Q. 19 Write short note on Hosting, Hardware, Firmware and Other Invisible Threats. (Refer Section 4.9) **(5 Marks)**

Q. 20 What are the benefits of Personas? (Refer Section 4.9.2) **(5 Marks)**

Q. 21 Explain Privacy Management Reference Model with suitable diagram. (Refer Section 4.10.1) **(5 Marks)**

Q. 22 Explain OSA with suitable diagram. (Refer Section 4.11) **(5 Marks)**

Q. 23 Write short note on SAMM. (Refer Section 4.12) **(5 Marks)**

Q. 24 Explain SDLC with suitable diagram. (Refer Section 4.13) **(5 Marks)**

Q. 25 Explain IoT threat model with suitable diagram. (Refer Section 4.14) **(5 Marks)**

Q. 26 Explain DDOS. (Refer Section 4.17) **(5 Marks)**

Syllabus Topic : International Standards for Operating System Security

Q. 27 Write short note on International Standards for Operating System Security. (Refer Section 4.18) **(5 Marks)**

Chapter Ends...

❑❑❑

CHAPTER 5 — Unit V

Virtual Machines and Cloud Computing

Syllabus Topic : Virtual Machines

5.1 Virtual Machines

Q. 5.1.1 Explain virtual machines and give its advantages and drawbacks. (Ref. Sec. 5.1) **(5 Marks)**

- A virtual machine is a computer file, typically called an image, which behaves like an actual computer. In other words, creating a computer within a computer.
- It runs in a window, much like any other programme, giving the end user the same experience on a virtual machine as they would have on the host operating system itself.
- The virtual machine is sandboxed from the rest of the system, meaning that the software inside a virtual machine cannot escape or tamper with the computer itself. This produces an ideal environment for testing other operating systems including beta releases, accessing virus-infected data, creating operating system backups and running software or applications on operating systems for which they were not originally intended.
- Multiple virtual machines can run simultaneously on the same physical computer. For servers, the multiple operating systems run side-by-side with a piece of software called a hypervisor to manage them, while desktop computers typically employ one operating system to run the other operating systems within its programme windows. Each virtual machine provides its own virtual hardware, including CPUs, memory, hard drives, network interfaces and other devices.
- The virtual hardware is then mapped to the real hardware on the physical machine which saves costs by reducing the need for physical hardware systems along with the associated maintenance costs that go with it, plus reduces power and cooling demand.

- A Virtual Machine (VM) is a software program or operating system that not only exhibits the behavior of a separate computer, but is also capable of performing tasks such as running applications and programs like a separate computer.
- A virtual machine, usually known as a guest is created within another computing environment referred as a "host". Multiple virtual machines can exist within a single host at one time.
- A virtual machine is also known as a guest.
- Virtual machines are becoming more common with the evolution of virtualization technology. Virtual machines are often created to perform certain tasks that are different than tasks performed in a host environment.
- Virtual machines are implemented by software emulation methods or hardware virtualization techniques. Depending on their use and level of correspondence to any physical computer, virtual machines can be divided into two categories:

1. System Virtual Machines
2. Process Virtual Machine

1. System Virtual Machines

- A system platform that supports the sharing of the host computer's physical resources between multiple virtual machines, each running with its own copy of the operating system.
- The virtualization technique is provided by a software layer known as a hypervisor, which can run either on bare hardware or on top of an operating system.

2. Process Virtual Machine

- Designed to provide a platform-independent programming environment that masks the information of the underlying hardware or operating system and allows program execution to take place in the same way on any given platform.

Some of the advantages of a virtual machine include :

- Allows multiple operating system environments on a single physical computer without any intervention.
- Virtual machines are widely available and are easy to manage and maintain.
- Offers application provisioning and disaster recovery options.

Some of the drawbacks of virtual machines include :

- They are not as efficient as a physical computer because the hardware resources are distributed in an indirect way.
- Multiple VMs running on a single physical machine can deliver unstable performance

Syllabus Topic : Cloud Computing

5.2 Cloud Computing

Q. 5.2.1 Write short note on cloud computing and explain its services. (Ref. Sec. 5.2) **(5 Marks)**

- Cloud Computing provides us means by which we can access the applications as utilities over the internet. It allows us to create, configure, and customize the business applications online.
- Cloud computing is the use of various services, such as software development platforms, servers, storage and software, over the internet, often referred to as the "cloud".
- In general, there are three cloud computing characteristics that are common among all cloud-computing vendors:
  1. The back-end of the application (especially hardware) is completely managed by a cloud vendor.
  2. A user only pays for services used (memory, processing time and bandwidth, etc.).
  3. Services are scalable
- Many cloud computing advancements are closely related to virtualization. The ability to pay on demand and scale quickly is largely a result of cloud computing vendors being able to pool resources that may be divided among multiple clients.
- It is common to categorize cloud computing services as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS).

5.2.1 Software as a Service (SaaS)

Cloud-based applications - or software as a service - run on distant computers "in the cloud" that are owned and operated by others and that connect to users' computers via the internet and, usually, a web browser.

The benefits of SaaS

- You can sign up and rapidly start using innovative business apps.
- Apps and data are accessible from any connected computer.

- No data is lost if your computer breaks, as data is in the cloud.
- The service is able to dynamically scale to usage needs.

5.2.2 Platform as a Service (PaaS)

Platform as a service provides a cloud-based environment with everything required to support the complete lifecycle of building and delivering web-based (cloud) applications - without the cost and complexity of buying and managing the underlying hardware, software, provisioning, and hosting.

The benefits of PaaS

- Develop applications and get to market faster.
- Deploy new web applications to the cloud in minutes.
- Reduce complexity with middleware as a service.

5.2.3 Infrastructure as a Service (IaaS)

Infrastructure as a service provides companies with computing resources including servers, networking, storage, and data center space on a pay-per-use basis.

The benefits of IaaS

- No need to invest in your own hardware.
- Infrastructure scales on demand to support dynamic workloads.
- Flexible, innovative services available on demand.

5.2.4 Comparison between IaaS, PaaS and SaaS

Q. 5.2.2 Give comparison between IaaS, PaaS and SaaS. (Ref. Sec. 5.2.4) **(5 Marks)**

Features	IaaS	PaaS	SaaS
What is offered	Users get the infrastructure such as virtual machines, load balancers, IP addresses and firewalls for them to create a platform, which it can use to test applications.	Users get a work environment on-demand. A platform made of software, hardware, and operating systems. It is a platform where new codes can be added for the development of the end product on a use & pay basis.	The user gets a ready to use package. The user just needs to install it on their systems and start using it. The pre-configured package is as per user requirement, and the user may or may not have to pay to use the services provided.

Features	IaaS	PaaS	SaaS
Importance	Basic layer of cloud computing useful for administrators.	The middle layer of cloud computing that enables development of applications.	The final product, ready to use package.
Technicalities Involved	Deep technical knowledge required. IaaS is the basic layer and if not built strongly, it will not be able to support the further development of the service.	Medium technical know-how necessary for further development of the service takes place in this layer. Proper knowledge of coding and application development is essential to eliminate any possible bugs.	No technical knowledge required. It is the end product. The end-user just needs to use the product that has been created. The SaaS provider handles all the technical aspects of the product.
Deals with	Servers, Load Balancers, Network arrays, virtual machines, storage disks.	Java Runtimes, databases like Oracle and Web Servers.	Applications like Gmail, Yahoo mail. Dropbox and Google Drive services.
Popularity Graph	Used mostly by highly experienced and skilled developers. Custom configuration according to their field of research.	Medium-skilled developers use the platform and the favorable work environment to develop their own applications. Developers don't need to worry about traffic loads or server management.	Most popular amongst users of emails and entertainment stream services. Users don't need to worry about technicalities. Users simply enjoy the end product or service.
Examples	Cisco Metapod, Amazon Web Services, Microsoft Azure	Apprenda, Google App engine, Heroku	Google Apps, Cisco WebEx, Workday

Syllabus Topic : Secure Development Lifecycle

5.3 Secure Development Lifecycle

Q. 5.3.1 Explain Secure Development Lifecycle. (Ref. Sec. 5.3) **(10 Marks)**

- The Secure Development Lifecycle is a different way to build products; it places security front and center during the product or application development process.

- From requirements to design, coding to test, the SDL strives to build security into a product or application at every step in the development process. A modern application company cannot survive without getting serious about security, and the way to get serious is to integrate an SDL into your everyday work.
- Customers demand secure products out of the box, so security should be a top priority that should be top of mind for everyone. But without a standard approach to security, it is almost impossible to deliver on the customers' expectations. That's where the Secure Development Lifecycle (SDL) comes in.
- SDL is a process. If you look at the many SDLs that exist across industries, you'll find that most include the same basic security phases and activities. They may have different names for the pieces, but everyone follows roughly the same process.
- Here's an essential guide to placing security front and center.

5.3.1 Defining the Secure Development Lifecycle

- In its simplest form, the SDL is a process that standardizes practices across a range of products and/or applications. It captures industry-standard security activities, packaging them so they may be easily implemented. The software development lifecycle consists of several phases, which I will explain in more detail below.
- The SDL was unleashed from within the walls of Microsoft, as a response to the famous Bill Gates memo of January 2002. In it Gates laid out the requirement to build security into Microsoft's products. He admitted that due to various virus and malware outbreaks, Microsoft had to embed security if it was to be taken seriously in the marketplace.
- This resulted in the Microsoft Trustworthy Computing endeavor, out of which the idea of SDL was born. Microsoft made the SDL mandatory in 2004, and a cottage industry was unleashed.
- Many other companies, including Cisco, Adobe, and Aetna, have since adopted Microsoft's SDL processes or created their own. And Microsoft has been gracious over the years in sharing its SDL successes with other companies and releasing many of its materials and tools as open source.

5.3.2 The Problems the SDL Solves

- The lack of a standard approach to securing products causes problems. For one thing, vulnerabilities run rampant in shipped products. The triage and response needed to deal with this are major resource sinks. As a result, developers spend too much time fixing code they wrote in the past and not enough focusing on the future.

- The second problem is that developers tend to repeat the same security mistakes, each time expecting a different response (which is the definition of insanity). The third issue is that problems are found at release or after deployment, beyond the reasonable time when the problems could be mitigated in an inexpensive manner.
- Finally, without a security standard customers have no assurance that a given product is secure. A single product considered for purchase may be one of the good ones, or it might be terrible from a security perspective.
- Without an SDL, there is no product security parity across the company. And without a standard process, some product teams ignore security altogether.

