A Protected Single Sign-On Technique Using 2D Password in Distributed Computer Networks

Mrs.P.V.Jothikantham
Department of Computer Science and Engineering
Shree Venkateshwara Hi Tech Engineering College, Gobi,
Tamilnadu, India.
jothikanthampv@gmail.com

Mr.S.Prakadeswaran
Department of Computer Science and Engineering
Shree Venkateshwara Hi Tech Engineering Collge, Gobi,
Tamilnadu, India.
prakades@gmail.com

Abstract- Single Sign-On (SSO) is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network. Recently, a new SSO scheme providing well-organized security argument failed to meet credential privacy and soundness of authentication. The main goal of this project is to provide security using Single Sign-On scheme meeting at least three basic security requirements, i.e., unforgetability, credential privacy, and soundness. User identification is an important access control mechanism for client–server networking architectures. The concept of Single Sign-On can allow legal users to use the unitary token to access different service providers in distributed computer networks. To overcome few drawbacks like not preserving user anonymity when possible attacks occur and extensive overhead costs of time-synchronized mechanisms, we propose a secure Single Sign-On mechanism that is efficient, secure, and suitable for mobile devices in distributed computer networks. In a real-life application, the mobile user can use the mobile device, e.g., a cell phone, with the unitary token to access multiservice, such as downloading music; receive/reply electronic mails etc. Our scheme is based on one-way hash functions and random nonce to solve the weaknesses described above and to decrease the overhead of the system. The proposed scheme is more secure with two types of password scheme namely, Text password and Graphical Password referred as 2D password in distributed computer networks that yields a more efficient system that consumes lower energy. The proposed system has less communication overhead. It eliminates the need for time synchronization and there is no need of holding multiple passwords for different services.

Keywords*-Single Sign- On, time-synchronized, security.*

*****

I. Introduction

Authentication is a function where a user presents some credentials to the system. If the system recognizes this set of credentials or the credentials match a given set on the system, then the user is said to be authorized otherwise the user is not authorized. Authentication is needed to let the system perform some tasks for the user. The user needs to be authorized to request services from the system. Before a user can be authenticated to the system, he has to be registered with the system for the first time. This step is called registration. So, for a new user, he has to get registered with a system and then authenticated before he can request services. In a basic authentication process, a user presents some credentials like user ID and Some more information to prove that the user is the true owner of the user ID This process is simple and easy to implement. The user submits user ID and an image as credentials to the system. If the image matches with the one stored in the system, the user is authenticated. Images are easy to remember. It is not easy to guess images. Performing brute force attacks on such systems is very difficult. A first time user has to register him with the system by providing all his details. The interface guides the user in a step-by step fashion. No major change is to be made to the existing password based systems to incorporate the use of images. The system remains simple as the password based one.

User identification is an important access control mechanism for client–server networking architectures. The concept of Single Sign-On can allow legal users to use the unitary token to access different service providers in distributed computer networks. Recently, some user identification schemes have been proposed for distributed computer networks. Unfortunately, most existing schemes cannot preserve user anonymity when possible attacks occur. Also, the additional time-synchronized mechanisms they use may cause extensive overhead costs. To overcome these drawbacks, we propose a secure Single Sign-On mechanism that is efficient, secure, and suitable for mobile devices in distributed computer networks.

A. Authentication

Authentication is one of the most important security service provided to system by the different authentication schemes or algorithms. To protect any system authentication must be provided, so that only authorized persons can have right to use or handle that system & data related to that system securely. There are many authentication algorithms are available some are effective & secure but having some drawback. Previously there are many authentication techniques were introduced such as graphical password, text password, Biometric authentication, etc. generally there are four types of authentication techniques are available such as:

- **Knowledge based**means what you know. Textual password is the best example of this authentication scheme.

- **Token based**means what you have. This includes Credit cards, ATM cards, etc as an example.

- **Biometrics**means what you are. Includes Thumb impression, etc.

- **Recognition Based**means what you recognize. Includes graphical password, iris recognition, face recognition, etc.

Ideally there are two types of authentication schemes are available according to nature of scheme & techniques used, those types are

A.1 Recall based

In this authentication technique user need to recall or remember his/her password which is created before. Knowledge based authentication is a part of this technique, E.g. Textual password, graphical password etc. this technique is commonly used all over the world where security needed.

