A Case Study of Criticality Based Access Control in a Cyber Physical System

M.Sharada Varalakshmi
Associate professor, CSE
Department of Computer Science and Engineering
St.Peters Engineering College, Hyderabad, India

Abstract

This paper gives a brief description about the criticality situation in a Cyber Physical System(CPS). This study introduces a unique behavior of a CPS which changes its state at the time of criticality. Two states of CPS are introduced to access the control called as Normal state and Critical state. The CPS changes its state from Normal state to critical state at the time of crisis.

I. INTRODUCTION

Emergencies in traditional systems were handled by disabling the security system to allow the relief workers to have full authority on the system to handle crisis [Simon, Richard T., and Mary Ellen Zurko]. Such approaches are well suited for traditional and non smart-infrastructures. But in the recent past, smart-infrastructure is equipped with the most sensitive information, so, disabling such systems may leave the system vulnerable to attacks and potential threats[Adelstein, Frank, et al, 2005]. For instance, consider a scenario where a person may face a health related emergency and his wearable health monitoring device system is disabled, therefore any doctor or a medical assistant can view the person's personal data without any security constraint. So, there may be a possibility of malicious attack on the subject's data by acquiring access rights. Also there may be a possibility of generating false alarms and raise emergency signals. This may lead to accessing of the sensitive information of the information system [S. Mehrotra, Kalashnikov, Dmitri V., et al]. The privacy of the data is also lost due to such malicious attacks. Smart- infrastructures work under a real time environment where, security has to be provided to the system during emergencies [Scheneier, Bruce, John, 1999]. Privacy preservation during emergencies is the primary concern of this paper which should provide necessary access privileges to the subjects during the time of emergencies[Venkatasubramanian, Krishna K., Tridib Mukherjee, and Sandeep KS Gupta.2005]. The principal concepts are discussed in the next section before we proceed to discuss our paper. In this paper, the term crisis, critical and emergency are used interchangeably which mean the same.

II. PROPOSED WORK

Consider a state where there are multiple crises in a process control unit. This situation is explained with the help of tables given in figure 1.1 the tables given on the left side are given as Normal state and on the right side is the Crisis state. Consider a scenario where a member in the control room has heart attack c1. The CBDAC routinely checks the system and notices that the system is in crisis state, now the system will have to attend the crisis state and return back to normal state. The system checks Subject –role table and Object table for the subjects those who can handle the situation. It immediately triggers an emergency message to the subjects logged in, based on the login table. Now the system is in response state which is handling the situation c1. If at the same time a fire breaks out, just before the response action of subject ID1, then another message is triggered to all logged in users to immediately handle the situation. An audit table is maintained to record the login time of the user attending the crisis state. The system also monitors the all the access privileges, and log out time of the dynamic user, so that, any misuse of the privileges can be recorded and pursued. The dynamic user is given the privileges only for certain time duration. The permission is rescinded immediately after the Window-of-Opportunity. It is shown in figure 1.1 the system states. The left portion shows the system under normal conditions and the right portion shows the system under crisis situation. The change of roles is represented in the Object-Access table and Dynamic - Subject table. The subjects are given permission to access the crisis dynamically. It can be noted that a health crisis occurred in the control room concerned doctor is not nearby. From the dynamic subject table it is evident that a medical assistant nearby was given privileges to access the medical data. Similarly, if there is a fire in the control room dynamic permissions are given to the technician to access the extinguisher. The permissions are rescinded immediately after the emergency

situation. The previous role and the current role are noted and are maintained in their respective tables.

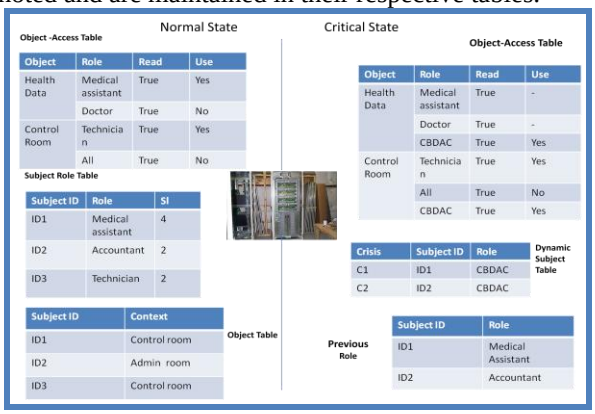


Fig: 1.1 shows the access control in Normal state and Critical state.