5.3.3 People, Process and Technology

- The SDL is a process with different phases that contain security activities that sits inside of the classic people-process-technology triangle. The SDL forms the process portion.
- It includes both the central security team that governs the process and updates it and the product or development teams that perform security activities.
- The technology portion consists of tools that assist in finding vulnerabilities in source code or discovering vulnerabilities in a running instance of the product or application.
- The SDL is methodology-neutral. Security activities fit within any product development methodology, whether waterfall, agile, or DevOps. Methodology differences show up in the cadence of security activities.
- The SDL was developed during the time of waterfall, so it is usually portrayed as a linear process that begins with requirements and ends with the release.
- When the SDL is extended to agile, some security activities get integrated into the normal sprint schedule, while others are pursued out-of-band. With DevOps, activities are embedded into the build pipeline using automation, while additional activities happen outside the pipeline.

5.3.4 SDL Phases

Q. 5.3.2 Enlist SDL phases and explain them. (Ref. Sec. 5.3.4) **(5 Marks)**

- An SDL is divided into phases that tie closely into the waterfall approach. The standard approach to SDL includes requirements, design, implementation, test, and release/response.

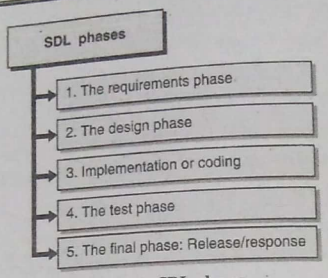

Fig. 5.3.1 : SDL phases

5.3.4.1 The Requirements Phase

- In the requirements phase, best practices for security are integrated into a product. These practices may come from industry standards or be based on responses to problems that have occurred in the past.
- Requirements exist to define the functional security requirements implemented in the product, and include all the activities of the SDL. They are used as an enforcement point to ensure that all pieces are properly considered.
- Requirements may take the classic form, stating that the product or application must, may, or should, do something. One example might be that the product must enforce a minimum password length of eight characters.
- In the agile world, requirements are expressed as user stories. These stories contain the same information as do the requirements, but security functionality is written from the user's perspective.

5.3.4.2 The Design Phase

- The design phase of the SDL consists of activities that occur (hopefully) prior to writing code. Secure design is about quantifying an architecture (for a single feature or the entire product) and then searching for problems. Secure design could occur in a formal document or on a napkin.
- With many systems, the plane is in the air as the wings are being designed, but the SDL can survive even this craziness. The key is to use threat modeling.
- Threat modeling is the process of thinking through how a feature or system will be attacked, and then mitigating those future attacks in the design before writing the code.

- Threat modeling is akin to perceiving crimes prior to their occurrence, as in the 2002 movie **Minority Report.**
- A solid threat model understands a feature's or product's attack surface, then defines the most likely attacks that will occur across those interfaces. A threat model is only as good as the mitigations it contains to fix the problems. But it is crucial to identifying security issues early in the process.

5.3.4.3 Implementation or Coding

- The next phase is implementation, or writing secure code. The SDL contains a few things programmers must do to ensure that their code has the best chance of being secure. The process involves a mixture of standards and automated tools.
- On the standards front, a solid SDL defines a secure coding guide (such as those published by SEI CERT for C, C++ and Java), that defines what is expected and provides guidance for when developers hit a specific issue and need insight.
- Implementation tools include Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) software. SAST is like a spell-checker for code, identifying potential vulnerabilities in the source code.
- SAST runs against a nightly build or may be integrated into your IDE. It may find and open new bugs in the bug management system nightly or prompt the developer to pause while coding to fix a problem in real time.
- DAST checks the application's runtime instantiation. It spiders through an application to find all possible interfaces and then attempts to exploit common vulnerabilities in the application. These tools are primarily used on web interfaces.

5.3.4.4 The Test Phase

- Formal test activities include security functional test plans, vulnerability scanning, and penetration testing. Vulnerability scanning uses industry-standard tools to determine if any system-level vulnerabilities exist with the application or product.
- Penetration testing involves testers attempting to work around the security protections in a given application and exploit them.
- Pen testing stretches the product and exposes it to testing scenarios that automated tools cannot replicate. Pen testing is resource-intensive, so it's usually not performed for every release.

5.3.4.5 The Final Phase : Release/Response

- Release occurs when all the security activities are confirmed against the final build and the software is sent to customers (or made available for download). Response is the interface for external customers and security researchers to report security problems in products.
- Part of the response should include a product security-incident response team that focuses on triaging and communicating product vulnerabilities, both individual bugs and those that will require industry-wide collaboration (e.g. Heartbleed, Bash bug, etc.).
- Other security activities are also crucial for the success of an SDL. These include security champions, bug bounties, and education and training.

Syllabus Topic : Application Security Practices

5.4 Application Security Practices

- IT security, it used to be said, resembles a certain type of candy: hard on the outside, and soft on the inside. This metaphor depicts the security approach that focuses on hardening the perimeter of the data center to prevent intrusion by external malefactors, while assuming that access by employees is benign and therefore does not require specific protective measures.
- If that metaphor was ever appropriate, it is certainly no longer tenable in today's world when you consider that :
  - Most application access comes from outside the company's perimeter, with a heterogeneous user mix of employees, customers, and partners. While some IT organizations assume that VPN use makes applications more secure, in one sense that is a false belief, since VPNs typically bypass many perimeter protections and offer direct access to applications.
  - This access comes from a bewildering array of devices. Moreover, individual users may use several different devices to access applications, depending on where they happen to be when using them. For example, an employee may access an application from a laptop while sitting in a coffee shop, and then use a mobile phone later to access it from a customer site.
  - The looming IoT explosion means many users will access applications with no ability to present a password for authentication.

5.4.1 Recommendations for App-Focused Security

Q. 5.4.1 Write short note on Recommendations for App-Focused Security. (Ref. Sec. 5.4.1) **(5 Marks)**

- For these reasons, enterprise IT must move to a new security approach, one that can address the new reality of next-generation applications.
- All this doesn't mean security isn't important, or that it should be short-changed in the urgency of creating a digital enterprise. Far from it. Security is, if anything, more important in this new world.
- The truth is that IT's role is changing dramatically, from being a back-office process automation function to deploying applications that are the primary way the enterprise conducts its business.
- Security failures now represent threats to the company's customer and employee relationships, brand, and even stock market valuation. Just witness the carnage left by the Target and Sony hacks.
- Given the importance of security, then, along with the changing conditions in which IT security must operate, what are best practices that IT organizations should pursue to meet their security responsibilities? Here are seven recommendations for application-focused security :

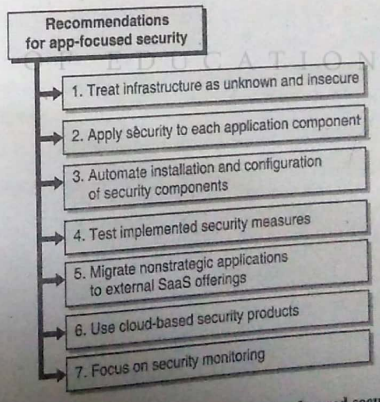

Fig. 5.4.1 : Recommendations for application focused security

1. Treat infrastructure as unknown and insecure

- This should be obvious, but since cloud providers are commonly rather opaque with regard to their security practices, the default position for enterprises should be to assume that their applications must implement enough measures to suffice for complete security. By the way, this isn't a bad approach for on-premises environments, either.
- As the Target and Sony examples illustrate, corporate security measures may be inadequate, so implementing application-level measures is appropriate. In any case, it's often unknown during development exactly where the application will be deployed, so implementing security measures that do not assume security capabilities for a particular environment is a good idea.

2. Apply security to each application component

- Analyze each component to determine what security measures are appropriate for it. Certain components (e.g., program execution resources) will require intrusion detection/prevention systems. Others (e.g., database or storage) will require access controls that prevent non-application components from touching data elements.
- Of course, network access controls that allow only approved users or application components from sending traffic to other parts of an application are critical (this latter area is rife with issues, as configurations are left too open for the application life cycle stage (i.e., during development it may be appropriate to maintain a very open component firewall configuration) but when an application moves to final staging or into production, firewall access should be constricted so that only appropriate traffic sources can access application resources.

3. Automate installation and configuration of security components

- This is difficult but critical. The lengthy audit, recommendation, and installation/configuration processes that were acceptable in the past are completely inadequate for next-generation applications.
- Worse, manual processes are subject to human error in execution and may be bypassed by a sense of urgency and business pressure. While the move to automation is a challenge, most security organizations find the new approach an improvement. automation ensures that recommended measures are implemented consistently, avoiding difficult-to-find security holes.

4. Test implemented security measures

- Too often, inspection and validation of security as implemented often gets overlooked. Penetration testing is a foundation for testing security and can provide valuable feedback on areas that need to be addressed. If you are running on Amazon Web Services, you may be able to use the open source Security Monkey tool that Netflix has made available.
- It goes through an application topology and evaluates whether its resources have implemented the organization's security measures. Many IT organizations contract with external parties to test application security measures. That's a good idea, since it provides an opportunity for impartial evaluation of application security and is likely to identify security gaps that internal personnel might overlook.

5. Migrate nonstrategic applications to external SaaS offerings

- IT security teams are often overworked and under-resourced. One good way to reduce their work scope is to offload nonstrategic applications to someone else, thereby enabling them to focus their efforts on truly important applications.
- For example, email (a common hacker target) will almost certainly be more secure if operated by a specialist provider. Why not let it take responsibility for security?

6. Use cloud-based security products

- One of the biggest impediments to good IT security practices is the lack of staff and budget to purchase and use appropriate products. SaaS-based security offerings provide two benefits.
- They do not require large capital investment to pay up-front license fees, and they do not necessitate IT staff to install and configure the products. Instead, IT staff can focus on configuration and use, and the lower cost of cloud-based services means security budgets go further.

7. Focus on security monitoring

- The new world of next-generation applications means many more resources must be tracked and protected. Configuring security settings to generate alerts is critical; it can be a delicate balancing act to get the configuration correct so that important alerts are not hidden in a blizzard of unimportant data.

- This typically requires ongoing assessment and configuration updates, along with use of tools to display security anomalies and send important alerts to staff so that security issues can be addressed immediately.
- It may seem as though next-generation applications impose uncomfortable change and complexity on traditional security practices. That's no doubt true, but it's also irrelevant.
- There is a new IT world emerging, and yesterday's approach to security is incapable of performing its duties. Only by moving to an updated approach to security can IT organizations uphold their responsibilities in a next-generation application era.

