Secure Authentication Protocol Based on Machine-metrics and RC4-EA Hashing

Ashraf Aboshosha[1], Kamal A. ElDahshan[2], Eman K. Elsayed[3] and Ahmed A. Elngar[2]

(Corresponding author: Ahmed A. Elngar)

NCRRT, Atomic Energy Authority, Cairo, Nasr City, Egypt[1]

Faculty of Science, Al-Azhar University, Cairo, Egypt[2]

Faculty of Science (Girls), Al-Azhar University, Cairo, Egypt[3]

1 Al Mokhaym Al Daem, Cairo Governorate, Egypt

(Email: elngar_7@yahoo.co.uk)

(Received Aug. 28, 2015; revised and accepted Nov. 27 & Dec. 15, 2015)

Abstract

Most authentication schemes are using physical token such as smart cards to restrict services. Although these schemes have been widely deployed for various kinds of daily applications; there are severe challenges regarding their infrastructure requirements and security. This paper proposes an efficient authentication protocol based on user's machine-metrics. The proposed protocol uses the machine physical metrics to identify machines in the network, which provides the basic capability to prevent an unauthorized machine to access resources. Thus, machine-merics based authentication for machine can be looked as an analog of biometric-based authentication for human. The proposed protocol is employing the *RC4-EA Hashing* function to secure the collected machine-merics. Since it is satisfying the basic requirements of a cryptographic hash function. Therefore, the purpose of the proposed protocol is theft-proofing and guarding against attacks based on stolen or lost tokens. Also, it offers strong protection against several attacks such as credential compromising attacks.

Keywords: Authentication, machine-merics authentication, RC4-EA hash function, user authentication

1 Introduction

Internet has become the most convenient environment for education, business, and content management system (CMS) around the world [16]. Thus, internet security is an important issue to prevent the confidential information from being accessed by illegal users [10]. Remote user authentication plays the most principal service on the internet. It is a process of identifying an authorized user for a particular web service on the internet [11].

Smart card based authentication scheme is one of the most convenient and effective authentication mechanism. Which used to restrict access of the web service [7]. Although these schemes have been widely deployed for various kinds of daily applications, such as e-commerce, e-health; there are severe challenges regarding their infrastructure requirements [14], security, and privacy. Therefore, a failure of any of these security goals may render the whole system completely insecure and unpractical [15].

A common feature of these schemes is that; their security based on the *tamper-resistance* assumption about smart cards, i.e. they assume that the security parameters stored on the smart card cannot be extracted. However, recent research results have demonstrated that common commercial smart cards shall no longer be considered to be fully tamper proof. Which means, the secret information stored on the smart cards memory could be revealed by reverse engineering, power analysis [17], techniques or fault injection attacks. Thus, this obstacle has restricted the application of smart card based authentication schemes [13].

As a consequence, these schemes are susceptible to some types of attacks such as offline password guessing attack, Smart card loss attack , replay attack, user impersonation attack, and denial of service attack [12]. Since, attack techniques have over grown to compromise a user credentials; it would not be enough to secure a user's credentials, but also to secure a user's machine [18] .

This paper proposed, a machine-metrics authentication protocol for remote user authentication. In the proposed protocol, the machine-metrics are collected and then hashed using *RC4-EA Hashing* function $RC4-EA\ Hashing$ [2]. Which is lightweight, structurally different from the broken hash class, and can reuse existing RC4 algorithm [6]. Therefor, the idea behind using machine-metrics authentication is to ensure integrity and authenticity of user credentials with his machine-metrics [1]. So that, for an attacker to compromise a user account; different independent metrics have to be compromised first before gaining full access to the user account [1].

The major goal of this paper is proposing a novel protocol to remote authentication depending on machine-metrics, instead of using the traditional smart card for remote user authentication. The proposed protocol is powerful, reliable, privacy-preserving and theft-proof. Hence, machine-merics are hashed using *RC4-EA Hashing* function $RC4 - EA\ Hashing$ to guarantee high security and usability. Which leads, to overcome the drawback of the credential compromising attack. Since, the new way of handling the machine-metrics gives higher privacy protection for authentication systems.

