, networks, & even end users w/ useless traffic, so that legitimate users can no longer gain access to those resources.
- The attacker is able to recruit a no. of hosts throughout the Internet to simultaneously or in a coordinated fashion launch an attack upon the target.

The process of a polymorphic infection:

1. The decryption routine 1st gains control of the computer & then decrypts both the virus body & the mutation engine
2. The " " transfers control of the computer to the virus, which locates a new program to infect.
3. The virus makes a copy of itself & the mutation engine in RAM.
4. The virus invokes the mutation engine, which randomly generates a new decryption routine capable of decrypting the virus but bearing little or no resemblance to any prior decryption routine.
5. The virus encrypts the new copy of the virus body & mutation engine.
6. The virus appends the new decryption routine with the newly encrypted virus & mutation engine, onto a new program.

→ Stealth viruses attempt to hide their presence from both the OS & the antivirus software by:
- Hiding the change in the file's date & time.
- Hiding the increase in the file's size.
- Encrypting themselves.

→ A virus hoax is a chain message that encourages you to forward it to your friends to warn them of the impending doom.

WORMS

- They can self-replicate.
- True worms require no intervention & are hard to create.
- They don't attach to a host file, but are self-contained & propagate across networks automatically.

FIREWALL CHARACTERISTICS

- All traffic from outside to inside & viceversa must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- The firewall itself is immune to penetration.

CAPABILITIES W/IN THE SCOPE OF A FIREWALL

→ A firewall defines a single choke point that keeps unauthorized users out of the protected network. This simplifies security management.

→ " " provides a location for monitoring security-related events.

→ " " is a convenient platform for several Internet functions that aren't security related.

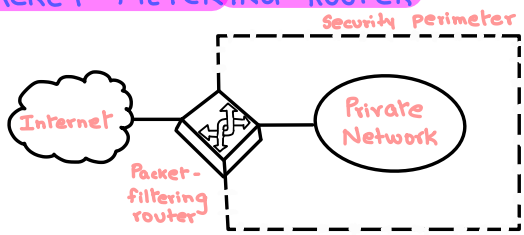
→ " " can serve as the platform for IPSec. " "can be used to implement VPNs

LIMITATIONS OF FIREWALLS

- The firewall cannot protect against attacks that bypass the firewall.
- The firewall doesn't protect against internal threats.
- The firewall cannot protect against the transfer of virus-infected programs or files.

TYPES OF FIREWALLS

① PACKET-FILTERING ROUTER



→ A " " applies a set of rules to each incoming & outgoing IP packet & then forwards or discards the packet.

→ Filtering rules are based on info. contained in a network packet:

- Source IP address
- Destination IP address
- Source & destination transport-level address.
- IP protocol field
- Interface

→ The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.

If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet.

→ If there isn't a match to any rule, a default action is taken:

- Default = discard : That which is not expressly permitted is prohibited.
- Default = forward : That which is not expressly prohibited is permitted.

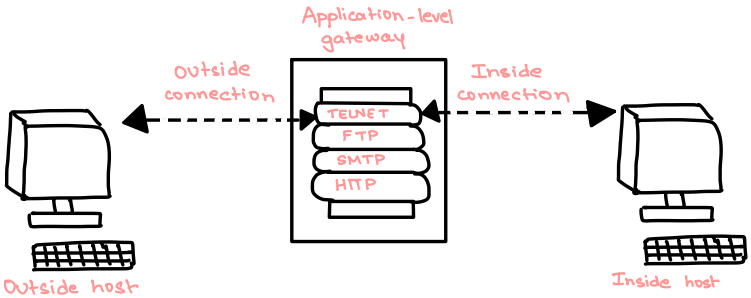
② APPLICATION-LEVEL GATEWAY

→ An " ", also called a proxy server, acts as a relay of app^n-level traffic.

→ These tend to be more secure than packet filters.

→ Rather than trying to deal with the numerous possible combinations that are to be allowed & forbidden at the TCP & IP level, the app^n-level gateway need only scrutinize a few allowable app^{n}s.

→ It is easy to log & audit all incoming traffic at the app^n level.