A.2 Recognition based

In this user need to identify, recognize password created before. Recognition based authentication can be used in graphical password. Generally this technique is not use much more as Recall based is used. Still both recall based & recognition based authentication techniques having some drawbacks & limitations when they are used separately or used single authentication scheme at a time.

Single Sign-On Scheme

Single Sign-On (SSO) is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network. The concept of Single Sign-On can allow legal users to use the unitary token to access different service providers in distributed computer networks.

The main goal of secure Single Sign-On scheme is to satisfy at least three basic security requirements, i.e., unforgetability, credential privacy, and soundness.

- **Unforgetability** demands that, except the trusted authority, even a collusion of users and service providers are not able to forge a valid credential for a new user.

- **Credential privacy** guarantees that colluded dishonest service providers should not be able to fully recover a user’s credential and then impersonate the user to log in to other service providers.

- **Soundness** means that an unregistered user without a credential should not be able to access the services offered by service providers

A.3 Project Objective

The main objective is to identify the flaws in their security arguments to explain why attacks are possible against their SSO scheme. Our attacks also apply to another SSO scheme. The user authentication (also called user identification) plays a crucial role in distributed computer networks to verify if a user is legal and can therefore be granted access to the services requested. To avoid bogus servers, users usually need to authenticate service providers. After mutual authentication, a session key may be negotiated to keep the confidentiality of the data exchanged between a user and a service provider. It presents a 2D password scheme for distributed computer networks to improve level of security using **Textpassword** and **Graphical password.** It yields a more efficient system that consumes lower energy and eliminates the need of holding multiple passwords for different services.

II. LITERATURE SURVEY

Distributed systems and networks have been adopted by telecommunications, remote educations, businesses, armies and governments. A widely applied technique for distributed systems and networks is the Single Sign-On (SSO) which enables a user to use a unitary secure credential (or token) to access multiple computers and systems where he/she has access permissions. However, most existing SSO schemes have not been formally proved to satisfy credential privacy and soundness of credential based authentication. To overcome this drawback, we formalize the security model of Single Sign-On scheme with authenticated key exchange. Specially, we point out the difference between soundness and credential privacy, and define them together in one definition. Also, we propose a provably secure Single Sign-On authentication scheme, which satisfies soundness, preserves credential privacy, meets user anonymity, and supports session key exchange.

User identification is an important access control mechanism for client–server networking architectures. The concept of Single Sign-On can allow legal users to use the unitary token to access different service providers in distributed computer networks. Recently, some user identification schemes have been proposed for distributed computer networks. Unfortunately, most existing schemes cannot preserve user anonymity when possible attacks occur. Also, the additional time-synchronized mechanisms they use may cause extensive overhead costs. To overcome these drawbacks, we propose a secure Single Sign-On mechanism that is efficient, secure, and suitable for mobile devices in distributed computer networks.

A. Problem Definition

With the development of distributed computer networks, it is easy for user terminals to share information and computing power with hosts. The distributed locations of service providers make it efficient and convenient for subscribers to access the resources. In general solutions, users must register with each service provider and keep different identity/password pairs for accessing each service provider. However, when users have to keep so much secret information, security problems can occur and increase the overhead for the networks. There are four important security problems that the user identification scheme must solve. They are

- It must determine whether users are legitimate or not;
- Service providers must be authenticated;
- A common session key must be appropriately established;
- The privacy of legal users must be ensured.

III.METHODOLOGY AND IMPLEMENTATION

A. Single Sign-On Scheme with 2D Password

We propose a secure Single Sign-On mechanism to allow mobile users to use the unitary token to access service providers. In a real-life application, the mobile user can use the mobile device, e.g., a cell phone, with the unitary token to access multiservice, such as download music; receive/reply electronic mails etc. Our scheme is based on one-way hash functions and random nonce to solve the weaknesses described above and to decrease the overhead of the system. The proposed scheme is more suitable for mobile users who use battery-limited devices due to its lower computational cost and lower communication cost. In addition, without additional time synchronized mechanisms, our scheme can be employed for distributed computer networks.

New scheme should be combination of image and token based authentication schemes. The proposed scheme is more secure with two types of password scheme namely, Text password and Graphical Password referred as 2D password in distributed computer networks that yields a more efficient system that consumes lower energy. The proposed system has less communication overhead. It eliminates the need for time synchronization and there is no need of holding multiple passwords for different services.

