Security in Graphical Authentication

Robert G. Rittenhouse[1], Junaid Ahsenali Chaudry[2] and Malrey Lee[3]

[1]*Keimyung Adams College, Keimyung University, Daegu, Republic of Korea*
[2]*Department of Computer Science and Engineering, Qatar University, Doha, Qatar*
[3]*Center for Advanced Image and Information Technology,*
School of Electronics & Information Engineering,
Chonbuk National University, JeonJu, 561-756, Republic of Korea
rrittenhouse@acm.org, junaid@qu.edu.qa
mrlee@chonbuk.ac.kr (Corresponding Author)

Abstract

Graphical Authentication Systems are a potential replacement or supplement for conventional authentication systems. Several studies have suggested graphical authentication may offer greater resistance to guessing and capture attacks but there are other attacks against graphical authentication including social engineering, brute force attacks, shoulder surfing, intercepted communication and spyware. In this paper we give a brief description and classification of different graphical password schemes followed by information about vulnerabilities in the various schemes and recommendations for future development.

Keywords*: graphical user authentication, graphical password*

1. Introduction

Authentication is the primary gatekeeper for computer systems. It both verifies authorized users of a system and distinguishes between different users. Halting and detecting intruders is only possible with a strong authentication mechanism and efficient access control. However, users dislike inconvenient authorization methods and may compromise them to make their lives easier.

The traditional and most common authentication method employs usernames and passwords composed of alphanumeric text. This method has proven to be insecure in practice [1]. For example, users may choose easily guessed passwords or, if a password is hard to guess, users may find it too difficult to remember leading to increased support issues, users writing down their passwords where they can be easily found [2] or users using the same password for multiple sites. The human factor is the weakest link in security [3] and authentication is one of the critical points where humans play an active role in security. Therefore we need substitutes or supplements for traditional authentication methods to have more secure and reliable authentication. Recently several new methods for authentication such as token-based authentication, biometric-based and graphical authentication have been developed [1]. All of these can be used together with conventional usernames and passwords.

The most commonly used approaches to authentication are knowledge-based techniques which include text and picture-based passwords [3]. Since it is easier for humans to remember pictures than text, graphical authentication schemes have been proposed as an alternative to text-based schemes [2]. With graphical authentication there is no need to remember long sequences of characters. Instead, a user can pass the authentication step by recognizing or recreating the graphical password. When the number of pictures is large enough graphical authentication may be superior to text-based methods [1].

2. Previous Research on Graphical Authentication

Authentication methods generally take three forms [4]:

1. Something you know, a shared secret, such as a password or the answer to a security question.
2. Something you have such as a one-time password generator or id card
3. Something you are, as represented by a fingerprint or iris scan.

Graphical Authentication, sometimes referred to as Graphical Passwords, is a new authentication method proposed and developed as an alternative to current methods. The motivation for graphical authentication is that people remember images better than text [5], [6]. Previous research has also found photos easier to recognize than random pictures [1]. Graphical passwords are claimed to make remembering passwords easier thus allowing more secure passwords to be produced and reducing the temptation for users to create unsafe passwords [7].

Renaud and Angeli have classified graphical authentication schemes into three categories [5]:

- Drawmetric schemes require the user to (re)create a secret drawing or pattern. Patternlock [8] in Android Phone authentication and Picture Password [9] in Microsoft Windows 8 are current examples of drawmetric schemes. More can be found in Table 1below.
- Searchmetric, also termed Cognometric, requires a user to select a known (usually pre-selected) image from a set of distractors. These are listed in Table 2.
- Locimetric systems, sometimes referred to as cued-recall based systems [10, 11], require identifying a series of positions within an image. These are listed in Table 3.

Table 1. Drawmetric Schemes

Scheme	Scheme
Syukri *et al.* [12]	Haptic Password [13]
Draw-a-Secret (DAS) [7]	Background DAS [14]
Passdoodle [15], [16]	YAGP [17]
Grid Selection [18]	PassShape [19]
Pass-Go [20]	GrIDSure [21]
Patternlock [8]	Picture Password [9]

A fourth category, the CAPTCHA, is not based on recognition or re-creation of pre-selected images but instead relies on human (as opposed to computer) capabilities to recognize obfuscated text presented as an image. CAPTCHAs are generally used to limit attacks by bots [45, 46]. CAPTCHA has become a standard security mechanism for addressing undesired or malicious internet bot programs [47]. CAPTCHA continues to be improved in response to advanced attacks [31, 46–48].

