IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555
Vol. 2, No.4, August 2012

IKM-based Security Usability Enhancement Model

Saeed Yazdanpanah
Software engineering department
Islamic Azad University of Iran, Khorramabad Branch
Khorramabad, Iran

Saman Shojae Chaeikar
Software engineering department
Islamic Azad University of Iran, Khorramabad Branch
Khorramabad, Iran

***Abstract*— Today by growth of hardware and software technologies new developed products are delivering more facilities while their security configuration is becoming more and more complicated. Security configuration of network-based products is not comprehensible for every user and therefore degrades system usability dramatically. IKM is a cryptographic key management framework which empowers end-user systems to generate keys for preserving security while it also has potential of usability enhancement particularly for network-based products. This paper describes background of security usability, IKM key management framework, and proposes a new method for using IKM to deliver security and usability features for designed network-based systems. In last section delivered security and usability of proposed model is evaluated based on cryptographic key-strength analysis and usability questionnaire.**

Keywords- Security usability; cryptography; IKM-based security model; IKM-based usability model

I. INTRODUCTION

Analyzing security and usability are two approaches of studying security usability of a system. Security deals with the famous triangle of confidentiality, integrity, and availability while usability evaluates easiness of authentication and utilization of the system especially for novices.

Usability talks about how easy the processes of protection of security and performing tasks are and in fact it studies how easy is utilizing a system for its users. Psychological acceptance of developed systems is one of usability measurements introduced in 1975 [1]. Zurko and Simon defined users, administrators, and developers as three groups which benefit from usability of a system [2]. Later in another research [3] *system owners* introduced as main group which benefit from high level of usability for counted three groups.

Process of authentication has both aspects of security and usability. Because of advances in software and hardware technical process of authentication is becoming more and more complicated while goal of system developers always is to make it easier than before. Today 8 characters password constituted from alphabet, numbers, and special characters delivers only average level of security while in 1980 five characters alphabetical password was secure enough.

Passphrase is an authentication method introduced by Sigmund Porter [4] in 1982 which uses one sentence rather than one word for authentication. Sigmund believed that memorizing one meaningful sentence is easier than memorizing a meaningless word. Two years later in 1982 James Haskett offered pass-algorithm authentication. In his method users must learn an algorithm and answer the authentication questions based on the given algorithm.

Cognitive password [5], another authentication method, asks some questions which their answers are known only for legitimate user. Although some close people may know these answers but results of evaluation studies show fair performance of this scheme.

Pass-face technique [6] was proposed by Angela and Sacha in 2000. To perform authentication in four stages the user must choose correct faces among displayed network of faces. Later Déjà vu [7] changed faces with objects. Pass-point is another authentication technique, proposed by Susan Wiedenbeck [8] in 2005, that shows a photo to users and they must click on predefined points on it.

Key management, encryption, and authentication techniques are the main important factors of preserving security. Key management techniques like Master-key and encryption techniques like DES, 3DES and so on can guaranty secrecy of transmitted and stored data on networks. Passwords, passphrases, pass-faces, pass-points, or even biometrics are different techniques of recognizing legitimate users against illegitimate ones for granting access.

Pretty Good Privacy (PGP) which by Bruce Schneier [9] is known in the same level with army encryption techniques is available both as a ready product and as a standard to be utilized in developed or under development software to preserve its security. PGP also is used in projects like OpenPGP and GNUPG and because of its decentralized architecture it widely penetrated in the market [10]. PGP utilizes concept of network of trust which in it all members cooperate in evaluation of trustworthiness of other members instead of relying on centralized certificate of authority.

II. IKM'S WORKFLOW AND COMPONENTS

IKM consists of two components which are a server and an interpreter. Server's four main tasks are:

- Producing interpreter
- Distributing interpreter among nodes
- Monitoring nodes' security status (intelligent attack resistant feature)
- Issuing revocation call

Interpreter is light weight software that produces keys by means of embedded knowledge in it. Embedded knowledge in

This work is part of a research project titled "Enhancing e-learning and software security usability by using cryptographic techniques" which is sponsored by Islamic Azad University of Iran, Khorramabad branch.

interpreter are time and date (agreed calendar and time zone), twenty four embedded digits, bit-stream source address, interpretation method (or key extraction algorithm), an interpreter revocation code, and in some circumstances hardware specifications [11].

