Enhanced Authentication Mechanism Using Multilevel Security Model

Abdulameer Hussain
Faculty of Science and Information Technology, Zarka Private University, Jordan

Abstract: *This paper presents a proposed multilevel authentication method which is implemented especially in sensitive applications where they contain multilevel secure and confidential data. The proposed method divides the system into multiple sensitive levels and tests users against different authentication methods for each level. Most levels are subdivided further into secure sublevels. Each sublevel contains its own privileges and data types which are managed by an Identity Manager (IM) whose responsibility is to transit users to other higher sublevels. The transition's decision is done by assigning different weights to each authentication method .After a series of tests, the IM must generate a status report describing the results and the decision made to each user's activity. This technique permits granting only the required privileges for a selected group of users and limits the configuration functions of those that users in a particular user group can perform.*

Keywords: *Security, multi level security, multi level -authentication, authentication, security management.*

Received February 18, 2009; Accepted Apritl19 2009

1. Introduction

Many businesses and organizations need to protect secret information, and most can tolerate some leakage. Organizations who use Multi Level Security (MLS) systems tolerate no leakage at all. Businesses may face legal or financial risks if they fail to protect business secrets, but they can generally recover afterwards by paying to repair the damage. At worst, the business goes bankrupt. Managers who take risks with business secrets might lose their jobs if secrets are leaked, but they are more likely to lose their jobs to failed projects or overrun budgets. This places a limit on the amount of money a business will invest in data secrecy. The defense community, which includes the military services, intelligence organizations, related government agencies, and their supporting enterprises, cannot easily recover from certain information leaks [1].

So it is important to use multilevel security which provides a security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. Multilevel Security provides a way to segregate users and their data from other users and their data regardless of access lists [2, 3].

2. Overview of Multilevel security (MLS)

Multilevel Security (MLS) is the application of a computer system to process information with different sensitivities (i.e. classified information at different security levels), permit simultaneous access by users with different security clearance and needs-to-know, and prevent users from obtaining access to information for which they lack authorization. MLS allows both easy access to less-sensitive information by higher-cleared individuals and higher-cleared individuals to easily share sanitized documents with less-cleared individuals. [4,5,6] .

A multilevel security (MLS) system has two primary goals: first, it is intended to prevent unauthorized personnel from accessing information at higher classification than their authorization. Second, it is intended to prevent personnel from declassifying information. Multilevel security (MLS) was developed by the US military in the 1970's to allow users to share some information with certain classes of user while preventing the flow of sensitive information to other classes of user [3]. MLS is also used in other domains like trusted operating systems, and in grid applications, where administrative users can set multilevel policies on their applications, thereby providing a fine grained control on the community users. The Bell-LaPadula security model (BLP) is a formalization of MLS [7,8, 9].Also , object-Orientation is an attractive approach to implementing MLS because objects are a natural way to represent system data and well defined interfaces are a natural place to enforce access [10, 11] .

MLS is concerned with controlling the flow of information in systems. The traditional view of multilevel security is one of ensuring that information at a high security classification cannot flow down to a lower security classification [12,13,14]. However, constraining how information may flow within a

3. Related Work

Most of research was concentrated on using multi-factor authentication. In [7], we find a description of a general Multi-mode Authentication Framework (MAF) for applying organizational security policies, organized into distinct policy contexts known as echelons, among which a user may transition. The design of the framework allows various types of authentication technologies to be incorporated readily and provides a simple interface for supporting different types of policy enforcement mechanisms.

Another description of the MLS system described in [22, 23]. The system is based on the security standard levels employed to transfer text and images through local area networks and wide area networks. It provides several levels of security, which include digital signature, encryption, compression, and smart card technology.

The Bell-LaPadula security model (BLP) [24] is a formalization of MLS. BLP defines two rules which, if properly enforced, have been mathematically proven to prevent information at any given security level from flowing to a "lower" security level. These rules are called No Read Up (NRU) and No Write Down (NWD). The NRU rule states that a subject cannot read an object that has a higher security level. Whereas, NWD states that a subject cannot write to an object that has a lower security level.

