Multilevel User Authentication and Identification Scheme for e-mail Clients

Artan Luma, Burim Ismaili, and Bujar Raufi

***Abstract*—User authentication and identification have always represented a challenge in web-based e-mail systems. The text-based authentication and user identification are not sufficient to address the security issues facing web-based e-mail systems. This sort of security is completely retrograde and obsolete for current security threats that easily undermine authentication, identification and non-repudiation. In this paper, a security increase in e-mail client is proposed by introducing multiple-level authentication and identification in e-mail clients. The proposed multilevel authentication and identification consist of four levels, where level-1 is the text-based authentication, level-2 involves an image based authentication and finally level-3 and level-4 use a specific algorithm that exploits the powerful properties of two mathematical operators called $Pentors$ and $UltraPentors$ applied against the image in level-2.**

***Index Terms*—user authentication, user identification, cryptography, image-based authentication**

I. Introduction

USER authentication and identification in e-mail clients have always represented a challenge in the Web. Email based user authentication and identification represent emerging techniques that appear as an alternative to the standard Public-Key-Infrastructure (PKI) and these approaches allow securing users from faulty impersonations and identity thefts [1]. However, the authentication and identification process in the web has not changed over the last twenty years and is mainly based on password identification and cookies [2]. The report from Google on email account security indicates that in 2011 and 2012 there is an increase in Google account blockings as a result of account hijacking and identity thefts [3]. The most widely used authentication strategy represents the text-based password scheme where users enter their login names and passwords. Despite their popularity, textual passwords suffer from several drawbacks. Although simple and straightforward textual passwords are easy to remember and maintain, they are more vulnerable to attacks. While complex and arbitrary passwords render the system substantially more secure, resisting the brute force search and dictionary attacks, they are difficult to guard and memorize [4]. Another aspect that advances the textual authentication is the graphical authentication which (compared to words) is easier to remember. Accordingly, it is difficult to formulate and orchestrate attacks for graphical authentication considering that the password space of graphical authentication extends more than that of textual passwords and makes them harder to crack and brute force attack resistant. Still, graphical authentication suffers from the so called shoulder-surfing which represents a hazard of intruder scrutinizing passwords by recording user sessions or directly supervising the users [5]. Some other related work regarding multilevel authentication is elaborated in [6] where the authors propose 3-level authentication based on textual, image based and one-time password fashion. However this kind of approach does not involve image encryption and their safe storage for avoiding direct compromise of the data used for authentication and identification. Other work involve the definition of a strict authentication system by introducing a multi-level authentication technique that generates a password in multi-level instances for accessing and using cloud services inside of which, an e-mail cloud service can reside as well [7]. The main goal of this paper is to focus mainly on securing user authentication and identification by the use of specifically designed encryption algorithms which is applied on the image while identifying the e-mail client. The rest of this paper is organized as follows: section 2 gives a brief introduction on two mathematical operators called $Pentor$ and $UltraPentor$ and elaborates their properties, section 3 introduces the three layer authentication and user identification methodology by using the above mentioned mathematical operators, section 4 gives a real life scenario of the above mentioned methodology with a use case and section 5 concludes this paper

Manuscript received March 6^{th}, 2013; revised April 5^{th}, 2013. This work was supported by South East Eurpean University, Research Department and Department of Contemporary Sciences and Technologies.

A. Luma is with the South East European University, Ilindenska no. 335, 1200 FYR. Macedonia (phone: (+389) 44 356 166; fax: (+389) 44 356 001 e-mail: (a.luma@seeu.edu.mk

B. Ismaili is a Master Student at South East European University, Ilindenska nn, 1200 FYR. Macedonia (e-mail: bi12858@ seeu.edu.mk)

B. Raufi with the South East European University, Ilindenska no 335, 1200 FYR. Macedonia (phone: (+389) 44 356 185; fax: (+389) 44 356 001; e-mail: b.raufi@seeu.edu.mk).

