International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:7, No:6, 2013

# LumaCert: Conception and Creation of New Digital Certificate for Online User Authentication in e-Banking Systems

Artan Luma, Betim Prevalla, Besart Qoku, and Bujar Raufi

***Abstract*—**Electronic banking must be secure and easy to use and many banks heavily advertise an apparent of 100% secure system which is contestable in many points. In this work, an alternative approach to the design of e-banking system, through a new solution for user authentication and security with digital certificate called *LumaCert* is introduced. The certificate applies new algorithm for asymmetric encryption by utilizing two mathematical operators called *Pentors* and *UltraPentors*. The public and private key in this algorithm represent a quadruple of parameters which are directly dependent from the above mentioned operators. The strength of the algorithm resides in the inability to find the respective *Pentor* and *UltraPentor* operator from the mentioned parameters.

***Keywords* —** Security, Digital Certificate, Cryptography.

## I. Introduction

IT is broadly known that the Internet has become an integral part of our lives, and the proportion of people who expect to be able to manage their bank accounts from everywhere is constantly growing. As such, the online system of e-banking has become a crucial component of any financial institution's multichannel strategy. It has been proven that information about financial institutions, their customers, and their transactions is, by necessity, extremely sensitive and doing such business via a public network introduces new challenges for security and trustworthiness. Any Internet banking system must solve the issues of authentication, confidentiality, integrity, and no repudiation, which means it must ensure that only qualified people can access an Internet banking account, that the information viewed remains private and can't be modified by third parties.

It has been proven that the e-banking, is a high-risk area with a potential for substantial economic loss. The high risk makes security a prime concern. The results indicate that U.S. victims of phishing attacks lost five times more money in 2006 than 2005. Although 80% of the victims in 2005 got their money back, in 2006 only 54% victims were refunded by their banks. In the U.K., online banking fraud increased by 55% during the first six months of 2006. It is reported that online attacks influenced nearly 30% of online banking users; more than 75% of those users logged in less frequently, and about 14% stopped paying bills online [1].

Based on the above mentioned research, it can be seen that the potential of becoming an internet victim is getting higher, and in this paper we will describe current authentications and we will propose a new solution for user authentication as well as how these solutions can be extended in the face of more complex future attacks.

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. Prevalla is a Master Student at South East European University, Ilindenska no 335, 1200 FYR. Macedonia (e-mail: bp11896@ seeu.edu.mk).

B. Qoku is a Master Student at South East European University, Ilindenska no 335, 1200 FYR. Macedonia (e-mail: bq13156@ 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. Security Mechanisms in e-Banking Systems

To have access in an online banking account all you need is a personal computer that will have an access to the internet. Clients will be able to check their online banking account from around the globe. Every client has a username and a password to gain access to the e-banking services. It is very easy for the client to remember only the password; however this will not provide the perfect protection against the internet crime such as fraud and phishing. The use of password solely is very risky, because it can be easily compromised and the scammers can take full control over your bank account. Therefore, only the use of password no longer can be a secure online authentication for an e-banking system.

Online banking systems worldwide use a wide range of technologies for authentication, including passwords, Personal Identification Numbers (PINs), digital certificates, and physical tokens such as smart cards, One-Time Password (OTP) generators and biometric identification.

Based on the aforementioned research [1], [2], [7], e-banking systems generally use two or three of these techniques, rather than relying on just one. A common authentication process runs as follows:

1) A customer logs into the website using their ID and password.
2) Online transaction records are digitally signed with the user's secret key stored in the user's PC or external memory.

Digital certificate systems, which represent one form of electronic authentication services, employ digital signatures that are created with public key cryptography. Although public key cryptography (PKI) - also known as asymmetric key cryptography is not a new technology, it is relatively new to the financial services industry.

We have created our online authentication system using the digital certificate *LumaCert* based on the (PKI), because that this infrastructure can provide a high level of security and also it is not expensive to develop and also to maintain this type of security. So the user to be able to login to the e-banking system he will need the *LumaCert* digital certificate and also the *Username* and *Password*.

The rest of the paper is organized as follows: section 3 gives a short overview on security methods, section 4 introduces some quick and basic concepts on *Pentor* and *UltraPentor* operators, section 5 elaborates the development and implementation phase of the *LumaCert* certificate using the encryption algorithm in [3] section 6 elaborates a brief case study regarding the proposed certificate and section 7 concludes this paper.