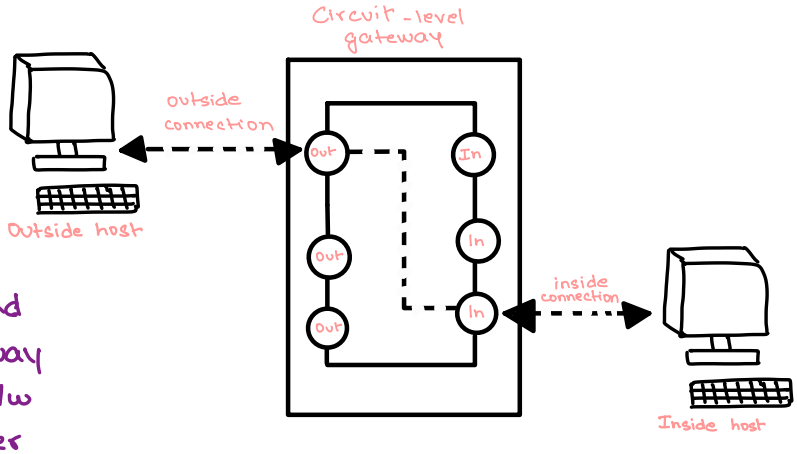


3 CIRCUIT-LEVEL GATEWAY

-> This can be a standalone system or a specialized function performed by an app^{n}-level gateway for certain applications.

-> It doesn't permit an end-to-end TCP connection; rather the gateway sets up 2 TCP connections, 1 b/w itself & a TCP user on an inner host & 1 b/w itself & a TCP user on an outside host

-> Once the 2 connections are establi-shed, the gateway typically relays TCP segments from 1 connection to the other w/out examining the contents.



-> The security function consists of determining which connections will be allowed.

PHASES A VIRUS GOES THROUGH

- **Dormant phase** - The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file. Not all viruses have this stage.
- **Propagation phase** - The virus places an identical copy of itself into other programs. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
- **Triggering phase** - The virus is activated to perform the function for which it was intended. It can be caused by a variety of system events.
- **Execution phase** - The function is performed. The function may be harmless, such as a msg on the screen, or damaging, such as the destruction of programs & data files.

WHY ATTACK & PENETRATION TOOLS ARE IMPORTANT

- Penetration tools help analyze overall security & how well the organization's assets are protected.
- Their purpose is to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of potential security measures, & confirm the adequacy of such measures after implementation.

These tools can be used in many different situations, like:

-> Audits & reviews - Tools are used to determine whether systems are properly patched, whether specific security policies & requirements are being followed, & whether the controls sufficiently gaurd against potential risk.

-> Network evaluations - These processes focus specifically on scanning, vulnerability scanning, & other system-related activity.

-> Penetration tests - Focused on finding exposed systems & vulnerable targets. Ethical hackers conduct these

ATTRIBUTES OF A GOOD SYSTEM ASSESSME -NT TOOL

→ 1 of the 1st things to consider is the type of **impact** the tool has **on the network.**
Testing for such tools is usually done during off-hours or on the weekends because of the amount of traffic the tool generates.
A good scanning tool should be low impact & not use excessive amounts of network bandwidth.

→ Another consideration is how the tool **affects** the **systems** being scanned. Some systems don't respond well to certain types of scans. If scans are going to cause the system to halt, freeze, or reboot, you need to know this well ahead of time to ward off any self-induced disasters.

→ Another consideration is **how many types of vulnerabilities** the software will **detect.**
This can be difficult to measure as different vendors measure the numbers differently.

→ Also consider by **what means** the **software examines** each system.
Some s/ware tools do not authenti -cate before performing checks — this is good as the tool is looking at the system the same way an attacker would. But threats could be internal as well, so a good assessment tool will also perform checks while being authenticated.

→ **Reporting** - After a scan is finished & the s/ware has compiled its findings, you need to create a report. The s/ware should provide a report that is easy to prepare & contains all the pertinant info.

↓

tests to determine what an attacker can find out about an info system, if a hacker can gain & maintain access to the system, & if the hacker's tracks can be successfully covered wlout being detected.

