STRONG ZERO-KNOWLEDGE AUTHENTICATION BASED ON THE SESSION KEYS (SASK)

Younes ASIMI[1] Abdellah AMGHAR[2] Ahmed ASIMI[3] and Yassine SADQI[4]

[134]Laboratoire des Systèmes informatiques et Vision (LabSiV),
Equipe de la Sécurité, Cryptologie, Contrôle d'Accès et Modélisation (SCCAM),
Departments of Mathematics and Computer Sciences
[2]Laboratoire des Systèmes informatiques et Vision (LabSiV),
Department of Physic
[1234]Faculty of Sciences, Ibn Zohr University, B.P 8106, City Dakhla, Agadir, Morocco.

ABSTRACT

In this article, we propose a new symmetric communication system secured, founded upon strong zero knowledge authentication protocol based on session keys (SASK). The users' authentication is done in two steps: the first is to regenerate a virtual password, and to assure the integrity and the confidentiality of nonces exchanged thanks to the symmetric encryption by a virtual password. The second is to calculate a session key shared between the client and the web server to insure the symmetric encryption by this session key. This passage allows to strengthen the process of users' authentication, also, to evolve the process of update and to supply a secure communication channel. This evolution aims at implementing an authentication protocol with session keys able to verify the users' identity, to create a secure communication channel, and to supply better cyber-defense against the various types of attacks.

KEYWORDS

Strong authentication, virtual password, shared secret session key, secure communication channel, cyber-defense.

1.INTRODUCTION AND NOTATION

The digital revolution has made enterprises most open and accessible thanks to the services of cyberspace. This IT technology became more relevant in their sustainable developments. Of course, speed, availability, accessibility, transparency, full dematerialization and simplicity have made it omnipresent in our lives. But, the increased security in this virtual space has not assured yet what always engenders problems of mutual trust, users' identification, and information validation. The cyberspace became middles of any transaction on the internet. The social or individual movements of the users are strongly based on these technologies. The social networks (Facebook, Gmail, Twitter,…) become important resources of the mobilization and the collective actions around the world [23]. The evolution, the importance and the diversity of cyberspace have rendered those omnipresent in our life [23]. Also, the developing of companies is strongly bound in this digital evolution. But, as the internet is a public space, thus very difficult of to manage and/or to control and/or to protect against the various possible attacks. The protection of the users' privacy against criminal activities is still a challenge which has no borders.

The security of cyberspace is one of the areas which engender more disquietude within the research laboratories, and the digital enterprises [7], [9], [18], [21], [33], [37], [41], [42], [44]. Certainly, the experts sacrificed more time to certify the objectives of the IT security. With the appearance of the new vulnerabilities, threats and risks degrading the level of security and hampering the digital development are bound to the cryptographic hash functions, to the JavaScript programming language [24], to the existing authentication systems, and also to the exchange protocol of data on the network HTTPS [26]. At that time, the HTTPS protocol was the only way to ensure the confidentiality and the integrity [6] of data which transit on the network. But, thanks to an analytical study made by American researchers [26], the surveillance of the Web traffics leaves enough information even if the data which transit are encrypted. In this interest, we introduce a new strong authentication system allowing to remedy these problems. We focus on the mutual authentication with zero knowledge based on virtual passwords and shared keys session. The purpose, is to face the problems of exchange of private data, in particular, the specific authentication settings at any session. The value of this development is to have a strong authentication system able to respond to user needs related to the memorization, and to the storage of passwords, also, to produce a cyber-defense can stand and fight against any kind of cybercriminal.

In all what that follows, we denote by:

ID_i	:	The user' identifier of U_i.
PW_i	:	A valid original password.
$PWVS_i$	:	The virtual password per session.
$HPWS_i$	:	The hashed of $PWVS_i$.
$EHPWS_i$	:	Encryption hashed password by session key.
RS_i	:	Random salt.
$CSRS_i$	:	Cryptographically secure random salt.
$SOTS_i$	:	Safe One Time Salt.
OTS_i	:	One Time Salt.
SK_i	:	Session Key.
CRC	:	Cyclic redundancy check.
CVL	:	CRC code of variable lengths.
Ni	:	A positive random integer. Its binary representation is the generator polynomial associated with each one-time salt OTS_i.
DR	:	Dynamic rotation.
E	:	Symmetric cryptographic primitive.
H	:	One-way hash function.
Tb_i, Ts_i	:	Random nonces.
CCi	:	Challenge of server calculated by the client.
RCS_i	:	Challenge and response of client calculated by the server.
RC_i	:	Client's response to server's challenge.
X_i^{new}	:	Renewal of the parameter X.
$\oplus$	:	XORing operation.
$\|\|$	:	Concatenation.
==	:	Comparison.

2.RELATED WORK

The authentication protocols by password have emerged by Bellovin and Merritt [43]. They proposed firstly a protocol for exchange of encrypted keys (EKE) and then these extensions. This protocol has been the subject of many improvements and enhancements such as the family of

protocols AuthA [25]. To this effect, Morris and Thompson [38] introduced another alternative to OTP which is based on the storage of passwords salted, and hashed to decrease the risk of compromise file [8], [18]. Despite the weak entropy of used passwords and the invention of best authentication techniques in cyberspace, none has succeeded to replace them a significant way in the market [10], [18], [37]. Undoubtedly, the alphanumeric passwords are easily attacked by shoulder-surfing and spyware software and very difficult to memorize [16]. Where from, to meet of the security recommendations relating to choose the complex passwords that have themselves the high entropies, ObPwd [27] is another alternative of system allowing to generate strong passwords enough basing itself on digital objects. The user does not need to memorize a very complex password. In 2008, and in the interest to introduce an authentication system able to fight against the theft, phishing, keylogger and shoulder surfing attacks, CPI Lei et al [22] proposed a virtual passwords system. This virtual system has been modified by Bhavin and Doshi [4] in order to minimize the processing time by the server. This system is theoretically breakable because all keys in {0,..., Z-1} are finished [47]. Also, other studies made in it discipline computing showed that the users remain unable to meet recommendations of the IT security bound to passwords [7], [12], [13], [34], [41], [42], [44]. More precisely, the problem of memorization and storage, even at the university level, a survey by Shay et al [36] showed that users are unable to meet requirements of IT security related to the storage of passwords. Especially, if we note that the average number of accounts per user exceeds 25 separate accounts [9], [18].