II. Cryptography With Pentor And Ultra Pentor

In [8],[9] a mathematical defintion for Pentor and Ultra pentor is introduced. A Pentor of a number is given as an integer number with base n and for every natural and integer number n there exists one $Pentor$ for the given base B. In order to represent this operator mathematically, we start from the modular equation for $Pentor$ of an integer number n with base B that fulfills the condition $gcd(n, B) = 1$. From the forementioned conditions the following was acquired [8]:

$$B^m P(n) \equiv 1(modn) \tag{1}$$

Where B represents the base of the integer number n, $P(n)$ is the $Pentor$ of the integer number, whilst n and m represent the order of the $Pentor$ for the given integer number. The modular expression 1 was transformed to the equality expression of the form:

$$B^m P(n) = 1 + nk \tag{2}$$

$$P(n) = \frac{1 + nk}{B^m} \tag{3}$$

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

where k is an integer number that fulfills the condition for the fraction to remain an integer number. For example if we want to find the $Pentor$ of the first order than $m = 1$, the Pentor of the second order than $m = 2$ and so on[8].

Likewise, the $UltraPentor$ of a number n with base B in which for every natural and integer number n there exists an $UltraPentor$ for the given base B [8]. In order to represent this operator mathematically, we start from modular equation for $UltraPentor$ of integer number n with base B that fulfills the condition $gcd(n, B) = 1$. Considering the above mentioned conditions, the modular equation for $UltraPentor$ will look like:

$$B^m \equiv 1(modn) \tag{4}$$

where m is an integer number. The modular expression [1], was transformed to the equality expression by applying logarithmic operations on both sides and finding the $UltraPentor$ as follows:

$$B^m = 1 + nl|\log_B \tag{5}$$

$$\log_B B^m = \log_B(1 + nl) \tag{6}$$

$$m \log_B B = \log_B(1 + nl) \tag{7}$$

where $\log_B = 1$ and there is:

$$m = \log_B(1 + nl) \tag{8}$$

If $m = UP(n)$ then $UltraPentor$ of an integer number n with base B can be written as:

$$UP(n) = \log_B(1 + nl) \tag{9}$$

where l is an integer number that fulfills the condition for $(1 + nl)$ to be written as B^a, where a is also an integer number [9]. The power of the above mentioned operators lie in their properties of irreversibility of retrieving the ID from the $Pentor$ or $UltraPentor$ itself which in our designed cryptosystem is kept secret on the user's side.

III. Multi-level Authentication for e-mail Applications

Based on the properties of the above mentioned two mathematical operators, a web application for an email client can be designed. This web application will be able to send / receive two types of e-mails:

- Send/receive regular (non-authenticated and non-identified e-mail)
- Send/receive authenticated and identified e-mail where the source of the sender is verified.

The aim of this web application is to authenticate and identify users while sending e-mails. The milestone of this application lies in the power of the two mathematical operators (Pentor and Ultra Pentor) as well as in the so called "Pentoric Attack" procedure.

The "Pentoric attack" is based on the following procedure. If we take, for example, the value for $ID = 13$ and based on the above mentioned formulas for Pentor 1 and Ultra Pentor 4 we can retrieve values for $Pentor(ID) = 4$ and $UltraPentor(ID) = 6$. Furthermore, if we take a particular value for a username such as $Username = art$ and by converting into an ASCII code we receive $Username = 97114116$ out of which we receive a vector by multiplying with the value of ID as follows:

$$Vector = 97114116 \cdot 13$$

$$Vector = 1262483508$$

Considering that Vector is consisted of 10-digit sequence which is greater than the value of the $UltraPentor$, we divide the sequence into 6-digit chunks starting from the right as illustrated below.