The National Security Agency (NSA) began a computer security development effort called the Multilevel Information Systems Security Initiative (MISSI). MISSI encompasses both the traditional Communications Security (COMSEC) and Computer Security (COMPUSEC) disciplines. MISSI's goal is to provide dependable and affordable security services necessary to protect information from unauthorized disclosure or modification and to provide mechanisms to authenticate users participating in the exchange of information [25]. European Commission Directorate General For Informatics described a proposed system for a multi-level authentication which includes different likelihood level definitions such as almost certain , likely, moderate unlikely and rare [26].

4. Proposed System

In this paper we present a multilevel authentication model applied by sensitive applications. In addition, this system is one that belongs and applies multilevel security. As we know, any sensitive application includes confidential and secret information and must be used effectively in complicated and authenticated procedures. Suppose that the application involves a set of different users $U=\{u_1,u_2,\ldots u_n\}$, so these users must work in different authentication sensitive levels $L=\{l_0,l_1,\ldots,l_m\}$ .The process of breaking the proposed system depends on the security classification as shown in Table1.

Table 1. Authentication classes

Authentication Level Class	Authentication Level Names
LowSecurity	l_{01}
LowMediumSecurity	l_{02}
MediumSecurity	l_{11}
MediumHighSecurity	*l12*
HighSecurity	*l2*

To ensure a proper and secure usage of application's information ,the authenticated system (proposed in this paper) must perform a severe test to each user by using different authentication methods which are in the set $AUTH=\{auth_1,auth_2,\ldots\ldots auth_k\}$ where each elements of this set represents a specific authentication method. We had implemented different authentication methods such as password, EL- Gammal , Handshaking, RSA and multiple private questions. These methods found in [27] . The system is divided into different authentication levels L and some of these levels are divided further into sub-levels .For example , the level l_0 may be broken down into two sub-levels l_{01} and l_{02} and each has its own users and a set of privileges and data types granted to these sublevel's users. The set of privileges $P=\{p_1,p_2,\ldots p_l\}$ are represented as an access control matrix containing certain privileges such as read (R) , write (W) ,execute (E) ,append (A) ,View (V) , Monitor (M), Assessment(AS),Management (M) and so on . If the access control contains n privileges we also can obtain 2^n combinations of privileges. For example, if the access control contains 4 privileges such as R, W, E, A, we can get 16 combinations such as R/W, R/E and so on. [28]. Furthermore the proposed system contains a set of data types $T=\{D,C,B,A\}$.These data types are assigned to each authenticated user according to the level number he/she resides. Data types are classified according to the international traditional classification of data importance as listed in Table2.

Table2. Different data types

Data type	Description
D	Represents unclassified data
C	Represents confidential data
B	Represents secret data
A	Represents top secret data

In Figure1 we notice that for each level, there is a sub-level manager who is responsible for monitoring user's behavior and granting users what privileges they deserve .This manager is called an Identity Manager (IM). To explain how the system works, let us first suppose that the manger needs to examine the result of a certain user who is tested against a specific authentication method. We begin at $level_0$ where there exits old authenticated users, but if we need to add a new user, this new user must be examined by a preliminary authenticated method such as password .This type of password is assigned for transition purpose and is given to authenticated users only before he is informed to make the examination and is different for each sublevel, so the purpose of this password is different from that being used as logging task. If the user passes the authentication test ,then the manager assigns this user to the first part of $level_0$ which is l_{01} so that this user grants read privilege (R) only from the access matrix and using the unclassified data type (D) .In addition , this user must remain in his sublevel (l_{01}) a certain amount of period (p_{01}) which is determined by the manager of each sublevel . If this period reaches its end then the manger must examine him with additional authentication methods such as password and private questions in order to transmit him to the next highest level (l_{02}) .The manager of this level assign marks for each authentication method depending on the weight (w) of each authentication method (some of the weights of for different levels are illustrated in table3.On the other hand, if the new user fails in the test, then he must be rejected. The manager must assign ranks (R) to each passed user depending upon the successful trials which qualified that user to transit to a certain sublevel. For example if number of successful trial is 2 the user's rank will be R2 .The rank values are arranged in a way that the lowest trials number is the highest user's rank. This procedure gives the manager a suitable indication about the degree of activity and honesty of each user. These ranks are explained in report manager within the result section. The important step in this paper is how to manage and examine multiple users resided in their own sub-levels. Now we will describe the transition procedure for some levels and the remaining levels works in the same manner. Let us begin with the users at $level_{01}$ where the manager wishes to examine a certain user U_i after he remains a certain amount of time (p_{01}) working in this sub-level in order to transit him to the next highest sub-level l_{02} .To perform this task, the user faces another authentication test which is composed of two authentication methods such as password and asking him some of authenticated private questions which contains answers to the questions only known to the illegal user. The manger decision depends on the result of this test, so that manager assigns certain marks (weights) to each authentication method as shown in Table3. These weights are dedicated to this level and may vary in other levels according to the IM's decision of those levels.