## III. Security Methods

There are several methods of ensuring more secure Internet banking:

1) Two-factor authentication.
2) Three-factor authentication

Based on the above methods, the Computer Crime Research Center has made a research for "How to make online banking secure" [2], and it is stated that the method of using only one factor of authentication definitely has its weaknesses. The security aspects of Internet banking need to be strengthened. At minimum there has been stated that a two-factor authentication should be implemented in order to verify the authenticity of the user before he is allowed to use Internet banking services. The first authentication factor can be the use of passwords and the second authentication factor can be the use of tokens such as a smartcard or digital certificates. The above security measures will greatly minimize incidents of Internet banking fraud. The digital certificate here provides a second layer of authentication. This will stop a perpetrator even if he manages to obtain the user's password. Intercepted passwords cannot be used if fraudsters do not have the digital certificate. Besides addressing fraudulent activities, this can instill customers' confidence in Internet banking.

However, based from the above stated research, for a better security, a three-factor authentication process should be considered. The third authentication factor is the use of biometrics such as iris or thumbprint recognition. With a three-factor authentication, a more secure method can be implemented - a password to ascertain what one knows, a token (smartcard or digital certificate) to ascertain what one has, and biometric recognition (for example fingerprint or thumbprint) to ascertain who one is. As such, if passwords have been compromised, fraudsters need to get through the other two levels of authentication to access a customer's account [2].

But as we know in theory, the three-factor authentication may provide a neat solution for user authentication. In practice, however, the three-factor authentication has proven to be difficult to deploy, it's expensive, and protecting the user's biometric information is hard and undergoes strict legal procedures. Also has been proven that the software's and hardware's for biometric recognition are expensive and very difficult to reach for every single user, if not totally impossible.

In this paper, a new solution for user authentication in online banking system that is easy to use is introduced. The solution provides a security using the username and password provided from the bank. Also there is a digital certificate called *LumaCert*, generated for user authentication and all the data inside will be encrypted with a new data encryption algorithm using the *Pentor* and *UltraPentor* operators.

The new data encryption algorithm is elaborated extensively in [3]. The algorithm using the operators of *Pentor* and *UltraPentor* has proven to be very powerful because once the operators have been generated, it is extremely burdensome to find the numbers out of which these operators have been generated. And through this algorithm we are capable of creating a powerful online authentication system for users that commit transactions. Also, out of this new cryptographic algorithm we have developed a new digital certificate called *LumaCert*, which can be implemented for online user authorization and authentication for e-banking systems.

## IV. Pentor and Ultra Pentor Algorithm

A *Pentor* is introduced as an integer number with base $n$. For every natural and integer number $n$ there exist one *Pentor* for the given base $B$. In order to represent this operator mathematically, it was started from modular equation for *Pentor* of an integer number $n$ with base $B$ that fulfills the condition $gcd(n, B) = 1$. From the above mentioned conditions it was gained [4]:

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

where $B$ represents the base of the integer number , $P\ (n)$ is the *Pentor* of the integer number $n$ and $m$ represents the order of the *Pentor* of integer number. From the modular expression 1 it was transformed to the equality expression of the form:

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

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

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 [4].

In [4], the *UltraPentor* of a number $n$ with base $B$ was introduced as well. For every natural and integer number $n$ there exist an *UltraPentor* for the given base $B$. In order to represent this operator mathematically, it was started 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:

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

where $m$ is an integer number. From the modular expression [4], it was transformed to the equality expression by applying logarithmic operations on both sides and finding the *UltraPentor* in the form:

$$B^m = 1 + nl \mid \cdot (log_B) \quad (5)$$
$$\log_B B^m = \log_B(1 + nl) \quad (6)$$
$$m \log_B B^m = \log_B(1 + nl) \quad (7)$$

where $\log_B B = 1$ and there is:

$$m = \log_B(1 + nl) \quad (8)$$

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

$$UP(n) = \log_B(1 + nl) \quad (9)$$

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 [5].

## V. Implementation of the LumaCert Digital Certificate Using the Algorithm

In the following we will describe how we have created the part which gave us the values of the *Pentor* and *UltraPentor*, and also how the two operators will be used to create the digital certificate *LumaCert*.

Because of the big numbers that needed *Pentor* and *UltraPentor* to be generated for, the SEE University research server SunFire X4600 was used. For faster and more reliable number generator, the range of $N$ numbers has been reduced from 1 to 2000 for testing purposes. Using the research server SunFire X4600 and the Java Technology it was managed to gain a *Pentor* and *UltraPentor* for the specific range of $N$ numbers.

To generate these two mathematical models we have created a function where as an input value is the *IDNumber* which is an unique number from the range of $N$ numbers, and as an output values are the *Pentor* and *UltraPentor*.

Here we will show the function to generate the *Pentor*:

**Require:** $IDNumber, Base, Order$
**Ensure:** $Pentor$
  $condition = TRUE$
  $k \leftarrow 1$
  **while** $condition$ **do**
    **if** $Base^{Order} | (1 + IDNumber \cdot k)$ **then**
      $(1 + IDNumber \cdot k) / Base^{Order}$
    **end if**
    $k \leftarrow k + 1$
  **end while**
**return** $Pentor$

In the same manner is created and implemented the function for generating the *UltraPentor*.