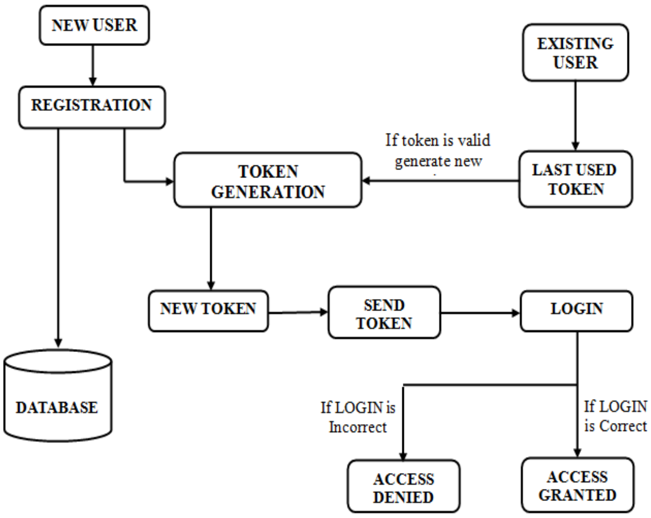


Fig1 : System Architecture of the proposed system

This section presents a secure single sign-on scheme with user anonymity for remote user authentication in distributed systems and networks. We use Schnorr signature to overcome the drawbacks in Chang-Lee scheme as their user proof cannot provide soundness and credential privacy while Schnorr signature can. As a provably unforgivable signature scheme, Schnorr signature allows a signer to authenticate him/herself by signing a message without releasing any other useful information about his/her private signing key. In the proposed scheme, the TCP first issues the credential for each user by signing the user's identity *IDi* according to Schnorr signature. Then, by treating his/her credential as another public/ private key pair the user can authenticate him/herself by signing a Schnorr signature on a temporal message generated in the protocol. In contrast, each service provider maintains its own public/private key pair in any secure signature scheme so that it can authenticate itself to users by simply issuing a normal signature. Finally, as does in Chang-Lee scheme [12], the session key is established by running a variant of Diffie-Hellman key exchange protocol, and the user anonymity is guaranteed by symmetric key encryption. The notations used in the scheme are summarised in Table I.

Table I

Notations Used in the Scheme

TCP	The trusted credential provider
Pj	A service provider
Ui	A user
SIDj	The unique identity of Pj
IDi	The unique identity of Ui
Ci	The credential of Ui
x	The long term private key of TCP
y	The public key of TCP
Ek(M)	Symmetric encryption of message M using key k
Dk(C)	Symmetric decryption of ciphertext C using key k
h(.)	A secure hash function

System Setup Phase: In this phase, TCP initializes his/her public and private parameters as Schnorr signature scheme. Firstly, TCP picks large primes p and q such that q|p-1, chooses a generator g of large safe prime order q in cyclic group G. Then, TCP sets its private key *SK* = *x*, where x ϵ Z*q is a random number, and publishes its public key PK = y, where y = gx mod p.

Registration Phase: In this phase, user asks TCP for registration, then TCP issues a unique identity *IDi*via *IdGen(RIi)* and signs a Schnorr signature (a; e;C) for user's identity as credential generation algorithm CGen(IDi; SK). C is kept secret by user, while (a; e) will be made public. The details are given below.

- User Registration: When a user *Ui* asks for registration, TCP selects a unique identity *IDi* and generates a credential *Ci = (a; e;C)* for *Ui* by selecting a randomness r 2 Z_q and computing a = gr mod p, *e = h(a; IDi)*, and C = r + xe mod q. Then, TCP sends identity *IDi* and credential *Ci*which is Schnorr signature for *IDi* to user *Ui*, where C should be kept as a secret.

- Service Provider Registration: Each *Pj* maintains a public/private key pair *(PKj ;SKj)* of any secure signature scheme. Here, algorithms SPPGen(.) and SPPVer(.) are identical to the signature generation and verification algorithms respectively.

