Worksheet notes

Exercise sheet 1:

Intro to CIA/AAA/Threat/Security Principles:

Q) With respect to the C.I.A. and A.A.A. concepts, what risks are posed by Trojan horses?
A) Confidentiality: N/A
Integrity: Original message altered (possibly for malicious purposes)
Availability: Looks fine on outside

Authenticity: Facade as secure, but underlying message data has been tampered with
Authorisation: Access to resources it shouldn't have access to
Accountability: Attacker would be unidentifiable

The concept of **security through obscurity (STO)** relies on the idea that a system can remain secure if the vulnerabilities are secret or hidden.

Exercise sheet 2:

Intro to Cryptography + Networking:

Q) What are the two basic functions used in encryption algorithms?
A) Transposition and substitution (+Permutation)

Q) What are the two basic functions used in encryption algorithms?
A) Transposition and substitution (+Permutation)

Q) How many keys are required for two people to communicate via a cipher?
A) One key for symmetric ciphers, two keys for asymmetric ciphers.

Q) What is the difference between a block cipher and a stream cipher?
A) A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

Q) What are the two general approaches to attacking a cipher?
A) Cryptanalysis and brute force.

Q) What is a trap-door one-way function?
A) A trap-door one-way function is easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known. With the additional information the inverse can be calculated in polynomial time.

Q) What requirements must a public-key cryptosystems fulfil to be a secure algorithm?

- It is computationally easy for a party B to generate a pair (public key PUb, private key PRb).
- It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext: C = E(PUb, M).
- It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message: M = D(PRb, C) = D(PRb, E(PUb, M)).
- It is computationally infeasible for an opponent, knowing the public key, PUb, to determine the private key, PRb.
- It is computationally infeasible for an opponent, knowing the public key, PUb, and a ciphertext, C, to recover the original message, M.

Q) Explain difference between Physical Links, Data Links, and Routes!
1) At the physical layer, a link between a host and a switch or between switches is called a **physical link.**
A single path a frame takes across a single network is called a **data link.**
A single path a packet takes across an internet is called a **route.**

Q) Which is a security attack at layer 1 of the OSI model?
A) Layer 1 refers to the physical aspect of networking. Disrupting this service, primarily resulting in Denial of Service (DoS) attacks.
Network vulnerabilities/threats which occur at this level are the following: 1) Access Control 2) Damage data bits 3) Environmental issues 4) Disconnection of Physical Links.

Q) What is a replay attack?
A) An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access

Exercise sheet 3:

Network Security:

Q) What is DNS cache poisoning?

A) In DNS cache poisoning or DNS spoofing, an attacker diverts traffic from a legitimate server to a malicious/dangerous server. The perpetrator enters false information -- such as a doctored website address -- into the DNS cache by pretending to be a DNS name server.
DNS cache poisoning is a highly deceptive attack that not only diverts traffic from legitimate websites, but also leaves users vulnerable to many risks, including malware infections and data theft.

Q) What is SamSam malware? How does it work?

A) SamSam is ransomware that 'spies' for a long time after its initial infection, without being detected. SamSam uses vulnerabilities to attack specific organisations. The creators of the ransomware ask for ransom after SamSam removes or makes it impossible for the victim to access his own data.

Q) What is the purpose of HTTPS?

A) Hypertext transfer protocol secure (HTTPS) is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted to increase security of data transfer. HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses, making it safer and more secure.

Q) What is the difference between ISO/OSI model and TCP/IP model?

A) OSI model is a generic model that is based upon functionalities of each layer. TCP/IP model is a protocol-oriented standard. OSI model distinguishes the three concepts, namely, services, interfaces, and protocols. TCP/IP does not have a clear distinction between these three. OSI model gives guidelines on how communication needs to be done, while TCP/IP protocols layout standards on which the Internet was developed. So, TCP/IP is a more practical model. In OSI, the model was developed first and then the protocols in each layer were developed. In the TCP/IP suite, the protocols were developed first and then the model was developed. The OSI has seven layers while the TCP/IP has four layers.