Syllabus Topic : Web Application Security

5.5 Web Application Security Best Practices

Q. 5.5.1 Explain web application security practices in detail. (Ref. Sec. 5.5) **(5 Marks)**

- As you can see, if you're part of an organization, maintaining web application security best practices is a team effort. There are certainly immediate steps you can take to quickly and effectively improve the security of your application.
- However, as applications grow, they become more cumbersome to keep track of in terms of security. Putting the proper web application security best practices in place, as outlined in the list above, will help ensure that your applications remain safe for everyone to use.
- Like any responsible website owner, you are probably well aware of the importance of online security. You may think that you have your ducks in a row in this department, but like many other website owners and companies, there probably hasn't been enough done to secure your web application(s).
- If your website was affected by the massive DDoS attack that occurred in October of 2016, then you'll know that security is a major concern, even for large DNS companies like Dyn. As shown below, the number of DDoS attacks have consistently grown over the past few years and are expected to continue growing. **(Source : Easy dns)**
- Although there is no way to guarantee complete 100% security, as unforeseen circumstances can happen **(Source : Evident by the Dyn attack)**.
- However, there are methods that companies can implement to help reduce the chance of running into web application security problems. There is various web applications security best practices to keep and mind as you harden your web security.

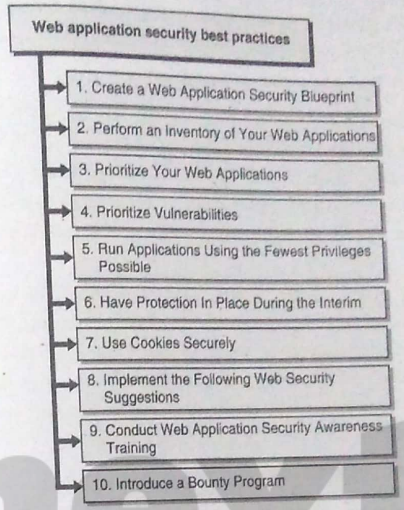

Fig. 5.5.1 : Web application security best practices

➜ 1. Create a web application security blueprint

- You can't hope to stay on top of web application security best practices without having a plan in place for doing so. All too often, companies take a disorganized approach to the situation and end up accomplishing next to nothing. Sit down with your IT security team to develop a detailed, actionable web application security plan. It should outline your organization's goals.
- For example, perhaps you want to enhance your overall compliance, or maybe you need to protect your brand more carefully. It should also prioritize which applications should be secured first and how they will be tested. Whether you choose to do so manually, through a cloud solution, through software that you have on site, through a managed service provider or through some other means.
- Although each company's security blueprint or checklist will differ depending on their infrastructure, Cigital created a fairly detailed 6 step web application security checklist you can reference as a starting point.
- Additionally, if your organization is large enough, your blueprint should name the individuals within the organization who should be involved in maintaining web

application security best practices on an ongoing basis. Finally, be sure to factor in the costs that your organization will incur by engaging in these activities.

➜ **2. Perform an inventory of your web applications**

- Organized as though you think your company may be, you probably don't have a very clear idea about which applications it relies on on a daily basis. In fact, most organizations have many rogue applications running at any given time and never notice them until something goes wrong. You can't hope to maintain effective web application security without knowing precisely which applications your company uses.
- How many are there? Where are they located? Performing such an inventory can be a big undertaking, and it is likely to take some time to complete. While performing it, make a note of the purpose of each application. Chances are that when it is all said and done, there will be many applications that are either redundant or completely pointless. This inventory will come in handy for the steps that are to follow too, so take your time and make sure to get every single application.

➜ **3. Prioritize your web applications**

- After completing the inventory of your existing web applications, sorting them in order of priority is the logical next step. You may doubt it now, but your list is likely to be very long. Without prioritizing which applications to focus on first, you will struggle to make any meaningful progress.
- Sort the applications into three categories :

(i) Critical
(ii) Serious
(iii) Normal

➜ **(i) Critical applications**

Critical applications are primarily those that are externally facing and contain customer information. These are the applications that should be managed first, as they are the most likely to be targeted and exploited by hackers.

➜ ***(ii) Serious applications***

Serious applications may be internal or external and may contain some sensitive information.

➜ **(iii) Normal applications**

Normal applications have far less exposure, but they should be included in tests down the road.

- By categorizing your applications like this, you can reserve extensive testing for critical ones and use less intensive testing for less critical ones. This allows you to make the most effective use of your company's resources and will help you achieve progress more quickly.

➜ **4. Prioritize vulnerabilities**

- As you work through the list of web applications prior to testing them, you need to decide which vulnerabilities are worth eliminating and which aren't too worrisome.
- The fact of the matter is that most web applications have many vulnerabilities. For instance, take a look Sucuri's Q2 hacked websites report which analyzed 9000 infected websites and categorized them by platform.
- Eliminating all vulnerabilities from all web applications just isn't possible or even worth your time. Even after categorizing your applications according to importance, it will take considerable amounts of time to test them all.
- By limiting yourself to testing for only the most threatening vulnerabilities, you will save a ton of time and will get through the work a lot more quickly.
- As far as determining which vulnerabilities to focus on, that really depends on the applications you're using. There are a few standard security measures that should be implemented (discussed further below) however applications-specific vulnerabilities need to be researched and analyzed.
- Keep in mind as well that as testing unfolds, you may realize that you have overlooked certain issues. Don't be afraid to put the testing on hold in order to regroup and focus on additional vulnerabilities. Finally, remember that in the future, this work will be much easier, as you are starting from scratch now and won't be later.

➜ **5. Run applications using the fewest privileges possible**

- Even after all of your web applications have been assessed, tested and purged of the most problematic vulnerabilities, you aren't in the clear. Every web application has specific privileges on both local and remote computers. These privileges can and should be adjusted to enhance security.

- Always use the least permissive settings for all web applications. This means that applications should be buttoned down. Only highly authorized people should be able to make system changes and the like.
- You might consider including this in your initial assessment. Otherwise, you will have to go back down the entire list adjusting settings again. For the vast majority of applications, only system administrators need complete access. Most other users can accomplish what they need with minimally permissive settings.
- In the unlikely event that privileges are adjusted incorrectly for an application and certain users can't access the features that they need, the problem can be handled when it occurs. It is far better to be too restrictive in this situation than to be too permissive.

➜ **6. Have protection in place during the interim**

- Even if you run a small and fairly simple organization, it may take weeks or even months to get through the list of web applications and to make the necessary changes.
- During that time, your business may be more vulnerable to attacks. Therefore, it is crucial to have other protections in place in the meantime to avoid major problems. For this you have a couple of options :
  - Remove some functionality from certain applications. If the functionality makes the application more vulnerable to attacks then it may be worth it to remove said functionality in the meantime.
  - Use a Web Application Firewall (WAF) to protect against the most troubling vulnerabilities.
  - A WAF filters and blocks unwanted HTTP traffic going to a web application and helps protect against XSS, SQL injection, and more.
- Throughout the process, existing web applications should be continually monitored to ensure that they aren't being breached by third parties. If your company or website suffers an attack during this time, identify the weak point and address it before continuing with the other work.
- You should get into the habit of carefully documenting such vulnerabilities and how they are handled so that future occurrences can be dealt with accordingly.

➜ **7. Use cookies securely**

- Another area that many organizations don't think about when addressing web application security best practices is the use of cookies. Cookies are incredibly convenient for businesses and users alike.
- They allow users to be remembered by sites that they visit so that future visits are faster and, in many cases, more personalized. However, cookies can also be manipulated by hackers to gain access to protected areas.
- While you certainly don't have to stop using cookies - indeed, to do so would be a major step backward in many ways - you should adjust the settings for yours to minimize the risk of attacks.
  1. First, never use cookies to store highly sensitive or critical information. For example, don't use cookies to remember users' passwords, as this makes it incredibly easy for hackers to gain unauthorized access.
  2. You should also be conservative when setting expiration dates for cookies. Sure, it's nice to know that a cookie will remain valid for a user for months on end, but the reality is that each one presents a security risk.
  3. Finally, consider encrypting the information that is stored in the cookies that you use.

➜ **8. Implement the following web security suggestions**

- Besides what we've already outlined in this post, there are a few other more "immediate" web application security suggestions that you can implement as a website or business owner. To learn more about each suggestion below, read the dedicated article pertaining to that topic and see if implementing each security enhancement is beneficial for your particular use-case.
  - Implement HTTPS and redirect all HTTP traffic to HTTPS.
  - Help prevent cross-site scripting attacks by implementing the x-xss-protection security header.
  - Implement a content security policy.
  - Help prevent man in the middle attacks by enabling public key pins.
  - Apply subresource integrity to your resource's <script> or <link> elements.

- Use an updated version of TLS. To learn more, read our TLS 1.2 vs TLS 1.1 article and avoid using SSL completely.
- This goes without saying, use strong passwords that employ a combination of lowercase and uppercase letters, numbers, special symbols, etc. Use a program such as KeyPass to generate and store strong passwords.

➜ **9. Conduct web application security awareness training**

- If you run a company, chances are that only certain people within your organization have a decent grasp of the importance of web application security and how it works. The majority of users have only the most basic understanding of the issue, and this can make them careless. This is also problematic because uneducated users fail to identify security risks.
- By educating employees, they will more readily spot vulnerabilities themselves. In essence, bringing everyone up to speed about web application security is a terrific way to get everyone in on the act of finding and eliminating vulnerabilities.
- With this in mind, consider bringing in a web application security specialist to conduct awareness training for your employees.
- By bringing everyone on board and making sure that they know what to do if they encounter a vulnerability or other issue, you can strengthen your overall web application security process and maintain the best possible web application security best practices.

➜ **10. Introduce a bounty program**

- A great way to get feedback from the community regarding potential web application security issues is to introduce a bounty program. Even if you run a company with dedicated security professionals employed, they may not be able to identify all potential security risks.
- Therefore, to help encourage the community to find security risks and report them, offer a "bounty" of monetary value.
- At KeyCDN, we've implemented our own security bounty program to help reduce the risk of any security issues while at the same time providing community users the chance to be rewarded.

Syllabus Topic : Client Application Security

5.6 Client Application Security

Q. 5.6.1 What are thick client applications ? Differentiate thick client with thin client applications. (Ref. Secs. 5.6 and 5.6.1) **(5 Marks)**

- A thick client, also known as Fat Client is a client in client–server architecture or network and typically provides rich functionality, independent of the server.
- In these types of applications, the major processing is done at the client side and involves only aperiodic connection to the server.

