**Question 1 2-3-4-5**

In the context of (CIA), Critical analysis the security taxonomy and the implementation principles. Elaborate on how CIA is used in an organizational context to ensure the Need-to- know, least privilege and Separation of duties from an organizational perspective. You may use a Bank or Hospital organizational goal and security goal for your evaluation.

Answer 1

* **Need-to-know**
* Users should only have access to information (or systems) that enable them to perform their assigned job functions.
* **Least privilege**
* Users should only have sufficient access privilege that allow them to perform their assigned work.
* **Separation of duties**
* No person should be responsible for completing a task involving sensitive, valuable or critical information from the beginning to end.
* No single person should be responsible for approving his/her own work.

**Question 2**

Assess taxonomies of security such as authentication, Access control, Nonrepudiation and Privacy implementation procedures ensure an organizational security requirement

Answer 2

* **Authentication** -- Ensuring that users are the persons they claim to be
* **Access control** -- Ensuring that users access only those resources and services that they are entitled to access and that qualified users are not denied access to services that they legitimately expect to receive
* **Nonrepudiation** -- Ensuring that the originators of messages cannot deny that they in fact sent the messages[2](http://www.albion.com/security/intro-4.html)
* **Privacy** -- Ensuring that individuals maintain the right to control what information is collected about them, how it is used, who has used it, who maintains it, and what purpose it is used for.

**Question 3**

Critically analyse security from a functional view using the five distinct functional areas.

Answer 3

* **Deterrence** -- Reduces the threat to information assets through fear. Can consist of communication strategies designed to impress potential attackers of the likelihood of getting caught.
* **Prevention** -- The traditional core of computer security. Consists of implementing safeguards like the tools covered in this book. Absolute prevention is theoretical, since there's a vanishing point where additional preventative measures are no longer cost-effective.
* **Detection** -- Works best in conjunction with preventative measures. When prevention fails, detection should kick in, preferably while there's still time to prevent damage. Includes log-keeping and auditing activities
* **Recovery** -- When all else fails, be prepared to pull out backup media and restore from scratch, or cut to backup servers and net connections, or fall back on a disaster recovery facility. Arguably, this function should be attended to before the others
* **Analysing** security by function can be a valuable part of the security planning process; a strong security policy will address all five areas, starting with recovery.

**Question 4 2A**

Developed a secure network security risk strategy and measures required to be set up to carry out the task of risk management? Use either ISO 27005 or ISO 131000 standard risk management implementation procedures.

Answer 4

The scope of this approach to risk management is to enable all strategic, management and operational tasks of an organization throughout projects, functions, and processes to be aligned to a common set of risk management objectives.

**ISO 31000 Risk Management**



**Question 5 2B**

Assess the relationship between threats, vulnerabilities, and risks of an organizational assets and the countermeasures required in the event of a potential cyberattack? You may use a diagram.

Answer 5

* **Threat Agent**. An entity that may act on a vulnerability.
* **Threat**. Any potential danger to information life cycle.
* **Vulnerability**. A weakness or flaw that may provide an opportunity for a threat agent.
* **Risk**. The likelihood of a threat agent exploits the discovered vulnerability.
* **Exposure**. An instance of being compromised by a threat agent.
* **Countermeasure / safeguard**. An administrative, operational, or logical mitigation against potential risk(s).


Fig1.2.pdf                                                     00ABB570  Mnementh                      BEAE7A2F:

**Question 5 3A compulsury**

In the context of password security, critically analyse the four general means of authenticating a user’s identity from a sender and receiver perspective. Use case study and diagrams to explain your concepts.

Answer 5

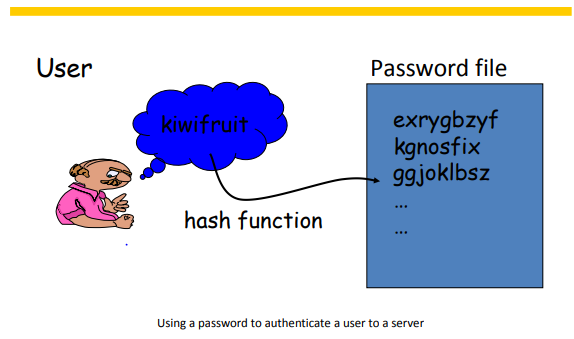
Four general means of authenticating a user’s identity

• Something the individual knows ─ E.g. password, PIN, answers to a prearranged set of questions

• Something the individual possesses ─ E.g. digital documents (digital certificate, digital key), smart cards

• Something the individual is (static biometrics) ─ E.g. recognition by fingerprint, retina, face

• Something the individual does(dynamic biometrics) ─ E.g. recognition by voice pattern, handwriting characteristics, typing rhythm.