Table 2. Searchmetric Schemes

Scheme	Scheme
Déjà Vu [22]	Convex Hull [23]
PassFace [24], [25]	Cognitive Authentication [26]
Triangle Scheme [27]	ColorLogin [28]
Moveable Frame [27]	Jetafida [29]
Intersection Scheme [27]	GUABRR [30]
Picture Password [9]	Wang *et al.* Scheme [31]
Takada and Koike [32]	ImagePass [33]
Man *et al.* Scheme [34]	Dynamic Block-style [35]
Story Scheme [36]	

Table 3. Locimetric Schemes

Scheme	Scheme
Blonder [37]	CCP [38]
Jimmy Scheme [18]	PCCP [39]
Inkblot Authentication [40]	Passlogix [41]
Passpoints [42]	Viskey SFR [43]
Suo's Scheme [44]	

Hybrid schemes [49] combine two or more schemes. Hybrid authentication can involve two or more layers of authentication. Examples include recall-based combined with recognition-based schemes such as text-based passwords combined with graphical passwords. For example, the TwoStep Scheme developed by Oorschot, *et al.*, [50] combines both a text-based password and recognition-based graphical password. Hybrid Schemes are listed in Table 4 below.

Table 4. Hybrid Schemes

Scheme	Scheme
Maple, *et al.*, [46]	TwoStep [10]
S3PAS [47]	Ayannuga [9]

3. Security Analysis

No single mechanism or scheme can completely stop threats from attacks on computer systems. Even though graphical password schemes promise to provide better security (*e.g.* larger password space) than text-based passwords, they still face potential attacks. Possible attacks on graphical password schemes include shoulder surfing, brute force attacks, dictionary attacks, guessing attacks, spyware and social engineering attacks. We discuss these attacks and schemes designed to resist them below.

3.1. Shoulder Surfing

Shoulder surfing refers to looking over someone's shoulder, possibly using binoculars or close-circuit television, in order to obtain information such as password, PIN and other sensitive information. It is effective if the attacker can observe what the user keys in, clicks or touches [51, 52]. Graphical authentication is generally more vulnerable to shoulder surfing attacks than text-based passwords [53]. For this reason, only a few graphical authentication methods are designed to resist shoulder surfing attack. None of the searchmetric or locimetric schemes are considered resistant to shoulder surfing. Previous research has found that the use

of mouse clicks, touch screens or stylus pens is vulnerable to shoulder surfing attacks [53]. Jebriel and Poet conducted a study on the usage of mouse clicks and keyboards and found that keyboard based systems are more secure than using a mouse [54].

3.2. Brute Force Attacks

Brute force attacks, where the attacker tries to guess the correct password, are the simplest attack form for an authentication scheme. To defend against brute force attacks the system should have a sufficiently large password space to make it impractical. English text-based passwords have a password space of 94^n where n is the length of the password, and 94 is the number of printable characters excluding spaces. Some graphical authentication schemes have larger password spaces than text-based passwords [42]. Having a large password space also can be achieved by increasing the numbers of pictures in the library. In practice however, most recognition-based schemes have smaller password spaces than recall-based schemes [2].

In recall-based schemes brute force attacks require programs that generate mouse motion to emulate humans [48]. It is more difficult to copy mouse motion than to intercept keyboard input. Hu et al. claim that graphical passwords are more resistant to brute force attack than text-based passwords [2].

Brute force attacks have two subtypes:

Dictionary Attacks. Dictionary attacks represent another possible threat to graphical authentication systems. A dictionary attack is a type of brute force attack where the attacker uses a dictionary of common text or graphical passwords. In the text-based password, dictionary attack creates a dictionary of memorable words such as birthdates, favorite foods, pet names, or person names as potential passwords.

To attack click based graphical authentication, the attacker creates a program that can spot the popular click points on the image [55]. When a dictionary has been created, the attacker can use a program to crack a user login page by trying passwords from the dictionary.