Table3. Weights assigned to different authentication methods

Sublevel Transitions	Authentication methods	Weights(w)
L_{01} to l_{02}	Password	40
	Multiple Questions	60
L_{02} to l_{11}	Multiple Questions	30
	El-Gamal	70
L_{11} t0 l_{12}	Multiple Questions	30
	Handshaking	70
L_{12} to l_2	RSA	20
	El-Gamal	40
	Handshaking	40

If the user fails in the password test then , he remains in its original sublevel $level_{01}$, but if he passes multiple questions methods , then the manager decides to transit him to the next highest level $level_{02}$ but with restricted privileges assigned to that level such as view privilege to some files , we called this decision as partial transition or partial pass .We proposed in this paper that the amount of privileges granted to the user with partial transition can be given at a certain percentage of the total privileges allowed for a specific sublevel .On the other hand , any user can be granted all privileges of this sublevel when he passes the two authentication methods successfully . Similarly ,each user in $level_{02}$ must reside a certain period of time and then must be tested by examining him with another set of additional authentication methods such as EI-Gamal scheme and handshaking scheme in addition to multiple questions method. The description of this sub-levels and the later phase is illustrated in Table 4 which summarizes the remaining transition procedures to sublevels.

As we said previously, each sublevel is supervised by a manger that is called an identity manager (IM). For example the manager of sublevel level01 is abbreviated as IM01and the manager of $level_{11}$ is IM_{11}.Each manager is responsible for monitoring the

Table4: Details of Some Sub-levels

Original level	New level	Authentication methods	Weight Wi	Transition Condition and Decision
$level_{02}$	$Level_{11}$	Multiple questions EI-Gamal	30 70	If w1=30 remains in $level_{02}$ Ifw2= 70 transit $Level_{11}$ to with restricted view and execute If w1=30and w2=70 the full transition
$Leel_{11}$	$Level_{12}$	Multiple questions Handshaking	20 80	If w1=20 remains in $level_{11}$ If w2=80 transit to $level_{12}$ with restricted view and execute Ifw1=20 and w2=80 transit $level_{12}$ with all privileges
$Level_{12}$	$Level_2$	El-Gamal Handshaking RSA	W1=20 W2=40 W3=40	Must be pass all the authentication methods (Full Access)