$$Vector = 1262|483508$$

By summing these two values, a new vector is acquired as follows:

$$Vector = 1262 + 483508 = 484770$$

This represent a 6-digit sequence which is smaller or equal to the value of Ultra Pentor and the "Pentoric Attack" procedure can be applied in following way:

```
     4 8 4 7 7 0 <- 4
+              0
-------------
     4 8 4 7 7 <- 4
+        2 8
-----------
     4 8 7 5 <- 4
+      2 0
---------
     5 0 7 <- 4
+    2 8
-------
     7 8 <- 4
+ 3 2
-----
   3 9 <- 4
+ 3 6
-----
   3 9
```

From the example, it is seen clearly that the final value from the "Pentoric Attack" is $N = 39$ which should be fully divisible by the value of ID, i.e. $13|39$. From here it can be certainly concluded that the vector originates from user with $Username = art$ and $ID = 13$.

The logic of authentication and identification process for this application is based on the following procedure. The user that wishes to use the services of the application initially sends the credentials such as $Name$, $Surname$, $Username$ and an $Image$ of its choice. During the registration process, in the database values for the user such as $Name$, $Surname$, $Image$ and $Vector$ is stored. In the $Image$ attribute, the location of the image is stored where initially the image is converted into an RGB matrix $M(R, G, B)$ and encrypted with the following formula:

$$M_c(R, G, B) \equiv M(R, G, B) \cdot ID \cdot UltraPentor(ID)$$

The $Vector$ attribute on the other hand is received by converting the username characters to their respective ASCII counterparts and by multiplying with the user's ID.

$$R = Username_{ascii} \cdot ID$$

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

This value of R should be divided into sequence chunks the size of $UltraPentor$ starting from the right side as follows:

$$R = R_n|R_{n-1}|\ldots|R_2|R_1$$

After each separation R_i, the divided chunks are added together $R = R_n + R_{n-1} + \ldots + R_2 + R_1$ and if the size of $Vector$ is greater than the value of $UltraPentor$, the procedure is repeated until the length is less or equal to that of $UltraPentor$. After registration, a secret ID is sent to the client and now the user is ready to use the web application by performing a simple text-based authentication with $username$ and $password$ input which is validated against user credentials on the database. If the user exists and is registered, access is granted, on the contrary the user is rejected or is asked to register. After successful login, a user interface for sending/receiving e-mail is introduced. The characteristic of this e-mail client web application is two types of emails that it supports. The first one is the regular non-authenticated e-mail and the second one is the authenticated e-mail sending. Of particular interest is the authenticated version of e-mails which is based on the $Pentor$ and $UltraPentor$ mathematical operators.

When the user composes an authenticated e-mail, it fulfills the $Messageto$ box together with $Subject$ field where he enters the subject of the e-mail. The user is also allowed to choose the $Emailtype$ field for non-authenticated or authenticated e-mails. If an authenticated e-mail is chosen the user should provide its $Image$ that it used while registering and the ID that was sent during registration phase. After completing the Message field the user tries to send the e-mail and during this phase a special authentication algorithm is used based on the above mentioned operators in the following order.

Initially, the $Image$ provided is converted into an RGB matrix $M(R, G, B)$ and furthermore this matrix is encrypted in the following way:

$$M_c(R, G, B) \equiv M(R, G, B) \cdot ID \cdot$$

$$\cdot UltraPentor(ID) mod(255)$$

Further on, we introduce multiple level of authentication enumerated as below:

In level one, the $Username$ provided by the client while initial sign-on is checked against user credentials in the database. Therefore,

$$Username = Username_{db}$$

The second level checks the encrypted matrix $M_c(R, G, B)$ generated on the fly while the user is authenticated against the encrypted matrix stored in the database.

$$M_c(R, G, B) = M_c db(R, G, B)$$

The third level checks whether the $Vector$ generated from the $Username$ and ID of the client is equal with the $Vector$ value stored in the database.

$$Vector = Vector_{db}$$

Finally, the fourth level of security is enforced by the condition $ID|N$, where the value of N is acquired by performing a "Pentoric Attack" against the $Vector$ as follows:

$$N = Vector \leftarrow Pentor(ID)$$

The whole process with the levels of authentication is illustrated as in figure III below.