UNIT-5

IDS - 1st & 2nd gen

- IDSs are considered first-generation products because by design they are detective systems.
- Although an IDS can be used to analyze both insiders & outsiders, its more common to see them used for outsiders.
- Misuse detection is targeted toward individuals w/ valid system access. Intrusion detection is targeted toward individuals w/ no authorized system access

- Second-gen IDSs are known as intrusion prevention systems (IPSs).
- whereas an IDS is seen as a detective, an IPS is seen as a prevent-ative.

Purpose of IDS

- An IDS can be used to inspect network/host activity.
- An IDS can identify suspicious traffic & anomalies.
- IDSs act like security gaurds - they monitor the activity of the network.

PARTS OF IDS

→ **Network sensors** - Detect & send data to the system.

→ **Central monitoring system** - Processes & analyzes data sent from sensors

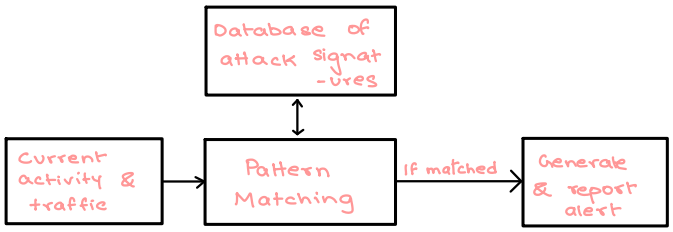
→ **Report analysis** - Offers info about how to counteract a specific event

→ **Database & storage components** - Perform trend analysis & store the IP address & info about the attacker.

→ **Response box** - Inputs info from the previously listed compo-nents & forms an apt response

IDS ENGINES

① SIGNATURE-BASED IDS



→ A signature-based/pattern-matching IDS relies on a database of known attacks.

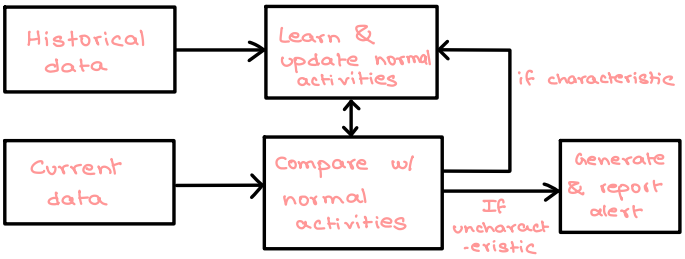
→ These known attacks are loaded into the system as signatures.

→ As soon as the signatures are loaded into the IDS, it can begin to gaurd the network.

→ These signatures are usually given a no. or name so that the admin can easily identify an attack when it sets off an alert.

→ DISADVANTAGE - They can trigger only on signatures that have been loaded. A new attack may go undetected.
eg: Snort

② ANOMALY-BASED IDS



→ These systems require the admin to place the IDS into a learning mode so that it can learn what constitutes normal activity.

→ A considerable amount of time needs to be dedicated to ensure that the IDS produces few false negatives.

→ If an attacker can slowly change his activity, over time the IDS may be fooled into thinking that the new behavior is actually acceptable.

→ This system is good at spotting behavior that is greatly different from normal activity.

SNORT RULES

- Snort matches the packets that are captured wl a set of rules that the admin provides.
- Snort rules can be used to match specific signatures or misuse.

Snort rules are made up of 2 basic parts:

① RULE HEADER

→ This is where the rule's actions are identified

→ Rule actions can include the following:

- Alert - creates an alert using whatever method has been defined
- Log - Logs the packet
- Pass - Informs Snort to ignore the packet
- Activate - creates an alert & turns on a dynamic rule
- Dynamic - Remains unused unless another rule calls on it

→ Next is the protocol. Snort supports — TCP, UDP, IP, ICMP.

→ The 3rd field is the IP address field.

→ The 4th field specifies what port Snort is working on.

② RULE OPTIONS

→ This is where the rule's alert messages are identified

→ They allow the Snort user to fine-tune Snort so that it can detect specific items in the TCP/IP packets.