After that server produced the interpreter it will be ready to be distributed among end-users. Legitimate nodes will download the interpreter via a secure channel established by Diffie-Hellman. After downloading the interpreter it will start downloading the bit-stream from embedded address and unifies its date and time either with server or one of publicly available sources on the network. Because of involving unified time and date in key generation process all nodes will be able to produce identical time dependent keys at same time. Key will be produced when is needed and key production intervals could be every minute, hour, or day. Keys will expire automatically after defined period passes and thus no key revocation and storage is needed [11].

A. *Server*

First task of server is producing interpreter. After generating interpreter it will be distributed among those systems which are going to use interpreter to establish secure sessions. Hereafter server's responsibilities would be analyzing nodes' security status, making convenient decisions against attacks, managing new nodes, answering time synchronization requests, and issuing interpreter revocation call [12].

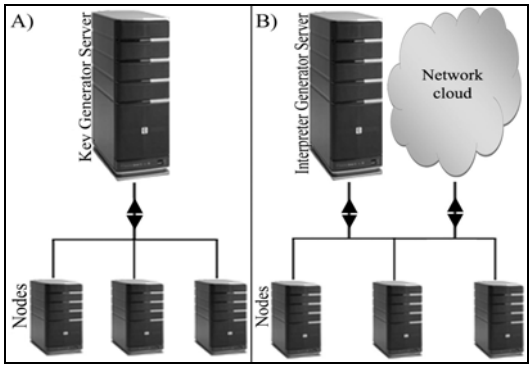

Figure 1. (A) Common key management practices main workflow (B) IKM main workflow.

In common practices main key management workflow is from server toward nodes, but in IKM only early flow is from server and afterward nodes will generate keys by using defined sources on network.

B. *Interpreter*

Interpreter is constituted from different components which are time and date (agreed calendar and time zone), twenty four digits, bit-stream source address, interpreting method (or key extraction algorithm), an interpreter revocation code, and in some circumstances hardware specifications. Main task of interpreter is producing time dependent keys. Reporting security status of node to server is another task of the interpreter.

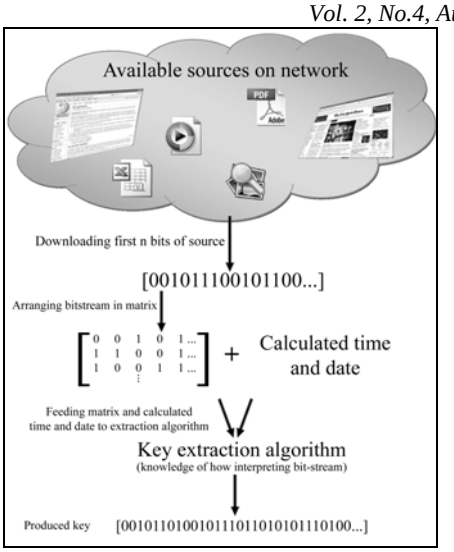

Figure 2. Process of key generation from downloading bit-stream to final generated key.

Time and date: the computers which are going to establish secure sessions might be spread around the world. Time and date are two of key generation involved factors. Therefore all computers should unify their time and date to be able to produce identical keys at the same time. Predefined calendar and time zone are two embedded items in interpreter that enable computers to unify themselves for key generation process. For example, they may agree on Gregory calendar and UTC time. In addition, local date and time of all computers might not be accurate. To solve this problem before going through key generation process computers must update accurate date and time by server or one of publicly online available sources [12].

Twenty four digits: to use unified date and time in key generation, it should be in full format to form twelve digits. Couple of these twelve digits constitutes a twenty four digits number that is needed to be fed into key extraction algorithm. Cracking these twenty four date and time digits is not hard and so to make impossible for attackers to find these numbers they will be added with the embedded twenty four digits. Result of adding constant embedded twenty four digits with twenty four time and date digits will be new twenty four digits that changes at the time of generating every new key [12].