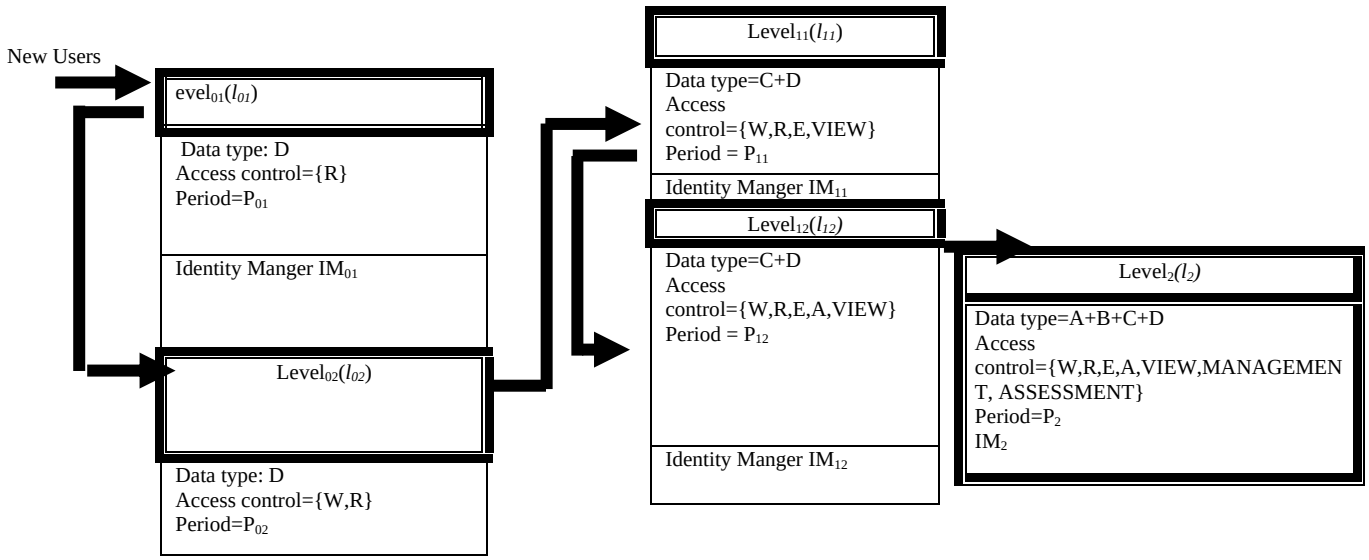

Figure 1. Multilevel Authentication System

user's activities and also granting different privileges and deciding which user is transited to a new level or remains in its original level .Each IM must develop a management report that can be used to track and monitor each user in the application. This report will provide the high manger of the application with a clear idea about the honesty of each user and may be used to evaluate each user's authenticity. If a specific user has many trails to transit, the manger's decision may be a cause to ignore this user totally from the application On the other hand if certain users behave in a more authenticated behavior, then the manager will appraise that user and may granted a sublevel management especially those who reach the sublevel l_{l2} .We will give a detail activities of these managers in result section. The final point, the period P2 in the highest level l2 are used not as a period for transition to other levels because this level is the highest, but this period can be used by the manager of that level to qualify the users to be a sublevel's manager in one of the lowest sublevels.

Algorithm

step1: Initilization of data

Let L be a set of sublevels such tat $L=\{l_0,l_1,\ldots,l_m\}$

Let U be a set of users such that $U=\{u_1,u_2,\ldots u_n\}$

Let AUTH be a set of authentication methods such that $AUTH=\{auth_1,auth_2,\ldots\ldots auth_k\}$

Let P be a set of privileges $P=\{p_1,p_2,\ldots p_l\}$

Let T be a set of data types $T=\{D,C,B,A\}$

Let IM be a set of Identity Managers for sublevels such that

$IM=\{IM_{0_{\{l0\}}},IM_{0_{\{l0\}}},IM_{1_{\{l1\}}}IM_{1_{\{l1\}}},\ldots\ldots IM_{n_{\{ln\}}}\}$

Let Wi be the weight of each authentication method in AUTH as defined in table 2

Let Trail [Ui] be an array for calculating trial numbers of each user.

Let Per be the period assign to each users by each IM

Let R be a set of Ranks assigned to each user's trial such that

$R=\{Rl01(n)\ Rl02\ (n),,,,,,,,,,,\ Rlkm\ (n)\}$, *where n= number of each user's trial*

Step2: Testing New User with $auth_1$=Password

2.1:Set Traial$[U_{inew}]=0$

2.2: Test (U_{inew}*) with password*

If Test matches the correct password then

{

$n=1$

IM_{01} *Decides to enter sublevel* l_{01}

Per (U_{inew}*)=X units of time*

Set $R_{01}(n)$ *to* U_{inew}

}
Else
}
U_{inew} is rejected
Trial[U_{inew}]= Trial[U_{inew}]+1// Up to 3 trials
n=n+1
Go to step2
}
Endif
Print IM_{01} // This report contains users' name, period, trial numbers, Rank