5.6.1 Thick Client Vs Thin Client Applications

- The thick clients are heavy applications which normally involve the installation of application on the client side (user computer). These application take up memory and run completely on the computers resources. This means that the security of the application is dependent on the local computer.
- Thick clients are often not well-suited for public environments. To maintain a thick client, IT needs to maintain all systems for software deployment and upgrades, rather than just maintaining the applications on the server.
- Additionally, thick clients often require specific applications, again posing more work and limitations for deployment.
- Typical examples of thick clients are G-Talk, Yahoo Messenger, Microsoft Outlook, online trading portals, etc…
- The thin client applications are web-based application which can be accessed on the internet using a browser. These types of applications do not require any installation of software on the client side.
- The complete processing is carried out on the server. Also, these are light weight and do not occupy any space on the client side (user computer).
- In addition, thin client apps can be accessed by any computer or mobile device that has internet access, making them very portable. With that said, thin client apps are only as fast and reliable as the user's internet connection and the server's bandwidth.
- Examples of thin client application are web-sites like google.com or yahoo.com.

- The thick client applications are made of two types :
  1. Two tier thick client application
  2. Three tier thick client application

➜ **1. Two tier thick client application**

- The two tier thick client application consists of the user computer and the server. In this type, the application is installed on the client side, which directly communicates with the database on the server.
- These usually involve legacy applications. (E.g. - The VB.NET application directly communicating with the database using Open Database Connectivity)

➜ **2. Three tier thick client application**

- These kinds of thick client applications involve three tiers, wherein the client talks to the application server, which in turn talks to the database.
- The communication in these applications is carried out using HTTP/HTTPS. Examples of these applications involve G-Talk or Yahoo Messenger.

5.6.2 Security Assessment of Thick Client Applications

- Application security assessments of thin client applications are comparatively easier than thick client application, as these are web based applications which can be intercepted easily and major processing takes place at the server side.
- Since the thick client applications include both local and server side processing, it requires a different approach for security assessment.
- The Table 5.6.1 distinguishes the vulnerabilities faced by a web based and a thick client application :

Table 5.6.1

Sr. No.	Vulnerabilities	Web based vulnerabilities	Thick Client based vulnerabilities
1.	Improper error handling	Applicable	Applicable
2.	SQL Injection	Applicable	Applicable
3.	Cross Site Scripting	Applicable	Not applicable - browser based vulnerability
4.	Clickjacking attacks	Applicable	Not applicable - browser based vulnerability

Sr. No.	Vulnerabilities	Web based vulnerabilities	Thick Client based vulnerabilities
5.	Parameter Tampering	Applicable	Applicable
6.	Insecure Storage	Applicable	Applicable
7.	Denial of Service	Applicable	Applicable
8.	Reverse engineering	Not Applicable	Applicable
9.	Broken access control	Applicable	Applicable
10.	Session management	Applicable	Applicable

- Refer to **www.owasp.org** for more details on the vulnerabilities listed above.

5.6.3 List of Tools that can used Intercepting Thick Client Applications

Q. 5.6.2 Write short note on list of tools that can used intercepting thick client applications. (Ref. Sec. 5.6.3) **(5 Marks)**

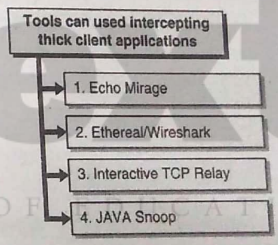

Fig. 5.6.1 : Tools can used intercepting thick client applications

➜ **1. Echo Mirage**

- Echo Mirage is a network proxy tool that uses DLL injection and function hooking techniques to intercept the traffic transmitted and received by the local applications. Traffic can be intercepted in real-time or manipulated with regular expressions and a number of action directives.
- Echo Mirage can be run in two different modes :
  1. By launching an executable from Echo Mirage
  2. Injecting into a currently running process

1. By launching an executable from Echo Mirage

- In this option, the path of the application is provided into the Echo Mirage tool and it launches the selected application. The data sent and received by the application is intercepted by Echo Mirage.
- The screenshot below shows the Gtalk traffic intercepted by the Echo Mirage tool.

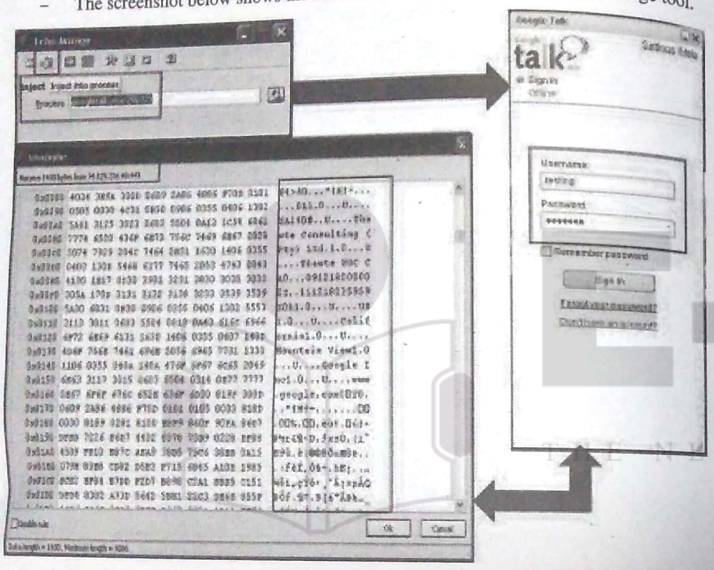

Fig. 5.6.2

2. Injecting into a currently running process

- In this, the Echo Mirage tool injects into the process by hooking into the socket calls.
- Select the thick client application from the list of running processes, and inject Echo Mirage using the "inject into a running process" option from the tool.
- Echo Mirage can also be useful in capturing data from JAVA Applets. For capturing data from a JAVA applet, inject Echo Mirage into the process "java.exe".

BURP Proxy invisible proxy mode

- BURP Proxy is an intercepting proxy server for security testing of web applications.

- The BURP proxy tool can be used in invisible proxy mode to intercept the request from non-proxy-aware thick client applications (HTTP/HTTPS traffic only).
- More Details can be found here :

  http://blog.portswigger.net/2009/04/intercepting-thick-client.html

Mallory : Transparent TCP and UDP proxy

- Mallory is a proxy tool that can intercept TCP and UDP traffic and can be used to capture network traffic or thick client applications using both HTTP(S) and non-HTTP(S) traffic.
- In many cases, the above mentioned tools like Echo Mirage get hanged due to heavy network traffic and become difficult to test. Mallory comes to the rescue in such cases.
- The ideal setup for Mallory is to have a "LAN" or "Victim" network that Mallory acts as the gateway for. This can be configured within a virtual machine environment using only network interfaces. The victim virtual machine then configures the Mallory machine as the gateway by manually setting its gateway.
- The gateway machine will have at least one WAN interface that grants Internet access. The victim network then uses the Mallory gateway to route traffic.
- More details can be found here : **http://intrepidusgroup.com/insight/mallory/**

2. Ethereal/Wireshark

- Wireshark is a network protocol analyzer tool that can be used to analyze the network traffic. This tool can be used to study the non-encrypted traffic sent by the thick client application.
- More details can be found here : **http://www.wireshark.org/**

3. Interactive TCP Relay

- It allows for intercepting the traffic for thick client applications. ITR serves as a TCP tunnel between the client and the server. By instructing the client to open its connection to the ITR instead of the server, the entire connection is shifted to work through the ITR, without the client or the server noticing a difference.
- More details can be found here :

  http://download.cnet.com/Interactive-TCP-Relay/3000-2383_4-10239124.html

➜ **4. JAVA Snoop**

- This tool can be used to intercept the methods, alter data and also test the security of JAVA applications on your computer.
- More details can be found here :

https://www.aspectsecurity.com/research/appsec_tools/javasnoop/

5.6.4 Critical Vulnerabilities Faced by Thick Client Application

In the following sections, we will discuss the critical vulnerabilities faced by thick client application.

5.6.4.1 Sensitive Data Storage on Files and Registries

- During the installation and execution of thick client applications, these apps tend to write/modify sensitive details in the files and registries.
- The sensitive data stored by these apps usually include username, passwords, database credentials, license details, cryptographic keys, and configuration details like IP address, port, etc…
- The attacker can get access to these sensitive details and might compromise the application. In order to assess the application for sensitive data storage, we need to analyze the files and registries used by the application.
- Using a sysinternal tool called "Process Monitor", we can identify the files and registries used by a particular thick client application.

5.6.4.2 Process Monitor

- Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, registry and process/thread activity.
- This tool by default starts monitoring all processes. By setting up proper filters, it can be set to only capture the data related to a particular process.

5.6.4.3 Registry Monitoring

- Set the Process Monitor tool to intercept the registry activity as shown below:
- Analyze the registries accessed by the application to check for sensitive details like keys, encrypted passwords, etc…

5.6.4.4 File Monitoring

- Set the Process Monitor tool to intercept the file access activity, as shown below:
- Analyze the files accessed by the application to check for sensitive details like configuration details, log writing, caching files in folders, etc…
- Other vulnerabilities that can be tested for in thick client apps are as follows :
  - SQL Injection
  - Session Management
  - Authentication
  - Authorization
  - Input validations
  - Password management

Syllabus Topic : Remote Administration Security

5.7 Securing Remote Desktop (RDP) for System Administrators

Q. 5.7.1 How secure is Windows Remote Desktop ? (Ref. Sec. 5.7) **(5 Marks)**

- Remote Desktop sessions operate over an encrypted channel, preventing anyone from viewing your session by listening on the network. However, there is a vulnerability in the method used to encrypt sessions in earlier versions of RDP.
- This vulnerability can allow unauthorized access to your session using a man-in-the-middle attack (link is external). Remote Desktop can be secured using SSL/TLS in Windows Vista, Windows 7, and Windows Server 2003/2008.
- While Remote Desktop is more secure than remote administration tools such as VNC that do not encrypt the entire session, any time Administrator access to a system is granted remotely there are risks. The following tips will help to secure Remote Desktop access to both desktops and server that you support.

5.7.1 Basic Security Tips for Remote Desktop

Use strong passwords

Use a strong password on any accounts with access to Remote Desktop. This should be considered a required step before enabling Remote Desktop. Refer to the campus password complexity guidelines for tips.

Update your software

- One advantage of using Remote Desktop rather than 3rd party remote admin tools is that components are automatically updated to the latest security fixes in the standard Microsoft patch cycle.
- Make sure your are running the latest versions of both the client and server software by enabling and auditing automatic Microsoft Updates. If you are using Remote Desktop clients on other platforms, make sure they are still supported and that you have the latest versions. Older versions may not support high encryption and may have other security flaws.

Restrict access using firewalls

- Use firewalls (both software and hardware where available) to restrict access to remote desktop listening ports (default is TCP 3389). Using an RDP Gateway is highly recommended for restricting RDP access to desktops and servers (see discussion below).
- As an alternative to support off-campus connectivity, you can use the campus VPN software to get a campus IP address, and add the campus VPN network address pool to your RDP firewall exception rule. See **http://net.berkeley.edu/vpn/** (link is external) for more information on the campus VPN service.