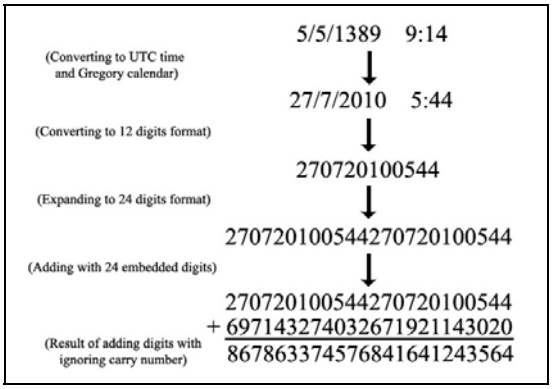

Figure 3. Process of calculating twenty four digits from date and time.

Bit-stream source: bit-stream source is one of preliminaries that help to unify key generation process. Bit-stream is first n bits of specific file on network. All interpreters will download first required n bits of defined file from embedded address to feed into key extraction algorithm. In light of having identical bit-stream, date and time, and key extraction algorithm, all computers will produce same fresh keys. Length of bit-stream is 512 bits and interpreter producer should be conscious about bit-stream source update intervals. If bit-stream source file is dedicated only for this purpose then its update intervals is completely under control and depend on decision of interpreter maker it might be constant or might replace at specific intervals. If bit-stream source is not constant after every update all nodes should download it again and all nodes should be aware about update intervals to resynchronize themselves.

Key extraction algorithm: the twenty four digits number is the hidden factor from attackers' eyes that guarantees IKM's security. Matrix method is process of key generation which in it major part of downloaded bits will be arranged into a matrix and will be surveyed according evenness or oddness of final twenty four digits. The survey starts from (0,0) item and continues regarding produced twenty four date and time digits. For even numbers key extraction algorithm picks up bits from matrix vertically and for odd numbers horizontally. This process continues until desired key length being produced and if twenty four digits ends before getting desired key length the process will continue again from the first digit. Matrix method picks up bits vertically or horizontally regarding twenty four digits and if one row or column ends before picking up all needed bits it will continue from beginning of next row or column respectively. Figure 4 visualizes matrix key extraction technique in smaller matrix size.

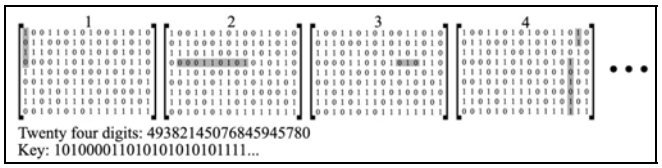

Figure 4. Matrix method key extraction technique.

Interpreter revocation code: Revocation code is secret code that is embedded in interpreter and when it receives from server means that the current interpreter version is expired because of compromising or periodical replacement for enhancing security.

Hardware specification: scope of deploying IKM is where nodes are trustable or well known for long term. In some circumstances, like ATM network, hardware specification of all computers is known for interpreter maker. Therefore to enhance security level, interpreter only will produce keys when current machine hardware specifications is identical with given specifications to avoid generating key when interpreter is compromised and is running on attacker's machine [11].

Key refreshment intervals: IKM introduces minutely, hourly, and daily key refreshment intervals which means that regarding the three intervals every minute, every hour, or every day a new key will be produced and deployed. For every new key, new twenty four digits will be calculated and along with bit-stream will be fed into key extraction algorithm to produce new time dependent key.

Joining and shutting down process of nodes: For first time joining, requester node should pass authentication process to become legitimate node for receiving interpreter. If a node was inactive for a period of time, before trying to joining sessions should send a test message to either server or one of nodes. If sent message has been replied, then current interpreter sill is valid and is not replaced or expired. But if no reply received then shows that current interpreter version is not valid anymore and the node for future sessions should go through process of authentication again.