Step 3: Testing users to transit to any other sublevels
Select the number of authentication methods n by the $IM_{ilevel0i}$
n=1

For i=1 to n
{
Test ($U_{i_{l_0}}$) with $auth_{i\ (see\ step2\ )}$
If w($Auth_i$) <50 then
{
IM_{01} decides to remain $U_{i_{l_0}}$ in its $level_{0i}$
Trail [$U_{i_{l_0}}$] = Trail [$U_{i_{l_0}}$] +1
} n=n+1
Else

If w($Auth_{i+1}$) >50 then
{
IM_{01} decides to transit u_{il0} to $level0_{i+1}$ with partial privileges
at percent y (y=the wight of $Auth_{i+1}$)of the total privileges of
$level_{0i+1}$
Trail [$U_{i_{l_0}}$] = Trail [$U_{i_{l_0}}$] +1

}
Else
If (w($Auth_i$) and w($auth_{i+1}$))=100 then
{
IM_{01} decides to transit u_{il0} to $level_{0i+1}$ with full
Privileges
}
Endif
} end for
Print IM_{02} // this report contains users' name, period, trial numbers, and Rank

Step4: Final level (level2) (Full Access)
Test (ui_{02}) with 3 authentication methods ($auth_1$, auth2, and $auth_3$)

If (w ($auth_1$) and w ($auth_2$) and w ($auth_3$)) =100 then
IM_2 decides to transit u_i from $level_{02}$ to $level_2$ with full access

Else
{
u_i is rejected
Trial [u_i]= Trial[u_i]+1 up to 2 times only .
}
Endif
Print IM_2 // this report contains users' name, period, trial numbers

….< $P(L_n)$ then the average probability is $(\sum_{i=1}^{i=n} P(L_i))/n$ which is less than P(X).

Another important point is that the privileges and data types are also granted in a manner that these privileges are assigned to the level of user's authenticity. This means that the lowest user's authenticity levels have trivial rights so when discovered it has little effect but gives an indication about the user's honesty. So, the access control used in this system is a grade access control which grants privileges to the degree of the importance of individual level. As a result, the multilevel system proposed ensures high security especially used in sensitive applications because we maintain a restricted amount of information relative to each sublevel sensitivity.

5. Results

Note: We will describe some of the results in detail, especially the transitions of new users to $level_{01}$ and the transition from $lvel_{01}$ to $level_{02}$ with the management action reports of each sublevel, but other levels transitions are described briefly since they are similar to the above levels . These results are obtained by using the proposed algorithm and they include different experimental results for selected users in different security levels and a limited numbers of user's trials

Table 5. Experimental results of amount of information

Total amount of information in one level H(X)	*Amount of information in l_{01} $H(x_{l01}),=H(x)*0.1$*	*Amount of information in l_{02} $H(x_{l01}),=H(x)*0.3$*	*Amount of information in l_{11} $H(x_{l01}),=H(x)*0.4$*	*Amount of information in l_{12} $H(x_{l01}),=H(x)*0.6$*	*Amount of information in l_{12} $H(x_{l01}),=H(x)*0.9$*
0.75	0.075	0.225	0.3	0.45	0.67 5
1.36	0.136	0.408	0.544	0.816	0.124
2.44	0.244	0.732	0.976	1.464	2.196
1.85	0.185	0.555	0.74	1.11	1.665

Fist: Examining new Users

Enter number of users: 5

The authentication method is: Password

The results are as follows (F=Fail, P=Pass):

Users	Result	Trial number	IM_{01}'s Decision
U_{1new}	F	1	Second trial
U_{2new}	P	1	Enter $level_{01}$
U_{3new}	P	1	Enter $level_{01}$
U_{4new}	F	1	Second trial
U_{5new}	F	1	Second trial

New users : Second Trial

Users	Result	Trial number	IM_{01}'s Decision
U_{1new}	F	2	Third trial
U_{4new}	P	2	Enter $level_{01}$
U_{5new}	F	2	Third trial