At the time, to deal with vulnerabilities in the HTTP protocol, integrity and confidentiality of data exchanged between the client and the Web server have been assured by the HTTPS protocol, in occurrence, the authentication settings and tracking of states. This protocol uses symmetric and asymmetric cryptographic methods supplied by the SSL / TLS protocol in order to insure the users' privacy on the network. But, with the diversity of types of attacks that adapt with every situation, this system remains unable to protect the users' privacy. In particular, if we note that the passwords generated static to weak entropy are totally breakables. So, according to an analytical study on this protocol by American researchers, monitoring of web traffics leaves sufficient information even if the data which transit are encrypted [26]. For ensuring the correlation between the clients and the web server, this protocol requires the use of cookies. Thus, to keep the state of clients connected, the given Web server creates a cookie file containing specific information to each client. It can also be used to ensure users identification by password. Several studies have been conducted in the discipline to suggest secure cookies. But, in general, almost all proposals are based on the SSL protocol, hash functions, fixed IP addresses and encryption / decryption of sensitive data to create secure cookies able to withstand at the different types of attacks [1], [17], [20], [32], [45], [48]. Of course, at the time, these protocols have presented the real solutions of security able to resist against various attacks. But, with the vulnerabilities discovered notably in the protocol SSL, and hash functions, and as, if we note that the generated passwords are static, these protocols are unable to struggle against different attacks. In order to solve these problems, other improvements have been proposed to fight against the dictionary, man-in-the-middle, phishing, and replay attacks [3], [5], [30], [31], [39], [40]. These protocols regenerate the different virtual passwords for each open session. But they do not arrive to push aside the vulnerabilities of the protocol SSL, and of the hash functions. And, they do not insure the cryptographic quality of the regenerated passwords, also the integrity of authentication settings.

Recently, the authentication mechanisms have been proposed to replace password-based authentication schemes [2], [11], [15], [28]. The goal for them is to protect users' privacy by using asymmetric digital signatures. The first problem of them, they are founded on SSL/STL protocol to provide a secure communication channel between the client and the server. It allows the users to authenticate to the server via a public key certificate and its associated private key. In

2011, Microsoft has proposed its authentication schemes called CardSpace, but, it is abandoned this project in same year [11], [29]. In 2012, Mozilla has deployed its authentication schemes called Persona [28] on its own web applications. It aims to provide a secure identification mechanism in different web applications without the centralized authentication services. It uses the e-mail addresses to identify their owners without need to create a new password. It improves usability and deployability of users' authentication [19]. But, the big problem of this authentication mechanism is the compromised file attack [2]. Hence, if an attacker arrives to compromise the user' identity in a given account, then, all other accounts that are founded on this identity provider account are compromised. Also, it is vulnerable to phishing attack. The aim in this article, is to innovate a strong authentication system can withstand the loss of information exchanged between the client and the web server, also, not fragile than the open session. Our object is to have an alternative scheme of SSL protocol that provides the users' privacy on the web applications. Indeed, for the same user, the virtual passwords regenerated are different for each session. So, integrity of authentication parameters is provided by the integration of a mechanism for errors detection of variable lengths. The cryptographic quality of the virtual passwords gets thanks to the nature pseudo-random, dynamic and unpredictable of salts regenerated in any open session. Hence, we would have the increase confidence of the connected users.

3.SAVP PROTOCOL

Today the importance of IT security related to passwords is not only to occupy the users to choose fairly strong passwords. Yet, to innovate systems able to hinder and resist against different types of attacks. Of course, this challenge is very difficult to attain 100%, especially, in a public environment such as the network. Because, in this IT discipline, the privacy of users is an inter-linked chain requires a fairly high level of protection. Really, the evolution of new technologies able to ensure the digital communication, the storage of personal data, and to associate and organize different datasets, has seduced and increased the use of internet in global level. In parallel, the innovation of attack protocols, as another evolution which affects at the bottom of personal privacy on the Internet, is able to monitor, disclose and usurp the privacy of every person on the Internet.

The cryptographic protocols based on the passwords have known very important evolutions. The innovation in this authentication technique comes from their ability to meet the security needs of users. Thereby, to create a secure communication channel, the user must memorize a lightweight password without needing a complex infrastructure such as PKI. But, according to all the studies made on the difficulties and the habits followed by users during the choice and storage passwords [7], [33], [37], [41], [42], [44]. It is very difficult to build on the man as being a security key, especially, in a highly sensitive environment. For this reason, we proposed an authentication protocol based on the virtual passwords which are composed of following processes (for all detail see [46], [47]):

Random Generator of a Safe Cryptographic Salt: The importance of integration of this regenerator in our authentication system aims to ensure the robustness, the complexity, and the cryptographic quality of the virtual passwords regenerated in any open session, also, integrity of authentication settings.

1) ***Code of errors detection of variable lengths (CVL):*** The importance of integration of this mechanism is to have an authentication system able to withstand against any leakage of information. It ensures salts safe integrity exchanged between the client and the web

server. It has a very special property that it adapts with any generator polynomial. It is as follows:

- In registration phase:
  i. It calculates a generator polynomial specific to any regenerated random salt.
  ii. It calculates the CRC of this random salt.
  iii. It stores the secure random salt as being the concatenation of random salt and its CRC.

- In identification phase:
  i. It checks random salt safe integrity.
  ii. It deduces the random salt.

2) ***Dynamic rotation algorithm of binary strings (DR):*** In order to properly to ensure on the cryptographic nature of virtual passwords regenerated comes the interest to introduce this algorithm in our system. It aims to ensure the unpredictability, and untraceability of original passwords completely breakable for minimal disruption:

- It generates a binary sequence from the concatenation of the original password and a random salt.
- It calculates the position of the dynamic rotation that is the sum of all bits of this binary sequence generated.
- It directs the dynamic rotation by the parity of this calculated position.

3) ***Extension Crypto-Services:*** It supplies, in both sides, the following features:

- The hash functions.
- The symmetric cryptographic primitives.
- The dynamic rotation of binary strings.
- The CRC code of variable lengths.
- Regeneration random salts RS_i specific to each user U_i.

4) ***Database:*** Each user U_i is characterized by four authentication parameters:

- Unique identifier (ID_i).
- Final password (HPW_i).
- Regenerator of random salts ($CSRS_i$).
- A positive integer (N_i) that corresponds to the sum of all bits of a primitive signal RS_i.