Authentication Phase: In this phase, to uthenticate him/herself user*Ui* signs a Schnorr signature the newly established session key *Kij* using credential C the signing key, while *Ui's* session key material k2 is used as the commitment. Note that the corresponding verification key of C is g^C, which can be recovered by computing $g^C = a\ .y^e mod\ p$. For service provider authentication, any provably secure signature scheme can be used to authenticate a service provider in proposed scheme. The session key is established by using modified Diffie-Hellman key exchange scheme which has been formally proved, and the user anonymity and unlinkability are preserved by using symmetric key encryption to encrypt a, e, and user's identity IDi. The details of this phase are illustrated and further explained below.

1) User Ui chooses a random nonce n1 and sends M1 = (Req; n1) to Pj , where Req is a service request.

2) Upon receiving (Req; n1), Pj picks random number r1 2 Z_q , computes its session key material k1 = gr1 mod p, u = h(k1jjSIDj jjn1) and signs u to get a signature v = SPPGen(SKj ; u), and sends M2 = (k1; v; n2) to the user.

3) User Ui first computes u = h(k1jjSIDj jjn1)
and verifies the signature v by checking if *SPPVer(PKj ; u; v) = 1*. If the output is "0", Uiterminates the protocol. Otherwise, *Ui* accepts the
service provider Pj 's authentication, and then selects a random number r$_2$ ϵ Z*q to compute k2 = g^{r2} mod p, kij = k1^{r2} mod p, and the session key K$_{ij}$= h(SIDj|| k$_{ij}$). After that, *Ui* signs K$_{ij}$ using his/her credential secret C by calculating e$_i$ = h(k$_2$;K$_{ij}$), *z = r2+Cei mod q* and ! = EK(IDi || n3||n2||e||a), where n3 is a nonce chosen by Ui. Finally, Ui sends M3 = (!; z; k2) to service provider Pj .

4) To verify z, Pj first calculates kij = k$_2$^{r1} mod p, derives session key Kij = h(SIDj || kij) and decrypt
! withKij to recover IDi||n3||n2||e||a. Then, Pj checks if e = h(ajjIDi). If this does not hold, Pj aborts the protocol. Otherwise, the service provider computes ei = h(k2;Kij) and verifies z by checking if gz = k2. a^{ei}. (ye)^{ei} mod p. If this holds, Pj accepts
Ui's authentication, believes that they have shared the same session key Kij , and sends V = h(n3) as M4 to Ui.

5) User Ui computes V 0 = h(n3) and checks if V 0 = V. If this holds, Ui believes that he/she has shared the same session key Kij with Pj .

After deriving the session token using the above procedure, the graphical password is set using the PCCP with dynamic user blocks approach presents a more feasible way of varying the security level depending upon the user's requirements.

B. Persuasive Cued Click Points (PCCP)

Using a skewed password distribution the attackers can guess the password in the previous graphical password schemes. Without the system guidance most of the users clicks on the hotspot in each image. In this method the system influence the user to select more random clicks, and also maintains the user memorability. In this scheme when the image is displayed the randomly selected block called the view port only clearly seen out. All the other parts of the image are shaded, so that the user can click only inside the view port. This is how the PCCP influence the user to select the position of the click point. The view ports are selected by the system randomly for each image to create a graphical password. It will be very hard for the attackers to guess the click point in all the images.

The users are allowed to click anywhere in the view port. There is an option for changing the viewport position also. This option is called the Shuffle. There is a limit on the number of times the shuffle option to be used.

While users may shuffle as often as desired, this significantly slows password creation. The viewport and shuffle button appear only during password creation. During later password entry, the images are displayed normally, without shading or the viewport, and users may click anywhere on the images.

Like PassPoints and CCP, login click-points must be within the defined tolerance squares of the original points. The theoretical password space for a password system is the total number of unique passwords that could be generated according to the system specifications.

Ideally, a larger theoretical password space lowers the likelihood that any particular guess is correct for a given password. Whereas text passwords have very skewed distributions resulting in an effective password space much smaller than the theoretical space, PCCP is specifically designed to significantly reduce such skews. The recall studies of the PCCP approach proved that remembrance of the graphical password is much better than the text-based passwords.

C. PCCP with Dynamic User Blocks

In PCCP approach the image of size 451x331 pixels is segmented in to approximately 400 blocks of size 19x19 pixels. This block is called the tolerance block or the threshold range. Since the threshold area is fixed in PCCP method, the security level provided by it is rigid and concrete in nature.