Let's suppose that the bank wants to provide it's users with the digital certificate *LumaCert* for a better security. So the bank will need to send the list of public information for the clients to the Certificate Generator. The Certificate Generator will create the digital certificate *LumaCert* for every client of the bank, which will be created with the *Username*, *Password* and *IDNumber*, also out of this information will be generated the Ciphertext and following with the *UltraPentor* help in the end is generated the Vector for that client [3].

Here we will show the pseudo code that generates the Vector by dividing the Ciphertext by the value of *UltraPentor* would look like:

**Require:** $c, UP, ID\_NUMBER$
**Ensure:** $V$
  $V_i \leftarrow 0$
  $i \leftarrow c, length$
  **while** $i > 1$ **do**
    $k \leftarrow UP$
    $j \leftarrow i$
    **if** $c[j] = 0$ **then**
      $V_i[j] \leftarrow UP$
      $j \leftarrow j - 1$
    **end if**
    **if** $k > 1$ **then**
      $k \leftarrow k - 1$
      $i \leftarrow j$
      $\Delta\ summing\ all\ separated\ sequence$
    **end if**
  **end while**
**return** $V$

After we collect every information data that is needed, we create encryption / decryption for this data with $ANZF$ Algorithm [6]. When all this steps are finished, for testing purposes there will be used the Makecert free tool to create a digital certificate which will contain all the information for the client and also the encrypted information.

Here we will show the two command code that has been used to generate the (PFX) file for the digital certificate *LumaCert* for a certain user:

```
string first_command = "makecert -sv " + Client_Name + "_" + Client_Surname + ".pvk -n \"CN=" + Client_Name + " " + Client_Surname + ",L=" + Client_Info_All_Encryption + ",E=" + Username + "\" -is my -in \"LumaCert Cryptosystem\" -ss my " + Client_Name + "_" + Client_Surname + ".cer -b " + Date_From + " -e " + Date_To + " ";
string second_command = "pvk2pfx -pvk " + Client_Name + "_" + Client_Surname + ".pvk -spc " + Client_Name + "_" + Client_Surname + ".cer -pfx " + Client_Name + "_" + Client_Surname + ".pfx -po " + Password + " ";
```

With this we have created a digital certificate *LumaCert*. And every single digital certificate will be distributed to the bank, whereas the bank will distribute them to its clients.

In the following lines, we will describe each steps of Fig. 1, where it is presented the design and implementation of the new digital certificate *LumaCert* used for online user authentication in e-banking systems in the following order:

1) The bank requests a digital certificates LumaCert from the Certificate Generator, for its clients.
2) The Certificate Generator provides the bank with digital certificates LumaCert for every client.
3) The bank distributes the LumaCert digital certificates to its clients.
4) The clients install their LumaCert digital certificates in the Personal Computer.
5) The client enters the credentials for login to the bank account.
6) Before proceeding to the database check, the SSL Protocol of the Bank System checks and validates if the users has the corresponding LumaCert digital certificate.
7) If the user doesn't have the corresponding LumaCert digital certificate, the user will not be allowed to continue to the e-banking system, and an error screen will be shown, that will inform the user.
8) If the user has the LumaCert digital certificate, then a database control for the credentials is made.
9) If this step returns that the credentials are wrong then the user will not be allowed to continue to the e-banking system, and an authentication failed error screen will be shown.
10) If the database control step is passed then the e-banking system will open a secure connection to communicate with the user.
11) And then all the transactions can be made in a secure connection.