Some examples:

- Ack - Matches a defined value in the TCP ACK field
- Flags - Matches a TCP flag setting such as SYN, FIN, or ACK
- Msg - Prints a message defined in the alert
- Content - Matches a defined value in the packets payload.

WIRED EQUIVALENT PRIVACY

→ WEP was designed to provide the same privacy a user would have on a wired network.

Steps for encrypting a msg:

* The transmitting & receiving stations are initialized w/ the secret key. This key must be distributed in an out-of-band mechanism such as email, posting it on a website, or giving it to you on a piece of paper.
* The transmitting station produces a seed, which is obtained by appending the 40-bit secret key to the 24-bit IV, for i/p into a pseudo-random number generator (PRNG).
* The " " i/ps the seed to the WEP PRNG to generate a key stream of random bytes.
* The key stream is XOR'd w/ plaintext to obtain ciphertext.
* The transmitting station appends the ciphertext to IV & sets a bit that indicates that it is a WEP-encrypted packet. This completes WEP encapsulation, & the results are transmitted as a frame of data. WEP encrypts only the data & not the header or trailer.
* The receiving station checks to see whether the encrypted bit of frame it received is set. If so, it extracts the IV from the frame & appends the IV to the secret key.
* The receiver generates a key stream that must match the transmitting station's key. This key stream is XOR'd w/ the ciphertext to obtain the sent plaintext.

→ The big problem w/ WEP is that the IVs are not exclusive & are reused. This results in a big vulnerability in that reused IVs expose the PSK. (pre-shared key)

WIFI - PROTECTED ACCESS (WPA)

- Delivers a level of security way beyond what WEP offers.
- WPA uses Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algo & adds an integrity-checking feature that verifies that the keys haven't been tampered with.
- WPA improves on WEP by increasing the IV from 24 bits to 48 bits.
- Key reuse is less likely to occur
- WPA avoids another weakness of WEP by using a different key for each packet.
- Another improvement in WPA is msg integrity (Michael). Michael is designed to detect invalid packets & can even take measures to prevent attacks.

WIRELESS LAN THREATS

① Wardriving - someone that uses a laptop & NIC to detect wireless networks. The entire act of searching for wireless networks has created some unique activities such as:

- Wardriving - Finding & marking the locations & status of wireless networks.
- Warchalking - Marking buildings or sidewalks w/ chalk to show others where its possible to access an exposed company wireless network.
- War flying - Similar to wardriving, except that a plane is used instead of a car.

② Eavesdropping - If a hacker can use Netstumbler & find an WAP that is configured w/ the manufact-urers default configuration, it will likely be a target for the attacker. Many hotels & restaurants provide wireless access w/ open authentication. In these situations, it it very easy for an attacker to gain unauthoriz-ed info.

↓

Dsniff allows an attacker to passively monitor a network for interesting data.

③ Rogue & Unauthorized Access Points
A rogue access point is an unauthorized connection to the corporate network.
2 primary threats can occur :
→ The employee's ability to install unmanaged APs.
→ The ability to perform WAP spoofing

④ DoS attacks.

UNIT-1

SUBSTITUTION TECHNIQUES

① Ceaser's cipher
→ shift
(eg, shift=3)

pt: a b c d e f g h i j k l m n o
D E F G H I J K L M N O P Q R

pt: p q r s t u v w x y z
S T U V W X Y Z A B C

plaintext → meet me here
PHHW PH KHUH

$C = E(K, P) = (p+K) \bmod 26$
$P = D(K, C) = (C-K) \bmod 26$

② Monoalphabetic
→ Any permutation of the 26 alphabet characters (26! possible keys).

③ Playfair Cipher
Example: Key → monarchy
Pt → instrumentsx

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

in → GA sx → XA
st → TL
ru → MZ
me → CL
nt → RQ

Encrypted text:
GATLMZCLRQXA

④ Hill Cipher
Example: key: GYBNQKURP
msg: ACT

$$\begin{bmatrix} G & Y & B \\ N & Q & K \\ U & R & P \end{bmatrix} \begin{bmatrix} A \\ C \\ T \end{bmatrix} = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

$$= \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \pmod{26} = \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$$

$C = PK \bmod 26 = E(K, P)$
$P = CK^{-1} \bmod 26 = D(K, C)$

⑤ Polyalphabetic Cipher
Using different monoalphabetic substitutions as 1 proceeds through the plaintext

TRANSPOSITION TECHNIQUES

① Rail fence technique
→ Pt is written down as a sequence of diagnols, then read off as a sequence of rows.