The rest of this paper is organized as follows: Section 2 presents an overview of Preliminary, Machine-Metrics Authentication, *RC4-EA Hashing* Function $RC4 - EA\ Hashing$. Section 3 introduces the proposed authentication protocol. Section 4 gives the implementation and security analysis. Finally, Section 5 contains the conclusion remarks.

2 An Overview

2.1 Preliminary

- **Authentication:** From the transcripts of server S, S can believe information $info$ is not modified. More specially, S can believe $info$ is indeed from a specific machine M.

- **Security of authentication protocol:** In the presence of attacker A, from the transcripts of the protocol Π the information $info$ is tampered to $info'$ by attacker A. Therefor, the probability that A can fool S to believe $info'$ is from the machine M without any change is negligible $negl$.

- **Negligible function:** A negligible function $negl$ is defined by [5]:
$$iff\ \forall c \in N\ \exists\ n_0 \in N, \text{ such that:}$$
$$\forall n \succcurlyeq n_0,\ negl(n) \prec n^{-c}.$$

- **Authentication protocol:** if for any attacker A, there exists a negligible function $negl$ satisfying Equation (1):

$$Pr[AthFool_{A,\Pi}(n) = 1] \preceq negl(n) \quad (1)$$

2.2 User Authentication

Remote user authentication plays the most significant process to verify the authorized users of a web service on the Internet. Authors in [1] proposed "Multi-Channel User Authentication Protocol based on Encrypted Hidden OTP" . Where, the protocol proposed an efficient one time password (OTP) based authentication over a multi-channels architecture. Which, applying the RC4-EA encryption method to encrypt the plain-OTP to cipher-OTP [2]. Then, Quick Response Code (QR) code is used as a data container to hide this cipher-OTP. Also, the purpose of the protocol is integrating a web based application with mobile-based technology to communicate with the remote user over a multi-channels authentication architecture [1].

2.3 Machine-metrics Authentication

Authentication is the process of confirming the identity of a person, machine, or other entity, which requesting access under security constraints. This is done for the purpose of performing trusted communications between parties for computing and telecommunications protocols [8].

In authentication protocols, all the transmissions of the data from a user's machine to the server can be reveal to attacker through interception. From the viewpoint of security strength, most common authentication protocols fail to guarantee a fault-secure method for keeping the login information away from the public [1]. To enhance the security strength of the authentication protocol, machine-metrics based authentication protocol is proposed.

Machine-metrics are metrics collected about a remote machine for the purpose of identification. Where machine-metrics based authentication uses the unique metrics of a machine to verify its identity. The metrics used in a machine-metrics based authentication protocols are unique, universal and permanent. Such metrics are suitable for authentication purposes as they cannot be lost or change. Hence, it would be possible to uniquely distinguish between all machines on a network.

Figure 1 shows a machine authentication between machine to server, and user authentication between human to machine.

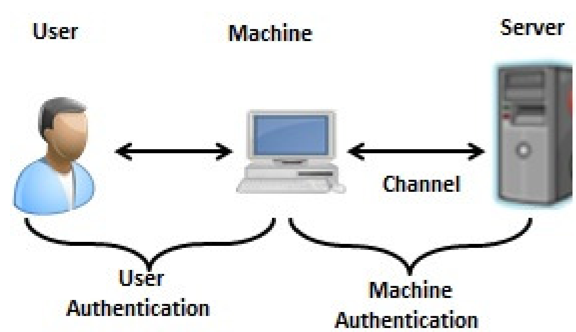

Figure 1: Machine authentication vs. user authentication

2.4 RC4-EA Hashing Function

Cryptography plays a significant procedure to prevent eavesdropping of sensitive information [9]. One of the fundamental components of many cryptographic protocols is a hash function [3].

Let $\{0,1\}^{\ell}$ denote the set of all messages of length strictly less than ℓ. A hash function is usually designed as follows; a compression function C :

$\{0,1\}^{<2^{64}} \rightarrow \{0,1\}^{160}$ is designed. Then, given a message msg such that $|msg| < 2^{64}-1$, a pad is appended at the end of the message. Then, iterates the compression function C to get its output.

A cryptographic hash function has to be resistant against three main attacks [4]:

1) **Collision resistance:** For any msg_1, it should be 'hard' to find msg_2 where $msg_1 \neq msg_2$ and $H(msg_1) = H(msg_2)$.