There may be some situations where the security levels need to be decreased. In those situations this PCCP method will not be feasible. To address these requirements, a new system is proposed, where the user can decide how strong the security of the system should be.

The tolerance area or the threshold area determines the level of security of the target system. For each click point, it is enough for the user to click in the threshold area of that click point during login. If the threshold area is larger, then the security level is smaller and vice versa.

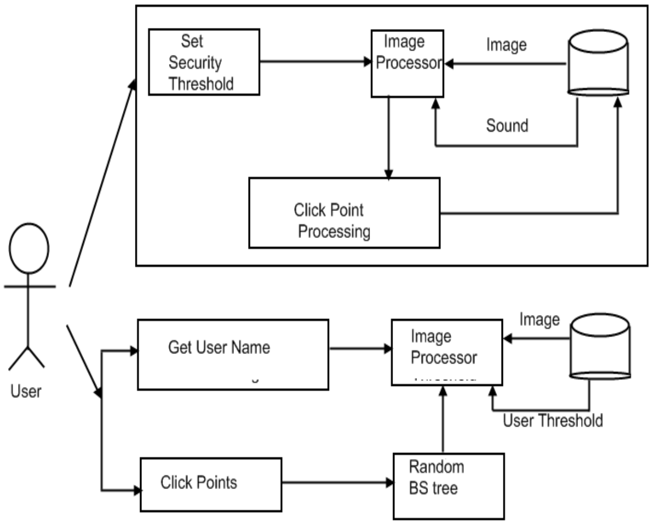
- **Password Registration**

In this approach, the user provides the threshold range say n (in pixels), where 18<n<101. This user defined threshold value is saved for future login. The view port remains the same as that of the PCCP method. But the threshold area is made variable in this proposal. For each threshold area the system assigns a sound tone. Now, the image is ready to be displayed. When the image is displayed, only the view port portion of the image is visible which is random. Thus the system influences the user to select the click points to avoid the attacker guessing of the hot spots. When the user clicks on the view port, the assigned sound tone is played. The click points and the relevant sound tones are stored for future usage.

- **User Login**

To login to the system the user enters the name first. Then the images stored are displayed without the viewport separation.

Now the user has to click on the correct threshold area. This can be checked by hearing the sound tone. Once the user get practiced with click points and sound tones, then, if the user by mistake clicks on a different threshold area, a different sound tone will be heard. With this difference the user can understand that he has clicked in a wrong position.



be used.

This can be useful only to the genuine user not to the attacker. Because the sound tones are repeated for other threshold areas also, the attacker does not know which block gives a particular sound.

3.3 Advantages

- More efficient
- Lower energy consumption
- Less communication overhead
- Time synchronization is not necessary
- No need of holding multiple passwords for different services

IV EXPERIMENT AND RESULT

The proposed model presents a unified definition of formally specifying soundness and credential privacy for authenticated key exchange single sign-on. Due to its high efficiency the scheme is suitable for mobile device users in distributed environment.

V. CONCLUSION

In Single Sign-On (SSO) scheme, we demonstrated two effective impersonation attacks. The first attack shows that their scheme cannot protect the privacy of a user's credential, and thus, a malicious service provider can impersonate a legal user in order to enjoy the resources and services from other service providers. The second attack violates the soundness of authentication by giving an outside attacker without credential the chance to impersonate even a non-existent user and then freely access resources and services provided by service providers. By employing an efficient verifiable encryption of RSA signatures, we proposed an improved scheme to achieve soundness and credential privacy and construct efficient and provably secure Single Sign-On schemes. To improvise the security and reach a higher level of security 2D password were introduced based on click point on an image.

The goal of a good authentication system is to provide a maximized of effective and secure password space. Here in this system the click point on the image have the scope of the view port area and since the view port cannot be exploited, the password created will be robust. Since shuffling of the view port increases the time for registration of new users, it is limited. The graphical click point passwords are more random and strong, so that no hacker can guess it, but easy to remember. The security strength is decided by the user himself, depending upon the requirement. The audio sound accompanied with every click helps the genuine user to identify the wrong clicks. The attacker does not know the difference between right and wrong clicks with the sound. It gives an idea of having an effective authentication system, which provides strong and easily remembered graphical passwords with dynamic security level.