New users : Third Trial

Users	Result	Trial number	$IM_0$1's Decision
U_{1new}	F	3	Rejected
U_{5new}	P	3	Enter level01

Management report:

Users	Trial number	IM_{01}'s Decision	Rank in l_{01} (R_{01})
U_{1new}	3	Rejected	$R_{01}(3)$
U_{2new}	1	Enter $level_{01}$	$R_{01}(1)$
U_{3new}	1	Enter $level_{01}$	$R_{01}(1)$
U_{4new}	2	Enter $level_{01}$	$R_{01}(2)$
U_{5new}	3	Enter $level_{01}$	$R_{01}(3)$

Second : Transition from $level_{01}$ to $level_{02}$:

First trial:

Enter the number of users: 6

Users	Period (in months)	Authentication methods And their weights		Result	IM_{02}'s Decision
		Password (40)	Multiple Questions(60)		
$U_{1Level01}$	3	P	F	F	Remains in $Level_{01}$
$U_{2Level01}$	3	F	P	Partial P	Transits to $level_{02}$ with restricted privileged (Partial P
$U_{3Level01}$	3	P	P	P	Transits to $level_{02}$
$U_{4Level01}$	3	F	P	Partial P	Transits to $level_{02}$ with restricted privileged (Partial
$U_{5Level01}$	3	P	P	P	Transits to $level_0$2
$U_{6Level01}$	3	F	F	F	Remains in $Level_{01}$

Transition from $level_{01}$ to $level_{02}$:

Second trial (with new users of $level_{01}$)

Enter the number of users: 6

Users	Period (in months)	Authentication methods		Result	IM_{02}'s Decision
		Password (40)	Multiple Questions(60)		
$U_{1Level01}$	5	P	P	P	Transits to $level_{02}$
$U_{2Level01}$	8	F	F	P	Returns to $level_{01}$
$U_{7Level01}$	3	P	P	P	Transits to $level_{02}$
$U_{4Level01}$	8	F	F	F	Returns to $level_{01}$
$U_{8Level01}$	3	P	F	F	Remains in $Level_{01}$
$U_{6Level01}$	3	F	P	Partial P	Transits to $level_{02}$ with restricted privileged (Partial

Transition from $level_{01}$ to $level_{02}$:
Third trial (with new users of $level_{01}$)
Enter the number of users: 8

Users	Period (in months)	Authentication methods		Result	IM_{02}'s Decision
		Password (40)	Multiple Questions(60)		
$U_{9Level01}$	3	F	F	F	Remains in $Level_{01}$
$U_{10Level01}$	3	F	P	Partial P	Transits to $level_{02}$ with restricted privileged (Partial
$U_{11Level01}$	6	P	P	P	Transits to $level_{02}$
$U_{4Level01}$	8	P	P	P	Transits to $level_{02}$
$U_{8Level01}$	8	F	F	F	Remains in $Level_{01}$
$U_{6Level01}$	8	P	P	P	Transits to $level_{02}$
$U_{12Level01}$	3	P	F		Remains in $Level_{01}$
$U_{13Level01}$	3	P	P	P	Transits to $level_{02}$

Management report:

Users	Trial number	IM_{01}'s Decision	Rank in l02 (R_{02})
$U_{1Level01}$	2	Transit to $level_{02}$	R_{02} (2)
$U_{2Level01}$	2	Transit to $level_{02}$	R_{02} (2)
$U_{3Level01}$	1	Transit to $level_{02}$	R_{02} (1)
$U_{4Level01}$	3	Transit to $level_{02}$	R_{02} (3)
$U_{5Level01}$	1	Transit to $level_{02}$	R_{02} (1)
$U_{6Level01}$	3	Transit to $level_{02}$	R_{02} (3)
$U_{7Level01}$	1	Transit to $level_{02}$	R_{02} (1)
$U_{8Level01}$	2	Remains in $level_{01}$ and have only one next trial	Maintains his rank in $level_{01}$
$U_{9Level01}$	1	Remains in $level_{01}$ and have only two next trials	Maintains his rank in $level_{01}$
$U_{10Level01}$	1	Partial pass in $level_{02}$ and have 2 next trials	R_{02} (4) ,the lowest rank
$U_{11Level01}$	1	Transit to $level_{02}$	R_{02} (1)
$U_{12Level01}$	1	Remains in $level_{01}$ and have only two next trials	Maintains his rank in $level_{01}$
$U_{13Level01}$	1	Transit to $level_{02}$	R_{02} (1)