2) **Preimage resistance:** For a given value $H(msg)$, it should be 'hard' to compute msg.

3) **Second preimage resistance:** Given msg_1 and $H(msg_2)$, it should be 'hard' to find msg_2 such that $msg_1 \neq msg_2$ and $H(msg_2) = H(msg_1)$.

RC4-EA Hashing function denoted as $(RC4-EA\ Hashing)_\ell$, $16 \leq \ell \leq 64$ where $(RC4-EA\ Hashing)_\ell : \{0,1\}^{<2^{64}} \rightarrow \{0,1\}^{8\ell}$. $(RC4-EA\ Hashing)_\ell$ function can be used to produce authenticator to authenticate the message msg. The $(RC4-EA\ Hashing)_\ell$ function is describing as follows [6]:

1) **Padding rule:** the input message msg is padded by the padding bits generated by evolutionary algorithm (EA). a padding rule is applied to the message msg such that:

$$pad(msg) = bin_8(\ell)||msg||1||0^k||bin_{64}(|msg|)$$

where, $bin_{64}(|msg|)$ is the binary representation of number of bits of msg; and k is the least non-negative integer such that $8 + |msg| + 1 + k + 64 \equiv 0$ mod 512. Then, $pad(msg) = msg_1||...||msg_t$ such that each $|msg_i| = 512$ bits, the maximum possible message length is $2^{64} - 1$.

2) **Classical iteration:** Let $msg_1||...||msg_t$ be the padded message. Let $(P_0, j_0) = (P^{IV}, 0)$ be an initial value. The iterations are followed as in Equation (2):

$$(P_0, j_0) \xrightarrow{msg_1} (P_1, j_1)...(P_{t-1}, j_{t-1}) \xrightarrow{msg_t} (P_t, j_t) = C^+(msg) \quad (2)$$

Where, $(P, j)\underset{\rightarrow}{B}(P^*, j^*)$ means that:

$$C((P, j), B) = (P^*, j^*)$$

Such that, $(B = B[0]||B[1]||...||B[63], B[i] = 8)$ and

$$C : Perm \times [N] \times \{0,1\}^{512} \longrightarrow [N]$$

3) **Post-processing:** Let the internal state after the classical iteration is (P_t, j_t) i.e., $OWT(C^+(msg)) = (P_t, j_t)$. Hence, the post processing is defined as follow:

- Computed $(P_{t+1}) = P_0 \circ P_t$ and $j_{t+1} = j_t$. Where, $\circ$ means the composition of the permutations.
- Define the final hash value $RC4-EA\ Hashing_\ell(msg)$ by hash byte generation algorithm such that; $HBG_\ell(OWT(P_{t+1}, j_{t+1}))$.

The algorithms of the compression C , One-Way Transformation OWT and Hash Byte Generation HBG_ℓ functions are given in Algorithms 1, 2 and 3 respectively [6]. Note all arithmetic is done modulo 256:

Algorithm 1 A compression function algorithm (C)

Input: *Internal state (P, j), 64-byte message block B*
Output: *The updated internal state (P, j)*

```
for i = 0 to 255 do
    j = (j + P[i] + B[z(i)])
    Swap(P[i], P[j])
end for
Return (P, j)
```

Where, the function $z : [256] \rightarrow [64]$ is known as reordering, i.e. z is the mapping restricted on $[0, 63]$, $[64, 127]$, $[128, 191]$ and $[192, 255]$ are injective.

Algorithm 2 One-way transformation algorithm (OWT)

Imput: *Internal state (P, j)*
Output: *Updated internal state after padded*

```
Temp_1 = P
for i = 0 to 511 do
    j = (j + P[i])
    Swap(P[i], P[j])
end for
Temp_2 = P
P = Temp_1 ∘ Temp_2 ∘ Temp_1
Return (P, j)
```

Algorithm 3 A hash byte generation algorithm (HBG_ℓ)

Imput: *Internal state* (P, j)
Output: *The message digest*

```
for i = 0 to ℓ do
    j = (j + P[i])
    Swap(P[i], P[j])
end for
H[i] = P[p[i] + p[j]]
Return H[i]
```