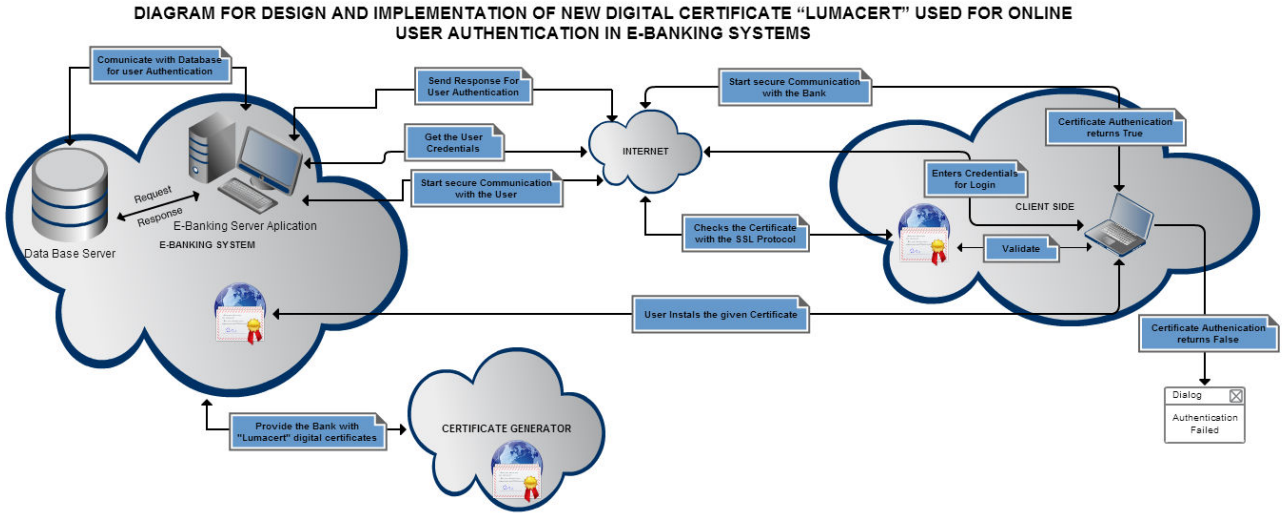


Fig. 1 Design and Implementation Process of LUMACERT

## VI. LumaCert: A Case Study

Let us illustrate the above stated steps through a real life example. Initially, let us adopt the values of one client of the bank. The initial data that will be needed are the name and surname of the client from where the Certificate Generator will generate *Username*, *Password* and the *IDNumber* of the client. For testing purposes we will use the values from the research case study given in [3] that are generated with the following attributes:

Username: a.luma
Password: art
ID Number: 13


Fig. 2 Digital Certificate After Installation

With this attributes the Ciphertext will be found, which is gained from multiplying the ASCII values of the *Username* and *Password* and multiplying them with the *IDNumber*. The Ciphertext will look like:

$$Ciphertext = Username \cdot Password \cdot IDNumber = 123043007650362697473747 6$$

Then the mathematical operators of *Pentor* and *UltraPentor* are generated for the *IDNumber* 13, where the *Pentor* will be 4 and the *UltraPentor* will be 6. Using the *UltraPentor* and the Ciphertext we generate the Vector of client, where the Vector of the client has the value of 971386.

Based on this data we can create the *LumaCert* digital certificate for the client Artan Luma, for whom we have this information:

Name: Artan
Surname: Luma
Username: a.luma
Password: art
ID Number: 13
Pentor: 4
Ultra Pentor: 6
Ciphertext: 123043007650362697473747 6
Vector of client: 971386

All this data are inserted in the *LumaCert* digital certificate, encryption with *ANZF* Algorithm. After the client has received the digital certificate *LumaCert* from the bank, he will install it to his Personal Computer and the *LumaCert* digital certificate after installation will look like this:

After the installation is done, and the client's computer has the *LumaCert* digital certificate, he will be able to have a secure connection for communication with the online e-banking system. And then all the transactions can be made in a secure connection.

## VII. Conclusion

Electronic Banking is offered by many banking institutions due to pressures from competitions. Moreover, there are many potential problems associated with this young industry in due to imperfection of the security methods. In order for electronic banking to continue to grow, the security and the privacy aspects need to be improved.

In this paper we have presented a completely new online user authentication using the *LumaCert* digital certificate. From the explained steps it has been shown that the online user authentication using the *LumaCert* digital certificate fully works and can be implemented in many other applications where highly secured user transactions are required.

## References

[1] M. Hertzum, J. N. Christian, N. Jørgensen and M. Nørgaard, Usable Security and E-Banking: ease of use vis-a-vis security J. Australasian Journal of Information Systems. 11,2, 2004.
[2] A. Nasir, M. Zin, Z. Yunos, How to make online banking secure, April 25 2005. http://www.crime-research.org/analytics/online banking
[3] A. Luma and B. Raufi, New data encryption algorithm and its implementation for online user authentication, In: The 2009 International Conference on Security and Managment. pp. 81–85, CSREA Press, USA, 2009.
[4] A. Luma, B. Raufi and Xh. Zenuni, Asymmetric Encryption /Decryption with Pentor and ultra Pentor Operators, J. Online Journal of Science and Technology (TOJSAT), 2,2 9–12, 2012.
[5] A .Luma, B. Raufi and Xh. Zenuni, Asymmetric Encryption /Decryption with Pentor and ultra Pentor Operators, In: 2nd International Science and Technology Conference (ISTEC'2011), pp. 79–82, 2011.
[6] A. Luma, Data encryption and decryption using ANZF algorithm, in 31st International Convention. Information Systems Security. pp. 90–94, MIPRO, Opatija, 2008.
[7] P. Hanacek, K. Malinka and J. Schafer, e-banking security - A comparative study, In: Aerospace and Electronic Systems Magazine, IEEE, 25, 1, 2010.