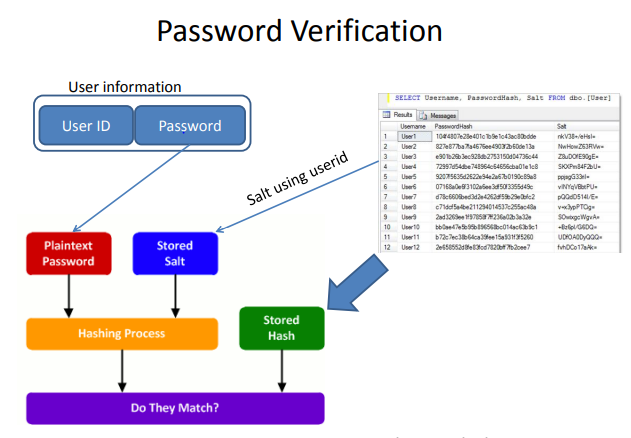
**Question 6 3b compulsary**

Analyse how a man in the middle attack technique can be deployed on each of the following. You may use a diagram to explain your techniques.

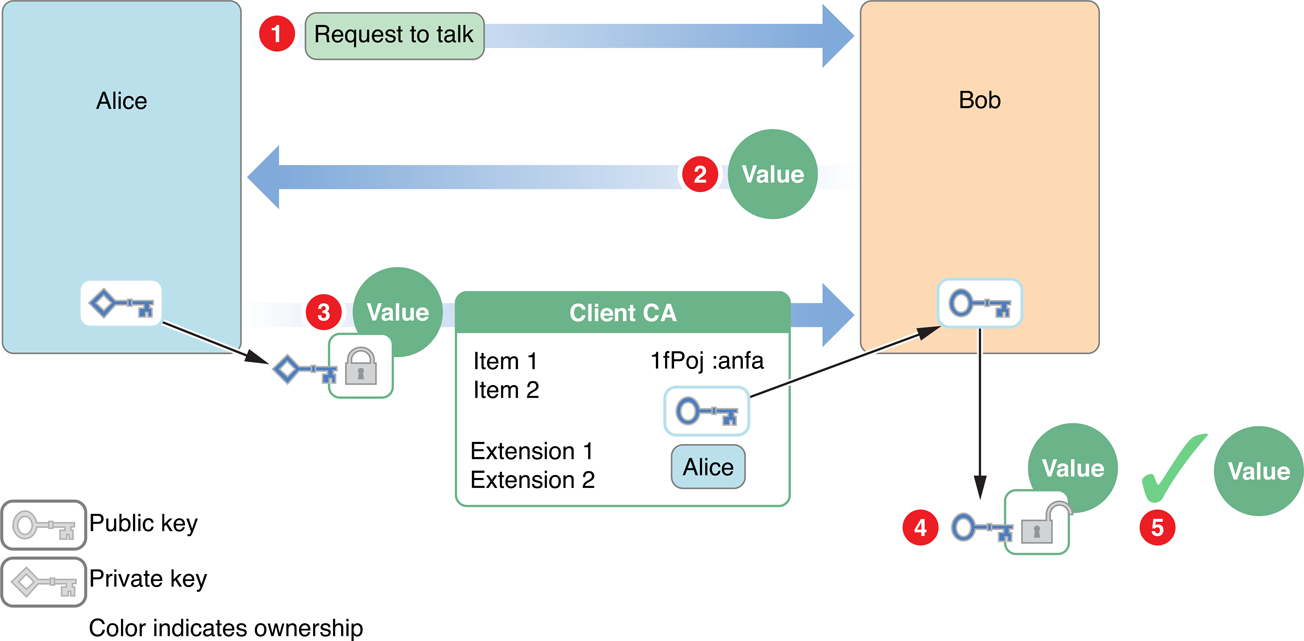
Password-based authentication (Hashed and Salt Value)

