Que 1. How you can build “Multilevel Physical and Personal Access Control Systems” to the data center of VJTI?

Answer -

In brief, access control is used to identify an individual who does a specific job, authenticate them, and then proceed to give that individual only the key to the door or workstation that they need access to and nothing more. Access control systems come in three variations: *Discretionary Access Control* (DAC), *Mandatory Access Control* (MAC), and *Role-Based Access Control* (RBAC).

For VJTI Datacentres I’d propose to use Role-Based Access Control.

Role-Based Access Control (RBAC)

- Also known as Rule-Based Access Control, RBAC is the most demanded in regard to access control systems. Not only is it in high demand among households, but RBAC has also become highly sought-after in the business world.
- In RBAC systems, access is assigned by the system administrator and is stringently based on the subject’s role within the household or organization and most privileges are based on the limitations defined by their job responsibilities. So, rather than assigning an individual as a security manager, the security manager position already has access control permissions assigned to it.
- RBAC makes life much easier because rather than assigning multiple individuals particular access, the system administrator only has to assign access to specific job titles.

Furthermore, mentioned below are the appropriate ways to build physical security to the VJTI Data Center.

1. Building design. Physical security can be addressed from the ground up by incorporating architectural and construction features that discourage or thwart the intrusion. Common threats also involve building in such a way that flooding doesn’t affect the center done by building on a higher platform, taking care of lightning and other disasters by properly securing the center. Generally, these features relate to potential entry and escape routes, meaning things like positioning the data center door in such a way that only traffic intended for the data center is near the door. Also, take care to protect access to critical infrastructure elements such as HVAC and wiring, and prevent potential sources of concealment for intruders. And keep the data center away from any other areas that present man-made risks, such as kitchens, and position it such that it doesn’t abut any outside walls.

2. Mantraps. A common and frustrating loophole in otherwise secure access control systems is the ability of an unauthorized person to follow through a checkpoint behind an authorized person. This is known as piggybacking when the authorized person is complicit in the act and tailgating when he isn’t. A solution is an airlock-style arrangement called a mantrap, which essentially entails having two doors at both the entrance and exit, with room for only one person in the space between the doors. Mantraps can be designed with access control for both entry and exit, or for exit only —in which case a failed attempt to exit the enclosure causes the entry door to lock and an alert to be issued indicating that an intruder has been caught. Another option is an overhead camera for optical tracking and tagging of individuals as they pass, issuing an alert if it detects more than one person per authorized entry.

3. Camera surveillance. Still, cameras can also be used for such things as recording license plates at vehicle entry points, or in conjunction with footstep, sensors to record people at critical locations, such as data center entry doors. Some things to consider when placing cameras:

- Is it important that the person in the camera view is easily identifiable, or only that the room is occupied?
- Do you need to be able to see if assets are being removed or do the camera simply serve as a deterrent?

If we opt to record video signals, we’ll need procedures to address issues such as:

- Indexing and cataloging tapes for easy retrieval
- Where the tapes will be stored – on- or off-site
- Who will be authorized to access the tapes
- How long the tapes will be kept

4. Security guards. Security experts agree that a quality staff of protection officers tops the list of methods for backing up and supporting access control. Armed with their human senses, guards provide superior surveillance capabilities plus the ability to respond with mobility and intelligence to suspicious, unusual, or disastrous events. Our security guards are present at the gate and with an already secure environment, this wouldn't be difficult to implement.

5. Sensors and alarms. In addition to the motion, heat, and contact (door-closed) sensors commonly used in office buildings, data centers may use additional forms of sensors. They include laser beam barriers, footstep sensors, touch sensors, and vibration sensors. If the sensors are network-enabled, they can be monitored and controlled remotely.

6. Visitors. Any security system design needs to include policies for how to handle visitors. Typical solutions are to issue temporary badges or cards for low-security areas, and to require escorting for high-security areas.