2.5 Security of RC4-EA Hashing Function

Since the generation (hash value) of $RC4-EA\ Hashing$ Function is close to uniform, it is impossible to find the

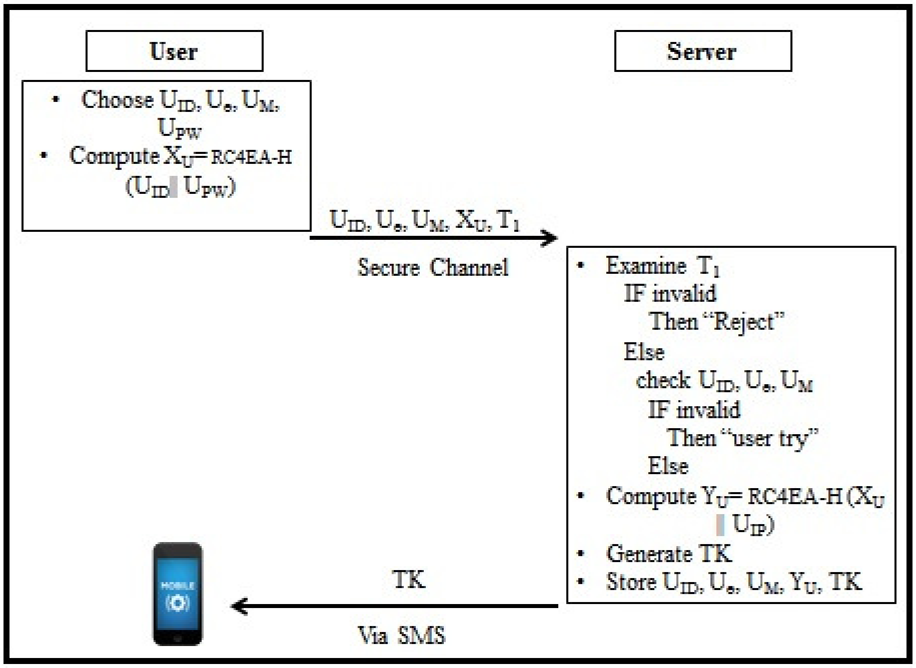

Figure 2: User enrollment phase

input through output and it is also computationally infeasible to find any two messages msg_1 and msg_2 such that $RC4{-}EA\ Hashing(msg_1) = RC4{-}EA\ Hashing(msg_2)$. Therefore, $RC4-EA\ Hashing$ function is one-way mapping and strongly collision free. Also, it is satisfies the basic requirements of a cryptographic hash function.

Therefore, the $RC4{-}EA\ Hashing$ Function is collision resistant, preimage resistant, and second preimage attack resistant. The efficiency of the $RC4-EA\ Hashing$ function is much better than widely used known hash functions and its structure is absolutely different from the broken hash function classes (e.g., SHA family). It is very secure out all possible generic attacks.

3 The Proposed Machine-metrics Authentication Protocol

The major aim of the proposed protocol is theft-proofing and guarding against attacks based on stolen or lost tokens. Also, it is defending the credential compromising attack A_{cc}; by introducing the machine-metrics. The proposed machine-metrics authentication protocol is enhancing a user authentication protocol proposed in [1].

The machine-metrics authentication protocol involves three parties: A server (S), a remote user (U) and Client Side Program CSP. The proposed protocol consists of three phases: User enrollment phase, machine-metrics enrollment phase, and machine-metrics authentication phase. The notations employed throughout this paper are shown in Table 1.

Table 1: Notations

Notation	Description
U	Remote user
U_{ID}	User identity
U_{PW}	User password
U_{IP}	User IP address
U_M	User mobile
U_e	User electronic mail
S	The server
M	The machine
CSP	The client side program
$RC4-EA\ Hashing$	RC4-EA hashing function
V_{UHI}	Hashing for index the user
D_{HMC}	Hashing machine-metrics
$\|\|$	Concatenation
T	Time stamp
TK	Token
RNC	Random nonce code

3.1 User Enrollment Phase

In this phase, U enrollments at S in order to use a service. The enrollment process is shown in Figure 2 and have execute the following steps:

1) U chooses an identity U_{ID}, electronic mail U_e, mobile number U_M, and password U_{PW}. Then computes $X_U = RC4{-}EA\ Hashing\ (U_{ID}||U_{PW})$. Then sends