Example → pt: meet me after the toga party
Rail fence depth of 2

m e m a t r h p r y
e t e f e t e a t

Encrypted msg:
MEMATRHPRYETEFETEAT

DES KEY GENERATION

Eg:

10 bit key → 1 1 0 0 0 1 1 1 1 0
(3 5 2 7 4 10 1 9 8 6)

P_{10}: 0 0 1 1 0 0 1 1 1 1

LS_1: 0 1 1 0 0 1 1 1 1 0
(6 3 7 4 8 5 10 9)

P_8: 1 1 1 0 1 0 0 1 → K_1

LS_2: 1 1 0 0 0 1 1 1 0 1 (once)
(to LS_1) 1 0 0 0 1 1 1 0 1 1 (twice)
(6 3 7 4 8 5 10 9)

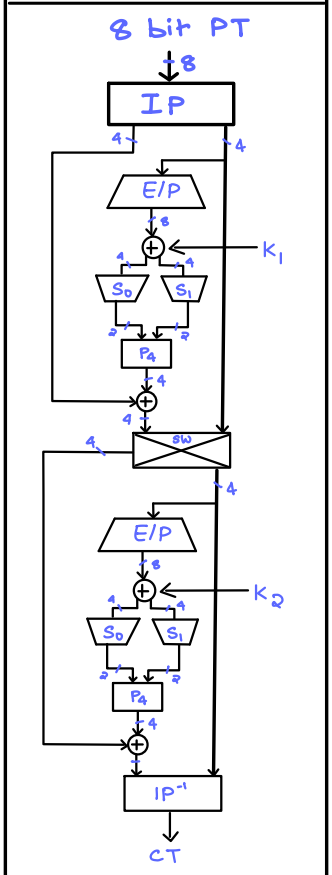
P_8: 1 0 1 0 0 1 1 1 → K_2

INGREDIANTS OF A SYMMETRIC ENCRYPTION SCHEME

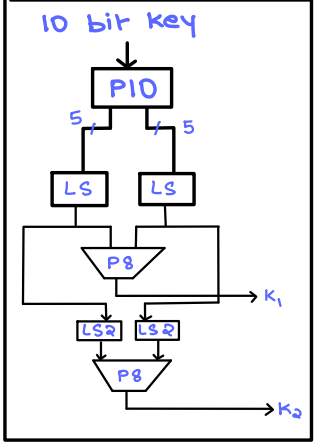
- Plaintext
- Encryption algo
- Secret key
- Ciphertext
- Decryption algo

Expl. → in my written notes

S-DES ENCRYPTION



S-DES KEY GENERATION



DES DESIGN CRITERIA

① Criteria for the S-boxes

→ No o/p bit should be too close a linear function of the i/p bits.

→ Each row of the S-box must include all 16 possible o/p bit combinations.

→ If 2 i/ps differ by exactly 1 bit, the o/p should differ by atleast 2 bits.

→ If " " 2 middle bits " " ".

→ If " identical in their last 2 bits & differ in their 1st 2 bits, the o/p cannot be the same.

→ For any non-zero 6-bit difference b/w i/ps, no more than 8 of the 32 pairs of i/p will result in the same o/p difference.

② Criteria for permutation P

→ The 4 o/p bits from each S-box at round i are distributed such that 2 of them affect middle bits & 2 affect end bits in round (i+1).

→ The 4 o/p bits " will affect 6 S-boxes in the next round, but no 2 bits will affect the same S-box.

→ For 2 S-boxes j & k, if an o/p bit from S_j affects a middle bit of S_k on the next round, then an o/p bit from S_k cannot affect a middle bit of S_j

CRITICAL ASPECTS OF BLOCK CIPHER DESIGN

The cryptographic strength of a Feistal cipher comes from 3 aspects of the design → No. of rounds, function F, & the key schedule algo.

