Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/050303

Employing Multi-Level Authentication Protocol for Securing Intelligent Systems

Ahmed A. Elngar[1,*], *Kamal A. ElDahshan*[1], *Ashraf Aboshosha*[2] *and Eman K. Elsayed*[1]

[1]Math & Computer Science Department, Faculty of Science , Al-Azhar University, Cairo, Egypt
[2] NCRRT, Atomic Energy Authority, Cairo, Egypt

Received: 27 Jul. 2016, Revised: 16 Aug.2016, Accepted: 26 Aug. 2016
Published online: 1 Sep. 2016

Abstract: Most authentication schemes are using passwords only to restrict access to services. Which are suffering from many weaknesses, such as key-logger attack and dictionary attack. Also, other authentication schemes are using physical token such as smart cards. These schemes are also impractical due to their infrastructure requirements. Since, many researchers have proposed a various of authentication schemes which rely on a single level security. So it is important to use multi-level security which is implemented especially in sensitive applications. This paper proposes an efficient multi-level user authentication protocol called *"ElDahshan Authentication protocol"* based on different authentication methods for each level. Where each level contains different authentication methods with its own privileges.These security levels are managed by an identity Manager. To validate the proposed protocol we applied it for user authentication on two web services such as Content Management System and Online Voting System.

Keywords: Authentication, Internet Security, Multi-Level Authentication, User Authentication

Nomenclature

EAP	ElDahshan Authentication protocol
IM	Identity Manager
CMS	Content Management System
OVS	Online Voting System
TBPA	Text Based Passwords Authentication
IPAuth	Internet Protocol Authentication
MMA	Machine-Metrics Authentication
MLA	Multi-Level Authentication
MCA	Multi-Channel Authentication

1 Introduction

With the rapid progress of computing technologies, internet has become the most convenient environment for businesses, content management systems (*CMSs*) and online voting systems (*OVSs*) around the world [1]. Thus, internet security is a significant issue to keep the confidential information secret from being accessed by unauthenticated users [2]. Since, remote user authentication plays the most important service on the internet. It is the process of identifying an authorized user, machine or any other entity, which requesting access for a particular web service on the internet under security constraints.[3].

Most authentication schemes are using text based passwords authentication *TBPA* only. Which are not secure enough for many applications that enforce security by access control mechanisms. Also, other authentication schemes are using smart cards to restrict services [4]. These schemes are also impractical due to their infrastructure requirements [5].

This paper proposes a security way regarding secure remote users authentication to the web service, by implementing Multi-Level Authentication (*MLA*) technique. *MLA* is simple enough, cost effective and does not need any additional hardware.

In this paper, the proposed ElDahshan Authentication protocol *EAP* makes the security measures of the remote user authentication more stringent. Where *EAP* is based on different authentication methods for each level; such as integrating text based passwords method with multi-channel authentication (*MCA*) method. Therefore, it helps to overcome many challenging attacks such as replay attack, DoS attack. Also, integrating text based passwords method with machine-metrics authentication

* Corresponding author e-mail: elngar_7@yahoo.co.uk

(MMA) method at another level. It offers a strong protection against several attacks such as stolen or lost tokens attacks, phishing attacks and credential compromising attacks. Hence, the major goal of this paper is proposing a protocol for remote user authentication depending on *MLA*. So highly confidential data, use *MLA* is much more secure than traditional authentication schemes.

The rest of this paper is organized as follows: Section 2 briefly reviews related works. Section 3 it is devoted to a survey of some of the existing authentication methods such as; IP Authentication, Multi-Channel Authentication, Machine-Metrics Authentication, Multi-Level Authentication. Section 4 introduces the Proposed Multi-Level Authentication Protocol. Section 5 gives the implementation and Mathematical Security Analysis. Section introduces applicable two systems using Eldahshan authentication protocol. Finally, Section 7 contains the conclusion remarks.

2 Literature Survey

Authentication, confidentiality, anonymity, and non-repudiation are four of the main principles to access e-services. Most of research was concentrated on using multi factor authentication. Authors of [6], describe 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 *MLA* system described in [7,8]. The system is based on the security standard levels employed to transfer text and images through wide area networks. It provides several levels of security, which include digital signature, encryption, compression, and smart card technology. This scheme is impractical due to their infrastructure requirements and lack of encryption method.

In our protocol we concentrate on *MLA* technology; because it is an essential part in a voting/WCMS procedure. Since, GNU.FREE is a free Internet voting system released by the GNU project [9]. In GNU.FREE, voting is not done over the Web. Rather, a stand-alone Java program is used to cast votes which are encrypted using a cipher (BlowFish). The system does not provide sufficient security (beyond preventing regular eavesdropping), and it is easy for a malicious system to correlate voters and their votes.