The Dynamic Subject table is updated stating that ID1 a medical assistant and ID2 an accountant are assigned the roles of CBDAC. The audit table updates the time the subject has taken the control of the crisis and the window of opportunity is assigned to each of the crisis to be handled. The time taken for execution of the multiple crisis is recorded in the audit table.

III. USER CATEGORIZATION AND ACCESS CONTROL

The policies of access control are high level directives that specify which subject has permission on which object on what data to access. Access control is a security policy which specifies the organizational rights. It restricts the actions requested by subjects on objects. In this paper, the subjects are categorized based on the entities they use to perform an action such as read, write and execute. The access control policy is based on the concept of security level that is associated with subjects and objects, where they have been derived from and the permission they are associated with. The access control policy gives different security rights in which every element is an ordered set. For example, Highly Confidential, Confidential, Personal and Public, where the policy says that HC $\geq$ C $\geq$ Pr $\geq$ Pu. For objects security level is called category level and for subjects it is called authorization level. A subject is authorized to access the object which comes under his category but not on the objects of other category.

The motivation to introduce this categorization of secured access control mechanism is the multi level security model of RBAC, where an organization can have many roles with many access rights. For example, in a company accessing a website and uploading data into their website are common permission which may be given to all the employees and can be said as Public users who have access to all the public data that is classified. Personal users are authorized to access only that local data of the company such as salary statements of the employees and any other Personal information. They also have access to Public data. Confidential category users are those users who have access rights on the confidential data of the information system and also have rights to access the Public and Personal data. Highly Confidential users are those users who can access only the top level information of the company. This information is high security information where the lower category users cannot have access rights to access it, but in turn the Highly Confidential users have the rights to use Confidential, Personal and Public information as

The users of type 4 can have the rights to access type 4,3,2,1. The users of tupe 3 can have the rights to access type 3,2,1. The users of type 2 can have the rights on type 2,1 and yhe user of type 1 can only have the permissions to access public information only but not higher to that.

IV. PERFORMANCE OF USER CLASSIFICATION

The users that are categorized into four categories, can access only that information that is classified into four classes. The results of figure 1.1 show that the sensitivity level 4(Highly Confidential level) data can be accessed only by user type 4(Highly Confidential) users. Similarly, sensitivity level 3 (Confidential level) data can be accessed by user types 3 and 4 (Confidential and Highly Confidential) users. In the same way sensitivity level 3 (Personal) data can be accessed by user type 2, 3 and 4 (Personal, Confidential, Highly Confidential) users. Also, the sensitivity level 1 (Public) data can be accessed by users of type 1, 2, 3 and 4(Highly Confidential, Confidential, Personal and Public) users.

Figure 1.2 shows the sensitivity levels of the data users. Each user is categorized based on the type of data they access.

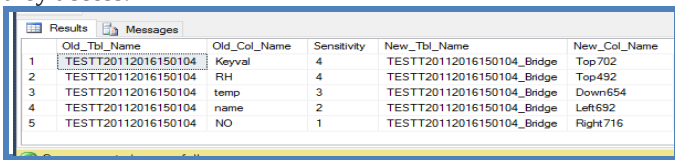
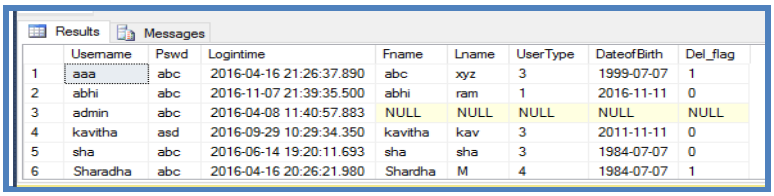


Fig: 1.2 show the sensitivity levels of the classified data.

The detailed login table comprises of the user type and their date of access of an object and login time is shown in figure 1.3.