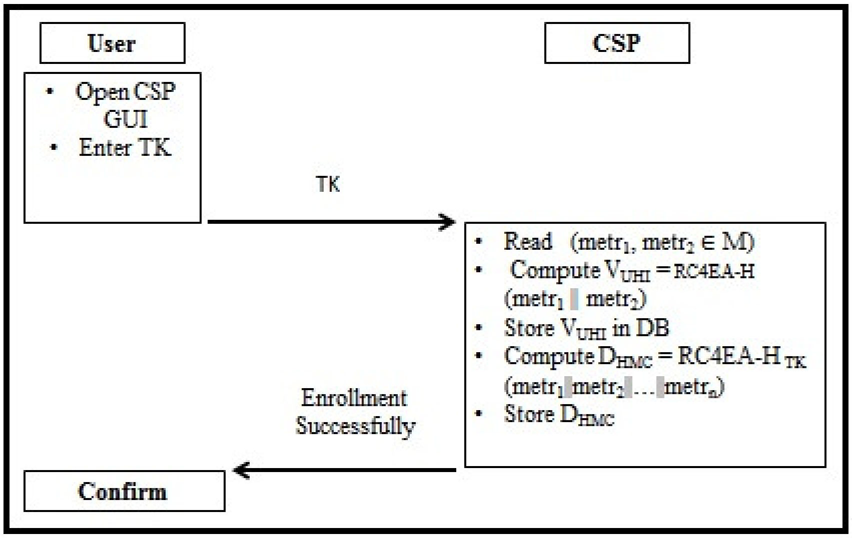

Figure 3: Machine-metrics enrollment phase

$\{U_{ID},\ U_e,\ U_M,\ X_U, T_1\}$ to S via a secure channel.

$$U \rightarrow S : \{U_{ID}, U_e, U_M, X_U, T_1\}$$

2) S examine the time stamp T_1. If it is invalid, then rejects it. Otherwise, checks whether U_{ID}, U_e, U_M is available for use. If it is, S computes $Y_U = RC4-EA\ Hashing(X_U||U_{IP})$. Finally, S stores the values U_{ID}, U_e, U_M and Y_U in its database.

$$S \rightarrow DB : \{U_{ID}, U_e, U_M, Y_U\}$$

3) S generate random token TK, then sends TK to U via mobile channel.

$$S \rightarrow U : \{TK\} \tag{3}$$

4) Finally, S stores the values TK in its database.

$$S \rightarrow DB : \{TK\}$$

3.2 Machine-metrics Enrollment Phase

In this phase, the physical metrics of a machine are collected to be used as the identification of the machine. Suppose the physical metrics space is M which consists of n metrics; $M = \{metr_1, metr_2, ..., metr_n\}$. The client side program CSP will returns $metr_i \in M, (i = 1, 2, ..., n)$. The enrollment process is shown in Figure 3. Then, U, S and CSP execute the following steps:

1) U received his TK from S via mobile channel.

2) U will enter his TK to CSP to enrollment his machine.

3) CSP read $metr_1,\ metr_2 \in M$. Then computes $V_{UHI} = RC4-EA\ Hashing(metr_1||metr_2)$. Then stores the value V_{UHI} in a remote database DB.

$$CSP \rightarrow DB : \{V_{UHI}\}$$

4) CSP will use TK as a secret seed for RC4-EA Hashing, then computes:

$$D_{HMC} = RC4-EA\ Hashing_{TK}(metr_1||metr_2||...||metr_n).$$

5) Finally, CSP stores the values D_{HMC} in a remote database DB.

$$CSP \rightarrow DB : \{D_{HMC}\}$$

3.3 Machine-metrics Authentication Phase

After U has a successful login. Now S wants to authenticate the machine upon client side program CSP. The machine-metrics authentication process is shown in Figure 4. Then, U, S and CSP execute the following steps:

1) CSP read $metr_1,\ metr_2 \in M$. Then computes $V'_{UHI} = RC4EA-H(metr_1||metr_2)$.

2) CSP checks whether $V'_{UHI} == V_{UHI}$. If it is, then CSP will get the TK.