A protocol in [10] also is designed without employing any cryptographic techniques. In this; voters would submit their vote along with a unique identification number to a validator who would then take their name off on a list of registered voters. Then the validator would then strip off the Unique Identification number and submit just the votes to the tallier who would count the votes. Although this system has the advantages of being flexible, convenient and mobile, this system is far from secure. If the validator is compromised votes can be easily traced back to the voter or votes could be changed. Both privacy and accuracy lack with this protocol. There is no way to ensure the voter's privacy and the tallier accurately records the votes.

Given that CMS is a software application, it is prone to bugs just like any other program [11]. Vulnerabilities have been found in WCMS. As one example, a vulnerability called ?absolute path traversal vulnerability? was found in the open source product OpenCms in 2006. This flaw would allow remote authenticated users to download arbitrary files.

Another security concern lies with protection of authentication credentials when accessing CMS. Many CMS products are designed primarily to solve the content management problem of websites rather than building a secure product. Some WCMS products do not provide adequate protection for logins and passwords for example, and these passwords including the administrator password are sent as plain text over the network [12].

Similarly, as part of the publishing/uploading process, a*CMS* might use file transfer protocols such as FTP to transfer files from the *CMS* data storage server to the web server. FTP is not a secure protocol in the sense that authentication credentials and passwords are sent as plain text over the network. In addition, because publishing is an automatic process from the *CMS* to the production web server, FTP credentials might be hard coded in certain configuration files. Usually a hard-coded login password like this will not be changed regularly. As a result, any leakage of this password could allow someone illegally access to web content on the production web server [13].

3 An overview

There are various different authentication methods. This section presents a general overview of some of the available authentication methods. And how are these methods used to verify the authorized users of a web service on the internet.

3.1 IP Authentication $(IPAuth)$

One way to secure the connection between the server S and a legitimate user (U) is internet protocol authentication $(IPAuth)$. Which restricting the access based on the IP address. Where, the server only accept addresses coming from specific addresses corporation IP^*. Thus, the server considers any access excepted these specific addresses to suspect belong to malicious users [14].

3.2 Text based passwords Authentication $(TBPA)$

Passwords are the most commonly method used for user authentication. It plays an important role in daily life in various computing applications like ATM machines, internet services, windows login, authentication in mobiles etc. Which restricting unauthorized users to access the system [15].

3.3 Machine-Metrics Authentication (MMA)

Machine-metrics are metrics collected about a remote machine for the purpose of identification. Authors in [18] proposed a machine-metrics authentication protocol. The proposed protocol enhances the security of remote authentication depending on machine-metrics, instead of using the traditional smart card for remote user authentication. The proposed protocol is powerful, reliable, privacy-preserving and theft-proof. Hence, machine-merics are hashed using *RC4-EA Hashing* function $RC4-EA\ Hashing$ to guarantee high security and usability.Therefore, the data can not be easily retrievable without adequate authorization. Thus, the proposed authentication protocol is more convenient, because the burden of carrying a separate hardware token is removed. Moreover, this protocol helps to overcome many challenging attacks such as stolen or lost tokens attacks, phishing attacks and credential compromising attacks.

3.4 Multi-Channel Authentication (MCA)

Remote user authentication plays the most significant process to verify the authorized users of a web service on the Internet. Authors in [16] proposed "Multi-Channel User Authentication Protocol based on Encrypted Hidden OTP" . Where, the protocol proposed an efficient one time password (OTP) based authentication over a multi-channels architecture. Which, applying the RC4-EA encryption method to encrypt the plain-OTP to cipher-OTP [17]. Then, Quick Response Code (QR) code is used as a data container to hide this cipher-OTP. Also, the purposed is integrating a web based application with mobile-based technology to communicate with the remote user over a multi-channels authentication architecture [16].

3.5 Multi-Level Authentication (MLA)

Multi-level Authentication (MLA) was developed by the USA military in the 1970 [19]. MLA is a technique used to Prevent users from accessing information with different sensitivities; for which they do not have authorization. Also MLA is used in grid applications, where administrative can set multi-level policies on their applications. Which allow users to share some information with particular classes, while preventing a sensitive information from the others [19]. Hence, MLA is concerned with controlling the flow of information in systems. Therefor, MLA is one of ensuring that information at a high security levels cannot flow down to a lower security levels [20].

4 The Proposed ElDahshan Authentication Protocol

The major aim of the proposed *"ElDahshan Authentication Protocol (EAP)"* based on different authentication methods is securing the confidential information. The proposed protocol is enhancing user authentication protocol in [18]. Suppose that the protocol involves a set of different users $U = \{u_1, u_2, ..., u_n\}$, so these users must work in different authentication levels $L = \{l_1, l_2, ..., l_m\}$. The process of breaking the proposed protocol depends on the security classes as shown in Table 1.