With these systems in place, we can be sure of multilevel and personal security for VJTI Datacentres

7.Registration: The process of registration phase is as follows The user chooses his or her identity and password for registration, and then enters a biometric (including image, fingerprint, or palmprint information, into the scanner-embedded device or records his or her voice on the recording equipment, which captures and stores the biometric template. The user encrypts the information with the public key. The user sends registration information. The AS decrypts the message with its private key, then checks its user list and confirms.

8.Login: After user registers and wants to log in to the server, the login and authentication phase works as follows The user chooses the biometric modality he or she wants to use according to the hardware configuration and environment, and then enters biometric information, such as fingerprint, palm print, voice, image, and so on, which is captured as information. The user inputs his or her password and biometric. It is verified with the values of them stored during the registration phase and checks whether it's correct. If they aren't correct, the user reenters them. The user randomly generates a value, with the same size as the hash value's output, which will be used as a session key and a masking value. The random value should be generated every session and should be different every time. The user sends his or her login request and related information to the AS. Upon receiving the message from the user , the AS decrypts, and checks. If all verifications are successful, the AS decrypts the user registration in the database. The user is permitted to log in.

9. Multilevel Access Control: We can introduce multilevel access control from the processes of writing, reading, and updating files If user tries to save his or her data into the remote server, referring to the levels of files, he or she should encrypt them before uploading the information. Hereafter, we assume User names the specific users to share this level of data. The user encrypts the requirement using session key α, which is generated during the login phase and sends the message to the AS. The AS decrypts the message with α, implements the user’s demand, and then transfers the queries to the corresponding TS. Upon receiving the message from the AS, the TS decrypts it with kat and executes the task of writing files in the user database. During this process, the data exists in the form of encryption; neither the AS nor the TS can read the plaintext file. Once the files are successfully saved in the TS database, the AS will generate a multilevel database access control. The AS returns level authentication values and then distributes file authentication values to users u1, u2, …, ul, with which the user can access the file of data from user DB.

Que 2 Illustrate Security Framework for Requirement Elicitation for Program Security of “Course Registration and Examination Declaration Systems” of VJTI in the cloud environment.

Ans - Security considerations are typically incorporated in the later stages of development as an afterthought. Security in a software system is put under the category of non-functional requirements by the researchers. Understanding the security needs of a system requires considerable knowledge of assets, data security, integrity, confidentiality, and availability of services. Countermeasures against software attacks are also a security need for a software system. To incorporate security in the earliest stages, i.e. requirement gathering helps building secure software systems from the start. For that purpose, researchers have proposed different requirements elicitation techniques. These techniques are categorized into formal and informal techniques on the basis of finiteness and clarity in activities of the techniques

The elicitation of security requirements (SRs) is a crucial issue to develop secure information systems of high quality. Although we have several requirements elicitation methods, most of them do not provide sufficient supports to identify security threats, security objectives, and security functions.