Guessing Attacks. In a guessing attack, the attacker tries possible passwords related to the user. For example, in a text-based password, the password could be the birthdate, English name, phone number, identity card number etc. These are very weak passwords that are easy for the attacker to guess. Among graphical password schemes the DAS scheme might create predictable passwords [56].

3.3. Spyware

Spyware is another possible attack mechanism for graphical passwords. There are several types of spyware including keyloggers, hijackers and spybots [57–59]. Spyware collects information entered by the user. With graphical passwords, it is more difficult to conduct spyware based attacks because it is harder to copy mouse motions exactly. Combinations of pass images and CAPTCHAs may be especially resistant to spyware [31].

4. Security Features of Graphical Passwords

Different graphical password schemes have different techniques to reduce the effectiveness of known attacks. For instance the matrix method [54] or random characters [30] require the user to enter the passcode into the given field. To build a good system, a balance of high security and usability must be achieved.

It is considered good practice to have security features in authentication to favor better security over usability. However, building a balance between usability and security can be difficult. It might be a particular graphical password technique has higher usability but less

security or higher security with low usability. For example increasing the picture library would provide a larger password space, but leads to longer login time due to crowdedness during authentication.

Combining several security features should increase the security level. For instance, implementing decoys, randomly assigned, and random characters could make it harder for the observer to obtain login session during shoulder surfing activity. Most graphical password schemes have decoys and randomly assigned features to mitigate known attacks such shoulder surfing. In addition the location of the images can be randomized and not the same for every authentication phase.

Limited login attempts block user access to the login page after several unsuccessful login attempts. This security feature can be found in the Jetafida scheme [60] and could be easily added to others. It is not unusual for attackers to try to guess any combination of username and password in order to get an access to the system.

Another security feature is generating random passwords as in one-time password techniques. Several graphical password schemes have this kind of security feature [33, 34], [61] and it is common for CAPTCHAs. This feature requires the user to enter the random characters generated that corresponds to pass-images. In schemes using this feature it is hard for shoulder surfers to obtain the pass-image because of the random characters generated by the system.

Table 5, below, shows the security features of the various recognition-based graphical password schemes.

Table 5. Possible Attacks on Recognition-based Graphical Passwords

Graphical Password Scheme	Attack						Security features					
	Brute Force	Spyware	Guessing	Shoulder Surfing	Dictionary Attack	Social Engineering	Decoys	Randomly	Large Password	Limited Login Try	Hash Function	Random Characters
Déjà Vu [22]	N	Y	N	N	Y	N	/	/				
Triangle [27]	N	X	N	Y	Y	Y	/	/	/			
Moveable Frame [27]	N	Y	X	Y	N	X	/	/	/			
Intersection [27]	N	X	N	Y	Y	X	/	/	/			
Picture Password [9]	N	N	X	N	X	X	/				/	
Man et al. [34]	X	X	X	Y	X	X	/	/	/			
Takada and Koike [32]	X	X	X	N	X	X	/	/	/			
Story [36]	N	X	N	N	X	X	/	/				
PassfacesTM [24]	X	X	N	N	X	X	/	/				
Weinshall [26]	X	Y	X	N	Y	Y	/	/				
ColorLogin [28]	X	Y	X	Y	X	X	/	/				
GUABRR [30]	Y	Y	Y	Y	Y	X	/	/				/
Jetafida [29]	X	X	N	N	X	X	/			/		
ImagePass [33]	X	Y	Y	X	X	X	/	/				/
Wang et al. [31]	X	Y	X	X	X	X	/	/	/			/
TwoStep [50]	Y	X	X	X	X	X	/	/				
Dynamic Block-style[35]	Y	X	X	Y	X	X	/	/	/	/		

Y: Resistant N: Non Resistant X: Not Researched /:Yes

5. Conclusion and Future Work

Graphical user authentication promises increased security by allowing more complex passwords to be easily remembered by users. In addition, graphical passwords can be made resistant to shoulder surfing and even spybots and similar compromises of user systems.

There are several security requirements for graphical password suggested by previous research [62]. These criteria, combined with the use of hybrid authentication, can provide a secure authentication method.