Q) What is the goal of the TCP session hijacker? How can we prevent it?

A) A form of cyber attack in which an authorized user gains access to a legitimate connection of another client in the network. Having hijacked the TCP/IP session, the attacker can read and modify transmitted data packets, as well as send their own requests to the addressee.
TCP/IP hijacking is a type of man-in-the-middle attack. The intruder can determine the IP addresses of the two session participants, make one of them inaccessible using a DoS attack, and connect to the other by spoofing the network ID of the former. The goal of the TCP session hijacker is to create a state where the client and server are unable to exchange data; enabling him/her to forge acceptable packets for both ends, which mimic the real packets. Thus, the attacker can gain control of the session.
Counter Measures: Using secure protocols instead of clear text protocols like HTTP, FTP. etc. Encrypting session id will increase the complexity of the session id prediction. Sending session id over SSL. Use long random numbers for session id. Implement timeout for the session when the session is logged out, or session id expires etc.

Q) For what applications is SSH useful?

A) The initial version, SSH1 was focused on providing a secure remote logon facility to replace TELNET and other remote logon schemes that provided no security. SSH also provides a more general client/server capability and can be used for such network functions as file transfer and e-mail.

Q) What is a Syn flood attack? And what are the countermeasures for it?

A) By consuming all the server resources, this type of attack can bring down even high-capacity components capable of handling millions of connections. SYN flood DDoS attacks exploit TCP three-way handshake connection and its limitation in handling half-open connections.
How to Protect Against SYN Flood Attacks?
1. Increase Backlog Queue.
2.Recycling the oldest half-open connection.
3.SYN Cookies.

Q) What is a TCP session hijack? And what are the countermeasures for it?

A) The goal of the TCP session hijacker is to create a state where the client and server are unable to exchange data; enabling him/her to forge acceptable packets for both ends, which mimic the real packets. Thus, the attacker can gain control of the session.
Counter Measures: 1) Using secure protocols instead of clear text protocols like HTTP, FTP. etc. 2) Encrypting session id will increase the complexity of the session id prediction 3) Sending session id over SSL 4) Use long random characters for session id 5) Implement timeout for the session when the session is logged out, or session id expires etc.

IPsec is below the transport layer (TCP, UDP).

Q) What is DHCP? How useful is it to help achieve security of IP addresses?

A) Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

Security Benefits:

DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.

Q) In IEEE 802.11, open system authentication simply consists of two communications. An authentication is requested by the client, which contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration.

A. What are the benefits of this authentication scheme?

B. What are the security vulnerabilities of this authentication scheme?

A) This scheme is extremely simple and easy to implement. It does protect against very simple attacks using an off-the-shelf Wi-Fi LAN card, and against accidental connection to the wrong network.

B) This scheme depends on all parties behaving honestly. The scheme does not protect against MAC address forgery.

Exercise sheet 4:

Web Security:

Q) What is the impact of a successful SQL injection attack?

A) A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information.

Some common SQL injection examples include:

1) Retrieving hidden data, where you can modify a SQL query to return additional results. Subverting application logic, where you can change a query to interfere with the application's logic.

2) UNION attacks, where you can retrieve data from different database tables. Examining the database, where you can extract information about the version and structure of the database.

3)Blind SQL injection, where the results of a query you control are not returned in the application's responses.

Q) What are the types of XSS attacks?

A) There are three main types of XSS attacks. These are:

1) **Reflected XSS**, where the malicious script comes from the current HTTP request.

2) **Stored XSS**, where the malicious script comes from the website's database.

3) **DOM-based XSS**, where the vulnerability exists in client-side code rather than server-side code.

Q) What is the difference between a packet filtering firewall and a stateful inspection firewall?

A) A traditional packet filter makes filtering decisions on an individual packet basis and does not take into consideration any higher layer context.

A stateful inspection packet filter tightens up the rules for TCP traffic by creating a directory of outbound TCP connections. There is an entry for each currently established connection. The packet filter will allow incoming traffic to high- numbered ports only for those packets that fit the profile of one of the entries in this directory.