Table 1: Notations of Security Classes

Authentication Class	Authentication Level
Low Security	l_0
Low Medium Security	l_1
Medium Security	l_2
High Security	l_3

Figure 1 illustrates the EAP architecture which consists of a server (S), a remote user (U_i) and Identity Manager (IM) of the Web service. The communication between the (S), the (U_i), and (IM) is based upon $HTTPS$. The EAP has three fundamental modules as shown in figure 1 which are:

1. Initialize setup module ISM is responsible of generate Random Nonce Codes.
2. User Registration and Generate Token Module RTM is responsible of handling the users' registration and request tokens.
3. Ticket Granting Module TGM is responsible of handling the users' authentication levels.

EAP consists of four phases : Preparation Phase, User enrollment phase, machine-metric enrollment phase, and authentication phase.

The notations employed throughout this protocol are shown in table 2.

4.1 Preparation Phase

In this phase, IM enrolls U_i at S in order to use Enrollment Phase. IM, U_i and S executes the following

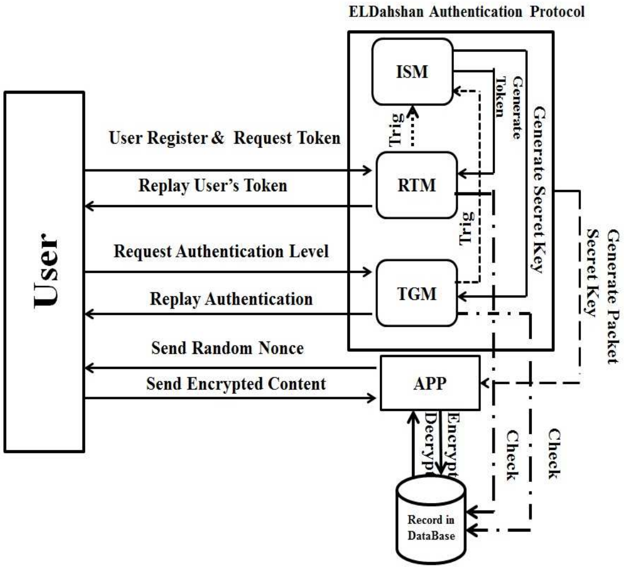

Fig. 1: Architecture of *EAP*

Table 2: Notations of *EAP*

Notation	Description
U_i	Remote User
U_i^{id}	User Identity
U_i^{PW})	User Password
U_i^{IP}	User IP Address
U_i^{WIP}	A White list of Allowed IP Addresses
ISM	Initialize setup module
RTM	User Registration and Generate Token Module
TGM	Ticket Granting Module
U_i^{Prox}	User Using Proxy
U_i^{SSN}	User Social Security Number
U_i^{rn}	Random Number
U_i^{mob}	User Mobile
U_i^{em}	User Electronic Mail
S	The Server
TK	Token
$h(.)$	One Way Hash Function
$(E/D)_{RC4-EA}$	Encryption / Decryption Using RC4-EA Method
$(E/D)_{QR}(.)$	Function that Encodes/Decodes Data into (QR) Code
$RC4-EA\ Hashing$	RC4-EA Hashing Function
$\|\|$	Concatenation
cc	confirmation code
T	Time Stamp
r_1,r_2,r_3	Random Nonce Generated by the Server
T_c, T_{end}	Time Created, Ended of Random Nonce
CSP	The Client Side Program
V_i^{UHI}	Hashing for Index the user
D_i^{HMM}	Hashing Machine-metrics
RNC	Random Nonce Code

steps:

1.IM enrolls user's a social security number U_i^{SSN} at S with status $stat = 1$ and time created T_c.
2.IM assigns IP address U_i^{IP} to U_i (option).
3.IM assigns authentication levels l_m with the privileges p_s to U_i.
4.S examines the U_i^{SSN}. If it is invalid, then rejects it. Otherwise, S stores the values U_i^{SSN}, $stat$, and T_c in its database.

$$S \rightarrow DB : \{U_i^{SSN}, U_i^{IP}, stat, T_c\} \quad (1)$$

4.2 User Enrollment Phase

In this phase, U_i enrollments at ISM and RTM modules in S, in order to use a service. U_i and S executes the following steps:

1.U_i enters his social security number U_i^{SSN} to open the enrollment phase.
2.RTM examine the U_i^{SSN}. If it is invalid, then rejects it. Otherwise, open the enrollment phase and change the value of $stat$ from 1 to 0, then store the time expired T_{exp}.
3.U_i chooses an identity U_i^{id}, mobile number U_i^{mob}, electronic mail U_i^{em}, and password U_i^{PW}. Then computes $X_i = h\ (U_i^{id}||U_i^{PW})$. Then sends $\{U_i^{id}, U_i^{mob}, U_i^{em}, X_i, T_1\}$ to S via a secure channel.