Achieving high security in an authentication system can be aided by including several security features that in graphical user authentication. The proposed graphical password should have all the following features:

- Decoys or distractors
- Randomly Assigned
- Large Password Space
- Random Characters
- Uniqueness

References

[1] X. Suo, Y. Zhu and G. S. Owen, "Graphical Passwords: A Survey", in 21st Annual Computer Security Applications Conference (ACSAC'05), **(2005)**, pp. 107–198.
[2] W. Hu, X. Wu and G. Wei, "The Security Analysis of Graphical Passwords", in 2010 International Conference on Communications and Intelligence Information Security, **(2010)**, pp. 200–203.
[3] F. A. Qazi, "A Survey of Biometric Authentication Systems", in Proceedings of the International Conference on Security and Management (SAM 04), **(2004)**, pp. 61–67.
[4] C. W. Beardsley, "Is your computer insecure?", IEEE Spectrum, vol. 9, no. 1, **(1972)** January, pp. 67–78.
[5] A. De Angeli, L. Coventry, G. Johnson and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems", International Journal of Human-Computer Studies, vol. 63, no. 1–2, **(2005)** July, pp. 128–152.
[6] F. Monrose and M. K. Reiter, "Graphical passwords", in Security and Usability, L. F. Cranor and S. Garfinkel, Eds. O'Reilly, **(2005)**, pp. 147–164.
[7] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, **(1999)**, pp. 1–14.
[8] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev and C. Glezer, "Google Android: A Comprehensive Security Assessment", IEEE Security & Privacy Magazine, vol. 8, no. 2, **(2010)** March, pp. 35–44.
[9] W. Jansen, S. Gavrila, V. Korolev, R. Ayers and R. Swanstrom, "Picture password: a visual login technique for mobile devices", US Department of Commerce, National Institute of Standards and Technology, NISTR 7030, **(2003)**.
[10] S. Wiedenbeck, J. Waters, J. -C. Birget, A. Brodskiy and N. Memon, "Authentication using graphical passwords", in Proceedings of the 2005 symposium on Usable privacy and security - SOUPS'05, **(2005)**, pp. 1–12.
[11] W. Z. Khan, M. Y. Aalsalem and Y. Xiang, "A Graphical Password Based System for Small Mobile Devices", International Journal of Computer Science, vol. 8, no. 2, **(2011)**, pp. 145–154.
[12] A. F. Syukri, E. Okamoto and M. Mambo, "A user identification system using signature written with mouse," in ACISP'98 Proceedings of the Third Australasian Conference on Information Security and Privacy, **(1998)**, pp. 403–414.
[13] M. Orozco, B. Malek, M. Eid and A. El Saddik, "Haptic-Based Sensible Graphical Password", in Proceedings of Virtual Concept, **(2006)**.
[14] P. Dunphy and J. Yan, "Do background images improve 'draw a secret' graphical passwords?", in Proceedings of the 14th ACM conference on Computer and communications security - CCS'07, **(2007)**, pp. 36.