If a node is going to leave sessions permanently, depend on decision of network security administrator either its interpreter should be removed or current interpreter should be expired to prevent compromising whole system. If node is trustable then revoking interpreter is not needed, but in normal cases a new version must be distributed instead of currently expired one. Always a new version of interpreter must be ready in hand of server for any emergency circumstance or periodical interpreter replacement to avoid delay in nodes' activities [11].

IKM security and performance: IKM falls in category of master key but has some changes in workflow which let it to deliver higher level of security and performance. One time interpreter distribution instead of many times key distribution, utilizing fresh keys, no necessity of key revocation, and reacting intelligently against attacks are main advantages of IKM against master key. Intelligent attack resiliency is important feature of IKM and depend on conducted attack it would be able to make proper decision to preserve security in desired level [13], [14].

In term of performance IKM imposes much less traffic on the network and server. Depend on chosen key lifetime imposed traffic on network would vary between 1/7 to 1/10344 of master key after 52 weeks [15].

III. Proposed Model for Using IKM in Security Usability

Since the proposed model is based on the IKM then nature of key generation is the same and only slight changes are made to tailor it to meet the requirements. In continue the necessary changes for providing authentication and confidentiality services are elaborated.

A. Target users

Best target user group of proposed model is when group identity of users is more important than personal identity. For example, particular batch of an e-learning system students or employees of a company in same level and with same responsibilities and needs are the groups which can benefit from it. However, if recognizing user's personal identity is important then combination of automated group authentication and a user identity code would satisfy the requirements.

B. Proposed changes in IKM structure

Changing bit-stream with hash output: IKM arranges downloaded bit-stream in a matrix to be surveyed in key generation process. Here bit-stream is replaced with hash value of group label. Group label is a brief description which explains about target users. The hash value of label supplies required bits of matrix.

C. Grouping

One of important provided features is possibility of grouping and establishing hierarchy among them.

Defining group identity by group-label: One of interpreter components is a label which indicates identity of group. To achieve a group key having group label and 24 digits are necessary. For instance, "Elementary Level English-course Students" could be used as label of particular group of students.

Establishing sessions between server and user groups: Since server must deliver service to various groups which each one may have many users, at the session establishment time it must at first recognizes that which group the user belongs to and then add the user's IP in IP-Group table.

When first packet receives from user to server, if sender's IP was not found in IP-Group table it would try to decipher received packet by current keys of all groups. When the proper key was found the server will add the user information into IP-Group table which stores which IP belongs to which user in which group. In continue of session server will use fresh key of the respective group to communicate the user.

Changing group: one of main advantages of this model is easiness of changing group membership. To join a group two parameters are needed. First parameter is group label which its hash value will be used in the matrix and second one is 24 digits which will be used in the key generation process.

Hierarchical access: If a user holds more than one group label and the 24 digits then would be able to join all respective groups at the same time. For example, a top level manager may need to have access to data and facilities of lower managerial levels or even all employees. To do so label and 24 digits of all groups must be added to the top manager interpreter to get access to all groups.

In this model to establish hierarchy among users only giving label and 24 digits of lower level users to higher ones would be enough and high level users can join and monitor lower level activities.

Recognizing individual identity of users: In two ways personal identity of a user can be recognized. First way is combination of token (interpreter) and user code. The server can recognize the user's group identity according the used encryption key and then in next step user's individual identity based on the entered user code. Presenting user code can be either automated or manual. If automated mode is chosen then user's identity will be stored within the interpreter and then automatically will be sent to server. In manual mode user must enter the user code to pass the identification process.

The second way, which is more user friendly, is using combination of "label hash value + 24 digits + user identity code" in process of key production. In this way the user's interpreter will send a particular session establishment message to server which is encrypted by user's current key.

Since session establishment message content is constant then server looks for the received packet among valid encrypted session establishment messages of all inactive users to find identity of the user. To accelerate this process server will generate encrypted message establishment request of all inactive users whenever encryption key changes. By comparing the received packet with encrypted session establishment messages of all inactive users, identity of the applicant user will be found and session will be established. For recognizing individual users, IP-Group table must be extended to "IP-Group-UserCode" table.