The analytical results [47] have showed the unpredictable cryptographic nature of the virtual passwords regenerated for the minimal conditions of the IT security. Likewise, in this proposition, the robustness of the regenerated virtual passwords is strongly bound to the cryptographic quality of unpredictable salts specific to each user and also for their behaviour. But, as the offenses in the virtual spaces have several sources which are very difficult to manage or to control, the importance of this article, is to propose a more robust authentication system which not fragile than the session opened. Also, to create a communication secured channel offering a better protection against the different types of attacks.

4.OUR PROPOSAL

The authentication mechanisms based on the identity of users present efficient solutions to reassure the access to IT systems and to services. We interest of the cryptographic protocols based on the session keys which melted themselves on the virtual passwords. This alternative aims to bring solutions to the problems of the exchange protocols of session keys melted on the protocol SSL or Diffie-Hellman. Of course, the robustness of the authentication systems based on passwords is strongly expressed in terms of the length, the range, the random nature, and the unpredictability of these primitive signals. Furthermore, it is bound to the behaviour of the users which has a very important impact on the cryptographic quality of their virtual passwords regenerated. It is impossible to control it, but can be evolved by the sensitization. In our proposal, the goal is to strengthen the strong authentication of the users by session keys. At this fine, we must to insure firstly on the robustness and the resistance of the virtual passwords at the multiple types of attacks notably the phishing, dictionary, brute force, and man in the middle attacks, and also at the problems of theft of the private data [3], [5], [30], [31], [39], [40]. Our system should be able to minimize the number of the passwords memorized by the users. To reach our goals, we integrated cryptographic mechanisms sophisticated to guarantee the purpose of our system. It builds on one-time salts OTSi regenerated by a random generator of a safe cryptographic salt per session [46], the dynamic rotation algorithm that deforms totally a binary string by a minimal perturbation [47], the mechanism of errors detection of variable lengths which guarantees the integrity of random salts exchanged between the client and the Web server [46], the one-way hash functions, the primitive symmetric cryptographies [6], the nonces to assure the mutual authentication, and also the dynamic and transparent update of authentication settings stored in the database during the connection phase. These improvements aim to check the user's identity and to prove the validity, and security settings which are going to calculate the session keys. The gain, is to create secure communication channels symmetrical between the clients Ui and the server thanks to recalculated session keys. The importance is to have an authentication system able to ensure the cryptographic quality of the session keys regenerated. Furthermore, it ensures the update of the original authentication parameters in the renewal phase.

Definition: We refer to [46], a salt is a safe one time (SOTS) if it's specific for each user session, regenerated by a pseudo-random and unfalsifiable regenerator.
Our system of strong zero-knowledge authentication based on the session keys (SASK) consists of three phases: the registration phase, the identification and authentication phase, and the renewal phase.

4.1.Registration phase

To enroll in the Web server, each user U_i is characterized by its identity IDi, and its valid password PWi. In order to give a unique representation, the Web server should verify its existence. These authentication parameters are very sensitive requiring a rather high level of confidentiality and integrity. Hence, we use the dynamic rotation algorithm of the binary strings (DR), and the mechanism of errors detection of variable lengths CVL [47].

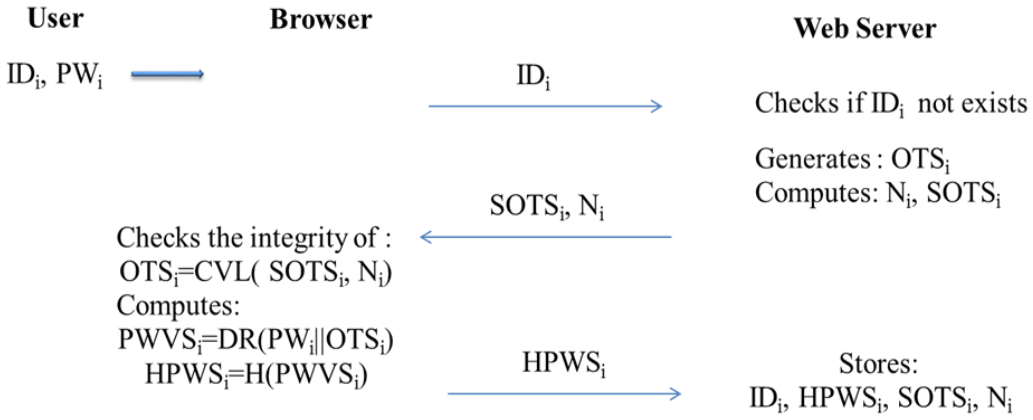

Figure 1: Registration phase

This registration phase generates for each user U_i, theirs own authentication parameters. Its security proof relies on the cryptography quality of random salts associated to the original passwords, the dynamic rotation algorithm of the binary strings, and integrity of exchanged data obtained by the use of a mechanism for errors detection of variable lengths (CVL). It carries out as follows:

- The user U_i must have a valid password PW_i, and the only identifier ID_i. The browser sends the identifier ID_i entered by the user U_i to the server.
- The server checks the existence of the user U_i.
  - If it exists, the server sends back a message of exception informing U_i to choose another identifier.
  - Otherwise:
    i. It generates a one-time salt OTS_i.
    ii. It calculates a number N_i and $SOTS_i$, and sends them to the browser.
- The browser:
  - Calculates of $OTS_i = CVL(SOTS_i, N_i)$.
  - Exercises the Dynamic Rotation (DR) on the concatenation of an original password and a random salt: $PWVS_i = DR(PW_i || OTS_i)$.
  - Calculates the final password by hashing of the virtual password with an one-way hash function H: $HPWS_i = H(PWVS_i)$.
  - Sends the final password HPWSi to server.
- The server saves the parameters of authentication associated to the user U_i: ID_i, $HPWS_i$, $SOTS_i$, N_i.

4.2.Authentication phase

The authentication process consists of four sub-processes which combine to make sure on the identity of users, the creating and the sharing of session keys, the users' authenticity, and the dynamic update of authentication parameters own for any opened session. Equally, we have watched over the random nature of the virtual passwords regenerated. This evolution has two advantages: the robustness of the virtual passwords against different types of attacks, and the confidentiality and integrity of data exchanged through encryption by password in the identification sub-processes. Furthermore, to innovate an interchange protocol of keys based secure passwords able to regenerate the session keys random, unpredictable, and independent from any past sessions.