Third: Transition from level02 to level11
First Trial:
Enter number of users: 4

Users	Period (in months)	Authentication methods And their weights		Result	IM_{02}'s Decision
		EL-Gamal(70)	Multiple Questions(30)		
$U_{1Level0}2$	5	P	F	Partial Pass	Transits to $level_{11}$ with restricted privileges
$U_{2Level0}2$	8	F	P	F	Remains in $Level_{02}$
$U_{3Level0}2$	3	P	P	P	Transits to $level_{11}$
$U_{4Level01}$	8	F	F	F	Remains in $Level_{02}$

Fourth: Transition from level11 to level12
First Trial:
Enter number of users: 3

Users	Period (in months)	Authentication methods		Result	IM_{02}'s Decision
		Handshaking (80)	Multiple Questions(20)		
	5	P	F	Partial Pass	Transits to $level_{12}$ with less restricted privileges
$U_{2Level}11$	8	F	P	F	Remains in Level*11*
$U_{3Level0}11$	3	P	P	P	Transits to $level_{12}$

Transit from level12 to level2
First Trial:
Enter number of users: 3

Users	Period (in months)	Authentication methods			Result	IM_{02}'s Decision
		RSA	EL-Gamal)	Handshaking		
$U_{1\ l12}$	5	P	F	P	F	Remains in Level 1_2
$U_{2\ l12}$	8	F	F	P	F	Remains in Level 1_2
$U_{3\ l12}$	3	P	P	P	P	Transits to level2

6. Conclusion

The multilevel authentication method proposed in this work relies on applying different authentication levels. Using different authentication levels protects especially sensitive system from fraud and penetration .The important property of this system is that the users working in one level must be tested against different authentication methods in order to transit to another highest authenticated levels. For each level, the users in that level are granted certain privileges and the value of these privileges depends closely to that level .So, if a certain user is at a lower level, he/she may use simple privileges in order to perform simple data types. In order to examine his/her honesty in the sensitive application, an identity manager for each sublevel whose responsibility is to apply more sophisticated authenticated methods and the users must pass these methods to transit him /her to the next highest sublevel.

One of the advantages of this system is that there are different authentication methods, each of which with a certain weight depending on the security class of these levels as explained in Table1. Also, the manager of each level designated periods to different users after which the users may be tested to grant them more advanced privileges and data types. Also, the proposed system presents a new technique which is different from other MLS systems in that this technique uses a transition's management according to the level's sensitivity instead of only labeling security levels as all other techniques implement.

Finally the manager of each sublevel must generate a report describing user's activities. This report is very important because it reflects user's behaviors and number of fail trials to be a monitoring agent about all users' authenticity and uses the security management concepts which are the effective way to enhance secure system.

References

[1] Hossein B., Handbook of Information Security, Volume 3, Threats, Vulnerabilities, Prevention, Detection and Management, ISBN 0-471-64832-9, John Wiley, 2005.

[2] ibm.com/servers/eserver/.../pdf/share_08_2003_ Multilevel_Overview.pdf

[3] George M., “Multilevel Security," *SHARE* Washington DC, Session 1736, RACF Development , 2003.

[4] Lampson B., "Dynamic protection structures," *Proc. AFIPS 1969 FJCC*, vol. 35, AFIPS Press, Niontvale, N.J., pp. 27-38.

[5] http://en.wikipedia.org/wiki/Multilevel_security

[6] Patel D., Collins R., Vanfleet W., Calloni B. , Wilding M., MacLearn L, & Luke J. A., (2002 November 13). "Deeply Embedded High Assurance (Multiple Independent Levels of Security/Safety) MILS Architecture," Center for research on economic development and policy reform, Retrieved on 2005-11-06.