Enable Network Level Authentication

- Windows Vista, Windows 7, and Windows Server 2008 also provide Network Level Authentication (NLA) by default. It is best to leave this in place, as NLA provides an extra level of authentication before a connection is established.
- You should only configure Remote Desktop servers to allow connections without NLA if you use Remote Desktop clients on other platforms that don't support it.

Enabling NLA on Windows 2008 Server

Enabling NLA on Windows 2012 Server, Windows 8, and Windows 10 :

- NLA should be enabled by default on Windows 2012 Server, Windows 8, and Windows 10.
- To check you may look at Group Policy setting Require user authentication for remote connections by using Network Level Authentication found at Computer\Policies\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security. This Group Policy setting must be enabled on the server running the Remote Desktop Session Host role.

5.7.2 Limit Users Who Can Log in Using Remote Desktop

- By default, all Administrators can log in to Remote Desktop. If you have multiple Administrator accounts on your computer, you should limit remote access only to those accounts that need it.
- If Remote Desktop is not used for system administration, remove all administrative access via RDP and only allow user accounts requiring RDP service. For Departments that manage many machines remotely, remove the local Administrator account from RDP access at and add a technical group instead.
  1. Click Start-->Programs-->Administrative Tools-->Local Security Policy
  2. Under Local Policies-->User Rights Assignment, go to "Allow logon through Terminal Services." Or "Allow logon through Remote Desktop Services"
  3. Remove the Administrators group and leave the Remote Desktop Users group.
  4. Use the System control panel to add users to the Remote Desktop Users group.
- A typical MS operating system will have the following setting by default as seen in the Local Security Policy :
  - The problem is that "Administrators" is here by default, and your "Local Admin" account is in administrators. Although a password convention to avoid identical local admin passwords on the local machine and tightly controlling access to these passwords or conventions is recommended, using a local admin account to work on a machine remotely does not properly log and identify the user using the system. It is best to override the local security policy with a Group Policy Setting.
  - To control access to the systems even more, using "Restricted Groups" via Group Policy is also helpful.
  - If you use a "Restricted Group" setting to place your group e.g. "CAMPUS\LAW-TECHIES" into "Administrators" and "Remote Desktop Users", your techies will still have administrative access remotely, but using the steps above, you have removed the problematic "local administrator account" having RDP access. Going forward, whenever new machines are added in the OU under the GPO, your settings will be correct.

5.7.3 Set an Account Lockout Policy

By setting your computer to lock an account for a period of time after a number of incorrect guesses, you will help prevent hackers from using automated password guessing

tools from gaining access to your system (this is known as a "brute-force" attack). To set an account lockout policy :

1. Go to Start-->Programs-->Administrative Tools-->Local Security Policy.
2. Under Account Policies-->Account Lockout Policies, set values for all three options.
3. Invalid attempts with 3 minute lockout durations are reasonable choices.

5.8 Best Practices for Additional Security

Q. 5.8.1 Enlist best practices for additional security. (Ref. Sec. 5.8) (5 Marks)

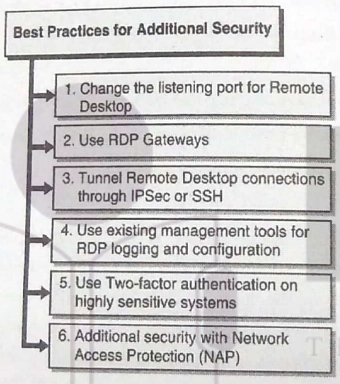

Fig. 5.8.1 : Best practices for additional security

➜ 1. Change the listening port for Remote Desktop

- Changing the listening port will help to "hide" Remote Desktop from hackers who are scanning the network for computers listening on the default Remote Desktop port (TCP 3389).
- This offers effective protection against the latest RDP worms such, as Morto. To do this, edit the following registry key (WARNING : do not try this unless you are familiar with the Windows Registry and TCP/IP) :

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp.

- Change the listening port from 3389 to something else and remember to update any firewall rules with the new port.
- Although this approach is helpful, it is security by obscurity which is not the most reliable security approach. You should ensure that you are also using other methods to tighten down access as described in this article.

➜ 2. Use RDP Gateways

- Using a RDP Gateway is strongly recommended. It provides a way to tightly restrict access to Remote Desktop ports while supporting remote connections through a single "Gateway" server.
- When using an RD Gateway server, all Remote Desktop services on your desktop and workstations should be restricted to only allow access only from the RD Gateway. The RD Gateway server listens for Remote Desktop requests over HTTPS (port 443), and connects the client to the Remote Desktop service on the target machine.
- There are many online documents for configuring this embedded Windows 2008 component. The official documentation is here : **http://technet.microsoft.com/en-us/library/dd983949** (link is external)(WS.10).aspx
- Installing the configuring the role service is mostly as described; however, using a Calnet issued trusted Comodo certificate is recommended. Using a self-signed cert is ok for testing and using a CalnetPKI cert can work if all clients have trusted the UCB root. The Comodo cert is usually better accepted so that your end users do not receive certificate warnings.
- Some campus units use a IST managed VPS as a RD Gateway, and a VPS seems fine for this purpose. A rough estimate might be that 30-100 concurrent users can use one RD Gateway.
- The HA at the virtual layer provides enough fault tolerant and reliable access, however a slightly more sophisticated RD gateway implementation can be done with network load balancing.
- Configuring your client to use your RD Gateway is simple. The official documentation for the MS Client is here : **http://technet.microsoft.com/en-us/library/cc770601.aspx** (link is external).

- In essence, a simple change on the advance tab of your RDP client is all that is necessary.

➜ **3. Tunnel Remote Desktop connections through IPSec or SSH**

- If using an RD Gateway is not feasible, you can add an extra layer of authentication and encryption by tunneling your Remote Desktop sessions through IPSec or SSH.
- IPSec is built-in to all Windows operating systems since Windows 2000, but use and management is greatly improved in Windows Vista/7/2008. (see : **http://technet.microsoft.com/en-us/network/bb531150** (link is external)).
- If an SSH server is available, you can use SSH tunneling for Remote Desktop connections. See **https://kb.berkeley.edu/kb1266** (link is external) for more information on IPSec and SSH tunneling.

➜ **4. Use existing management tools for RDP logging and configuration**

- Using other components like VNC or PCAnywhere are not recommended because they may not log in a fashion that is auditable or protected. With RDP, logins are audited to the local security log, and often to the domain controller auditing system.
- When monitoring local security logs, look for anomalies in RDP sessions such as login attempts from the local Administrator account. RDP also has the benefit of a central management approach via GPO as described above.
- Whenever possible, use GPOs or other Windows configuration management tools to ensure a consistent and secure RDP configuration across all your servers and desktops.
- By enforcing the use of a RDP gateway, you also get a third level of auditing that is easier to read than combing through the domain controller logins, and is separate from the target machine so is not subject to tampering. This type of log can make it much easier to monitor how and when RDP is being used across all the machines in your environment.

➜ **5. Use Two-factor authentication on highly sensitive systems**

- Departments with sensitive data should also consider using a two-factor authentication approach.
- That is beyond the scope of this article, but RD Gateways do provide a simple mechanism for controlling authentication via two factor certificate based smartcards.

Other two factor approaches need another approach at the Remote Desktop host itself e.g. YubiKey, RSA.

➜ **6. Additional security with Network Access Protection (NAP)**

- Highly motivated admins can also investigate the use Network Access Protection (NAP) with an RD Gateway, however, that technology and standard is not well developed or reliable yet.
- Many clients will not work if you enforce it, although by following the documentation, you can audit the system to see if it *thinks* the clients are security compliant.

Syllabus Topic : Classification of Assets

5.9 Classification of Assets

Q. 5.9.1 Write short note on classification of assets. (Ref. Sec. 5.9) **(5 Marks)**

- The two most widespread classification schemes are :
  - A) The government/military classification and
  - B) The private sector classification.

☞ **Top Secret**

It is the highest level in this classification scheme. The unauthorized disclosure of such information can be expected to cause exceptionally grievous damage to the national security.

☞ **Secret**

Very restricted information. The unauthorized disclosure of such data can be expected to cause significant damage to the national security.

☞ **Confidential**

A category that encompasses sensitive, private, proprietary and highly valuable data. The unauthorized disclosure of such data can be expected to cause serious, noticeable damage to the national security.

These three level of data are collectively known as 'Classified' data.

Unclassified

It is the lowest level in this classification scheme. Furthermore, this data is neither sensitive nor classified, and hence it is available to anyone through procedures identified in the Freedom Of Information Act (FOIA).

Syllabus Topic : Physical Security, Physical Vulnerability Assessment

5.10 Physical Security

Q. 5.10.1 What do mean by physical security ? Explain. (Ref. Sec. 5.10) **(5 Marks)**

- Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.
- Effective physical security of an asset is achieved by multi-layering the different measures, what is commonly referred to as 'defence-in-depth'.
- The concept is based on the principle that the security of an asset is not significantly reduced with the loss of any single layer. Each layer of security may be comprised of different elements, including for example :
  - Measures to assist in the detection of threat weapons, including for example explosives, knives, firearms, chemical, biological, radiological material etc.
  - Measures to assist in the detection, tracking and monitoring of intruders and other threats, such as unmanned aerial vehicles.
  - Access control and locking systems.
  - Physical and active barriers to deny or delay the progress of adversaries.
  - Measures to protect people or assets from the effect of blast or ballistic attack.
  - Measures to protect against or limit the spread of chemical, biological or radiological material.
  - Measures to protect sensitive (e.g. classified) material or assets.
  - Command and control.
  - The response to an incident.
  - Security personnel (covered within the Personnel and People Security).
  - The above measures are interdependent and their effectiveness will be dictated by

their ability to support one another. For this and a variety of other reasons, CPNI recommends that all security measures are developed following the Operational Requirements (OR) process.

  - It is very important that the OR is based upon the correct threat planning assumptions and that exercises (e.g. table top) are conducted to ensure that planned security measures will work together to deliver the intended effect.
  - Considering the physical security requirements at the outset, as part of the building or facility design, will often result in more effective and lower cost security. For new builds, high level security requirements should be incorporated into the original brief.
  - Physical security requirements should also be considered during the construction phase of new builds or the modification of existing facilities, as these are likely to be subject to different risks and issues.

Consideration should be given to :

- Identification and assessment of existing and new security risks.
- Identification of security requirements for both the construction works and any changes to the security of the facility itself (this will depend on whether the construction works are adjacent to or within the facility).
- Determination of the transition of the security measures from 'construction phase' into normal operations.
- Further guidance on the security measures identified earlier on this page is provided below. These are grouped into topics and themes.