In this phase, we have to make sure on:

- The users' identity.
- The regeneration of one-time salts OTS_i.
- The integrity and the confidentiality of exchanged original password, one-time salts and nonces.
- The validity of the recalculated virtual passwords.
- The mutual authentication.
- The creation and the sharing of the session keys.
- The automatic updates of the authentication parameters by session.

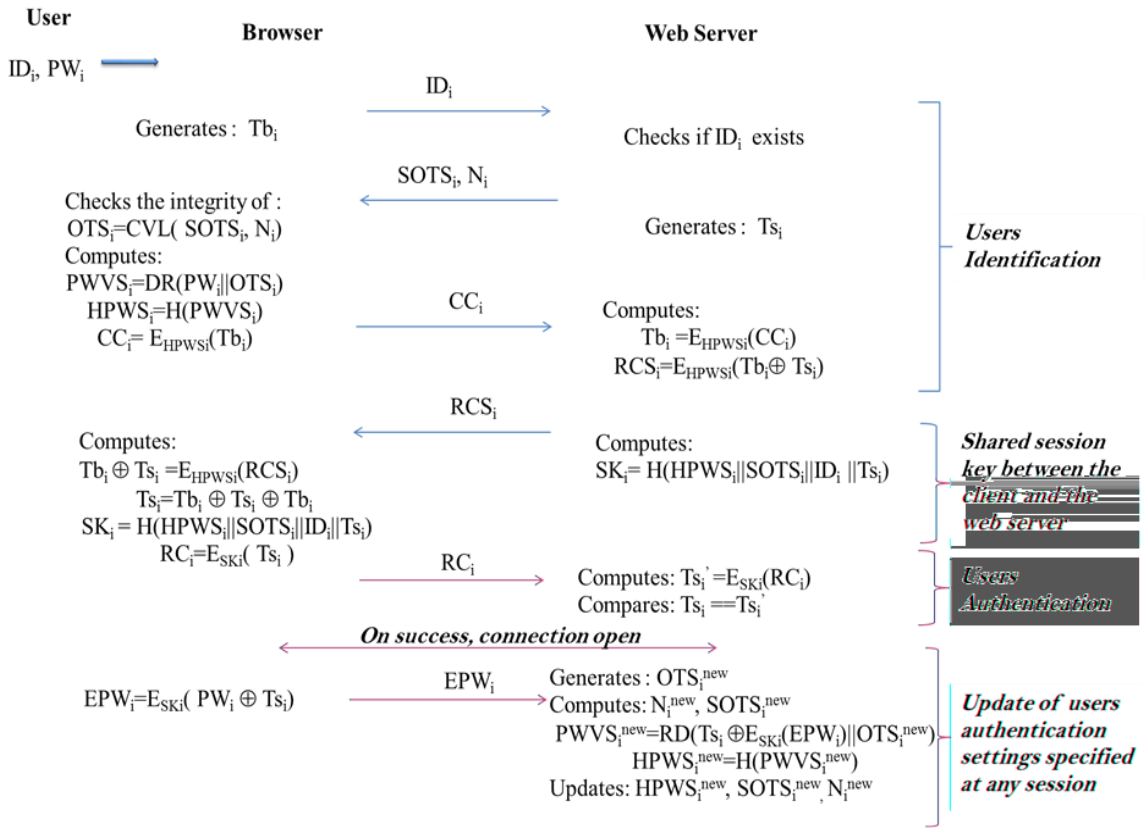

Figure2 : Authentication phase

This process is done as follows:

- The browser:
  - Sends the identifier ID_i of a user U_i to the server.
  - Generates a nonce Tb_i.
- The server checks the existence of the user:
  - If it exists, it sends its safe one-time salt $SOTS_i$ and N_i number to the browser and generates a nonce Ts_i.
  - Otherwise, it returns an error message.

- The browser:

- Checks the integrity of $SOTS_i$ by calculating OTS_i =CVL($SOTS_i$, N_i).
- Calculates the virtual password of a user U_i by Dynamic Rotation applied to the concatenation of its original password valid PW_i and its one-time salt OTS_i: $PWVS_i$=DR(PW_i|| OTS_i).
- Calculates the final password of the user U_i by hashing of the virtual password PWVSi: $HPWS_i$=H($PWVS_i$).
- Encrypts the nonce Tb_i by using the final password $HPWS_i$: CC_i=E_{HPWSi}(Tb_i).
- Sends CC_i, as an authentication challenge, to the server.

- The server:

  - Encrypts the message received: Tb_i =E_{HPWSi}(CC_i).
  - Calculates: RCS_i =E_{HPWSi}(Tb_i⊕Ts_i).
  - Sends RCS_i, as an authentication challenge, to the browser.

- The browser:

  - Encrypts the message received: Tb_i ⊕Ts_i = E_{HPWi}(RCS_i).
  - Calculates: Ts_i = Tb_i⊕Tb_i⊕Ts_i.
  - Calculates the session key SK_i as being the hashed of the concatenation of the final password $HPWS_i$, random salt $SOTS_i$, the identifier user ID_i and the nonce Ts_i : SK_i=H($HPWS_i$||$SOTS_i$||ID_i||Ts_i).
  - Encrypts the nonce Ts_i by using the session key SKi: RC_i = E_{SKi}(Ts_i).
  - Sends RC_i, as a response to the authentication challenge, to the server.

- The server:

  - Calculates the session key SK_i as being the hashed of the concatenation of the final password $HPWS_i$, random salt $SOTS_i$, the identifier user ID_i and the nonce Ts_i : SK_i=H($HPWS_i$||$SOTS_i$||ID_i||Ts_i).
  - Encrypts the message received: Ts_i' = E_{SKi} (RC_i).
  - Compares the nonce received Ts_i' with one who sent Ts_i: Ts_i'==Ts_i.
    i. If the comparison is successful, therefore, mutual authentication is assured between the browser and the server.
    ii. Successful Connection.

- The browser:

  - Encrypts the XORing result of the original password PW_i and nonce Ts_i by the session key SK_i: EPW_i=Esk_i(PW_i⊕Ts_i).
  - Sends EPW_i to the server.