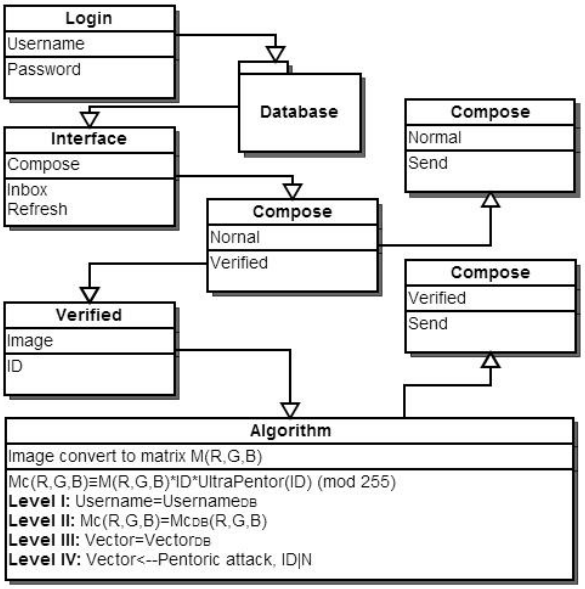

Fig. 1. Multi-level authentication with the use of Pentor and Ultra Pentor Operators

After all these levels, the user is allowed to send an authenticated e-mail and the person receiving this e-mail will also receive a text attached at the end of the message stating that the message is authenticated with the above mentioned algorithm.

IV. Multi-level Authentication: A Case Study

The above mentioned procedures and levels can be illustrated with a real example. Suppose that we would like to register a user with the following credentials:

$$Name = Artan$$

$$Surname = Luma$$

$$Username = a.luma@seeu.edu.mk$$

$Image$ as given below in Figure 2

Fig. 2. Image provided by the user

Based on this data, $Name$, $Surname$, $Username$ and $Vector$ will be stored in a database, where in the $Image$

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

attribute the path of the encrypted $Image$ will be stored. The process of encrypting the image as shown in the previous section is done by initially converting the image into a RGB matrix where each pixel is represented through RGB colors as given below with an image composed of $150x150$ pixels.

$$M(R,G,B) = \begin{pmatrix} M_{1,1}(85,83,84) & \dots & M_{1,150}(88,86,87) \\ M_{2,1}(88,86,87) & \dots & M_{2,150}(41,40,35) \\ \vdots & \dots & \vdots \\ M_{150,1}(56,56,56) & \dots & M_{150,150}(70,52,68) \end{pmatrix}$$

This matrix is encrypted by having the ID of the client which is generated by the administrator and sent later to the user after the Vector generation. The encrypted matrix is acquired as follows:

$$M_c(R,G,B) \equiv M(R,G,B) \cdot ID \cdot$$

$$\cdot UltraPentor(ID) mod(255)$$

$$M_c(R,G,B) = \begin{pmatrix} M_{1,1}(0,99,177) & \dots & M_{1,150}(63,240,105) \\ M_{2,1}(234,78,156) & \dots & M_{2,150}(138,60,180) \\ \vdots & \dots & \vdots \\ M_{150,1}(111,111,111) & \dots & M_{150,150}(105,231,204) \end{pmatrix}$$

The encrypted matrix represents the encrypted Image depicted as in Figure 3

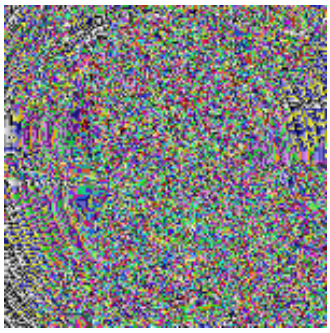

Fig. 3. Encrypted Image of the User

This encrypted Image of the user is stored in a folder on the server's side of the web application. The calculation of the Vector is done by multiplying the ASCII version of the Username with the ID as shown in section 3.