$$U \rightarrow RTM : \{U_i^{id}, U_i^{mob}, U_i^{em}, X_i, T_1\} \quad (2)$$

4.ISM module generate random nonce U_i^{rn}.
5.RTM modules examine the time stamp T_1. If it is invalid, then rejects it. Otherwise, checks whether U_i^{id}, U_i^{mob}, U_i^{em}, is available for use. If it is, RTM computes $Y_i = h(X_i||U_i^{rn})$. Finally, RTM stores the values U_i^{id}, U_i^{mob}, U_i^{em}, U_i^{rn}, and Y_i with U_i^{SSN} in its database.

$$RTM \rightarrow DB : \{U_i^{id}, U_i^{em}, Y_i, U_i^{rn}, U_i^{mob}\} \quad (3)$$

6.ISM generate random Token TK, then RTM sends TK to U_i via U_i^{em}/U_i^{mob}.

$$RTM \rightarrow U_i : \{TK\} \quad (4)$$

7.Finally, RTM stores the values TK in its database.

$$RTM \rightarrow DB : \{TK\} \quad (5)$$

4.3 Machine-metrics Enrollment Phase

In this phase, the physical metrics of a machine are collected to be used as the identification of the machine. Suppose the physical metrics space is C which consists of n metrics; $C = \{metr_1, metr_2, ..., metr_n\}$. The CSP will returns $metr_i \in C, (i = 1, 2, ..., g)$. U_i, S and CSP execute the following steps:

1. After U_i received his TK from RTM via U_i^{em}/U_i^{mob}..
2. U_i enters his TK to CSP to enrollment his machine.
3. CSP reads $metr_1$, $metr_2 \in C$. Then computes: $V_i^{UHI} = RC4 - EA\ Hashing(metr_1||metr_2)$. Then stores the value V_i^{UHI} in DB.

$$CSP \rightarrow DB : \{V_i^{UHI}\} \quad (6)$$

4. CSP uses TK as a secret seed for $RC4 - EA\ Hashing$, then computes:

$$D_i^{HMM} = RC4 - EA\ Hashing_{TK}(metr_1||metr_2||...||metr_g)$$

5. Finally, CSP stores the values D_i^{HMM} in a remote database DB.

$$CSP \rightarrow DB : \{D_i^{HMM}\} \quad (7)$$

4.4 Authentication Phase

After U_i has a successful enrollment, TGM in S wants to authenticate U_i upon his authentication level l_m with the privileges p_s granted by IM. This phase is evaluated by multiple levels authentications:

–User's Authenticated at l_0
$(IPAuth)$ is a protocol suite for securing internet communications by authenticating each IP packet of a communication session. $IPAuth$ takes place between two parties of a TGM in S and a user U_i. Which considered as preliminary authentication level l_0 to authenticate U_i. If the U_i passes this level l_0, then he assigns to next authentication level with grants privilege. Otherwise he blocked. The various steps of $(IPAuth)$ will be explain below:

1. Assume that U_i requests TGM to join the web service.
2. TGM checks U_i^{Prox} :
   If U_i access the web service using proxy.
   then TGM block the U_i connection
3. The TGM gets U_i^{IP}
4. The TGM checks the white list of IP addresses
   $if(U_i^{IP} == U_i^{WIP})$.
   then U_i assigns to next authentication level
   else
   Reject connection and block

–User's Authenticated at l_1
After U_i has a successful passes level l_0, User's at this level must be examined by password authentication Technique to grant his privilege. The authentication at this level is shown in the following steps:

1. U_i enters his U_i^{id} and U_i^{PW}, and computes $X_i^{'} = h(U_i^{id}||U_i^{PW})$, then send U_i^{id}, $X_i^{'}$, T_2 to TGM.

$$U \rightarrow TGM : \{U_i^{id}, X_i^{'}, T_2\} \quad (8)$$

2. TGM examines the time stamp T_2. If it is invalid, then rejects it. Otherwise, S computes $Y_i^{'} = h(X_i^{'}||U_i^{rn})$, then checks whether U_i^{id} is valid and $Y_i^{'} == Y_i$. If it is, user authentic at this level and use his privilege. Otherwise, S ask U_i a maximum 3 attempts to provide his correct U_i^{id} and U_i^{PW}.
   If U_i exceeds this threshold, then S considers U_i as an attack and block his account.

–User's Authenticated at l_2
After U_i has a successful passes level l_0. User's at this level must be examined by password authentication Technique. Additionally will face another authentication technique such as MMA to grant his privilege.