- The server:

  - Generates a new one-time salt OTS_i^{new}.
  - Calculates a new number N_i^{new} and a new safe one-time salt $SOTS_i^{new}$.
  - Calculates the new virtual password of the following session of a user U_i:
    i. The Dynamic Rotation: $PWVS_i^{new}$=DR(Ts_i ⊕ Esk_i(EPW_i)|| OTS_i^{new}).
    ii. The hashing of the virtual password: $HPWS_i^{new}$=H($PWVS_i^{new}$).
  - Updates of the authentication settings: $HPWS_i^{new}$, $SOTS_i^{new}$ and N_i^{new}.

Therefore, the mutual authentication is insured and the symmetric secure communication channel created between the client and the Web server.

4.3.Renewal phase

This interesting phase is more recommended especially for newly registered users. Here, each legitimate user should choose a new password PW_i^{new} also retypes the old password PW_i. In this phase, the user should be authenticated in the previous phase, and the session key created. The goal, is to open a secure communication channel allowing the renewal of all the authentication settings in a more secure environment than the registration phase.

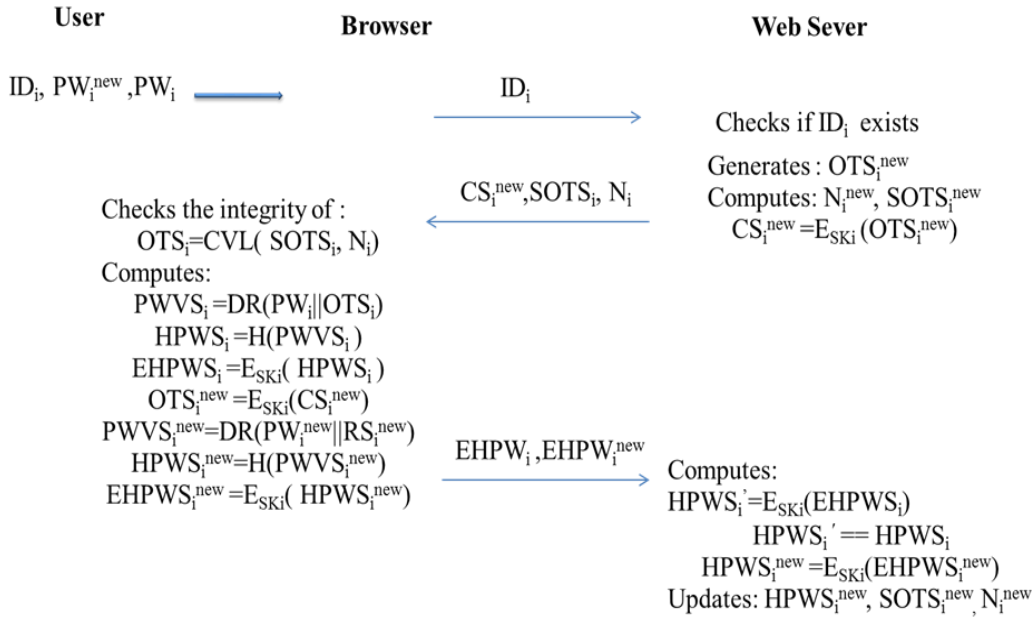

Figure 3: Renewal phase

This process accomplishes as follows:

- The browser sends the identifier ID_i of a user U_i to the server.
- The server checks the existence of the user:
  - If it exists:
    i. Generates a new one-time salt OTS_i^{new}, and calculates a new number N_i^{new}.
    ii. Encrypts the new one-time salt OTS_i^{new} genrated by the session key SK_i of user U_i: $CS_i^{new}=E_{SKi}(OTS_i^{new})$.
    iii. Sends: CS_i^{new}, $SOTS_i$ and N_i to the browser.
  - Otherwise, it returns its an error message.

- The browser:

  - Checks the integrity of $SOTS_i$ by the calculation of OTS_i =CVL($SOTS_i$, N_i).
  - Calculates:
    i. The virtual password of a user U_i by the Dynamic Rotation exercised on the concatenation of its original password valid PW_i and its one-time salt OTS_i: $PWVS_i$=DR(PW_i|| OTS_i).
    ii. The final password of the user U_i by hashing of the virtual password: $HPWS_i$=H($PWVS_i$).

iii. The encryption of the final password calculated with the session key: $EHPWS_i=E_{SKj}(HPWS_i)$.
iv. The encryption of the message received CS_i^{new} by the session key in order to have the new one-time salt regenerated for the user U_i: $OTS_i^{new} =E_{SKi}(CS_i^{new})$.
v. The new virtual password of a user U_i by the dynamic rotation (DR) exerted on the concatenation of its new original password valid PW_i^{new} and new one-time salt $PWVS_i^{new}=DR(PW_i^{new}|| RS_i^{new})$.
vi. The new final password of the user U_i by hashing of the new virtual password: $HPWS_i^{new} =H(PWVS_i^{new})$.
vii. The encryption of the new password calculated with the session key: $EHPWS_i^{new}=E_{SKi}(HPWS_i^{new})$.

- Sends $EHPWS_i$ as an authentication challenge, and a new final password valid $EHPWS_i^{new}$ to the server.

- The server:

  - Encrypts the message received $EHPWS_i$ in order to have the old final password calculated by the browser: $HPWS_i^{'} =E_{SKi}(EHPWS_i)$.
  - Compares the old password final $HPWS_i^{'}$ calculated by the browser with one that have stored in the database $HPWS_i$: $HPWS_i^{'}== HPWS_i$
    i. If the comparison is successful, then the user is legitimate, otherwise, the update will be blocked by the server.
    ii. Encrypts the received message $EHPWS_i^{new}$ in order to have the new final password calculated by the browser: $HPWS_i^{new} =E_{SKi}(EHPWS_i^{new})$.
    iii. Updates of the authentication settings: $HPWS_i^{new}$, $SOTS_i^{new}$ et N_i^{new}.

5.SECURITY ANALYSIS

In this section, we estimate the importance of this improvement the level of safety of our protocol proposed against attacks. Obviously, the attackers follow all possible avenues to reach these goals. In general, in any IT discipline, they are based themselves on traceability, the weaknesses of the protocols, and the theft of private data. In addition, the software malware and data theft are very complex, sophisticated, very difficult to monitor in a real-time by antivirus or software of anti-espionages or Firewalls or the intrusions detection/protection systems. Whence, all online transactions should be carried out in a secure communication channel. To this effect, comes the importance to introduce our strong authentication system which bases itself on virtual passwords and keys of session to establish a secure communication channels without protocol SSL.