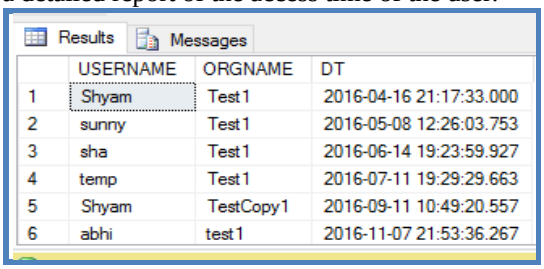


Results | Messages

	Username	Pswd	Logintime	Fname	Lname	UserType	DateofBirth	Del_flag
1	aaa	abc	2016-04-16 21:26:37.890	abc	xyz	3	1999-07-07	1
2	abhi	abc	2016-11-07 21:39:35.500	abhi	ram	1	2016-11-11	0
3	admin	abc	2016-04-08 11:40:57.883	NULL	NULL	NULL	NULL	NULL
4	kavitha	asd	2016-09-29 10:29:34.350	kavitha	kav	3	2011-11-11	0
5	sha	abc	2016-06-14 19:20:11.693	sha	sha	3	1984-07-07	0
6	Sharadha	abc	2016-04-16 20:26:21.980	Shardha	M	4	1984-07-07	1

Fig: 1.3 show the categorized user types.

A detailed audit table is maintained to understand the behavior of the users. Figure 1.8 shows that all the details of the users are recorded along with the login time and number of hours the user is logged. This gives us a detailed report of the access time of the user.



Results | Messages

	USERNAME	ORGNAME	DT
1	Shyam	Test1	2016-04-16 21:17:33.000
2	sunny	Test1	2016-05-08 12:26:03.753
3	sha	Test1	2016-06-14 19:23:59.927
4	temp	Test1	2016-07-11 19:29:29.663
5	Shyam	TestCopy1	2016-09-11 10:49:20.557
6	abhi	test1	2016-11-07 21:53:36.267

Fig: 1.4 show the audit report.

A log report of the users, the information accessed, the date and time of duration of access is maintained is given in figure 1.4.

V. PERFORMANCE OF SECURE ACCESS CONTROL BY COMPARATIVE ANALYSIS

The performance of secure access control mechanism is compared with the security parameters such as Confidentiality, Integrity, Authorization and Availability. In this paper, Confidentiality of data is maintained by providing secured access categorization to the data stored in the information system. Also, the data is encrypted in such a novel method so that confidentiality is not lost. In this method, detailed security policies are maintained where access rights are defined and categorized in four different levels. Authorization is well handled by maintaining a detailed audit table which maintains a detailed report of all the movements of the users. The secured access control mechanism adds a unique feature of handling crisis dynamically and granting the privileges to users only at the time of emergencies.

Secure access control in smart infrastructures maintains integrity which ensures that data is not changed by unauthorized parties. Therefore, availability of data to authorized users is succeeded.

VI. CONCLUSION

In this phase of the paper, a secured access control of smart infrastructure is designed and developed. A novel Crisis Based Dynamic Access Control mechanism is introduced which is both adaptive and proactive in nature. The CBDAC grants access permissions to the logged in users dynamically at the time of emergencies. The subjects are granted permissions to change the roles at the time of criticality. A onetime code is generated automatically and is passed to the users by the system to authenticate that a valid user is being granted the permissions. Using this code the subject can acquire access permissions on the object. A log table is maintained to record all the details of the users such as Login time, Logout Time, Time taken to handle the crisis, Date, Sensitivity level of the user, Access permissions of the subject. The system also records the details of the subjects at the time of criticality.

References

REFERENCES

[1] Adelstein, Frank, et al. Fundamentals of mobile and pervasive computing. Vol. 1. New York: McGraw-Hill, 2005.

[2] Simon, Richard T., and Mary Ellen Zurko. "Separation of duty in role-based environments." Computer Security Foundations Workshop, 1997. Proceedings., 10th. IEEE, 1997.

[3] Venkatasubramanian, Krishna K., Tridib Mukherjee, and Sandeep KS Gupta. "CAAC--an adaptive and proactive access control approach for emergencies in smart infrastructures." ACM Transactions on Autonomous and Adaptive Systems (TAAS) 8.4 (2014): 20.

[4] S. Mehrotra, Kalashnikov, Dmitri V., et al. "Index for fast retrieval of uncertain spatial point data." Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems. ACM, 2006.

[5] Schneier, Bruce, and John Kelsey. "Secure audit logs to support computer forensics." ACM Transactions on Information and System Security (TISSEC) 2.2 (1999): 159-176.