3) CSP computes:

$$D'_{HMC} = RC4-EA-Hashing_{TK}(metr_1||\ metr_2||...||metr_n)$$

using TK as a secret seed.

4) CSP checks whether $D'_{HMC} == D_{HMC}$. If it is, then CSP will generate random nonce code RNC

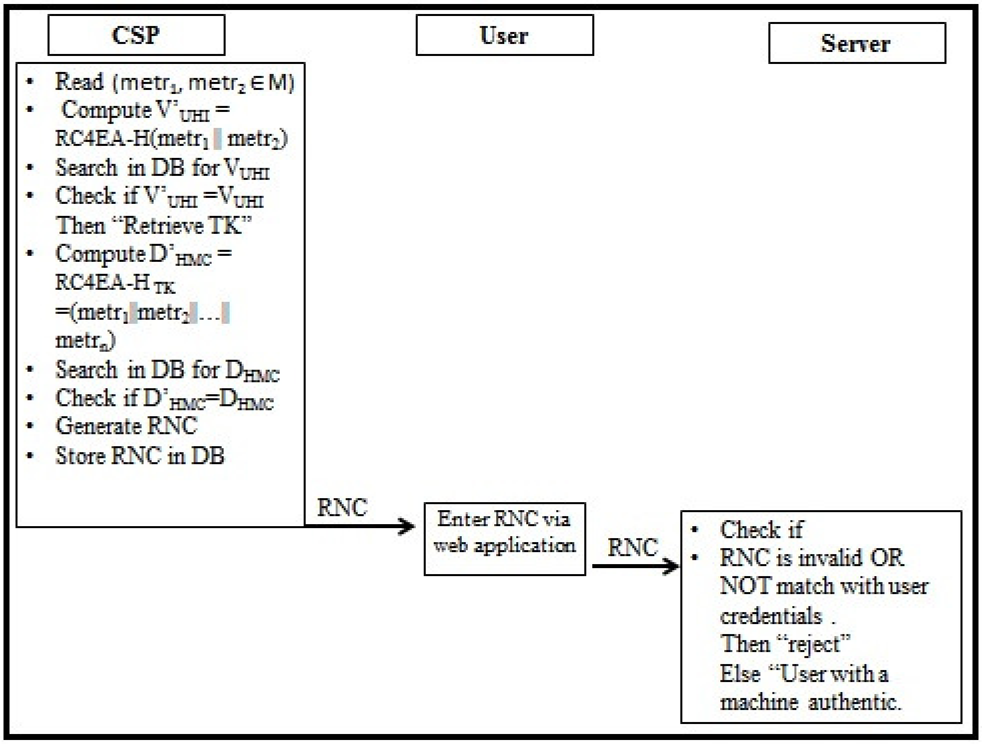

Figure 4: Machine-metrics authentication phase

to U with the $status = 1$ using *RNGCryptoServiceProvider* which gives an unguessable crypto strength seed. Hence, it gives the random object with a different crypto strength number each time. Which mean is that, it will go on to return a different random number for each call. Then CSP stores the values RNC in a remote database DB.

$$CSP \rightarrow DB : \{RNC\}$$

5) U sent RNC to S via web application.

6) Finally, S checks whether RNC is invalid or not match with user credentials at the DB then, "request is rejected". Otherwise, user's machine is authentic and convert RNC status to 0.

4 Implementation and Security Analyses

The proposed machine-metrics authentication protocol is adopting the RC4-EA Hashing function $RC4 - EA\ Hashing$ to hash the machine physical metrics. The machine-metrics takes the responsibility for achieving mutual authentication between the M and S.

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

4.1 Implementation

The proposed machine-metrics Authentication protocol is implementing the RC4-EA Hashing function $RC4 - EA\ Hashing$ to hash the machine physical metrics, which are collected via the client side program CSP like {Total Machine Memory (TMM), Procesor Id (PId), Name of CPU ($NCPU$), MotherBoard Id (MId), Hard Desk Id ($HDId$) }as shown in Table 2. Thus, it helps in mitigating the credential compromising attack A_{cc}. Whenever a user U wishes to login the website, first step is to enter U_{ID} and U_{PW} for remote User authentication. The second step is that; a machine physical metrics will be collected via client side program CSP. Then, the CSP will hash the machine physical metrics using $RC4 - EA\ Hashing$. The third step is that; CSP will generate RNC to authentic the machine as shown in Tables 3, 4, 5. Thus, the proposed machine-metric authentication protocol is integrating a web based application with desktop based application to make it more secure than the general authentication protocols.