[15] J. Goldberg, J. Hagman and V. Sazawal, "Doodling our way to better authentication", in CHI'02 extended abstracts on Human factors in computing systems - CHI '02, **(2002)**, pp. 868.
[16] C. Varenhorst, "Passdoodles: A lightweight authentication method", **(2004)**.
[17] H. Gao, X. Guo, X. Chen, L. Wang and X. Liu, "YAGP: Yet Another Graphical Password Strategy", in 2008 Annual Computer Security Applications Conference (ACSAC), **(2008)**, pp. 121–129.
[18] J. Thorpe and P. C. van Oorschot, "Graphical dictionaries and the memorable space of graphical passwords", in 13th USENIX Security Symposium, **(2004)**.
[19] R. Weiss and A. De Luca, "PassShapes", in Proceedings of the 5th Nordic conference on Human-computer interaction building bridges - NordiCHI'08, **(2008)**, pp. 383–392.
[20] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords", International journal of Network Security, vol. 7, no. 2, **(2008)**, pp. 273–292.
[21] Cryptocard, "GrIDsure-high security ID authentication technology", http://www.gridsure-security.co.uk/, **(2012)**.
[22] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication", in Proceedings of the 9th USENIX Security Symposium, **(2000)**.
[23] S. Wiedenbeck, J. Waters, L. Sobrado and J. -C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme", in Proceedings of the working conference on Advanced visual interfaces - AVI'06, **(2006)**, pp. 177–184.
[24] S. Brostoff and M. A. Sasse, "Are passfaces more usable than passwords? A field trial investigation", in People and Ccomputers XIV - Usability or else!., Y. Wærn, S. McDonald, and G. Cockton, Eds. London: Springer Netherlands, **(2000)**, pp. 405-424.
[25] Passfaces Corporation, "The Science Behind Passfaces", **(2012)**.
[26] P. Golle and D. Wagner, "Cryptanalysis of a Cognitive Authentication Scheme (Extended Abstract)", in 2007 IEEE Symposium on Security and Privacy (SP'07), **(2007)**, pp. 66–70.
[27] L. Sobrado and J.-C. Birget, "Graphical passwords", The Rutgers Scholar, vol. 4, **(2002)**.
[28] H. Gao, X. Liu, R. Dai, S. Wang and X. Chang, "Analysis and Evaluation of the ColorLogin Graphical Password Scheme", in 2009 Fifth International Conference on Image and Graphics, **(2009)**, pp. 722-727.
[29] A. M. Eljetlawi, "Study and develop a new graphical password system", Universiti Teknologi Malaysia, **(2008)**.
[30] A. H. Lashkari, A. Gani, L. G. Sabet and S. Farmand, "A new algorithm on Graphical User Authentication (GUA) based on multi-line grids", Scientific Research and Essays, vol. 5, no. 24, **(2010)**, pp. 3865–3875.
[31] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu and U. Aickelin, "Against Spyware Using CAPTCHA in Graphical Password Scheme", in 2010 24th IEEE International Conference on Advanced Information Networking and Applications, **(2010)**, pp. 760–767.
[32] T. Takada and H. Koike, "Awase-E: Image-based authentication for mobile phones using user's favorite images", in Human Computer Interaction with Mobile Devices and Services, L. Chittaro, Ed. Springer Berlin / Heidelberg, vol. 2795, **(2003)**, pp. 347–351.
[33] M. Mihajlov and B. Jerman-Blažič, "On designing usable and secure recognition-based graphical authentication mechanisms, "Interacting with Computers", vol. 23, no. 6, **(2011)**, pp. 582–593.
[34] S. Man, D. Hong and M. Matthews, "A shoulder-surfing resistant graphical password scheme-WIW," in Proceedings of International conference on security and management, **(2003)**, pp. 105–111.
[35] W. C. Seng, Y. K. Khuen and N. L. Shing, "Enhanced Graphical Password by using Dynamic Block-style Scheme", in 2011 International Conference on Information and Intelligent Computing IPCSIT, vol. 18, **(2011)**, pp. 139–145.
[36] D. Davis, F. Monrose and M. K. Reiter, "On user choice in graphical password schemes", in 13th USENIX Security Symposium, **(2004)**.
[37] G. E. Blonder, "Graphical password," U.S. Patent 55599611996.
[38] S. Chiasson, P. Van Oorschot and R. Biddle, "Graphical Password Authentication Using Cued Click Points", in Computer Security–ESORICS, , vol. 4734, **(2007)** September, pp. 359–374.
[39] S. Chiasson, A. Forget, R. Biddle and P. C. van Oorschot, "Influencing users towards better passwords: persuasive cued click-points", in Proceedings of the 22nd British HCI Group Annual Conference on HCI, **(2008)**, pp. 121–130.
[40] A. Stubblefield and D. R. Simon, "Inkblot Authentication", Microsoft Research, **(2004)**.
[41] Oracle, "Oracle and Passlogix," http://www.oracle.com/us/corporate/Acquisitions/passlogix/index.html, **(2010)**.
[42] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies, vol. 63, no. 1–2, **(2005)** July, pp. 102–127.