5.1 Defends against theft of data

This attack touches all cyberspace environments. The flight of sensitive data can be in the server, over the network or else client side. Obviously, this latter space is strongly bound to the consciences of users by the importance of safety on the survival of these accounts. The passwords stored in a Web server or which transit on the network are virtual. Also, to break the correlation between the passwords regenerated during all session, we have strengthened our system by a random generator of a safe cryptographic salt (OTS), the dynamic rotation algorithm of the binary strings (DR) which gives unpredictable results for minimal disturbances and an one-way hash function (e.g $HPWS_i=H(DR(PW_i||OTS_i))$). Likewise, our system is enhanced by the regeneration of session keys whose interest evolving user authentication using passwords and create a secure communication channel. They have a random, unpredictable, and dynamics characteristic which

are more difficult to guess: $SK_i=H(HPWS_i||SOTS_i||ID_i||Ts_i)$. We have watched over their cryptography quality to avoid the problems of espionages and theft of sensitive data breakable. In our system, the untraceability of the private parameters is assured, also, the renewal of the original passwords is carried out in secure channels that protect the confidentiality and the integrity of exchanged data (e.g $CVL(SOTS_i,N_i)$, $E_{HPWSi}(Tb_i)$, $E_{HPWSi}(Tb_i \oplus Ts_i)$, $E_{SKi}(Ts_i)$, $CS_i^{new} = E_{SKi}(OTS_i^{new})$ and $E_{SKi}(PW_i \oplus Ts_i)$) without using the SSL protocol. Moreover, the parameters used in this session will never be reused in order to have a system that does not fragile the next session. Hence, the robustness of our protocol is assured against flight of private data such as passwords, nonces, and session keys.

5.2 Defends against phishing attacks

We refer to [16], [34], this attack is a technique of computer hacker who uses social engineering, and pharming to usurp the users' identity. It is very sophisticated, more dangerous, efficient, and target on the big companies across the world (Banking and shopping sites). It requires a strategy of global security. In this interest, comes the importance of our contribution which presents one cyber-defense able to resist against this attack. Our authentication system inspires its robustness of the unpredictable, dynamic and random nature of these authentication parameters notably the virtual passwords, and the shared session keys. It also insures untraceability of any original information exchanged between the client and the Web server. Furthermore, the users' identification process is not based only on the regeneration of the virtual passwords during the whole session (e.g $E_{HPWSi}(Tb_i)$, $E_{HPWSi}(CC_i)$, $E_{HPWSi}(Tb_i \oplus Ts_i)$ and $E_{HPWSi}(RCS_i)$), but, it is evolved by a second authentication factor: it is the users' identification by session keys (e.g $E_{SKi}(EPW_i)$, $E_{SKi}(Ts_i)$ and $E_{SKi}(RC_i)$). In order to attack our system, the fraudulent server should have all users' identification parameters $\{ID_i, HPWS_i, SOTS_i, N_i\}$. That is impossible due to the dynamic nature of our system. Equally, the first message exchange between the client and the Web server only allows checking the existence of a given user. For more confidentiality, we never transmitted the passwords when identification neither in clear nor encrypted. But, we use them as keys of symmetric encryption to assure the confidentiality, and the integrity of private data exchanged in the users' identification (e.g $E_{HPWSi}(Tb_i)$, $E_{HPWSi}(CC_i)$ and $E_{HPWSi}(RCS_i)$). Similarly, during updating settings, the sending of original passwords not done that after the opening of the secure connection, but, we encrypt the XORing result of original password and nonce created by the Web server: $E_{SKi}(PW_i \oplus Ts_i)$. The interest, is to benefit from the cryptographic quality of encryption by the session key regenerated to guarantee the more confidentiality of the exchanged passwords, and also to evolve the level of user's identification. Therefore, our system is secure against phishing attack.

5.3 Defends against the dictionary attack

This attack founds primarily on user behaviour that is unable to store complex passwords of strong entropies. It is very effective in case of authentication protocols using the classic passwords. For this reason, in our system, the virtual passwords inspire their robustness of the unpredictable salts appropriate to any sessions, of the dynamic rotation, and of the one-way hash function (e.g $PWVS_i=DR(PW_i||OTS_i)$, $HPWS_i=H(PWVS_i)$). The goal is not just to have one-time passwords, but we have watched over the complexity and unpredictability of the virtual passwords regenerated. So, our system is effectively protected against this attack.

5.4 Defends against brute force attack

If unsuccessful dictionary attack, the attacker can exercise brute force attack in order to get the original password. The attacker would have to test exhaustively all possible combinations of

passwords. Of course, this process is valid in the case of authentication protocols by the classic passwords. By contrast, in our proposal, the attacker should guess correctly two parameters (e.g PW_i and OTS_i) in a real polynomial time from a final virtual password $HPWS_i$. But, thanks to the dynamic rotation algorithm which breeze any correlation between binary strings obtained by the minimal disturbances, and the nature of one-time salts. Besides, after any connection success, we apply a dynamic updating to the authentication settings. Our proposed protocol is secured against the brute forces attacks.

5.5 Defends against Man in the Middle attack

This technique of hacker requires an approach more sophistic than the other attacks. It builds on the social engineering and the mechanisms of classic mutual authentication to falsify communication channels between the clients and the Web server. The attacker should be able of push the legitimate client to visit a fake Web site and to intercept their encrypted data exchanged. For more complexity against this attack, we combined two approaches of authentication namely: the virtual passwords and the session keys. As a result, an attacker could intercept any identification messages and replay them in real time. That is impossible due to their cryptographic nature. Even, if an attack arrives to find the final password and the key of this shared session, this information will not have any influence on the safety of the next session. Because, in our proposal, the authentication parameters are be regenerated of a dynamic and unpredictable manner. Hence, the resistance of our protocol is insured against this attack.