Syllabus Topic : Choosing Site Location for Security

5.11 Choosing Site Location for Security

Q. 5.11.1 Explain factors need to be considered when selecting a new location. (Ref. Sec. 5.11) **(5 Marks)**

- There are many things to consider when choosing a location for your business venture, whether setting up an office or a shop for the first time, or looking to expand into new areas.
- Following the recent release of a new interactive crime report which revealed fascinating insights about crime and security across the UK, entrepreneur Jake

- Fox reveals the key factors a business needs to consider when selecting a new location.

1. Accessibility
2. Security
3. Competition
4. Business Rates
5. Skill base in the area
6. Potential for growth

1. Accessibility

- Does your business rely on frequent deliveries? If so, it's important to consider local transport links, particularly main roads and motorways. Property rental and purchase prices are often steeper in higher density, more commercialised areas, so there are certainly cost benefits to seeking a more out of town location, providing your daily business operations won't be hampered by poor transport links.
- Equally, if you rely on high customer footfall, then ensuring your location is accessible by car, bus and even train will all be important considerations.
- Don't forget your employees too, as a good location is often a critical factor in recruiting the right people into your business, particularly if they have been offered several jobs and need to evaluate the pros and cons of each.

2. Security

- Believe it or not, your location can increase your odds of being affected by crime, which in turn can influence your insurance premiums, as well as the additional security measures you made need to take to keep your premises safe.
- It's fair to say that in business, we all make decisions based on information, intuition and probability mixed in with a little luck. But knowing the chances of crime in the areas you are considering is an important part of the decision making process.
- We recently analysed released statistics from the UK government crime report and compared this to population data to help businesses make an informed decision about where to set up a new shop, office or warehouse.
- This report conveniently provides a quick snapshot of how safe a particular area is - simply enter your postcode here for your stats summary. Knowing the risks of potential criminal activity can help you better prepare and take adequate precautions.

3. Competition

- Your proximity to other competing businesses could be crucial to your success. Could they provide a benefit to your business or cause a hindrance? Establishing which competitors are in your area and their offering could help guarantee you choose the right location for your business.
- If there is too much competition then it may be a warning sign to expand your horizons to a new location. There are exceptions to this such as car dealerships who want to be near each other as customers compare and choose the best car deal, hence their close proximity.
- Likewise, if you have an element of your offering that is unique or offers some kind of new innovation, then choosing an area that already has a ripe market could be the ideal way to pick up customers very quickly and establish a presence in a new area in a relatively short time frame.

4. Business Rates

- Cash is king! Cash flow is critical as it determines the viable ability for a business to survive and pay its bills. Therefore, it is important to research the average Business Rates including rent, utility bills and taxes in the area to ensure you can afford the premises.
- Simple hidden costs such as deposits and whether you need to pay to park need to be snuffed out before committing to a location. Estimating the living cost of the location will prevent a commitment outside your means.

5. Skill base in the area

- Find out the skill base in the area - can it fulfill your needs? Take into account employment rates as well. If you rely on skilled workers it is best to go to where there is a healthy bank of talent.
- Employees are often a business's biggest asset thus choosing a location that's lacking in required talent may be the start of your business's downfall. Some recruitment agencies will happily send you CVs on spec to gauge the market, only charging if you subsequently decide to interview and hire someone.
- Alternatively, posting a free job via an online jobsite will quickly show you the calibre of employees in a particular area.

6. Potential for growth

- Will the premises be able to accommodate business growth or a spike in demand? Moving premises is a big upheaval and can be time consuming and costly. A decision needs to be made as to whether the premise you are choosing is a short-term location or if you would like to stay there for the long haul.
- Consequently, a location's flexibility could be a very important factor regarding the premises' suitability for your business needs.
- Whilst a perfect business location is different for every business, covering these crucial areas will certainly give you the best chance of beating the odds and keeping your business on track.

5.12 Assets and Security Requirements

- An *asset* is something of value to an organization. An information-security risk evaluation focuses on a subset of those assets: information-related assets..
- These assets are grouped into the following categories : information, systems, services, applications, and people.
- During the data-gathering workshops of Phase 1, participants identified about 55 information-related assets. The analysis team reviewed this list to identify the organization's critical assets.

5.12.1 Critical Assets

Q. 5.12.1 Write short note on critical assets. (Ref. Sec. 5.12.1) **(5 Marks)**

- **Critical assets** are those information-related assets that would cause a large adverse impact on the organization if :
  - They are disclosed to unauthorized people
  - They are lost or destroyed
  - They are modified without authorization
  - Access to them is interrupted
- The analysis team identified the following critical assets for the hospital :
  - **Patient Information Data System (PIDS) :** PIDS is a database system maintained by the contracting organization. This system contains most of the important patient information at the hospital.

  - **Paper medical records :** This is the official documentation source for all patient medical information.
  - **Emergency Care Data System (ECDS) :** This system is used to maintain and update patient records and billing related to emergencies.
  - **Personal computers :** The hospital's staff is dependent on personal computers to access systems and information required for completing day-to-day tasks.
  - **The contracting organization that maintains the hospital's computing infrastructure :** The hospital is almost completely dependent on the contractor for maintaining PIDS and the network.

5.12.2 Security Requirements

- The first step in analyzing a critical asset is determining what about that asset is important. ***Security requirements*** outline the qualities of an asset that are important to protect. Typical security requirements include confidentiality, integrity, and availability.
- The team reviewed data that the consultant elicited during the early workshops, and constructed the following security requirements for PIDS :
  - **Availability :** Access to information is required 24/7; it must be available for patient encounters.
  - **Confidentiality :** Information on PIDS should be kept confidential (restricted to those with "need to know"). Information is subject to the Privacy Act.
  - **Integrity :** Records on PIDS must be kept accurate and complete. Only authorized users should be allowed to modify information on PIDS.
- Each of the security requirements was judged to be important for PIDS. However, the team determined that availability was slightly more important than the other two requirements, because ensuring the availability of patients' medical information enables healthcare professionals to treat their patients in a timely manner, which the team viewed as the primary mission of the hospital. Integrity was judged to be second in importance.
- After completing the organizational piece of the OCTAVE Method, the team turned its attention to the computing infrastructure.

Syllabus Topic : Securing Assets

5.13 Securing Assets

Q. 5.13.1 Explain securing assets in detail. (Ref. Sec. 5.13) **(10 Marks)**

- There are a number of physical security controls available in the market that the organization should consider for implementing physical access controls both inside and outside of the facility. Some of the controls include :
  - Security Guards at each of the entry and exit points.
  - ID cards and badges to all employees, and contractors.
  - Electronic Access cards for all the major doors.
  - Electronic monitoring and Surveillance cameras.
  - Metal Detectors.
  - Electric Fencing.
  - Alarms and Alarm systems.
  - Specialized access to computer labs, data centers, server rooms, and R&D labs.
  - Biometrics.
  - Automatic Locks and keys.

5.13.1 ID Cards and Badges

ID cards and badges are a common method for physical access to the premises. Photo ID and digital smart cards are two common types.

1. Photo ID cards
2. Magnetic Access Cards

➜ 1. Photo ID cards

- Photo ID cards are simple identification cards with a photo of the personnel who is identified to provide access to the facility.
- Every organization provides to its employees a photo ID card for the purpose of identification and this should be worn by the employee at all times within the premises. Any violations of rules or policies within the facility by an employee can be easily identified through his/her ID.
- Digital-coded cards contain chips or magnetic encoded strips on the photo ID card, which also contains all the information related to a person/employee. These types of cards are generally used in credit cards, ATM, and debit cards.

➜ 2. Magnetic Access Cards

- Magnetic access cards are programmed by the security personnel for an entry into specific location. All the major entry and exit points of an office premise may have

access points where one needs to flash this magnetic access card so that the door opens automatically.

- Otherwise, the access is restricted. For example, a server room or an R&D facility in the campus have special access to only few people. The door opens only when they swipe the access card at the door entrance. This will prevent any intrusions, even within the organization.

5.13.2 Other Access Mechanisms

Other access mechanisms that are prominently used include :

- Wireless proximity readers do not require users to physically swipe the card. The card reader senses the card automatically and allows the user who is in possession of the card to enter the door, which opens automatically.
- Radio Frequency Identification (RFID) technology is the one typically used by wireless proximity readers. Fig. 5.13.1 shows one example of a RFID reader that is used for access control.

Fig. 5.13.1

☞ RFID Reader

- One of the inherent weaknesses of such systems is tailgating. Tailgating is a method / technique used by an unauthorized person who enters the premises by following the authorized person.
- As soon as the authorized person swipes his/her card and the door opens and he enters the room, just behind this authorized person, another person enters before the door closes, who may or may not be authorized.

Syllabus Topic : Locks and Entry Controls

5.13.3 Locks and Keys

Q. 5.13.2 Write short note on programmable locks. (Ref. Sec. 5.13.2) **(5 Marks)**

Locks and keys are probably one of the oldest access control methods ever used besides security guards. There are two types of locks :

- These are normal locks used in the houses and door locks. They are preset and the keys are fixed, you cannot change the keys.

Programmable locks

- These are either mechanical or electronic. A mechanical lock is generally an electromagnetic lock where a combination of numbers has to be entered to unlock.
- Common mechanical type programmable locks can be found in earlier labs and office doors. These are the common five-key pushbutton lock that requires users to enter a combination of numbers.
- This is a very popular lock for IT operations, server rooms, and so on. Nowadays, the mechanical locks have been replaced by electronic combinations, where the user is required to punch in a code on a number pad to get the access. This type of lock is known as a cipher lock or keypad access control.

5.13.4 Electronic Monitoring and Surveillance Cameras

- Electronic monitoring controls such as Closed Circuit Television (CCTV) Cameras are used to monitor areas where either guards or dogs are not watching. These CCTV cameras may also complement the guards and the dogs.
- Also, the facilities are monitored 24/7 from a central location. The video footage of the CCTVs are normally recorded and stored for future investigations.
- The main drawback of the electronic monitoring system is that it is a passive device. It can only monitor the intrusion but it cannot prevent intrusions.
- People who are monitoring the activities from the central location have to trigger an alarm in case they detect intrusion. In case the people who are monitoring the systems are not alert, intrusions cannot be stopped and later the recorded videos have to be viewed to identify the intruders and the intrusion activities.

5.13.5 Alarms and Alarm Systems

- Alarm systems are closely related to electronic monitoring systems. But, alarms will notify whenever there is an unauthorized access. Alarms are very similar to Intrusion Detection System (IDS) that can detect any physical intrusion or any other events such as a fire, burglary, smoke, or environmental disturbance such as flooding.
- Motion sensors are sensors that monitor the motion within a confined area using infrared, microwave, or optical technology.
- Sensors are widely used in current-day scenarios. Sensors are also additionally used in data centers to alert about temperature changes, water leakages, humidity increases, and so on.