① **No. of rounds** - The greater the no. of rounds, the more difficult it is to perform cryptanalysis, even for a weak F.
The criterion is that the no. of rounds should be chosen so that cryptanalysis requires greater effort than a simple brute-force key search.

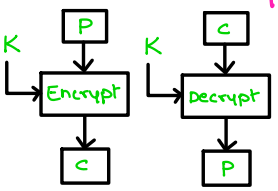
② **Design of F** - F provides the element of confusion in Feistal cipher.
It should be difficult to "unscramble" the substitution performed by F.
F has to be non-linear. A change in 1 i/p bit must produce a change in many o/p bits (Avalanche effect). Any o/p bit should change w/ probability 1/2 when an i/p bit is inverted (Strict Avalanche Effect). O/p bits should change independently when any i/p bit is inverted (Bit Independence Criterion)

③ **S-box design** - we need any change in the i/p bits to result in random-looking changes in the o/p. S-box should satisfy SAC & BIC. Larger s-boxes are more resistant to linear & differential cryptanalysis, but are also more difficult to design. For a 1-bit i/p change, at least r o/p bits change (Guaranteed Avalanche).

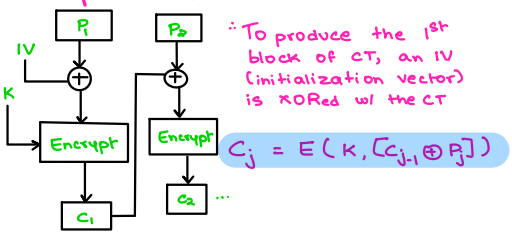
④ **Key Schedule Algo** - At min, it should satisfy SAC & BIC.

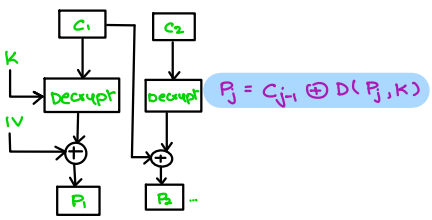
BLOCK CIPHER MODES OF OPERATION

① **Electronic code book**
Pt is handled 1 block at a time & the blocks are encrypted using the same key.

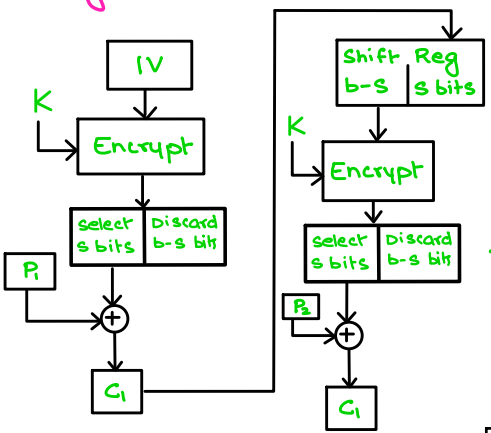


② **Cipher Block Chaining**
The i/p to the encryption algo is the XOR of the current P.T block & the preceeding CT; the same key is used.

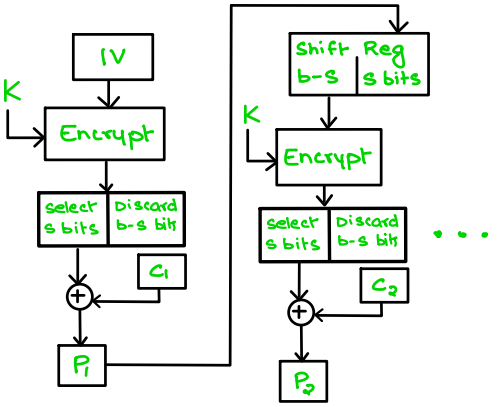




③ **Cipher Feedback Mode**
Encryption - i/p to the encryption func. is a b-bit shift register initialised to IV. The most significant s-bits of the o/p of EF are XORed w/ the PT1 to produce C1. The contents of the shift register are shifted left by s bits & C1 forms the least significant s-bits of the register.