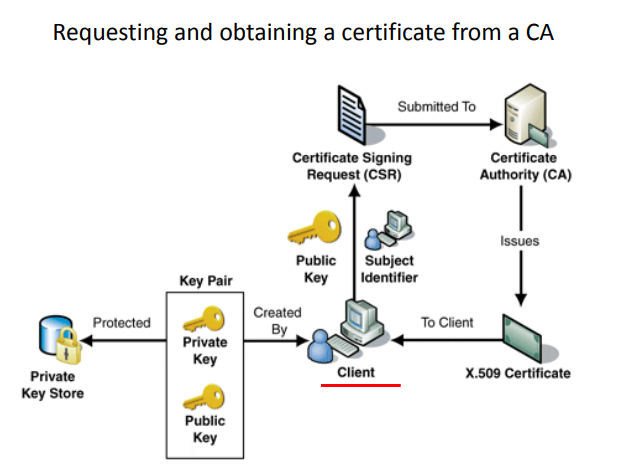
Graphical user interface, diagram

Description automatically generated with medium confidence

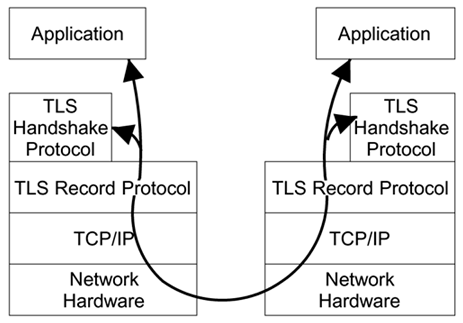


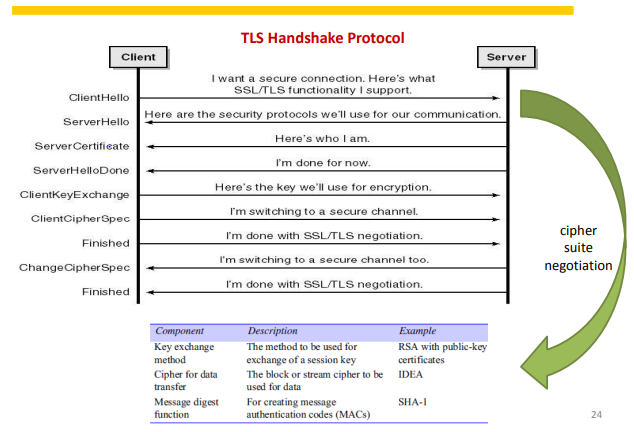
Certificate-based authentication (Public key Authentication)





SSL/TLS authentication (Client SSL, Server SSL, Certificate Authorities)



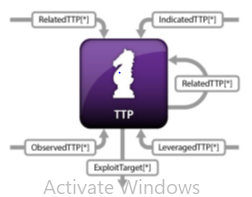


**Question 7 4A compulsay**

Analyse the Tactics, Techniques and Procedures (TTP) methods used by the cybercriminals for threat intelligence gatherings to understand adversary behaviour and courses of action? You may use an example of an attack such as using phishing malware to steal credit card credentials to explain the TTP methods.

Answer 7

* TTPs are representations of the behavior or *modus operandi* of cyber adversaries.
* It is a term taken from the traditional military sphere and is used to characterize what an adversary does and how they do it in increasing levels of detail.
  + For instance, to give a simple example, a tactic may be to use malware to steal credit card credentials.
  + A related technique (at a lower level of detail) may be to send targeted emails to potential victims, which have documents attached containing malicious code which executes upon opening, captures credit card information from keystrokes, and uses http to communicate with a command and control server to transfer information.
  + A related procedure (at a lower level of detail) may be to perform open source
    - research to identify potentially:
    - gullible individuals, craft a convincing socially engineered email and document,
    - create malware/exploit that will bypass current antivirus detection,
    - establish a command and control server by registering a domain
      * Called mychasebank.org, and send mail to victims from a Gmail account
      * called [accounts-mychasebank@gmail.com](mailto:accounts-mychasebank@gmail.com).



**Question 8 4B compulsary**

With the aid of a diagram, implement the seven-stage Cyber Attack Lifecycle of the Kill chain attack model. Use the case study of the phishing email for stealing credit cards credentials.

**Answer 8**

**A picture containing logo

Description automatically generated**

**Question 9 4C compulsary**

Critically analyse the seven kill chain prevention mechanisms in line with cybersecurity controls. Explain the techniques in your own words of how the model can be used to better characterize and describe the post-compromise adversary behaviour and to prevent the attack steps.

Answer 9

Timeline

Description automatically generated

**Question 10 5A optional**

With the aid of a diagram, implement the six processes using the techniques in digital forensics investigations?