5.6 Defends against SQL injection

This technique of attack allows an attacker to impersonate a legitimate user without having the original password. It is very effective in standard architectures that base on a positive response to a given request. To react in front of this attack, it is recommended to filter any information seized by the user to avoid the execution of the requests unplanned by the application. Thus, in our proposal, the first request only allows to check the existence of the users U_i and to retrieve these specific random salts. More critically, the communicate entities should be able to regenerate these authentication parameters, and to respond of the mutual authentication challenges in the reel time. The attack complexity relies upon the impossible to regenerate neither the virtual password $HPWS_i=H(DR(PW_i||RS_i))$ nor the session key $SK_i=H(HPWS_i||SOTS_i||ID_i||Ts_i)$ without having the original password PW_i. Indeed, these authentication parameters are used to guarantee the confidentiality of mutual authentication challenges. The interest, is to have a very difficult identification processes for illegitimate user. Consequently, our proposal resists against this attack.

6.CONCLUSION

The evolving nature and the complexity of the threats of the cybercrime represent real stakes for the cyber-security requiring cyber-defenses sophisticated. The strategy of the world security should be collaborative and global protecting any environment of the information systems. Where from, the solutions of the computer security proposed should aim jointly on the limits and the constraints of the users, and the evolutions of the attacks systems. More critical, the consciousness and the behaviour of the users have very remarkable influences on the survival of their accounts. But, it is impossible to see them as a key of safety at the level university. Our contribution comes in the optics to insure and to create symmetric secure communication channel between the clients and the Web server. The interest, is to have a dynamic identification system which combines three approaches. The first one insures the regeneration of the virtual passwords,

and the confidentiality and the integrity of the nonces of mutual authentication exchanged. The second calculates the secret session key shared between the client and the web server. The aim is to have secure communication channels resist to loss of information. The last one serves to ensure the dynamic and transparent update of authentication settings in a secure environment. This protocol aims to adopt an authentication system meets the requirements of the security of computer systems and to protect the users' privacy. In order to react to the different types of attacks, in our proposal, user' identification is carried out in two communication distinct sub-channels. One of them founded on the virtual passwords, and the other one on the shared session keys. It requires each user (legitimate or attacker) to have a valid original password in order to authenticate to a web server. It ensures the independence, the portability and the unpredictability of authentication parameters. It is practical, efficient, and secured against different kinds of attacks notably the attack by phishing, dictionary, brute force, man in the middle, SQL injection, and also to the problem of theft of private data.

REFERENCES

[1] A.X. Liu, J. M. Kovacs, C. T. Huang, and M. G.Gouda, "A secure cookie protocol," Proceedings of 14th IEEE International Conference on Computer Communications and Networks, pp. 333-338, Oct. 2005.

[2] Alexei Czeskis , Michael Dietz , Tadayoshi Kohno , Dan Wallach , Dirk Balfanz, "Strengthening user authentication through opportunistic cryptographic identity assertions", Proceedings of the 2012 ACM conference on Computer and communications security, Oct, 16-18, 2012, Raleigh, North Carolina, USA .

[3] A. Herzberg and A. Gbara, "Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks," Cryptology ePrint Archive, Report 2004/155, 2004. http://eprint.iacr.org/2004/155.

[4] Bhavin Tanti ,Nishant Doshi. A secure email login system using virtual password.

[5] Blake Ross, Collin Jackson, Nick Miyake, Dan Boneh, John C Mitchell. "Stronger Password Authentication Using Browser Extensions". Supported by NSF through the PORTIA project. 2005.

[6] B. Schnier, "Applied Cryptography", Second Edition, 1996.

[7] danah boyd. "answers to questions from Twitter on teen practices". apophenia, April 2009.

[8] David C. Feldmeier and Philip R. Karn. "UNIX Password Security - Ten Years Later". In CRYPTO'89: Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology, pages 44–63, London, UK, 1990. Springer-Verlag.

[9] Dinei Florêncio and Cormac Herley. "A large-scale study of web password habits". In WWW '07: Proceedings of the 16th international conference on World Wide Web, pages 657–666, New York, NY, USA, 2007. ACM.

[10] Dirk Weirich and Martina Angela Sasse. "Pretty good persuasion: a first step towards effective password security in the real world". In NSPW '01: Proceedings of the 2001 workshop on New security paradigms, pages 137–143, New York, NY, USA, 2001. ACM.

[11] D. Chappell, "Introducing Windows CardSpace", April 2006. http://msdn.microsoft.com/library/default.asp , last visited 08 January 2007.

[12] E. Jung. Passwordmaker. http://passwordmaker.mozdev.org.

[13] Gilbert Notoatmodjo and Clark Thomborson. "Passwords and Perceptions". In Ljiljana Brankovic and Willy Susilo, editors, Seventh Australasian Information Security Conference (AISC 2009), volume 98 of CRPIT, pages 71–78, Wellington, New Zealand, 2009. ACS.

[14] Greg Aaron, (L'APWG (anti-phishing working group), http://www. antiphishing. Org.), "Phishing Activity Trends Report, 1ST Quarter", http://docs.apwg.org/reports/apwg_trends_report_q1_2013.pdf, Published July 23, 2013.

[15] IETF, "RFC 5246The Transport Layer Security (TLS) protocol version 1.2", August 2008. url http://www. ietf. org/rfc/rfc5246. txt

[16] J. A. Halderman, B.Waters, and E. Felten. "A convenient method for securely managing passwords". To appear in Proceedings of the 14th International World Wide Web Conference (WWW 2005), 2005.