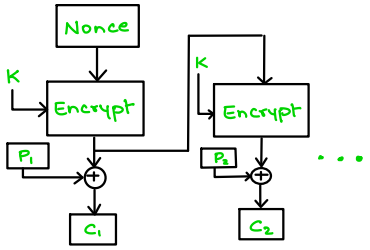
ENCRYPTION



DECRYPTION

④ Output Feedback Mode

Same as CFB, but here the o/p of the EF is sent as feedback, & all the bits are sent.



⑤ Counter Mode

Counter value is initialised to some value & then incremented by 1 for each subsequent block.
This value must be different for each PT block.

UNIT-2

HOW DIFFIE-HELLMAN ALGO IS SUSCEPTIBLE TO MAN-IN-THE-MIDDLE ATTACK

Suppose A & B want to exchange keys & D is the adversary. The attack happens as follows:

- → D prepares for the attack by generating 2 random private keys x_{D1} & x_{D2} & then computing the corresponding public keys Y_{D1} & Y_{D2}.
- → A transmits Y_A to B.
- → D intercepts Y_A & transmits Y_{D1} to B. D also calculates $K2 = (Y_A)^{x_{D2}} \bmod q$.
- → B receives Y_{D1} & calculates $K1 = (Y_{D1})^{x_B} \bmod q$
- → B transmits Y_B to A.
- → D intercepts Y_B & transmits Y_{D2} to A. D calculates $K1 = (Y_B)^{x_{D1}} \bmod q$.
- → A receives Y_{D2} & calculates $K2 = (Y_{D2})^{x_A} \bmod q$.

A & B think that they share a secret key, but insted D & B share K1, & A & D share K2.

All future communications b/w A & B are intercepted in the following ways:

- A sends an encrypted message.
- D intercepts & decrypts this msg.
- D sends B either the same msg, or another random msg.

ELLIPTIC CURVE ENCRYPTION / DECRYPTION

An elliptic curve is a plane curve over a finite field which is made up of points satisfying the eqn:

$$y^2 = x^3 + ax + b$$

An encryption/decryption system requires a point G & an elliptic group $E_q(a, b)$ as parameters

A selects a private key n_A & generates a public key, $P_A = n_A \times G$.
To encrypt & send a message P_m to B, A chooses a random +ve integer K & produces CT, $c_m = \{KG, P_m + KP_B\}$.

To decrypt this CT, B multiplies the 1st point by B's secret key & subtracts it from the 2nd point:

$$P_m + KP_B - n_B(KG)$$
$$= P_m + K(n_B G) - n_B(KG) = P_m$$

SHA-512 LOGIC

- The algo takes as i/p a msg w/ max length less than 2^{128} bits & produces as output a 512-bit msg digest. The i/p is processed in 1024 bit blocks

Processing steps:

Step 1: Append padding bits – The msg is padded so its length $\equiv 896 \bmod (1024)$. Padding is always added, even if the msg is of desired length. The padding consists of a single 1 bit followed by 0s.

Step 2: Append length – A block of 128 bits is appended to the msg. This block is treated as an unsigned 128-bit integer & contains the length of the original msg (w/out padding).

The outcome of the 1st 2 steps yields a msg that is an integer multiple of 1024 bits in length.

The expanded msg is represented as the sequence of 1024-bit blocks $M_1, M_2, \ldots M_n$ so that the total length of the expanded msg is $N \times 1024$ bits.

Step 3: Initialize hash buffer – A 512-bit buffer is used to hold intermediate & final results of the hash function. The buffer can be represented as 8 64-bit registers (a, b, c, d, e, f, g, h). These registers are initialized to some 64-bit integers.

Step 4: Process message in 1024-bit blocks – The heart of the algo is a module that consists of 80 rounds.