Despite second way has high processing overhead but has three important benefits. Firstly encryption, identification, and authentication of the user will be done fully automated. Secondly each user will use separate key which is ever changing and delivers very high level of secrecy. And finally third important advantage of delivering individual user recognition is possibility of putting a user in black list. In group authentication access will be granted or denied to all members while in this way each one of users can be managed individually.

D. Preserving stored data secrecy

By considering that generated keys are ever changing they cannot be used for stored data encryption. Encryption and decryption of online data transmission happens almost at the same time while encryption and decryption time of stored data is different.

To support stored data encryption and decryption time and date parameters should be removed from key generation factors. Therefore combination of hash of label and 24 digits will constitute key generation parameters.

IV. Evaluation of Proposed Model

Proposed security usability technique must be evaluated from both aspects of security and usability. In term of security mathematical computations can show how long encrypted data would be confidential depend on key length, and in term of usability evaluation of users through running a questionnaire survey can evaluate efficiency and acceptance of proposed model.

A. Security evaluation

As the proposed model follows IKM cryptosystem for key generation and IKM produces 128 bits and longer symmetric keys then security of encrypted information is guaranteed for more than the year of 2050. IKM key length is optional and has possibility of generating shorter and longer keys but IKM's default key length is 128 bits. Following table shows the key length and the period which each key length would be safe. Growth of software and hardware technologies and facilities

and also cost of running attack on particular key are the main factors which determine security lifetime margin of a key [16].

TABLE I. SECURITY LIFETIME OF SYMMETRIC KEYS [16]

Year	Key Length (bits)
2010	78
2015	82
2020	86
2025	89
2030	93
2040	101
2050	109

According Table I security lifetime margin of keys of proposed model would be far beyond the year 2050 and for majority of applications is safe enough. If longer safe lifetime is needed then the key length can be expanded to achieve desired security margin.

B. Usability evaluation

To evaluate usability of proposed technique 100 users were chosen randomly to participate in evaluation of IKM based security usability enhancement technique. Minimum age of chosen candidates defined as 12 and there was no maximum age limit. Attendees were classified in 3 age groups as 12 to 20(group A), 20 to 40 (group B), and above 40 (group C). Again based on their technical experience attendees were grouped as beginner, intermediate, and professional users. Those who could not install OS, common software, and configure security configurations were placed in beginner group. Intermediate group was constituted from users were able to install OS and common software but they had no experience of performing security configuration. Last group members, professionals, were able to fulfill all tasks.

Attendees were taught how to use IKM based provided facilities and were given the equivalent manual and instruction to achieve same level of security manually. Then they were asked to fill in the questionnaire and give their possible recommendations. Following tables reflect gathered results.

TABLE II. USABILITY EVALUATION QUESTIONAIRE

Question	Answer	
1. Please specify your age:		
2. Can you install Operating System (like Windows, Android, or Linux)?	Yes	No
3. Can you install common software (like antivirus or Microsoft office package)?	Yes	No
4. Can you install or configure firewall or other complicated security products?	Yes	No
5. How many years do you have computer experience?		
6. Do you prefer to use a token for authentication or combination of username/password?	Token	User/ Pass
7. Do you prefer to configure security of your sessions manually or automatically?	Automatic	Manual
8. Do you prefer to use automatic IKM-based method or manual method to protect your sessions' security?	IKM-based method	Manual
If you have any recommendation or explanation for questions 6,7, and 8 please write here:		

TABLE III. PREFERENCE PERCENTAGE OF TOKEN-BASED AUTHENTICATION AND USERNAME/PASSWORD

	Token	Username/Password
Beginner	80.77%	19.23%
Intermediate	23.07%	76.93%
Professional	0%	100%

TABLE IV. PREFERENCE PERCENTAGE BETWEEN AUTOMATIC AND MANUAL SECURITY CONFIGURATION

	Automatic	Manual
Beginner	100%	0%
Intermediate	86.15%	13.85%
Professional	44.45%	55.55%