Q) What are two common techniques used to protect a password file?

A) 1) **One-way encryption:** The system stores only an encrypted form of the user's password. When the user presents a password, the system encrypts that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the encryption function and in which a fixed-length output is produced.

2) **Access control:** Access to the password file is limited to one or a very few accounts.

Q) Why is it useful to have host-based firewalls?

A) Filtering rules can be tailored to the host environment. Specific corporate security policies for servers can be implemented, with different filters for servers used for different application.

• Protection is provided independent of topology. Thus, both internal and external attacks must pass through the firewall.

• Used in conjunction with stand-alone firewalls, the host-based firewall provides an additional layer of protection. A new type of server can be added to the network, with its own firewall, without the necessity of altering the network firewall configuration.

Q) What are three benefits that can be provided by an intrusion detection system?

A) 1) Damage limitation, 2) Deterrent, 3) Enables collection of information on intrusion techniques, i.e., incrementally better

Exercise sheet 5:

Security Protocols and Private Network:

Q) What is a VPN and what are its benefits?
A) VPN facilitates communications between two remote networks in a secure manner. It is mainly based on establishing an IP tunnel to exchange data.

IPSec VPNs are useful for Remote access scenario and Interconnecting LANs.
TLS VPNs is useful for Remote access to private network scenario.

IP tunnelling is creating a private channel where two distant devices can communicate as if they were local. It is based on encapsulating an IP packet into another IP packet.

Q) A client and server want to communicate, explain the steps of establishing TLS exchanges?
A) TLS handshake protocol, TLS cipher spec protocol, TLS alert protocol

Q) Why was SSL discarded?
A) SSL was not secure enough so it was discarded and TLS has taken its place.

Q) What network attacks do you think we can stop using TLS?
A) Because the communication is encrypted, TLS can stop **eavesdropping**, **tampering**, and **message forgery** between two communicating network endpoints.

Q) What network attacks do you think we can stop using IPSec?
A) **Network-based attacks from untrusted computers**, attacks that can result in the **denial-of-service** of applications, services, or the network, **Data corruption**.
Using IPSec keeps the data encrypted and makes sure they all reached their destination without any alterations on their way.

Exercise sheet 6:

Intro to Software Security:

Q) What is control hijacking in the context of exploitation? Explain one possible way to hijack control in the presence of stack overflow bug?
A) Control hijacking is taking control of the execution of a program, enabling it to run code or paths through the code that would not normally be taken by standard execution.
One way to hijack control would be to overwrite the return address of a function on the stack to point to code the attacker wishes to run.

Q) What is a format string bug?
A) Format string is a memory bug that can lead to the contents of the stack being leaked. Also, %n causes overwriting a memory location.

%n: used is to print nothing and to write the number of characters printed thus far to an int variable specified

Exercise sheet 7:

OS structure:

Q) Compare System call, interrupt, and trap, give examples for each of them to be triggered
1) An **interrupt** is a signal sent to the processor that interrupt (hence the name) the current execution thread. It can be generated by hardware (e.g. memory) or software.
2) A **trap** is a software generated synchronous interrupts. It may be the result of a fault (e.g. division by zero).
3) A **system call** is a way for programs to interact with the operating system. A computer program makes a system call when it makes a request to the operating system's kernel.

The Ring restrict the execution of certain type of instructions and memory accesses. MIPS architecture only have two privilege levels.

Q) What is the main role of an operating system?
A) A computer program that Multiplexes hardware resources and implements resource abstractions. It helps managing the hardware while hiding any complexity using abstractions.

Q) How can we trigger a change in modes?
A) Sleeping beauty approach: can be done through: trap, interrupts and system calls. Alarm clock approach.
Q) What happens after a trap has been invoked?
A) After handling the cause of the trap, the process returns to its previous activity.

Exercise sheet 8:

OS and Memory:

Q) Why are abstractions necessary?

A) They are there to make programming simpler. Without them user level program will have to understand the logic of every piece of hardware they may have to interact with.