Information systems deployed at Course Registration and Examination Declaration Systems” of VJTI different sites are being connected to each other through networks and their users can obtain various services anytime and anywhere. In this circumstance, it is very significant to protect assets in an information system from events and/or malicious actors that compromise their security and therefore it is necessary to develop the information systems with functions that protect from security threats. In usual information system development like waterfall style, the requirements for an information system are elicited after a business process modeling stage. It is necessary to elicit the requirements for security functions (simply security requirements) as early as possible, in order to reduce the development cost and to develop the information system of higher quality. Some techniques to elicit security requirements have been proposed and put into practice, e.g. misuse case, abuse case, security use case, the application of I*, and secure Tropos. Almost all of them are the extended versions of use case modeling and goal-oriented approaches, which are requirements elicitation ones originally for functional requirements (FRs) so that they can adapt to the elicitation of security requirements. However, since security functions are closely related to system architecture design, i.e. artifacts on a solution space of the problems, thus it is difficult to elicit appropriate security requirements without considering the system architectures. For instance, let’s consider the database system that stores university students’ grades and their functions for the students to access their grades. There is a potential of the threat that grade data of a student can be read by others. The technique of password authentication can be adopted to mitigate the occurrences of this threat so that the only student that is authenticated and identified can read her grade data from the database system. Therefore, a file system of password data used for authentication and identification (password file) is newly adopted in the system and it stores pairs of student IDs and passwords. The malicious person illegally and furtively may read password data from the password file and impersonates other students to get their grade data when adopting such a technique. To mitigate this threat further, we can have a solution to encrypt the password data in the file. We can consider threats as concepts of a problem space, while the countermeasure techniques to mitigate the threats, e.g. password authentication, password file, and cryptography are the concepts in a solution space of this problem domain. Thus, not only both of them are closely connected, but also a new threat (a problem) may be invented from the newly adopted solutions. This relation expresses just a twin-peak model where development activities in these two spaces. Requirement elicitation activities both in a problem space and in a solution space are indispensable to appropriate security requirements elicitation. The existing studies are biased to requirements elicitation on the problem space side, and there are quite a few studies that both sides are simultaneously considered. To make the methods for eliciting security requirements work well, requirements analysts should have not only knowledge of a problem space but also the knowledge related to security functions on a solution space, e.g. password authentication and cryptography, etc. However it may be a rare case where a requirements analyst has sufficient knowledge of both spaces, and some techniques to provide an analyst with knowledge of security functions are necessary to be weaved with an elicitation method.

Que 3 How can you use a Common Criteria based security Requirement Engineering Process(SREP) for the program security of the following project:
Today, there is a shortage of teaching faculty in educational institutions throughout the country. On the other hand, there are a huge number of students across the country who wish to pursue education from premier educational institutions but are unable to do so due
to a variety of reasons ranging from financial constraints, family responsibilities, limited available seats in colleges, tough competition, etc. E-Learning Tool - an initiative would help
overcome these obstacles and enable the aspiring students and teachers to realize their dreams to be educated.
E-learning tool which would enable the participating actor, say a professor to create his own synchronous interactive learning material using multimedia resources. This when coupled with database management is intended to serve as a repository of lectures in video
(along with audio) and text in various file types on the website that would enable aspiring students from remote centers all around the nation to acquire knowledge and pursue their
education just by a stroke on the keyboard.

1. Introduction E-learning facilitates and enhances the learning process through the use of devices based on computer and communications technology. E-learning covers a broad category of applications and processes, such as education via the Internet / Intranet (web-based learning), education provided via computer (computer-based learning), virtual classrooms, and digital collaboration. The content is offered electronically through the Internet, Intranet, audio or videotapes, satellite, CD-ROM, or DVD. Usually, the e-learning term is understood as online education (web-based learning) and online courses. Considering this aspect, the computer-based learning process can be seen as an eLearning component which does not require continuous interaction with an instructor and other students. E-learning offers substantial advantages to companies and it is perfectly adapted to specific and exact training in business. E-learning is a form of distance learning because the participants and the instructor can reside in different locations, and the interaction is mostly asynchronous. Below are presented some characteristics of the e-learning systems: the learning process takes place in a virtual classroom; the educational material is available on the Internet and includes text, images, links to other online resources, images, audio, and video presentations; the virtual classroom is coordinated by an instructor who plans the activity of the students, discusses aspects of the course using a discussion forum or chat, provides auxiliary resources, etc; the learning becomes a social process; a learning community is created through the interaction and collaboration between the instructor and students; most e-learning systems allow the activity monitoring of the participants, and some of them also simulations, the work on subgroups, audio, and video interaction, etc. Due to the new trends in the development of educational systems and the necessity of developing applications that can be accessed remotely, the security management of e-learning systems and the access control have attracted more and