TABLE V. PREFERENCE PERCENTAGE OF UTILIZING IKM-BASED SECURITY USABILITY METHOD AND MANUAL METHOD

	Automatic	Manual
Beginner	92.30%	7.70%
Intermediate	81.54%	18.46%
Professional	22.22%	77.78%

TABLE VI. EXPERIENCE AVERAGE OF MANUAL AND IKM-BASED AUTOMATED METHOD USERS (YEARS)

	Group	Automatic	IKM-based method
Beginner	4.46	7	4.29
Intermediate	5.23	8.2	4.49
Professional	8.1	9.14	4.5

TABLE VII. EXPERIENCE AVERAGE OF TOKEN AND USERNAME/PASSWORD USERS (YEARS)

	Token	Username/Password
Beginner	3.95	6.40
Intermediate	3.75	5.71
Professional	-	8.1

TABLE VIII. AVERAGE EXPERIENCE OF MANUAL SECURITY CONFIGURATION AND IKM-BASED AUTOMATED SECURITY CONFIGURATION USERS

	Automated (IKM-based)	Manual
Beginner	4.46	-
Intermediate	4.75	8.2
Professional	6.75	9.2

TABLE IX. AUTHENTICATION METHOD PREFERENCE TABLE BASED ON GROUPS' AGE CLASSIFICATION

Users' age classifications	Token	Username/Password
Beginners group A	80%	20%
Beginners group B	83.34%	16.6%
Beginners group C	80%	20%
Intermediate group A	26.31%	73.69%
Intermediate group B	12.9%	87.1%
Intermediate group C	46.7%	53.3%
Professional group A	0%	100%
Professional group B	0%	100%
Professional group C	0%	100%

TABLE X. SECURITY CONFIGURATION METHOD PREFERENCE TABLE OF ALL GROUPS BASED ON AGE CLASSIFICATION

Users' age classifications	Automated (IKM-based)	Manual
Beginners group A	100%	0%
Beginners group B	100%	0%
Beginners group C	100%	0%
Intermediate group A	84.21%	15.79%
Intermediate group B	87.1%	12.9%
Intermediate group C	86.7%	13.3%
Professional group A	66.7%	33.3%
Professional group B	25%	75%
Professional group C	50%	50%

TABLE XI. SECURITY AND USABILITY METHOD PREFERENCE TABLE OF ALL GROUPS BASED ON AGE CLASSIFICATION

Users' age classifications	Automated (IKM-based)	Manual
Beginners group A	100%	0%
Beginners group B	100%	0%
Beginners group C	86.7%	13.3%
Intermediate group A	84.21%	15.79%
Intermediate group B	77.42%	22.58%
Intermediate group C	86.7%	13.3%
Professional group A	33.3%	66.7%
Professional group B	0%	100%
Professional group C	50%	50%

C. Analysis of results

Gathered results show that, on average, users with less experience are more tend to employ IKM-based proposed technique. Outstanding majority of beginners preferred to use token instead of using username/password while majority of intermediate level users and all of professionals preferred memorizing username/password instead of carrying given token. Main reason of beginners for preferring token explained as lack of self confidence and trusting tangible facilities.

All the beginners supported automatic security configurations rather than manual configuration. Considerable majority of intermediates chose to use automatic technique and for professionals results showed almost near half of them chose automatic method. Beginner and intermediate level users expressed reason of their choice as lack of security knowledge and strangeness of technical protocols.

Between using token and username/password majority of users preferred to memorize username/password instead of carrying a token. Between automatic and manual security configuration majority of users preferred to trust automated process instead of relying on their knowledge. But when users were asked to chose either IKM-based method or manual method outstanding majority chose to employ IKM-based model and only some of professional users preferred manual model.

When users were grouped based on their chosen method results showed that in all cases more experienced users chose to work in traditional method while those who trusted to automated process were less experienced.

Statistical analysis of collected questionnaires proofs that proposed method could enhance security and usability of systems when its end users have not deep knowledge of computer. Employing the IKM-based method will enhance satisfaction level and security of both users and system owners.