After U_i has a successful Machine-metrics Enrollment. Now TGM wants to authenticate the machine upon CSP. The machine-metrics authentication process is shown in the following steps:

1. CSP reads $metr_1$, $metr_2 \in C$. Then computes: $V_i^{UHI'} = RC4 - EA\ Hashing(metr_1||metr_2)$.
2. CSP checks whether $V_i^{UHI'} == V_i^{UHI}$. If it is, then CSP gets the TK.
3. CSP computes:

   $$D_i^{HMM'} = RC4 - EA\ Hashing_{TK}(metr_1||metr_2||...||metr_g)$$

   using TK as a secret seed.
4. CSP checks whether $D_i^{HMM'} == D_i^{HMM}$. If it is, then CSP generates RNC to U_i with the $status = 1$ using $RNGCryptoServiceProvider$, which gives an unguessable crypto strength seed. Hence, it gives the random object with a different crypto strength number each time. Which mean is that, it will go on to return a different random number for each call. Then CSP stores the values RNC in DB.

$$CSP \rightarrow DB : \{RNC\} \quad (9)$$

5. U_i sent RNC to TGM via web application.
6. Finally, TGM checks whether RNC is invalid or not match with user credentials at the DB then, "request is rejected". Otherwise, user's machine is authentic at this level with his privilege and convert RNC status to 0.

–User's Authenticated at l_3
After U_i has a successful passes level l_0, User's at this level must examined by password authentication

Technique, and MMA. Also faces another authentication Technique such as MCA to grant his privilege. where, MCA composed of two Technique $OTQR$ and OTP. The authentication at this level is shown in the following steps:

Authentication by Email:

1. ISM generates a random nonce r_1 to TGM. Then TGM computes $Z_i = E_{RC4-EA}(r_1)$, then computes $A_i = (E)_{QR}(Z)$. Also S generates a confirmation code cc. Finally, TGM stores A_i, cc, T_c, T_{end}, where A_i is $OTQR$.

$$TGM \rightarrow DB : \{A_i, cc, T_c, T_{end}\} \quad (10)$$

2. TGM sends A_i, cc, T_3 to U_i via mail channel.
3. U_i examines the cc which is an identification code for this mail, U_i should match with cc displayed on the screen; if matched, then the $OTQR$ sent in this mail is the $OTQR$ to be entered on the screen. Otherwise this mail is created by an attacker.
4. U_i examines the time stamp T_3. If it is valid, U_i send A_i', T_3' to TGM.
5. TGM checks whether $T_c \preceq T_3' \preceq T_{end}$ and $A_i' == A_i$. If it is, then user is authentic. Otherwise, not authentic user.

Authentication by Mobile:

1. ISM generates a random nonce r_2 to TGM. Then TGM computes $F_i = h(r_2)$. Finally, TGM stores F_i, T_c, T_{end}, where F_i is OTP.

$$TGM \rightarrow DB : \{F_i, T_c, T_{end}\} \quad (11)$$

2. TGM sends r_2, T_4 to U_i via mobile channel, then discards r_2 .
3. U_i examines the time stamp T_4. If it is valid, U_i enters r_2, then computes $F_i' = h(r_2)$ and sends F', T_4' to TGM.
4. TGM checks whether $T_c \preceq T_4' \preceq T_{end}$ and $F_i' == F_i$ is valid. If it is, then user authentic. Otherwise, not authentic user.

Now If U_i^{PW}, $OTQR$ and OTP holds, then TGM in S is convinced that user U_i is authentic at this level with his privilege. Otherwise, TGM asks U_i a maximum 3 attempts to provide his correct U_i^{PW}. If U_i exceeds this threshold, then S considers U_i as an attack and block his account.

After U_i has a successful passes his authentication levels in order to use a service and grants his privilege. U_i , EAP and web service execute the following steps as shown in figure 1:

1. EAP generates a random nonce r_3 (packet key) as a combination of user credentials to the web service .
2. The web service send a random nonce r_3 to U_i via secure channel.
3. U_i encrypts his contents using r_3. Then sends it to the application.
4. The web service decrypts the contents then sent to database.

5 Implementation and Security Analysis

The proposed EAP based on different authentication methods is securing a sensitive information.

The performance of the proposed authentication protocol is tested using server 32 core AMD opteron processor 6376 with 32 GB of RAM and 4 RAID 1s, laptop (Intel i5, 1.80 GHz processor, 2 GB RAM) and simple mobile phone. The experiments have been implemented using PHP-MySql and C-sharp language environment.

5.1 Implementation

The proposed EAP is integrating a different authentication methods at each level to grant U_i his privilege, which makes it more secure than the general authentication protocols. Tables 3, 4, 5, and 6 show some of results, especially the examining users at l_0 by using the $(IPAuth)$ authentication method. Also, the result shows the transition of users from l_0 to l_1 and the transition from l_0 to l_2 finally, the transition from l_0 to l_3. These results are obtained by using the proposed protocol and they include different experimental results for selected users in different security levels and a limited numbers of user's trials.