Abstractions also help with portability, indeed, as long as the same interface is presented to software building upon it, the underlying implementation/hardware should not matter.

Q) Explain in your own the difference between policy and mechanism. How does this relate to abstractions?

A) A policy is a sort of "contract" describing what an interface/piece of software should do, while the mechanism is the implementation effecting this policy.

Q) What piece of hardware do threads, address spaces and files help to abstract?

A) Thread: CPU, address space: RAM, files: disk.

Q) Processes are not tied to a specific piece of hardware. What is their role?

A) They encapsulate other abstractions necessary for the execution of a task (i.e., thread, address space and files).

Q) What are inter-process and intra-process communications?

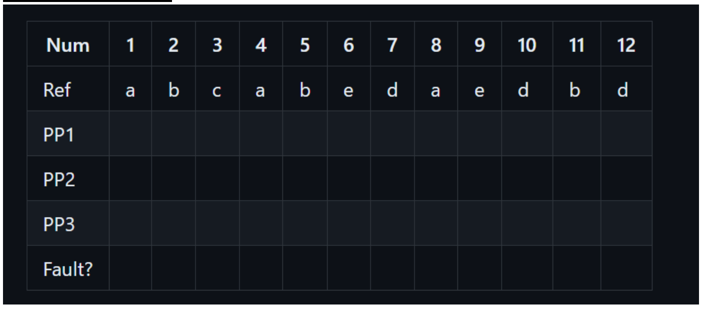
A) Intra-process communication is achieved through the use of shared memory between the thread of a given process and synchronization primitives.

Inter-process communications are used for interaction between different processes, they include pipes, sockets, message queues etc.

Q) What is a page fault?

A) Page faults occur when the virtual-physical address translation is not available in the TLB (Translation Lookaside Buffer).

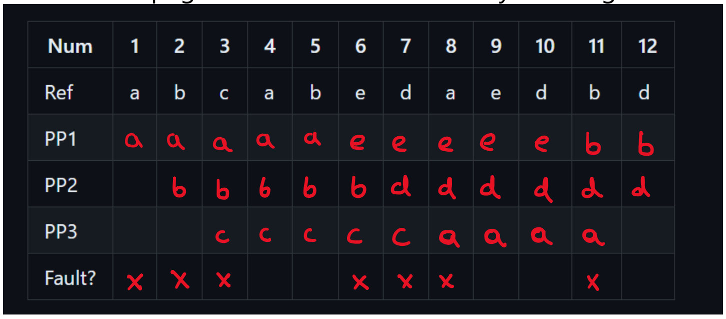
Blank Table:



Num	1	2	3	4	5	6	7	8	9	10	11	12
Ref	a	b	c	a	b	e	d	a	e	d	b	d
PP1												
PP2												
PP3												
Fault?												

FIFO replacement policy:

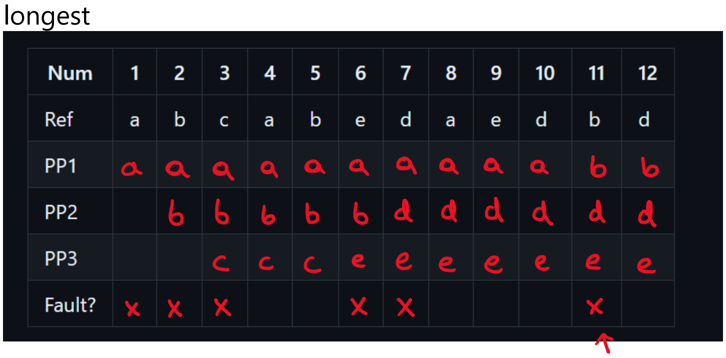
Remove the page that has been in memory the longest



Num	1	2	3	4	5	6	7	8	9	10	11	12
Ref	a	b	c	a	b	e	d	a	e	d	b	d
PP1	a	a	a	a	a	e	e	e	e	e	b	b
PP2		b	b	b	b	b	d	d	d	d	d	d
PP3			c	c	c	c	c	a	a	a	a	
Fault?	x	x	x			x	x	x			x	