$$Vector = Username_{ascii} \cdot ID$$

$$Vector = 97461081171099764115101 10...$$

$$...11174610110011746109107 \cdot 13$$

$$Vector = 126699405522429693349631431452 69...$$

$$...931430152699418391$$

Considering that the result is a 50-digit sequence, it should be "chopped" into 6-digit sequences starting from the right side as follows:

$$Vector = 12|669940|552242|969334|963143|145269|...$$

$$|931430|152699|418391$$

Summing these sequences altogether results in the value for $Vector$ given as below:

$$Vector = 12+669940+552242+969334+963143+145269+...$$

$$+931430 + 152699 + 418391$$

$$Vector = 4802460$$

Considering that $Vector$ is a 7-digit sequence which is greater than the value of Ultra Pentor, the process is repeated once again yielding the following result:

$$Vector = 4|802460$$

$$Vector = 4 + 802460$$

$$Vector = 802464$$

This value of the Vector which is unique for each user is stored in a database and the value of the ID is sent to the user which is kept secret. The overall process of client activity on the web application consists of the following steps. At the beginning the user authenticates with a simple text-based authentication method by providing Username and Password (the Login step in Fig. III). The Login form is depicted as in Figure 4.

Fig. 4. Initial User Login Form

After successful login, a window with user's mailbox appears where he can check for mails and compose new ones as illustrated in figure 5

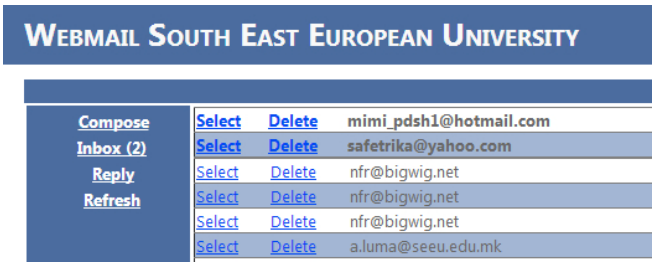

Fig. 5. User's mailbox after authentication

If the user wants to send an email, by clicking in the Compose button a new form for email composing and sending appears. In this form the user has to fill and choose the following options: $Messageto$, $Subject$, $Emailtype$ (normal, verified e-mails), $Image$ (where user chooses its Image), ID and $Message$. This is illustrated in figure 6

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

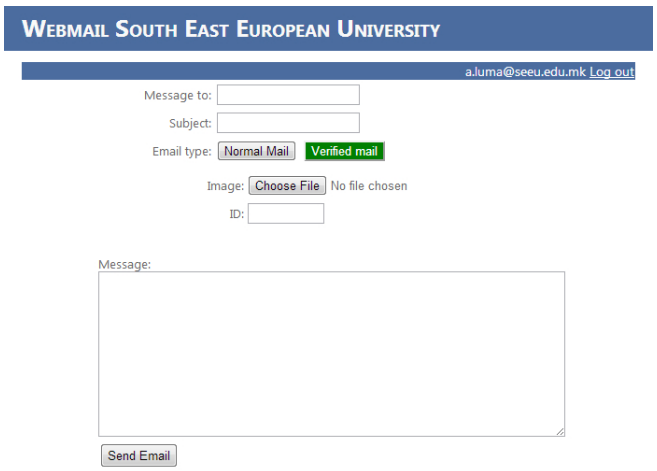

Fig. 6. Composition of verified e-mails

When the Send Email button is clicked, the 4-level authentication process is initiated. At the beginning its image is converted into a matrix as given below:

$$M(R,G,B) = \begin{pmatrix} M_{1,1}(85,83,84) & \dots & M_{1,150}(88,86,87) \\ M_{2,1}(88,86,87) & \dots & M_{2,150}(41,40,35) \\ \vdots & \dots & \vdots \\ M_{150,1}(56,56,56) & \dots & M_{150,150}(70,52,68) \end{pmatrix}$$