more the attention of researchers and web application developers. Meeting the security requirements in an e-learning system is an extremely complex problem because it is necessary to protect the content, services, and personal data not only for the external users but also for the internal users, including system administrators. 2. Basic security requirements The following basic security aspects should be met for e-learning platforms: authenticity, access control, confidentiality, integrity, availability, non-repudiation. Secure authentication is required to identify the user who will use the web application and determine his access privileges. This mechanism prevents the attackers to access another user's account, to view sensitive information or to perform unauthorized operations. Also, once authenticated, the user should have the possibility to change his password. Below are listed some good practices regarding authentication: requiring re-authentication at specified time intervals; enforcing the users to set only strong passwords (including some capital letters, at least one number, some special characters, etc); implementing the access control based on roles. The access control is realized during the authentication time when the user is granted with all the necessary rights. In this way, the user will perform in the system only his allowed operations. A role-based authorization model is an approach of restricting the system access of unauthorized users; it allows groups definition, users inclusion in groups, or even groups in other groups. This model allows flexible and granular control of the rights of each user. The permissions of performing certain operations are assigned to some specific roles (administrator, editor, instructor, student, registered user, unregistered user, etc). Staff members (or other system users) are assigned with particular roles, and therefore they acquire the permissions to perform particular system functions. Since the users don't have the permissions directly assigned to them, but they only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning appropriate roles to the user. The confidentiality of an e-learning system must be ensured through the access control to resources and by securing the transmission and the storage of the data. The integrity of the data and programs is a very important subject even though it is often neglected in daily life. Integrity means that only authorized subjects (i.e. users or computer programs) are permitted to modify data (or executable programs). The secrecy of data is closely connected to the integrity of programs and operating systems. If the integrity of the operating system is violated, then the reference monitor might not work properly anymore. The reference monitor is a mechanism that ensures that only authorized subjects are able to access data and perform operations. It is obvious that secrecy of information cannot be guaranteed if this mechanism that checks and limits access to data is not working. For this reason, it is important to protect the integrity of operating systems in order to protect the secrecy of data itself. The data replication through different sites represents a good security practice which helps to maintain integrity. The replication process increases the security of the system and also improves the speed of data operations. Non-repudiation means that users are not able to plausibly deny to have carried out operations. Let us assume that a teacher deletes his/her student's exam results. In this case, it should be possible to trace back who deleted them by using some log files. In addition, these log files must be reliable and tamper-proof. Auditing is the mechanism used to fulfill this requirement. Another countermeasure for non-repudiation is a digital signature.

(OPTIONAL FOR PERSONAL REFERENCE AND LEARNING)

Que 4.(a)Every timing channel can be transferred into an equivalent storage channel? Explain how the transformation could be done.?
(b) How can you do a search for potential covert channels involves finding all shared resources and determining which processes can write to and read from the resources search using Shared Resource Matrix?
(c)Can you develop controls and protection mechanisms for covert channels?. How?

a)

Covert channels typically require access to a shared clock to a time when bits become available in covert resources and when bits can be replaced. Thus with pure storage channels, there is an element of timing.

A covert timing channel works by modulating the time at which something occurs. But something which might be an interrupt our access to CPU or unblocking a semaphore for example) is itself a resource(the interrupt, the processing or the semaphore) represented by a storage table entry. Thus the table entry or the something becomes the shared resource visible to the 2 cooperating processes from which the covert channel is built.

b)

Richard Kemmerer introduced the Shared Resource Matrix Methodology (SRMM). The idea is to build a table describing system commands and their potential effects on shared attributes of objects.

	READ	WRITE	DESTROY	CREATE
File Existence	R		M	M
File Size	R	M	M	M
File Level	R	M	M	M

An R means the operation References (provides information about) the attribute under some circumstances. An M means the operation Modifies the attribute under some circumstances
But this works for only Storage channels and not for Timing channels.

c)

Covert channels can tunnel through secure operating systems and require special measures to control. Covert channel analysis is the only proven way to control covert channels. By contrast, secure operating systems can easily prevent misuse of legitimate channels, so distinguishing both is important. Analysis of legitimate channels for hidden objects is often misrepresented as the only successful countermeasure for legitimate channel misuse. Because this amounts to the analysis of large amounts of software, it was shown as early as 1972 to be impractical. Without being informed of this, some are misled to believe an analysis will "manage the risk" of these legitimate channels.