Answer 10

Preservation, Identification, Transport, Acquisition /Extraction, Documentation of digital evidence and Report Writing

Diagram

Description automatically generated

**Question 11 5B optional**

Assess why the following digital forensic investigations concepts are important to ensure that digital evidence is admissible in court?

Answer 11

Authentic, Accurate, Complete, and Convincing to juror

* Authenticity: Does the evidential material come from where it claim to come from?
* Accurate: Can the substance of the story the material tells or be believed and is it consistent?
  + In the case of computer derived material, are there reasons for doubting the correct working of the computer.
* Completeness: Is the story that the material claims to tell complete? Are there other stories that the material also tells that might have a bearing on the legal dispute or hearing.
* Convincing to jurors: Evidences must be freedom from interference and contamination. Are these evidences and levels acceptable as a result of forensic investigation and other post event handling.

**Question 12 5C optional**

A cyberattack incident occurred and the criminal was suspected to have used the computer to have committed cybercrimes. The Internet history on the computer included a Google search “how to hack into a system”

As a digital forensic investigator working as part of a cyber incident response team, use the major approaches such as the system preservation phase, evidence searching phase and event reconstruction phase to explain the investigation processes that are used to find evidence and arrive at a conclusion?

You are to use the investigation techniques in the major phases of the incident response process as follows.

1. Identify the type of crime scene to be investigated e.g., Dead or Life Analysis
2. PreserveEvidence
3. Acquisition Methods
4. Evidence Search methods
5. Analysis methods

Answer 12

1. Answer : Type of crime scene

**Digital Forensic Crime Scene Investigation Process:**

* There is no single way to conduct an investigation.
  + Everyone has a point of view
  + Different investigators may use different approach
* These processes can be used when investigating both live and dead systems.
  + A live analysis occurs when you use the operating system or other resources of the system being investigated to find evidence.
  + With a live analysis, you risk getting false information because the software could maliciously hide or falsify data.
* A dead analysis occurs when you are running trusted applications in a trusted operating system to find evidence
  + A dead analysis is more ideal but is not possible in all circumstances.

1. Preserve evidence answer:

In acquisition phase where we try to preserve the state of the digital crime scene

* The actions that are taken in this phase vary depending on the legal, business, or operational req of the investigation
* For example, legal requirements may cause you to unplug the system and make a full copy of all data.

* On the other extreme could be a case involving a spyware infection or a **honeypot**
* The purpose of this phase is to reduce the amount of evidence that may be overwritten
* This process continues after data has been acquired from the system because we need to preserve the data for future analysis and search for evidence
* Never work off the original image; create a backup for analysis.
* Before working on a backup, hash it. Keep the original evidence in a safe.
* Create a log of everyone who has access to the original evidence and copies.
* Make notes of all findings, especially important ones.
* Save often to prevent data losses in case of power outages
* The focus of a digital investigation is going to be some type of digital device that has been involved in an incident or crime.

1. Acquisition methods :

* A digital investigation is a process where we develop and test hypotheses (theory) that answer questions about digital events.
* This is done using the scientific method where we:
  + Develop a hypothesis using evidence that we find and
  + Then test the hypothesis by looking for additional evidence that shows the hypothesis is impossible.

1. Evidence search methods :

The theory behind the searching process involves two keys

**Two Key steps:**

* We **define** the general characteristics of the object for which we are searching
* And then **look for that object** in a collection of data.
  + For example, if we want all files with the JPG extension, we will look at each file name and identify the ones that end with the characters ".JPG."

1. Analysis methods :

**Analyzing Network Data**

* When analyzing network data, we may search for all packets from a specific source address or all packets going to a specific port.
* We also may want to find packets that have a certain keyword in them.

**Network Traffic Analysis**

**Question 13 6A optional**

In the context of cyber security and digital forensics investigations, critically evaluate the roles computers can play in a cybercrime analysis?

Answer :

**A computer can play one of three roles in a computer crime:**

* A computer can be the **target** of the crime
* It can be the **instrument** of the crime
* Or it can serve as an **evidence repository storing valuable information** about the crime.

**Question 14 6B**

In the context of cyberattacks and cyber threat intelligence gatherings, evaluate the attack concepts using the “Method, Opportunity and Motive” (MOM) approach that is used by cybercriminals to deploy cyberattacks.

**Question 15 6C**

Digital Forensics Investigations guidelines require that we follow technical procedures such as preservation, isolation, correlation, and logging (PICL) during the investigation process. Use the PICL procedures and techniques to implement an investigation at a crime scene.