[7] Wayne J., Korolev S., and Thomas H., "A Framework for Multi-mode Authentication: Overview and Implementation , Guide Computer Security Division," *Information Technology Laboratory* ,National Institute of Standards and Technology , 2003

[8] Bell D., and LaPadula L., "Secure computer systems," *Unified exposition and ,mastics interpretation. MITRE technical report*, MITRE Corporation, Bedford Massachusetts, 2997

[9] Anderson J. P, "Computer security technology planning study," *Technical report*, ESD-TR-73-51, Oct. 1972.

[10] Laddad R., "AspectJ in Action: Practical Aspect-Oriented Programming," *Manning*, 2003.

[11] Welch I., and Stroud R., "Re-engineering security as a crosscutting concern," *Computer . J*, 46(5):578–589, 2003.

[12] Bell D.,and La Padula L., "Secure computer system,″ Unified exposition and MULTICS interpretation. Report ESD-TR-75-306, The MITRE Corporation,March 1976.

[13] Denning D., "A lattice model of secure information flow," *Communications of the ACM*, vol. 19, no. 5, pp 236-243, 1976.

[14] TNI. "Trusted computer system evaluation criteria: trusted network interpretation," Technical report, National Computer Security Center, 1987. Red Book.

[15] Foley S., "Aggregation and separation as noninterference properties," *Journal of Computer Security*, 1(2):159{188, 1992.

[16] Sandhu R., "Lattice based access control models," *IEEE Computer*, vol. 26, no. 11, pp 9-19, November 1993.

[17] Foley S., "The specification and implementation of commercial security requirements including dynamic segregation of duties," *In ACM Conference on Computer and Communications Security*, pp 125-134, 1997.

[18] Lee T., "Using mandatory integrity to enforce `commercial' security,". *In Proceedings of the Symposium on Security and Privacy*, pages 140{146, 1988.

[19] Sandhu R., "Role hierarchies and constraints for lattice-based access controls," *In ESORICS*, 1996.

[20] Popescu B., Crispo B., and Tanenbaum A., "Support for multi-level security policies in drm architectures," *In 13th New Security Paradigms Workshop*, 2004.

[21] Schellhorn G., Reif W., Schairer A., Karger P., Austel V., and Toll D., "Verification of a formal security model for multiplicative smart cards," *In ESORICS*, pp 17-36, 2000.29. F.B. Schneider. Enforcable

[22] Rivest R., Robshaw M., Sidney R., and Yin Y., "The RC6TM Block cipher, ", *M.I.T Laboratory for Computer Science*,USA, 1998.

[23] Farag A., and Osama S., "Multilevel Security Computer Networks,", Msc Thesis, Dept. of Computer Sciencand Engineering, Faculty of Electronic engineering, Menoufia University, Menouf, Egypt, Aug. 2001.

[24] Bell D. and LaPadula L., "Secure computer systems: Unified exposition and multics interpretation," MITRE technical report, MITRE Corporation, Bedford Massachusetts, 2997:ref A023 588, 1976.

[25] Robert C., and Gloria B., "The Need for Information Security Providing the Basic Building Blocks for Computer & Communications Security*," The Multilevel Information Systems Security Initiative(MISSI*), 1995.

[26] European Commission Directorate General For Informatics," Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms" , Brussels, Version: v1.1, 5 Sept. 2007

[27] Seberry J., Pieprzk J., "Cryptography : An introduction to Computer Security," Printice Hall, 1989.

[28] Dietel H., *Operating Systems*, Second Edition , Addison-Wesley Publishing Company ,1990.

Andulameer Hussain is an assistant professor at the Faculty of Science and Information Technology at Zarka Private University (ZPU), Jordan. He got his B.Sc. in 1975 from Baghdad University, M.Sc. and in 1993 from Saddam University and Ph.D. in 2002 from Al-Neelain University, Sudan. Before joining ZPU, he worked as a staff member in the 7-of April University (Libya) .His research interests include Cryptography, Network Security, System Management.