Syllabus Topic : Physical Intrusion Detection

5.13.6 Biometrics

- We have watched in many movies how various kinds of complicated physical security measures are easily broken by intelligent planning and executing by spies and others. We have also watched in movies how various kinds of biometrics are used by military and other organizations.
- We have seen these biometrics systems being defeated by the severed finger of an authorized but slain officer, through static pictures of iris, through forged fingerprints.
- While biometrics has advanced over a period of time, additional aspects are being envisaged to be considered along with the main traits like pressure exerted or lack of pressure exerted during the fingerprint scan, and so on.
- Biometrics is a technology for measuring and analyzing biological data of a human body such as fingerprints, eye retinas, irises, voice patterns, facial patterns, and hand geometry, and vascular patterns and DNA.
- Biometrics is mainly used for authentication purposes. Biometrics technology is used to prevent fraud, enhance security, and reduce identify theft.
- There are several applications of biometrics in both government and commercial fields. Biometrics have been in use in forensic analysis for over 100 years. Biometrics have aided in criminal investigations, identification of missing children and people during disasters.

- Biometrics provides a higher degree of accuracy which would not be possible by human experts and has helped to solve many problems.
- Governments constantly make use of biometric measures to prevent passport fraud hence preventing intruders getting inside the country by using fake VISAs and passports. Most international airports have adopted iris, fingerprint, or face recognition systems to prevent terrorists or illegal immigrants entering the country using false identity.
- In some developed countries, biometrics identities are included even in the driver's license (smart chips) for extra security. In India, the Aadhaar card (a unique identity for every citizen) has adopted biometric identity of all 10 hand fingerprints, face, and iris of both the eyes.
- Many commercial organizations are using biometrics to protect customers' identity theft and secure commercial transactions. Most of the ATMs in developed countries have face recognition and fingerprint identity as passwords to withdraw money.
- Low cost biometric sensors and technology have led to the deployment of many biometric systems at ATMs, grocery stores, smartphones (iPhone 5s), laptop computers, and so on.
- Apart from commercial applications mentioned above, many organizations are using biometric access control. These biometric access controls are installed and connected to door locks.
- When the biometric identity, such as fingerprints or retina or irises are matched with the data already captured during the enrollment process in the central database, lock systems unlock the door so that the person can enter.
- Biometrics allows employees to access facilities based on the following methods :
  - Acquiring data
  - Extraction of features
  - Encryption of template so that it is not tampered with
  - Capture of data and matching
  - Access is allowed or denied based on the match or no-match.

5.13.6.1 Some of the Important Biometric Mechanisms

- The biometric systems work on the basis of the behavioral traits of the users or the physical traits of the users or a mix of these.

- Behavioral biometric systems use methods such as voice recognition, signature verification, keystroke recognition, gait, and so on.

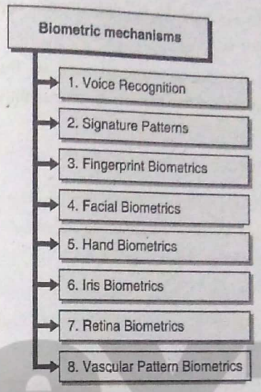

Fig. 5.13.2 : Biometric Mechanics

➜ **1. Voice Recognition**

- Voice patterns differ from person to person. The pitch value and frequency value are unique to each person and hence voice patterns are easily used for identity / authentication / verification purposes.
- Input voice is captured and the features are extracted from this using suitable training methods and the voice sample is stored as a template in the database. Training the voice samples is an important step.
- When the actual voice has to be tested, it is processed, the features out of the same are extracted and compared with the templates saved in the database. When there is a match the person is verified. Cleaning up the voice sample for noise is an important step and is carried out during preprocessing.

➜ **2. Signature Patterns**

- Keystrokes, the style of writing, orientation of writing, and the pressure applied while writing are the features of writing which differ from one person to the other.

- Hence, for a long time, banks and financial systems are relying upon the signature verification against the lodged signatures for authenticating a person or the documents signed by a person. Various government agencies also use this method effectively and extensively.
- Physical biometric systems use methods such as fingerprint biometrics, facial biometrics, hand biometrics, Iris biometrics, retina biometrics, and vascular pattern biometrics.

3. Fingerprint Biometrics

- It is well known that fingerprints are most used in criminal investigations. In many countries fingerprints were taken as additional authentication to the signatures during the registration of properties, deeds, and so on.
- Fingerprint biometrics has almost percolated to most of the fields including companies to passport authorities to immigration authorities to many other fields.
- This is one of the comparatively cost effective, easy to use, and easy to implement systems available for identification and authentication or verification. The fingerprint biometrics uses the minutiae like arches, whorls, loops, ridges, valleys, and furrows which allow one fingerprint to be differentiated from the other.

4. Facial Biometrics

- Facial features like distance between two eyes; geometry of eyes, nose, lips, ears, and so on are the features used to differentiate one face from the other. Faces are captured and the facial features are extracted and used as a template.
- When the face is to be matched, again the same process is used to extract the features, the features so extracted are matched with the stored templates and when there is a match that means that the person is authenticated or verified. Some people have privacy reservations about this method.

5. Hand Biometrics

- Here the hand features such as size, length, width of the hand; lengths and angles of the fingers, bones, muscles, and ligaments of the hand are used to identify a person.
- Even the pressure applied by the hand on the scanner is one of the features that may be used.

6. Iris Biometrics

- The use of Iris biometrics is picking up in critical and sensitive areas which require better entry controls. Iris differs from person to person significantly. Even iris may differ from left eye to right eye of the same person.
- Iris is the area surrounding the pupil in the eye of a human being. This is the area of the eye that determines eye color such as blue eyed, black eyed, and so on. The ring structures, furrows, and freckles pertaining to the iris are used as the features.
- This is easy to implement but requires specific readers and the eye has to be positioned appropriately for effective reading and is relatively costly to implement. Some people still express it as a privacy invasion.

7. Retina Biometrics

- Retina is the area within the human eye that reflects the image. This has different blood vessels flowing through it. These are captured as features as these differ from person to person significantly.
- This is difficult to capture as it requires appropriate lighting and exposure for a sufficiently long time span.

8. Vascular Pattern Biometrics

- Here the thickness and location of veins in a person's hand are used as features. These differ from person to person. Scanning the hand is easy and also does not involve privacy issues.

5.13.6.2 Biometric Access System

Q. 5.13.3 How the biometric system works ? (Ref. Sec. 5.13.6.2) **(5 Marks)**

- Biometric system is a pattern recognition system where a biological pattern is analyzed, matched, and processed for further actions. This process has two stages :

1. Enrollment stage
2. Recognition stage

- A basic biometric system is illustrated in Fig. 5.13.2.

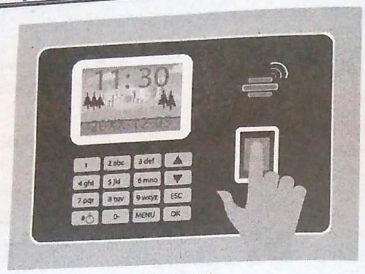

Fig. 5.13.2

➜ **1. Enrollment**

- During the enrollment, a user's biological traits are captured with a scanner, camera, or appropriate reader. The captured data is preprocessed to remove any noise.
- The features are extracted from the captured data and the extracted features are then placed in an electronic template which is stored in a secured database in a central location for future recognition.

➜ **2. Recognition**

- During recognition, a sensor captures a user's biometric data. The data that is captured is analyzed with an algorithm that extracts only relevant features.
- Then this information is compared with the previously captured electronic template. If the match is found, further actions take place or else an alert is generated.

5.13.6.3 Performance of the Biometrics System

- In order to be successful in commercial implementation, performance of the biometrics system has to be good. With the cost of memory and processors having come down significantly, there is more computing power available at less cost.
- This has propelled the usage of the biometrics systems in identification or authentication or verification processes. However, when the number of templates stored in the database increases significantly, the performance can start declining.
- The enrolment and matching and each of their constituent steps can take significant memory and processing time. However, as specified above, the advances in the field of computers have brought down the response time considerably.

5.13.6.4 The Test of a Good Biometric System

A biometric system is considered good only if the following five characteristics are fulfilled :

☞ **Unique**

The feature being captured for matching purposes should be unique to each person.

☞ **Repeatable**

If again, after time lapse, the same characteristics are captured, the features extracted should be the same as that of earlier time, that is, it should be repeatable over a period of time. It should not change from one period of time to the next period of time.

☞ **Accessible**

The characteristics should be easy to be captured, such as through a simple scanner.

☞ **Universal**

Any biometrics system is not useful if it can be applied to only a portion of the target group. It should be easy to apply to all the target personnel. It should not require having some other alternative system for certain people as the system in question is not possible to be used by them.

☞ **Acceptable**

The method of biometrics should be acceptable to all. People should not have any objections about the same, like privacy related objections.

Furthermore, the following rates of acceptance and rejection by a good biometrics system should be at the minimum.

☞ **False Acceptance Rate (FAR)**

A person's biometric characteristics match with somebody else's from the template database. This should not be the case as this can allow access to somebody else in the place of the genuine person. This is also known as False Match Rate.

☞ **False Rejection Rate (FRR)**

A person's biometric characteristics do not match even though his feature template is already captured in the corresponding template database. This should not be the case as the person who requires genuine access may be denied access. This is also known as False Non-Match Rate.

Finally, the following rates need to be "high" for a good biometrics system:

- **True Acceptance Rate (TAR)**

  This is rate of correct match, that is, the person's identity is established correctly.

- **True Rejection Rate (TRR)**

  This is the rate of non-match correctly established, that is, if the person is falsifying the identity, that is correctly found by the biometrics system and the match is rejected correctly.

- **Possible information security issues with the Biometric Systems**

  The following information security breaches are possible with biometric systems :

  - Possibility of forging the fingerprint by molding or fabricating it.
  - Possibility of false acceptance match.
  - Leakage of biometrics data may raise privacy and misuse concerns.
  - If not stored in encrypted mode, it may be possible for hackers to substitute the template and hence get unauthorized entry into an organization.
  - Possibility of the registration of a wrong person instead of a genuine person during the enrolment process without verifying the identity of the person being enrolled.

It is strongly suggested that the biometrics data are not shared with others and also are not duplicated in some other systems even within the organization. Further, the biometric data has to be held encrypted so that it is not copied or replaced fraudulently by others.