[43] SFR Software GMBH, "SFR Software: Windows Mobile - SFR Password, login solution with picture password," 2012. [Online]. Available: http://www.sfr-software.de/cms/XX/pocketpc/sfr-password/index.html. [Accessed: 05-Jun-2012].
[44] X. Suo, "A design and analysis of graphical password," Georgia State University, **(2010)**.
[45] S. W. Jung, "CAPTCHA-based DDoS Defense System of Call Centers against Zombie Smart-Phone," International Journal of Security and Its Applications, vol. 6, no. 3, **(2012)**, pp. 29–36.
[46] H. Gao and X. Liu, "A new graphical password scheme against spyware by using CAPTCHA", in Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS'09, **(2009)**, pp. 1.
[47] J. Yan and A. S. El Ahmad, "Usability of CAPTCHAs or usability issues in CAPTCHA design", in Proceedings of the 4th symposium on Usable privacy and security - SOUPS'08, **(2008)**, pp. 44.
[48] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first generation", Ottawa, **(2009)**.
[49] O. Ayannuga, Olanrewaju, F. Olusegun and A. T. Akinwale, "Evaluation of a usable Hybrid Authentication System", in International Journal of Computer Applications, vol. 17, no. 8, **(2011)**, pp. 27–31.
[50] P. C. Oorschot and T. Wan, "TwoStep: An Authentication Method Combining Text and Graphical Passwords", ETechnologies Innovation in an Open World, vol. 26, no. 3, **(2009)**, pp. 233–239.
[51] M. Kumar, T. Garfinkel, D. Boneh and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry", in Proceedings of the 3rd symposium on Usable privacy and security-SOUPS'07, **(2007)**, pp. 13.
[52] L. K. Seng, N. Ithnin and H. Mammi, "An Anti-Shoulder Surfing Mechanism and its Memorability Test", International Journal of Security and its Applications, vol. 6, no. 5, **(2012)**, pp. 87–95.
[53] F. Tari, A. A. Ozok and S. H. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords", in Proceedings of the second symposium on Usable privacy and security - SOUPS'06, **(2006)**, pp. 56.
[54] S. M. Jebriel and R. Poet, "Preventing shoulder-surfing when selecting pass-images in challenge set", in 2011 International Conference on Innovations in Information Technology, **(2011)**, pp. 437–442.
[55] F. Towhidi, A. A. Manaf, S. M. Daud and A. H. Lashkari, "The Knowledge Based Authentication Attacks", in World Congress in Computer Science, **(2011)**.
[56] D. Nali and J. Thorpe, "Analyzing User Choice in Graphical Passwords", Ottawa, **(2004)**.
[57]S. Saroiu, S. D. Gribble and H. M. Levy, "Measurement and analysis of spyware in a university environment," in Proceedings of the ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI), **(2004)**, pp. 141–153.
[58] W. Ames, "Understanding spyware: risk and response", IT Professional, vol. 6, no. 5, **(2004)** September, pp. 25–29.
[59] S. Shukla and F. F.-H. Nah, "Web browsing and spyware intrusion", Communications of the ACM, vol. 48, no. 8, **(2005)** August, pp. 85.
[60] A. M. Eljetlawi and N. Ithnin, "Graphical Password: Prototype Usability Survey", in 2008 International Conference on Advanced Computer Theory and Engineering, **(2008)**, pp. 351–355.
[61] A. H. Lashkari, S. Farmand, D. O. Bin Zakaria and D. R. Saleh, "Shoulder Surfing attack in graphical password authentication", International Journal of Computer Science and Information Security, vol. 6, no. 2, **(2009)** December, pp. 10.
[62] S. Farmand and O. Bin Zakaria, "Improving graphical password resistant to shoulder-surfing using 4-way recognition-based sequence reproduction (RBSR4)", in 2010 2nd IEEE International Conference on Information Management and Engineering, **(2010)**, pp. 644–650.

Authors

Robert G. Rittenhouse is an associate professor at Keimyung Adams College in Daegu Korea. He received his Ph.D. from the University of California at Irvine in 1987. His research interests include security, ubiquitous computing and social informatics.

Junaid Chaudhry is a researcher at Qatar University in Doha Qatar. He received his Ph.D. from Ajou University in South Korea in 2009. His research interests include security, ubiquitous computing and networking.

Malrey Lee received a Ph.D. in Computer Science from the University of Chung-Ang. She has been a Professor at the ChonBuk National University in Korea. She has over seventy publications in various areas of Computer Science, concentrating on Artificial Intelligence, Robotics, Medical Healthcare, ubiquitous computing and Software Engineering.