Table 2: CSP collected machine physical metrics table

TMM	PId	$NCPU$	MId	$HDId$
21...48	BF...652	In.(R)C.i3-M330@2.GHz	.4X...4876.	20...058
32...72	BF...655	In.(R)C.i3-M380@2.GHz	.4C...00RW.	20...436
85...92	BF...6A7	In.(R)C.i7-2MCPU@2.GHz	.PC...A0UG.	W7...5YK

Table 3: User register table to main website

U.N	Password	Email	Mobil No.	Token TK.
Jack	895*/66!	Jack@ egywow.com	968935810	K8*roMS1
Henary	P**2334	Henary@ egywow.com	968925612	D4A/gE7S
Bill	Ad2*!98	Bill@ egywow.com	966954523	1B6loP3S

Table 4: Hashing machine metrics table via $RC4 - EA\ Hashing$

$U.N$	TK	V_{UHI}	D_{HMC}
Jack	K8*roMS1	600eaw73b...	MDWKcEMZ3...
Jack	D4A/gE7S	ds734be484...	PXmnnMCa4Rp...
Jack	1B6loP3S	83d91a2d58...	3i18E1aaZby...

Table 5: Machine authentication code table

V_{UHI}	TK	D_{HMC}	RNC
600eaw73b...	K8*roMS1	MDWKcMEMZ3...	Ez8U89w91
600eaw73b...	K8*roMS1	MDWKcMEMZ3...	5Vr2uo5XD
600eaw73b...	K8*roMS1	MDWKcMEMZ3...	x99ICN41C

4.2 Security Analyses

The security of the proposed protocol is analyzed under the possibilities of the types of attacks listed below:

1) **Prevent Man-in-the-middle attack:** In this type of attack, the attacker listens to the communication channel between S and U. In the proposed protocol, the attacker may intercept the mobile communication messages, but he will never be able to compute the D_{HMC}. Since, it is based on $RC4-EA\ Hashing$. So attacker should know the hash function and use same user's machine physical metrics. Hence, the proposed protocol is secure against man-in-the-middle attacks.

2) **Prevent phishing attack via the web:** This attack aims to steal sensitive information. In the proposed protocol, if the attacker knows U_{ID} and can get the U_{PW} from the server by replacing the actual web page with a similar one, it would be difficult to get the token TK because it send over mobile channel as in Equations (3). This, the proposed protocol is secure against the phishing attacks.

3) **Prevent credential compromising attack:** Denoted as A_{cc}, this attack aims to hacked, modified, exposed, or cloned softwares or hardwares for a machine identification. In the proposed protocol, as the hash function $RC4 - EA\ Hashing$ is secure, attacker cannot compute D_{HMC}. It can be looked as a computed credential of a machine to guarantee the authentication security. That is, $Pr[AthFool_{A_{cc},\Pi}(n) = 1] \preceq negl(n)$. Therefor, the proposed protocol is secure against credential compromising attacks.

4) **Prevent impersonation attack:** In this type of attack, the malicious user forges the security parameters from the authentication protocol and tries to impersonate as a legitimate user. In our protocol, the malicious user has to guess the parameters Y_U, V_{UHI} and TK which is used in the calculation of D_{HMC} for generating a valid login request. The RC4-EA hashing function $RC4 - EA\ Hashing$ is impossible to solve in real polynomial time, thus the$RC4 - EA\ Hashing$ parameter cannot be forged. Therefore, the malicious user will fail to launch an impersonation attack on this proposed protocol.

5 Conclusions

The major contribution of this paper, is proposing machine-metrics authentication protocol. The proposed protocol enhances the security of a remote user login; by using the physical metrics of a machine. Also, the proposed protocol is adopting the *RC4-EA Hashing* function to secure these machine metrics. Therefore, the data can not be easily retrievable without adequate authorization. The purpose of this paper is to integrate a web based application with desktop based application to make the proposed protocol more secure than the general authentication schemes. Thus, the proposed authentication protocol is more convenient, because the burden of carrying a separate hardware tokens are removed. Moreover, this protocol helps to overcome many challenging attacks such as phishing attacks and credential compromising attacks.