V. CONCLUSION

Field of security usability is science of simplifying utilization of complicated developed products particularly for novices. IKM is a cryptographic key management framework, under category of Master-key, which produces time dependent keys in user side. This paper proposes a new security usability enhancement model which uses IKM to deliver encryption, identification, and authentication services automatically. In term of secrecy evaluation results show that secrecy of encrypted data is guaranteed beyond the year of 2050. Usability of the proposed model evaluated by means of a questionnaire and results showed that beginners and intermediate level users are mostly willing to use proposed model for protection of online data transmission, user identification, and authentication while expert users prefer current practices. Also less experienced users were more interested to use proposed model than experienced ones.

REFERENCES

[1] J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," *IEEE* 1975.

[2] M. E. Zurko and R. T. Simon, "User-Centered Security," in *Proc.* New Security Paradigms Workshop, California, 1997.

[3] M. A. Sasse, S. Brostoff and D. Weirich, "Transforming the 'weakest link': a human-computer interaction approach to usable and effective security," *BT Technical Journal*, 19 , pp 122-131, 2001.

[4] S.N.A. Porter, "A Password Extension for Improved Human Factors," *Computers & Security*, vol. 1, no. 1, pp. 54–56, 1982.

[5] M. Zviran and W.J. Haga, "Cognitive Passwords: The Key to Easy Access Control," *Computers & Security*, vol. 9, no. 8, pp. 723–736, 1990.

[6] S. Brostoff and A.M. Sasse, "Are Passfaces More Usable than Passwords? A Field Trial Investigation," in *Proc. Human-Computer Interactions* (CHI 00), 2000, pp. 405–424.

[7] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in *Proc. 9th Usenix Secu-rity Symp*., 2000, pp. 45–58.

[8] S. Wiedenback, "Authentication using Graphical Passwords: Effects of Tolerance and Image Choice," in *Proc. ACM Symp. Usable Privacy and Security*, New York, 2005, pp. 1–12.

[9] B. Schneier, *Applied Cryptography*, 2nd ed., Wiley, 1996.

[10] S.L. Garfinkel, "Design Principles and Patterns for Computer Systems that Are Simultaneously Secure and Usable," Ph.D dissertation, Dep. Electrical Engineering And Computer Science, Mass. Inst. of Technology, 2005.

[11] S. S. Chaeikar, H. S. Moghaddam and H. R. Zeidanloo, "Node Based Interpretative Key Management Framework" in *Proc. The 2010 Congress in Computer science, Computer engineering, and Applied Computing (The 2010 International Conference on Security and Management SAM'10), WORLDCOMP'2010*. Las Vegas, 2010, pp. 204-210.

[12] S. S. Chaeikar, S. A. Razak, S. Honarbakhsh, H. Rouhani Zeidanloo, M. Zamani and F. Jaryani, "Interpretative Key Management (IKM), A Novel Framework," presented at the IEEE Second International Conference on Computer Research and Development ICCRD 2010, Kuala Lumpur, May 7-10, 2010.

[13] S. Yazdanpanah, S. S. Chaeikar, M. Zamani and R. Kourdi, "Security features comparison of master key and IKM cryptographic key management for researchers and developers," presented at the IEEE International Conference on Software Technology and Engineering, 3rd (ICSTE 2011), Kuala Lumpur, August 12-14, 2011.

[14] S. S. Chaeikar and A. B. A. Manaf, "Security and performance analysis between IKM and master key," presented at Postgraduate annual Research on Informatics Seminar (PARIS 2012), Kuala Lumpur, January 11, 2012.

[15] S. S. Chaeikar, A. B. A. Manaf and M. Zamani, "Comparative analysis of Master-key and Interpretative Key Management (IKM) frameworks" in *Cryptography and security in computing*, Jaydip Sen, Ed. Croatia: Intech, 2012, pp. 203-218.

[16] A. K. Lenstra and E. R. Verheul, "Selecting cryptographic key sizes", *Journal of Cryptology*, vol. 14, no. 4, pp. 255-293, 2001.