MIN replacement policy:

Replace the page that will not be referenced for the longest

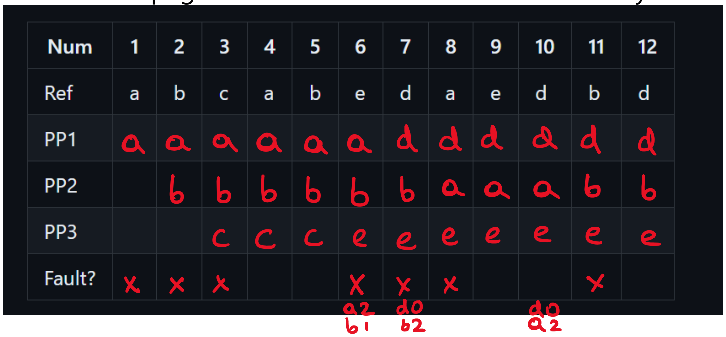


Num	1	2	3	4	5	6	7	8	9	10	11	12
Ref	a	b	c	a	b	e	d	a	e	d	b	d
PP1	a	a	a	a	a	a	a	a	a	a	b	b
PP2		b	b	b	b	b	d	d	d	d	d	d
PP3			c	c	c	e	e	e	e	e	e	e
Fault?	x	x	x			x	x				x	

↑ a or e can be replaced

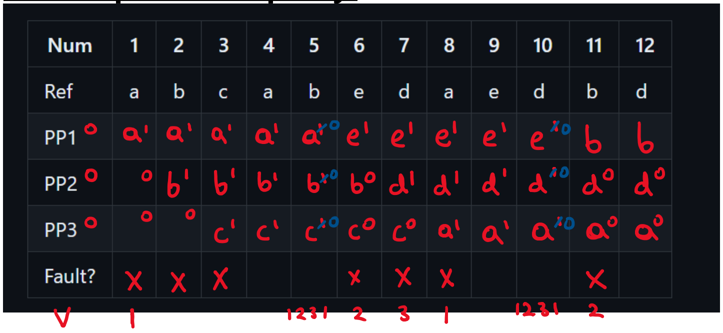
LRU replacement policy:

Remove the page that has been used the least recently



Num	1	2	3	4	5	6	7	8	9	10	11	12
Ref	a	b	c	a	b	e	d	a	e	d	b	d
PP1	a	a	a	a	a	a	d	d	d	d	d	d
PP2		b	b	b	b	b	b	a	a	a	b	b
PP3			c	c	c	e	e	e	e	e	e	e
Fault?	x	x	x			x	x	x			x	
						a2 b1 e0	d0 b2 e1			d0 a2 e1		

Clock replacement policy:



Num	1	2	3	4	5	6	7	8	9	10	11	12
Ref	a	b	c	a	b	e	d	a	e	d	b	d
PP1 ^{0}	a^1	a^1	a^1	a^1	$a^{\cancel{1}0}$	e^1	e^1	e^1	e^1	$e^{\cancel{1}0}$	b	b
PP2 ^{0}	^{0}	b^1	b^1	b^1	$b^{\cancel{1}0}$	b^0	d^1	d^1	d^1	$d^{\cancel{1}0}$	d^0	d^0
PP3 ^{0}	^{0}	^{0}	c^1	c^1	$c^{\cancel{1}0}$	c^0	c^0	a^1	a^1	$a^{\cancel{1}0}$	a^0	a^0
Fault?	X	X	X			x	X	X			X	
V	1				1231	2	3	1		1231	2	

Pseudocode:

Inputs: victim (v), page (p), number of frames (n), use bit (.ub), frames (f)

```
if page exists in frames:
  set page.ub = 1;

while victim.ub = 1:
  set victim.ub = 0;
  victim = (victim + 1) % n;

evict victim
set frames[victim] = page;
set page.ub = 1;
victim = (victim + 1) % n;
```