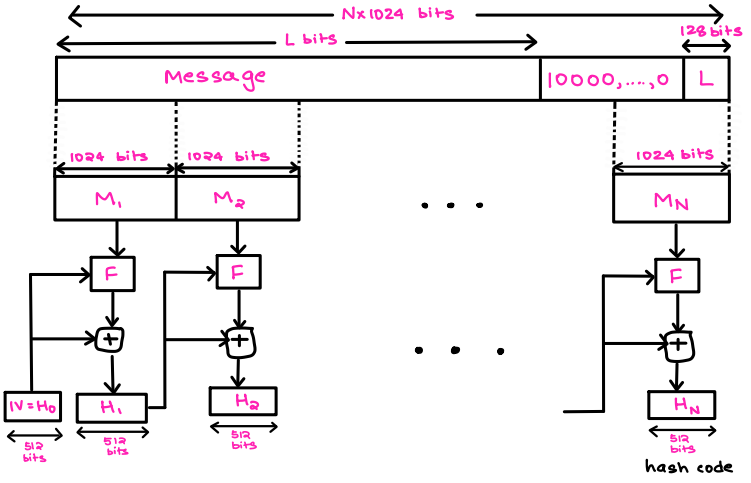
Each round takes as i/p the 512-bit buffer value, & updates the contents of the buffer.

At i/p to the 1st round, the buffer has the value of the intermediate hash value H_{i-1}. Each round t makes use of a 64-bit value w_t, derived from the current 1024-bit block being processed (M_i). Each round also uses an additive constant K_t.

The constants provide a "randomized" set of 64-bit patterns, which should eliminate any regularities in the i/p data.

The o/p of the 80th round is added to the i/p to the 1st round (H_{i-1}) to produce H_i. The add^n is done independently for each of the 8 words in the buffer w/ each of the corresponding words in H_{i-1}.

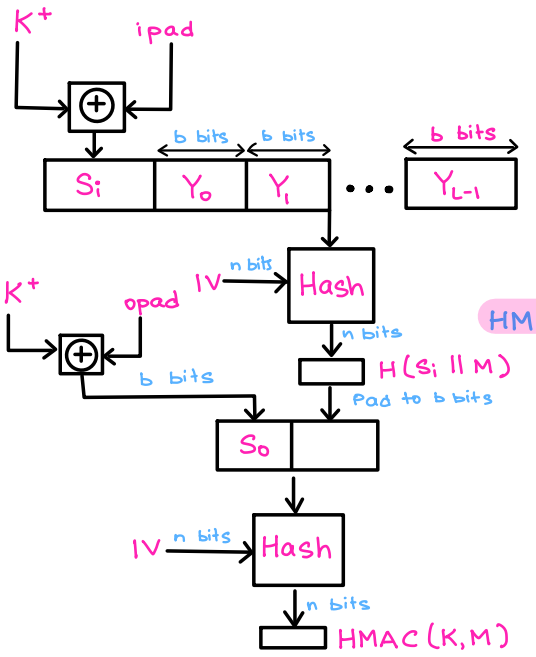
Step 5: Output – After all N 1024-bit blocks have been processed, the o/p from the N^{th} stage is the 512-bit message digest.



COMPARING ECC w/ RSA

- Most of the products that use public-key cryptography for encryption & digital signatures use RSA.
- The key length for secure RSA use has increased over recent years, & this has put a heavier processing load on app^{n}s that use RSA.
- This burden has consequences, especially for e-commerce sites that conduct large numbers of secure transactions.
- ECC challenges RSA.
- The principal attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead.
- The confidence level in ECC isn't as high as that in RSA.
- ECC is fundamentally more difficult to explain than RSA.

HMAC - MACs based on Hash Functions



K → key, K^+ → K padded w/ 0's
H → embedded hash function
IV → initial value i/p to hash func.
M → Message i/p to HMAC
Y → blocks of M
L → No of blocks in M
n → length of hash code produced by embedded hash func.

$$HMAC(K,M) = H[(K^+ \oplus opad) \,||\, H[(K^+ \oplus ipad) \,||\, M]]$$

Algo:

1. Append 0s to the left end of K to create a b-bit string K^+
2. XOR K^+ w/ ipad to produce the b-bit block S_i.
3. Append M to S_i.
4. Apply H to the stream generated by step 3.
5. XOR K^+ w/ opad to produce the b-bit block S_o.
6. Append the hash result from step 4 to S_o.
7. Apply H to the stream generated in step 6 & output the result.