5.13.6.5 Multimodal Biometric System

- Unimodal biometric systems, that is, biometric systems which use single characteristic like fingerprint biometrics or retina biometrics or iris biometrics have been found to have some limitations like propensity for attacks, noise in sensors, improper usage of the sensors for scanning or improper way of scanning or inadequate lighting provided (in case of iris scan), and improper exposure during retina scan leading to the noise in the traits captured for matching, and so on.
- Multimodal biometric systems use more than one biological trait of a person for recognition and access. For example, retina and fingerprint both can be used for establishing a person's identity. This enhances the security and also reduces the difficulties faced during recognition phase which the user experiences sometimes. It is also possible to collect data from different sensors, use different algorithms, use multiple samples, and so on.
- In multimodal biometric systems the captured data can be fused at different levels and match or no-match is established. Multimodal biometric systems provide higher accuracy levels.

- **Advantages of biometric systems**

  Biometric recognition has several advantages compared to the traditional access system with simple passwords and IDs.

  - Users do not need to remember passwords.
  - Users need not have to carry an ID card.
  - Unless the person is physically present, access is denied. No impersonation of identity is possible.
  - Biometric traits cannot be stolen or duplicated.
  - Biometric systems are hard to break.
  - Biometric systems have good accuracy.
  - With the advent of the computers, the declining cost of computers, the cost of the biometric systems have significantly reduced.

5.14 Administrative Controls

In addition to the physical and technical controls, administrative controls are also very important from the perspective of ensuring totality and effectiveness of the controls. Some of these administrative controls are detailed in the following section.

5.14.1 Fire Safety Factors

- Fire is an important risk each organization has to protect against. The fire risk arises from electric short circuits, gas leakage, consequential fire / fire mishaps on the premises, friction / malfunctioning of machinery leading to fire, and so on.
- Fire can turn uncontrollable within a few minutes depending upon the location of the fire, if not contained immediately.
- Fire can burn the organizational infrastructure including cabling, computers, and network equipment leading to an almost complete shutdown of the organization unless the organization has a well thought out and well-structured Disaster Recovery and Business Continuity Plans.

- Some of the precautions that need to be taken to reduce the threat of fire are :
  - Do not stock any inflammables like oil, old papers, and chemicals within the office premises. If you need to store them, store them separately in a secluded area and ensure that the area does not have any fire threats.
  - Have smoke detectors installed at all the important places and high risk fire prone places within the organization.
  - Have a good fire alarm system installed which has the capability to identify the zone in which the fire has originated and provide sufficiently audible strong alarm across the place impacted by fire.
  - Have appropriate fire extinguishers installed at all the strategic and important locations within the organization, in sufficient numbers.
  - Train your security guards, Emergency Response Team members, other staff members on effectively using the fire extinguishers.
  - Maintain, test, and understand continued effective working of the smoke detectors.
  - Ensure that the fire extinguishers have the requisite pressure maintained, the contents have not expired.
  - Ensure that the electrical wiring and the switches used are of high quality and adhere to the product specifications.
  - If there is an in-house canteen, ensure safe fire handling precautions. Also, have the fire extinguishers installed in sufficient numbers in that area.
  - Get water sprinklers installed across the organization so that in case of huge fires the water sprinklers are activated and can control the fire.
  - Train all the Emergency Response Team members in effectively handling emergency responses, effective evacuation of the employees. Carry out periodical fire-drills and ensure that the staff members understand the do's and don'ts to be followed during any fire emergency. Record the learnings of the fire drill and ensure that the Emergency Response Plans (in most of the organizations part of Disaster Recovery & Business Continuity Plans) are updated to reflect the applicable learnings.
  - Ensure that the electrical earth points are well maintained.
  - Emergency exits to be clearly marked and the path to the nearest emergency exit clearly specified.
- During audits that we have carried out, we have discovered some of the following issues :
  - Security guards and others did not know how to handle the fire extinguishers.

  - Security guards did not know the priority of evacuation. When the security guards were asked, they mentioned that the computers which are costly have to be evacuated first as they are costly and surprisingly not human beings!!
  - Fire Alarm Panels were not working.
  - Smoke detectors were not working.
  - Fire extinguishers had expired / did not have the requisite pressure.
  - Fire exits were physically locked and they had a difficult time locating the key.
  - Fire drills were carried out for the sake of complying with certain certifications. The learnings were not recorded and acted upon.
  - Earth pits were not maintained.
  - Electrical wiring was substantially old and was patched up at many places. Electrical panels were not well maintained.
  - Old papers and inflammables were stored very near to the canteen area.
  - Sufficient care was not exercised during the fire drills and some of the laptops were stolen by somebody when all the doors were opened automatically!!
- Fire requires important consideration like other parameters by the organization. Otherwise, the organization will be at substantial risk.

5.15 Interception of Data

- Data cables running within the organization, particularly in infrequently used areas, should be completely concealed so that they cannot be tampered with and to avoid the possibility of anybody fixing a monitoring / sniffing device to them.
- Data cables running outside the organization should be completely concealed and should be well protected so that there is no possibility of tampering by anybody.
- In case of wireless devices, it should be seen that there is hardly any possibility of anybody using any rogue wireless router from outside the perimeter of the organization.
- The communication from the wireless devices needs to be encrypted through a strong encryption mechanism so that they are not interfered with and tampered with.
- LAN points should not be normally provided in the visitor area or discussion rooms where the visitors are allowed so that there is no possibility of any visitors connecting to the LAN and manipulating the network.

5.15.1 Mobile and Portable Devices

- Mobile phones and portable devices like laptops are highly prone to theft. Along with the theft of this system, substantial confidential data of the organization is also at risk.
- Particularly, mobile phones and laptops are issued to senior people within the organization and the loss of these systems can lead to substantial information security risks to the organization.
- The following best practices apply to laptops :
  - When not in use and needs to be left unattended, lock it to the desk using the locking cable.
  - While travelling, ensure that the laptop is held securely by you. Do not leave the laptop unattended at airports. Do not leave your laptop in your car when you are away from the car. Data on a laptop should be always held in encrypted form.
  - Do not leave your mobile phones unattended anywhere. Ensure again that the organization has the policy to encrypt the data on the mobile. In case of loss of mobile, the organization should have the capability to wipe out the data on the mobile remotely.
  - Always keep as little data as required on the mobile devices. If you are storing some content on these while not being connected to the office servers, ensure that the data is appropriately transferred back to the office servers once you are back at office or able to connect to the office servers; and delete the data from your mobile device.
- As far as employee personal mobile devices are concerned, these have to be controlled as per the organizational policies. Nowadays, these mobile devices like mobile phones have high resolution cameras and have the capability to store documents and other data.
- Hence, a considered decision has to be taken by the organization after analyzing the risks and the benefits. If employee mobile phones are allowed to be used for official purposes, then appropriate controls as above have to be implemented so that they are not stolen placing the organization at risk.
- Further, employees should be strictly instructed about the do's and don'ts of the use of mobile phones within the office if personal mobile phones are allowed within the organization (e.g., not to photograph any confidential document or client sensitive data, etc.).

5.15.2 Visitor Control

- Control over visitors is often neglected but is an important control from the perspective of physical security. Visitors normally have to be restricted to the reception area and any discussion rooms which are around the reception area but outside of the working area.
- If any visitor is required to come inside the organizational working area, they have to be necessarily escorted by a responsible person from the organization. Visitors should not be allowed to wander at will within the organization and have to be always escorted by a responsible person from the organization.
- Visitors should be required to declare all their personal belongings including mobile phones, laptops, and pen drives. The details have to be written down in the Visitor Personal Belonging Register and have to be allowed inside the organization only on an as needed basis.
- Normally visitors are allowed to bring their mobile phones inside the organization. In such cases, the escort has to ensure that the mobile phones are not used to capture any sensitive document or sensitive work area.
- Further, while entering highly sensitive zones, they may be made to deposit the mobile phones with the security outside the area. Normally USB devices and memory cards should not be allowed within the organization.
- Staff members have to follow the "clear screen" policy when the visitors are at their desk, so that even unintentionally, they do not allow the visitors to understand some sensitive information.

5.16 Exam Pack (Review Questions)

Syllabus Topic : Virtual Machines

Q. 1 Explain virtual machines and give its advantages and drawbacks. (Refer Section 5.1) **(5 Marks)**

Syllabus Topic : Cloud Computing

Q. 2 Write short note on cloud computing and explain its services. (Refer Section 5.2) **(5 Marks)**

Q. 3 Give comparison between IaaS, PaaS and SaaS. (Refer Section 5.2.4) **(5 Marks)**

Syllabus Topic : Secure Development Lifecycle

Q. 4 Explain Secure Development Lifecycle. (Refer Section 5.3) **(10 Marks)**

Q. 5 Enlist SDL phases and explain them. (Refer Section 5.3.4) **(5 Marks)**

Syllabus Topic : Application Security Practices

Q. 6 Write short note on Recommendations for App-Focused Security. (Refer Section 5.4.1) **(5 Marks)**

Syllabus Topic : Web Application Security

Q. 7 Explain web application security practices in detail. (Refer Section 5.5) **(5 Marks)**

Syllabus Topic : Client Application Security

Q. 8 What are thick client applications ? Differentiate thick client with thin client applications. (Refer Sections 5.6 and 5.6.1) **(5 Marks)**

Q. 9 Write short note on list of tools that can used Intercepting thick client applications. (Refer Section 5.6.3) **(5 Marks)**

Syllabus Topic : Remote Administration Security

Q. 10 How secure is Windows Remote Desktop ? (Refer Section 5.7) **(5 Marks)**

Q. 11 Enlist best practices for additional security. (Refer Section 5.8) **(5 Marks)**

Syllabus Topic : Classification of Assets

Q. 12 Write short note on classification of assets. (Refer Section 5.9) **(5 Marks)**

Syllabus Topic : Physical Security, Physical Vulnerability Assessment

Q. 13 What do mean by physical security ? Explain. (Refer Section 5.10) **(5 Marks)**

Syllabus Topic : Choosing Site Location for Security

Q. 14 Explain factors need to be considered when selecting a new location. (Refer Section 5.11) **(5 Marks)**

Q. 15 Write short note on critical assets. (Refer Section 5.12.1) **(5 Marks)**

Syllabus Topic : Securing Assets

Q. 16 Explain securing assets in detail. (Refer Section 5.13) **(10 Marks)**

Syllabus Topic : Locks and Entry Controls

Q. 17 Write short note on programmable locks. (Refer Section 5.13.2) **(5 Marks)**

Syllabus Topic : Physical Intrusion Detection

Q. 18 How the biometric system works ? (Refer Section 5.13.6.2) **(5 Marks)**