Table 3: First : Examining Users at l_0 The Authentication method : $(IPAuth)$, The Results $(F = Fail, P = Pass)$

U's	Result of $(IPAuth)$	Trial	Decision
u_1	F	1	Second Trial
u_2	P	1	Pass l_0
u_3	F	2	Third trial
u_4	F	3	Reject
u_5	P	3	Pass l_0

Table 4: Second : Transition from l_0 to l_1, The Results $(F = Fail, P = Pass)$

U's	Auth Method		Res	Trial	privilege
	$(IPAuth)$	Pass			
u_1	P	F	F	1	Second Trial
u_2	P	P	P	1	R
u_3	F	–	F	2	Third Trial
u_4	P	P	P	3	R
u_5	P	F	F	3	Reject

Table 5: Third : Transition from l_0 to l_2, The Results ($F = Fail, P = Pass$)

U's	Auth Method			Res	Trial	privilege
	$(IPAuth)$	Pass	MCA			
u_1	P	P	P	P	1	R/I
u_2	P	F	–	F	1	Second Trial
u_3	P	P	F	F	2	Third Trial
u_4	F	–	–	F	3	Reject
u_5	P	P	P	P	3	R/I

Table 6: Forth : Transition from l_0 to l_3, The Results ($F = Fail, P = Pass$)

U's	Auth Method				Res	Trial	privilege
	$(IPAuth)$	Pass	MCA	MM			
u_1	P	P	P	P	P	1	Full Access
u_2	P	F	–	–	F	1	Second Trial
u_3	P	P	P	F	F	2	Third Trial
u_4	F	–	–	–	F	3	Reject
u_5	P	P	P	P	P	3	Full Access

5.2 Mathematical Security Analysis

The security of the proposed protocol is analyzed under the probability of cracking its levels. It consists of m levels, where Multi authentication methods $auth_k$ are applied at each level for security purposes. I.e. $AUth = \{auth_1\}$ form the authentication for level l_0, and $AUth = \{auth_2, auth_3, auth_4\}$ together form the authentication for level l_3. Therefore, to access privileges available at level l_3, the expected authentication will be $AUth = \{auth_1, auth_2, auth_3, auth_4\}$.

Let eve be the event of cracking the protocol levels. The event can either be a success or a failure. Let $prob$ be the probability of success at each level. So in order to crack the proposed protocol levels, eve initially needs to crack the preliminary level l_0 and then Level l_b where, $b = 1, 2, ..., m$. Therefore, the probability of cracking Level b successfully is $P(eve) = Prob^{auth_k}$. Assuming $Prob = 0.1$, the possibility of successfully cracking l_3 will be 0.0001. Hence the probability of completely cracking the proposed is very less than the traditional authentication schemes.

5.3 Computational Complexity

The performance comparison of several password authentication schemes and our protocol are listed in Table 8. Where, T_E denotes the computation complexity of exponential operation. T_s denotes the computation complexity of symmetric encryption/decryption operation. T_H denotes the computation complexity of cryptographic hash operation. T_{dh} denotes the computation complexity of data hide into (QR) Code.

Note that, in our protocol, the computation complexity does not include the authentication steps for the user to validate the server. It is shown that our scheme uses less computational resources than others, thus our protocol is more suitable to be used in most online services. Furthermore, our protocol also provides mutual authentication which is important on ensuring the security of remote authentication protocols.

6 Applicable Web Services Using ElDahshan Authentication Protocol

To analyze the performance of ElDahshan proposed authentication protocol, a performance comparison between two applicable web services using the protocol is conducting. ElDahshan authentication protocol is configured based on what is common and what is dependent on the problem nature. The experiments of the two web services are evaluated in order to keep authorized users and there data in high confidential authentication levels.

Case Study 1: Content Management System (CMS)

A content management system (CMS) is a web service that facilitates a group of users, usually from different departments in an enterprise, to collaboratively maintain and organize the content of a website in an effective manner.

More enterprises are creating CMS that are personalized through the process of authentication and authorization. Hence, a specific series of contents is made available to a site users once they identify themselves through a pre-set of authentication methods.
To that extent it is vital that the enterprise's CMS integrate with the authentication system in a suitable manner such that appropriate content is presented to the user after they have been authenticated. Specifically a user should only see what they are authorized to see. Furthermore, under no circumstances should that web user be presented with any content that they are NOT authorized to see.

Case Study 2: Online Voting System (OVS)

Online voting system OVS is a significant tool. Which to allow voters to vote over the internet without the geographical restrictions with considers important criteria in evaluating $OVSs$ such as the democracy, mobility, and privacy.
OVS is a practicable alternative on account of the swift computer network and the benefits from cryptographic and hidden information techniques. The main aim of a secure OVS is to ensure the privacy of the voters and the accuracy of votes.
The full process of integrating ElDahshan authentication protocol to protect gated content/vote need

not be difficult for use today. The authentication process ensures that the right content gets delivered to the right user at the right time. It is a very scalable process to ensure the safety and confidentiality of the content as shown in figure 2 .