[17] J. S. Park and R. Sandhu, "Secure cookies on the Web," IEEE Internet Computing, vol. 4, no. 4, pp.36-44, Aug. 2000.
[18] Joseph Bonneau and Sören Preibusch. "The password thicket: technical and market failures in human authentication on the web", The Ninth Workshop on the Economics of Information Security, WEIS 2010.
[19] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," 2012.
[20] K. Fu, E. Sit, K. Smith, and N. Feamster, "Dos, and Don'ts of client authentication on the web," Proceedings of 10th USENIX Security Symposium, pp. 1-16,Aug. 2001.
[21] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, 1981.
[22] M. Lei, Y. Xiao, S. V. Vrbsky, C.-C. Li, and L. Liu, "A virtual password scheme to protect passwords," in Proceedings of IEEE International Conference on Communications (ICC'2008).IEEE, 2008, pp. 1536–1540.
[23] M. Milton Joe, Dr. B. Ramakrishnan and Dr. R.S. Shaji ,"Prevention of Losing User Account by Enhancing Security Module: A Facebook Case", journal of emerging technologies in web intelligence, vol. 5, no. 3, august 2013.
[24] Matasano, "Javascript Cryptography Considered Harmful," 2011. http://www.matasano.com/articles/javascript-cryptography/.
[25] Mihir Bellare et Phillip Rogaway. "The AuthA Protocol for Password-based Authenticated Key Exchange". Contributions to IEEE P1363, mars 2000.
[26] Miller, Brad and Huang, Ling and Joseph, AD and Tygar, JD, "I Know Why You Went to the Clinic: Risks and Realization of HTTPS Traffic Analysis", arXiv preprint arXiv:1403.0297, 3 Mar 2014.
[27] Mohammad Mannan and P.C. van Oorschot. Carleton University, Canada. "Digital Objects as Passwords".Version: July 14, 2008.
[28] Mozilla, "mozilla personal an identity system for the web -- mozilla.org", 2011, http://mozilla.org/en-US/persona.
[29] M. Dietz, Czeskis, A., Balfanz, D., & Wallach, D. S. (2012, August). "Origin-Bound Certificates: A Fresh Approach to Strong Client Authentication for the Web". In USENIX Security Symposium (pp. 317-331).
[30] N. Chou, R. Ledesma, Y. Teraguchi, and J. Mitchell. "Client-side defense against web-based identity theft". In Proceedings of Network and Distributed Systems Security (NDSS), 2004.
[31] Netcraft. "Anti-Phishing Toolbar". http://news.netcraft.com/archives/2004/12/28/netcraft_antiphishing_tool% bar_available_for_download.html.
[32] P. Wang, Y. Kim, V. Kher, and T. Kwon, "Strengthening password based authentication protocols against online dictionary attacks," Proceed-ings of ACNS'2005, LNCS 3531, pp. 17-32, SpringerVerlag, May 2005.
[33] Paul Dourish, E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. Personal Ubiquitous Comput., 8(6):391–401, 2004.
[34] "Proofpoint Targeted Attack Protection", www.proofpoint.com/tap.
[35] Richard M. Conlan and Peter Tarasewich. "Improving interface designs to help users choose better passwords". In CHI '06: CHI '06 extended abstracts on Human factors in computing systems, pages 652–657, New York, NY, USA, 2006. ACM.
[36] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. "Encountering Stronger Password Requirements: User Attitudes and Behaviors". In SOUPS '10: Proceedings of the Sixth Symposium on Usable privacy and Security. ACM, 2010.
[37] Robert Morris and Ken Thompson. "Password security: a case history". Commun. ACM, 22(11):594–597, 1979.
[38] S. Goldwasser, S. Micali, and C. Racko_. "The knowledge complexity of interactive proof-systems". In STOC '85: Proceedings of the seventeenth annual ACM symposium on Theory of computing, pages 291{304, New York, NY, USA, 1985. ACM Press.
[39] S. K. Sood, A. K. Sarje, and K. Singh, "Dynamic identity based single password anti-phishing protocol," Security and Communication Networks, Accepted, Oct. 2009.

[40] Sandeep Kumar Sood, Anil K. Sarje, and Kuldip Singh, "Inverse Cookie-based Virtual Password Authentication Protocol", International Journal of Network Security, Vol.13, No.2, PP.98–108, Sept. 2011 98.
[41] Shannon Riley. "Password Security: What Users Know and What They Actually Do". Usability News, 8(1), 2006.
[42] Shirley Gaw and Edward W. Felten. "Password Management Strategies for Online Accounts". In SOUPS '06: Proceedings of the Second Symposium on Usable Privacy and Security, pages 44–55, New York, NY, USA, 2006. ACM.
[43] Steven M. Bellovin and Michael Merritt. "Encrypted Key Exchange: Password-Based Protocols SecureAgainst Dictionary Attacks". In SP '92: Proceedings of the 1992 IEEE Symposium on Security and Privacy, page 72, Washington, DC, USA, 1992. IEEE Computer Society.
[44] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. "Password Sharing: Implications for Security Design Based on Social Practice". In CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems, pages 895–904, New York, NY, USA, 2007. ACM.
[45] V. Goyal, V. Kumar, M. Singh, A. Abraham, and S. Sanyal, "A new protocol to counter online dictionary attacks," Computers & Security, vol. 25, no. 2, pp.114-120, Mar. 2006.
[46] Younes ASIMI, Abdellah AMGHAR, Ahmed ASIMI and Yassine SADQI: "New Random Generator of a Safe Cryptographic Salt per session (RGSCS)" , International Journal of Network Security,IJNS-2013-11-14-2, (Submitted).
[47] Younes ASIMI, Abdellah AMGHAR, Ahmed ASIMI and Yassine SADQI: "Strong zero-knowledge Authentication based on the Virtual Passwords (SAVP)", International Journal of Network Security, Accepted, November. 2014.
[48] Y. Wu, H. Yao, and F. Bao, "Minimizing SSO effort in verifying SSL anti-phishing indicators," Proceedings of 23rd International Information Security Conference, vol. 278, pp. 47-61, Sep. 2008.

Authors

ASIMI Younes Received his Master's degree in Computer Science and Distributed Systems in 2012 from Departments of Mathematics and Computer Science, Faculty of Science, University Ibn Zohr, Agadir, Morocco. He is currently pursuing Ph.D in Departments of Mathematics and Computer Sciences, Information Systems and Vision Laboratory, Morocco. His research interests include Authentication Protocols, Computer and Network Security and Cryptography.

Abdallah AMGHAR is a Professor in the Physics Department, Faculty of Science, University Ibn Zohr, Morocco. He received his DEA and DES degree in 1994 from Department of Physics, Faculty of Science, University Hassan II , Morocco. In January 2002, he has Ph.D degree in microelectronic from Department of Physics, Faculty of Science, University Ibn Zohr, Morocco. His areas of research interests include Cryptography, DNT, embedded systems and microelectronic.

ASIMI Ahmed received his PhD degree in Number theory from the University Mohammed V – Agdal in 2001. He is reviewer at the International Journal of Network Security (IJNS). His research interest includes Number theory, Code theory, and Computer Cryptology and Security. He is a full professor at the Faculty of Science at Agadir since 2008.

SADQI Yassine received his Master's degree in the field of Computer Science and Distributed Systems at Ibn Zoher University in 2012. He is currently a Ph.D. candidate of the Ibn Zoher University, Agadir, Morocco. His main field of research interest is Web Applications Security, Computer Security and Cryptography.