The encryption process of this matrix is done in the following way:

$$M_c(R,G,B) \equiv M(R,G,B) \cdot ID \cdot$$

$$\cdot UltraPentor(ID) mod(255)$$

$$M_c(R,G,B) = \begin{pmatrix} M_{1,1}(0,99,177) & \dots & M_{1,150}(63,240,105) \\ M_{2,1}(234,78,156) & \dots & M_{2,150}(138,60,180) \\ \vdots & \dots & \vdots \\ M_{150,1}(111,111,111) & \dots & M_{150,150}(105,231,204) \end{pmatrix}$$

After the encryption, this matrix is stored as an encrypted image. In the first level, the $Username$ given by the user and the one stored on the server's side is checked and if this $Username$ is identical to $a.luma@seeu.edu.mk$, level two is initiated where on-the-fly encrypted matrix is checked against the encrypted matrix stored in the database. If these two values coincide level three is introduced. In level three, the generated $Vector$ from the user is checked against the $Vector$ value stored in the database which after being identical with the one in the database, the level four kicks off in which "Pentoric Attack" against $Vector = 802464$ is performed. The attack results in value $N = 39$ which is divisible with Ultra Pentor, i.e. $13|39$ and the a-mail is sent. In any other case, if one of the conditions would not be fulfilled the verified e-mail procedure would fail and the user rejected.

V. Conclusion And Future Work

In this paper we have introduced a method of user authentication and identification in the process of sending verified e-mails. The methodology uses a multi-level approach of identifying the user while sending verified e-mails and it consists of the following steps:

1) The first step represents a classical text-based authentication.
2) The second step involves an image based authentication where the user's image is encrypted by multiplying it with a secret key provided to the user.
3) Finally step three is concentrated around level-3 and level-4 elaborated earlier that use a specific algorithm that exploits the powerful properties of two mathematical operators called $Pentor$ and $UltraPentor$ applied against the image in step two.

Further research is needed on $Pentor$ and $UltraPentor$ properties and their application in the development of various cryptosystems [9]. One direction of this application would be the possibility of digitally signing the emails by using $Pentor$ and $UltraPentor$ and this is currently the focus of our further research.

References

[1] S. L. Garfinkel, "E-mail based authentication and identification: An alternative to pki," *IEEE Computer Society*, 2003.
[2] D. W. M. Dietz, A. Czeskis and D. Balfanz, "Origin-bound certificates: A fresh approach to strong client authentication for the web," in *Proceedings of the 21st Usenix Security Symposium*, 2012.
[3] M. Hearn, "An update on our war against account hijackers," online, 2013, http://googleonlinesecurity.blogspot.com/2013/02/an-update-on-our-war-against-account.html.
[4] S. B. et al, "Authentication techniques for engendering session passwords with colors and text," *Advances in Information Technology and Management*, vol. 1, no. 2, 2012.
[5] H. Zhao and X. Li, "S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07)*, 2007, pp. 467–472.
[6] S. Anand, P. Jain, Nitin, and R. Rastogi, "Security analysis and implementation of 3-level security system using image based authentication," in *Computer Modelling and Simulation (UKSim), 2012 UKSim 14th International Conference on*, 2012, pp. 547–552.
[7] H. A. Dinesha and V. K. Agrawal, "Multi-level authentication technique for accessing cloud services," in *In Proc: International Conference on Computing, Communication and Applications (ICCCA)*, 2012, pp. 1–4.
[8] A. Luma and B. Raufi, "New data encryption algorithm and its implementation for online user authentication," in *Proc of International Conference on Security and Managment*. CSREA Press, USA, 2009, pp. 81–85.
[9] A. L. Bujar Raufi and X. Zenuni, "Asymmetric encryption decryption with pentor and ultra pentor operators," *Online Journal of Science and Technology (TOJSAT)*, vol. 2, no. 2, pp. 9–12, 2012.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)