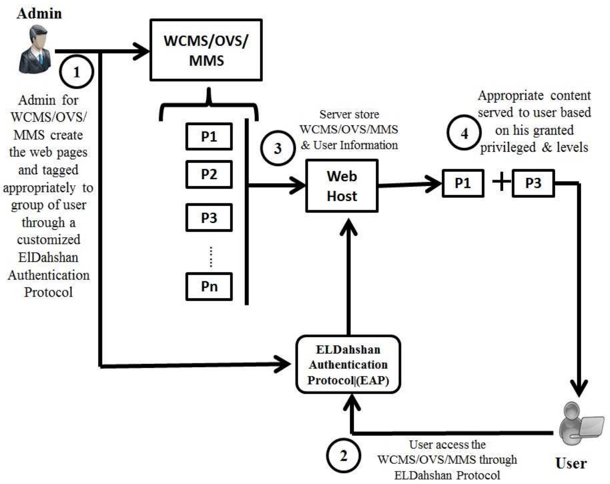

Fig. 2: Full process diagram depicting the integration between ElDahshan authentication protocol and the Web Service

The configuration of proposed ELDahshan authentication protocol which employed on the two web services CMS/OVS as shown in table 7

Table 7: The configuration of ElDahshan Authentication Protocol

ELDahshan Protocol	CMS	OVS
IPAuth	✓	×
Password	✓	✓
Multi Channel	✓(option)	✓(option)
Machin Metric	✓	×
Multi Level	✓	✓

Table 8: Comparison of Computational Complexity of Several Schemes and Our Protocol.

	Hwang [21]	Awas [22]	Ramas [23]	Ours
Enroll	$1T_E$	$1T_H + 1T_E$	$1T_E$	$2T_H$
Auth l_1	$1T_H + 3T_E$	$2T_H + 3T_E$	$1T_H + 2T_E$	$2T_H$
Auth l_2	$1T_H + 3T_E$	$1T_H + 3T_E$	$2T_H + 3T_E$	$1T_s + 1T_{dh} +$ $1T_H + Auth\ l_1$
Auth l_3	-	-	-	$2T_s +$ $4T_H + Auth\ l_1$
Mut-Auth	NO	NO	NO	Yes

7 Conclusions

The main contribution of this paper, is proposing ElDahshan authentication protocol. The proposed protocol enhances the security of a remote user authentication; by using different authentication methods for each level. Therefore, users at one level are granted certain privileges according to that level. Since, the sensitive information can not be easily retrievable without adequate authorization. Therefore, in order to examine user honesty in this sensitive proposed, an identity manager whose responsible to apply more sophisticated authenticated methods for each level. Thus, user should successfully across these methods in order to got his privileges. However, this protocol ensures that information at high authentication level cannot flow down to lower authentication level. Thus, ElDahshan authentication protocol is much more secure than traditional authentication schemes. ElDahshan proposed authentication protocol is applied for users authentication in two web services such as content management system (CMS) and online voting system (OVS), to keep there data in high confidential authentication levels.

References

[1] P.E.S.N. K. Prasasd , A.S.N. Chakravarthy, and B. D. C. N. Prasad, Performance Evaluation of Password Authentication using Associative Neural Memory Models, International Journal of Advanced Information Technology (IJAIT), vol. 2, no. 1, (2012), pp. 75-85.

[2] A. Hiltgen, T. Kramp, T. Weigold , ”Secure Internet Banking Authentication”, IEEE Transactions on Security and Privacy, vol. 4, no. 2,(2006), pp. 21-29.

[3] Sh. Kalra , S. Sood , ”Advanced remote user authentication protocol for multi-server architecture based on ECC”, journal of information security and applications, vol. 18, (2013), pp. 98- 107.

[4] C. Ma , D. Wang , and S. Zhao, ”Security flaws in two improved remote user authentication schemes using smart cards”, Int. J. Commun. Syst., (2012) .

[5] S. SK, ”Secure dynamic identity-based authentication scheme using smart cards”, Information Security Journal: A Global Perspective, vol. 20, no. 2, (2011), pp. 67-77.

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

[7] A. Farag , and S. Osama , ”Multilevel Security Computer Networks”, Msc Thesis, Dept. of Computer Sciencand Engineering, Faculty of Electronic engineering, Menoufia University, Menouf, Egypt, (2001).

[8] R. Rivest, M. Robshaw , R. Sidney , and Y. Yin , ”The RC6TM Block cipher”, M.I.T Laboratory for Computer Science, USA, (1998).

[9] GNU.FREE: Heavy-Duty Internet Voting, http://www.j-dom.org/users/re.html.