VI. REFERENCES

[1] Guilin Wang, Jiangshan Yu, and Qi Xie, "Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks", IEEE Transactions On Industrial Informatics, Vol. 9, No. 1, February 2013.

[2] D. AnuRadha, "A Persuasive Cued Click-point based Authentication Mechanism with Dynamic User Blocks " , IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013.

[3] Jiangshan Yu, Guilin Wang, and Yi Mu, "Provably Secure Single Sign-on Scheme in Distributed Systems and Networks", IEEE Transactions On Industrial Informatics, Vol. 7, No. 1, March 2012.

[4] Cui Hui, Cao Tianjie, "A New Secure Anonymous Protocol for Distributed Computer Networks" , Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops(ISECS '10) Guangzhou, P. R. China, 29-31,July 2010, pp. 197-201.

[5] Yi-Pin Liao, Shuenn-Shyang Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment" , Computer Standards & Interfaces 31 (2009) 24–29.

[6] Chien-Lung Hsu and Yu-Hao Chuang, "A Robust User Authentication Protocol with Anonymity,Deniability, Key Agreement and Efficiency", Appl. Math. Inf. Sci. 7, No. 1, 127-132 (2013).

[7] Vishal Kolhe, VipulGunjal, SayaliKalasakar, PranjalRathod, "Secure Authentication with 3D

Password", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013.

[8] A. C. Weaver and M. W. Condtry, "Distributing internet services to the network's edge," IEEE Trans. Ind. Electron. , vol. 50, no. 3, pp. 404–411, Jun. 2003.

[9] L. Barolli and F. Xhafa, "JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing," IEEE Trans. Ind. Electron. , vol. 58, no. 6, pp. 2163–2172, Oct. 2010.

[10] L. Lamport, "Password authentication with in secure communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, Nov. 2001.

[11] W. B. Lee and C. C. Chang, "User identification and key distribution maintaining anonymity for distributed computer networks," Comput. Syst. Sci. Eng. , vol. 15, no. 4, pp. 113–116, 2000.

[12] W. Juang, S. Chen, and H. Liaw, "Robust and efficient password authenticated key agreement using smart cards," IEEE Trans. Ind. Electron. , vol. 15, no. 6, pp. 2551–2556, Jun. 2008.

[13] Y. Jiang, C. Lin, M. Shi, and X. Shen, "A self-encryption authentication protocol for teleconference services," Int. J. Security Netw. , vol. 1, nos. 3–4, pp. 198–205, 2006.

[14] J. Teo, C. Tan, and J. Ng, "Low-power authenticated group key agreement for heterogeneous wireless networks," Int. J. Security Netw. , vol. 1, nos. 3–4, pp. 226–236, 2006.

[15] C. Tartary and H. Wang, "Efficient multicast stream authentication for the fully adversarial network model," Int. J. Security Netw. , vol. 2, nos 3–4, pp. 175–191, 2007.

[16] M. Asadpour, B. Sattarzadeh, and A. Movaghar, "Anonymous authentication protocol for GSM networks," Int. J. Security Netw. , vol. 3, no. 1, pp. 54–62, 2008.

[17] S. Huang and S. Shieh, "Authentication and secret search mechanisms for RFID-aware wireless sensor networks," Int. J. Security Netw. , vol. 5, no. 1, pp. 15–25, 2010.

[18] M. Yang, "Lightweight authentication protocol for mobile RFID networks," Int. J. Security Netw. , vol. 5, no. 1, pp. 53–62, 2010.

[19] S. Chiasson, E. Stobert, A. Forget, R. Biddle,andP. vanOorschot," Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism", IEEE Dependable And Secure Computing, March/Arril 2012.

[20] S. Chiasson, R. Biddle, and P. van Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," Proc. ACM Symp. Usable Privacy and Security (SOUPS), July 2007.

[21] E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2010.

[22] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int'l J. Information Security, vol. 8, no. 6, pp. 387- 398, 2009.

[23] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds. , ch. 7, pp. 129-142, O'Reilly Media, 2005.

[24] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.

[25] L. Jones, A. Anton, and J. Earp, "Towards Understanding User Perceptions of Authentication Technologies," Proc. ACM Workshop Privacy in Electronic Soc., 2007.