References

[1] A. Aboshosha, K. A. ElDahshan, E. K. Elsayed and A. A. Elngar, "Multi-channel user authentication protocol based on encrypted hidden OTP," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 13, no. 6, pp. 14–19, 2015.

[2] A. Aboshosha, K. A. ElDahshan, E. K. Elsayed and A. A. Elngar, "EA based dynamic key generation in RC4 ciphering applied to CMS," *International Journal of Network Security (IJNS)*, vol. 17, no. 4, pp. 405–412, 2015.

[3] M. Bellare and P. Rogaway, "Collision-resistant hashing: towards making UOWHFs practical," in

Advances in Cryptology (Crypto'97), LNCS 1294, pp. 470–484, Springer-Verlag, 1997.

[4] M. Bellare and T. Kohno, "Hash function balance and its impact on birthday attacks," in *Advances in Cryptology (Eurocrypt'04)*, LNCS 3027, pp. 401–418, Springer-Verlag, 2004.

[5] M. Bellare and O. Goldreich, "On defining proofs of knowledge," in *Advances in Cryptology (Crypto'92)*, LNCS 740, pp. 390–420, Springer-Verlag, 1992.

[6] D. Chang, K. C. Gupta and M. Nandi, "RC4-Hash: A new hash function based on RC4," in *7th International Conference on Cryptology in India*, vol. 4329, pp. 80–94, Springer-Verlag, 2006,

[7] D. Chatterjee, J. Nath, S. Mondal, S. Dasgupta and A. Nath, "Advanced symmetric key cryptography using extended MSA method: DJSSA symmetric key algorithm," *Jounal of Computing*, vol. 3, no. 2, pp. 66–71, 2011.

[8] M. A. Fairuz and K. Renaud, "Multi-channel, multi-level authentication for more secure ebanking," In ISSA, 2010.

[9] S. Gupta, A. Chattopadhyay, K. Sinha, S. Maitra and B. Sinha, "High-performance hardware implementation for RC4 stream cipher," *IEEE Transactions on Computers*, vol. 62, no. 4, pp. 730–743, 2013.

[10] A. Hiltgen, T. Kramp, T. Weigold, "Secure internet banking authentication," *IEEE Transactions on Security and Privacy*, vol. 4, no. 2, pp. 21–29, 2006.

[11] S. Kalra, S. Sood, "Advanced remote user authentication protocol for multi-server architecture based on ECC," *journal of information security and applications*, vol. 18, pp. 98–107, 2013.

[12] M. Kumar, "An enhanced remote user authentication scheme with smart card," *International Journal of Network Security*, vol. 10, no. 3, pp. 175–184, 2010.

[13] H. Le, C. Chang and Y. Chou, "A novel untraceable authentication scheme for mobile roaming in GLOMONET," *International Journal of Network Security*, vol. 17, no. 4, pp. 395–404, 2015.

[14] J. Malik, D. Girdhar, R. Dahiya and G. Sainarayanan, "Multifactor authentication using a QR code and a one-time password," *Journal of Information Processing Systems*, vol. 10, no. 3, pp. 483–490, 2014.

[15] C. Ma, D. Wang and S. Zhao, "Security flaws in two improved remote user authentication schemes using smart cards," *International Journal of Communication Systems*, vol. 27, no. 10, pp. 2215–2227, 2012.

[16] P. E. S. N. K. Prasasd, A. S. N. Chakravarthy and B. D. C. N. Prasad, "Performance evaluation of password authentication using associative neural memory models," *International Journal of Advanced Information Technology (IJAIT)*, vol. 2, no. 1, pp. 75–85, 2012.

[17] S. K. Sood, "Secure dynamic identity-based authentication scheme using smart cards," *Information Security Journal: A Global Perspective*, vol. 20, no. 2, pp. 67–77, 2011.

[18] X. Sun, S. Men, C. Zhao and Z. Zhou, "A security authentication scheme in machine-to-machine home network service," *Security and Communication Networks*, vol. 10, no. 16, pp. 2678–2686, 2012.

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

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

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

Ahmed A. Elngar graduated with a B.Sc. in computer

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