[10] I. Ray and N. Narasimhamurthi, ”An Anonymous Electronic Voting Protocol for Voting over the Internet, 3rd International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems (WECWIS?01), (2002), 21-22 June.
[11] G. Schryen , ”Security of open source and closed source software: An empirical comparison of published vulnerabilities”, Proceedings of the 15th Americas Conference on Information Systems, San Francisco, California, (2009) August 6-9.
[12] M. Meike, J. A. Sametinger , ”WiesauerSecurity in Open Source Web Content Management Systems”, IEEE Security and Privacy, vol. 7, no. 4,(2009), pp. 44-51.
[13] C. Payne , ”On the security of open source software”, Information Systems Journal, vol. 12, (2002), pp. 61-78.
[14] A. Aboshosha, K. A. ElDahshan, E. K. Elsayed, and A. A. Elngar, ””An Intelligent Secure Authentication Protocol for CMS Applications, Al-Azhar UniversityWorkshops Advances in Computer Research Work(ACR-2015), (2015).
[15] M. V. Prakash, P. A. Infant , and S. J. Shobana , Eliminating Vulnerable Attacks Using One Time Password and PassText Analytical Study of Blended Schema, Universal Journal of Computer Science and Engineering Technology, vol. 1, no. 2, (2010), pp. 133-140.
[16] A. Aboshosha, K. A. ElDahshan, E. K. Elsayed, and A. A. Elngar, ”Multi-Channel User Authentication Protocol based on Encrypted Hidden OTP”, International Journal of Computer Science and Information Security(IJCSIS), vol. 13, no. 6, (2015) pp. 14-19.
[17] A. Aboshosha, K. A. ElDahshan, E. K. Elsayed , and A. A. Elngar, ”EA Based Dynamic Key Generation in RC4 Ciphering Applied to CMS”, International Journal of Network Security (IJNS), vol.17, no.4,(2015), pp. 405-412.
[18] A. Aboshosha , K. A. ElDahshan, E. K. Elsayed , and A. A. Elngar , ”Secure Authentication Protocol based on Machine-metrics and RC4-EA Hashing”, International Journal of Network Security (IJNS), vol. 18, no. 6,(2016), pp.1080-1088.
[19] M. George , ”Multilevel Security”, SHARE Washington DC, Session 1736, RACF Development,(2003) .
[20] D. Denning , ”A lattice model of secure information flow”, Communications of the ACM, vol. 19, no. 5,(1976), pp 236-243.
[21] M. S.Hwang and L. H. Li , ”A new remote user authentication scheme using smart cards”, IEEE T. Consum. Electr., vol. 46, no. 1,(2000), pp. 28-30.
[22] A. K. Awasthi and S. Lal , ”A remote user authentication scheme using smarts cards with forward secrecy”, IEEE T Consum Electr, vol. 49, no. 4, (2003) pp. 1246-1248.
[23] R. Ramasamy, A. P. Muniyandi , ”New remote mutual authentication scheme using smart cards”, T. data privacy, vol. 2,(2009), pp. 141-152.

Ashraf Aboshosha graduated with a B.Sc. in industrial electronics from Menoufia University, Egypt at 1990. At 1997 he received his M.Sc. in automatic control and measurement engineering. From 1997 to 1998 he was guest researcher at research centre Julich (FZJ), Germany. From 2000 to 2004 he was a doctoral student (DAAD-scholarship) at Eberhard-Karls-University, Tubingen, Germany. Where he received his Doctoral degree (Dr. rer. nat.) at 2004. He is the CEO of ICGST LLC, Delaware, USA.

Kamal ElDahshan is a professor of Computer Science and Information Systems at Al-Azhar University in Cairo, Egypt. An Egyptian national and graduate of Cairo University, he obtained his doctoral degree from the Universite de Technologie de Compiegne in France, where he also taught for several years. During his extended stay in France, he also worked at the prestigious Institute National de Telecommunications in Paris. Professor ElDahshan’s extensive international research, teaching, and consulting experiences have spanned four continents and include academic institutions as well as government and private organizations. He taught at Virginia Tech as a visiting professor; he was a Consultant to the Egyptian Cabinet Information and Decision Support Center (IDSC); and he was a senior advisor to the Ministry of Education and Deputy Director of the National Technology Development Center. Prof. ElDahshan has taught graduate and undergraduate courses in information resources and centers, information systems, systems analysis and design, and expert systems. Professor ElDahshan is a professional Fellow on Open Educational Resources as recognized by the United States Department of State. Prof. Eldahshan is interested in training instructors to be able to use OER in their teaching and hopes to make his university a center of excellence in OER and offer services to other universities in the country.

Eman K. Elsayed is assist. Prof. Computer science, Al-azhar university, Master of computer science, Cairo University 1999, Bachelor of Science, mathematics and computer science Department, Cairo University 1994. I Published thirty four papers until 2015 in data mining, Ontology engineering, e-learning and software engineering. I also published two books in Formal methods and event B on Amazon database. I am a member of Egyptian mathematical society and Intelligent computer and information systems society. Finally, I’m a certified trainer in AQATC Alazhar Quality Assurance and Training Center.

Ahmed A. Elngar graduated with a B.Sc. in computer Science from computer science Department, Al-Azhar University 2004, Master of computer science in Intrusion Detection System (IDS) from Ain Shanm university 2012. Now he is a P.hD student at computer science Department, Al-Azhar University. Also he is a member in Egyptian Mathematical Society (EMS) and International Rough Set Society(IRSS).