Ranking of Authentication Schemes based on Critical Limiting Factors

Sangeeth Kumar.S
Department of Computer Science and Engineering
PSG College of Technology, Coimbatore

R.Venkatesan, Ph. D
Department of Computer Science and Engineering
PSG College of Technology, Coimbatore

ABSTRACT
In any of the computing environment ranging from a traditional computing to the emerging service based computing, security and privacy has been an important consideration in the architecture. Particularly user authentication is an entry point to almost each and every application and services published. Extensive research work in user authentication has yielded several authentication schemes but the existing schemes focuses largely on the benefits rather than their downside in terms of security, usability and deploying ability, which are found to be ineffective when deployed in the real world. To overcome this issue, a ranking model is proposed in this paper that analyzes the authentication scheme based on their limitations and gives a prioritized scheme based on which the best mechanism at a particular instance of time could be chosen and implemented.

Keywords
Authentication Schemes, Critical limiting factor, Survey, Impact Factor Value.

1. INTRODUCTION
Authentication is a major consideration in any multi user software application which uniquely identifies the user and enables protection for the application usage from fake users. A lot many authentication schemes have been proposed and research is going for new authentication schemes also. But these authentications possess usability and deployment issues more than security issue and become ineffective when deployed in real world. Hence, a ranking model is required to identify the best authentication at a particular instance of time.

The dramatic increase of computer usage has given rise to many security concerns. One of the major security concerns is authentication, which is the process of validating who you are to whom you claimed to be. Authentication of communicating entities and confidentiality of transmitted data are the foundations in establishing secured communications over public networks. Recently, many researchers have proposed a variety of authentication schemes to confirm legitimate users. In general, there are four human authentication techniques:

1. What you know (knowledge based).

2. What you have (token based).

3. What you are (biometrics).

4. What you recognize (recognition based).

Any authentication scheme will fit into any one of the above categories. With the rapid growth of research work on Computer security specifically on authentication of user leads to increased population of authentication schemes. Many of the researchers have proposed different authentication schemes considering the benefits and advantages of the scheme over the existing schemes. But a few critical factors have not been considered by them. In this paper, the consideration is given to these factors as they could benefit the genuine user of the application. There is always a high chance that in spite of having plenteous benefits, a scheme would fail if a few critical factors affect the scheme. In this paper, proposal has been made to implement a ranking model that yields a prioritized list of authentication schemes based on certain critical limiting factors.

2. CRITICAL LIMITING FACTORS IN AUTHENTICATION
The critical factors are those which directly influence authentication schemes. These could be broadly categorized as:

- Security Issues
- Usability Issues
- Deployability Issues

2.1 Security Issues
The security issues are those that directly affect the security and confidentiality of the system and these are recommended to be evaluated based on a numeric score from probability of occurrence of the issue. These are considered to be the loop holes and vulnerabilities in the authentication schemes that facilitate the attackers to get through the authentication wall.

2.2 Usability Issues
Usability with respect to authentication is the extent to which an authentication scheme can be used by the user or a group of users with ease of use, effectiveness, efficiency, and satisfaction specific to a context. These Issues either directly or indirectly influence the user satisfaction and thereby creating a profound effect on the authentication mechanism.

2.3 Deployability Issue
For an authentication scheme to be accepted and adapted by the service provider, it is highly required that the scheme facilitates the developer to deploy it with minimal degree of implementation issues. An authentication scheme which does not possess the security and usability issues is considered to be a failure scheme when it is not deployable. Hence, the need to consider deployability issues plays a vital role when it comes to ranking authentication schemes.

3. AUTHENTICATION SCHEMES

A lot many researchers have proposed a number of authentication schemes. In this paper, some of these schemes are grouped into a category based on the similarity which is given in Table – 1. The advantages and limitations of these authentication schemes have been discussed in this section. Their characteristics have been analyzed and critical factors are identified based on Security, Usability and Deployability aspects.

Table 1 – List of Authentication Schemes

I.Legacy Passwords:
- ✓ Simple Text password

II.Graphical based Authentication
- ✓ One Time Image
- ✓ Sketching Authentication
- ✓ Graphical coordinates
- ✓ Scribble a secret

III.One Time Password
- ✓ Sms OTP
- ✓ Email OTP
- ✓ Separate device
- ✓ Mobile Application

IV.Mobile Phone Authentication
- ✓ Recent Messages

V.Location based Authentication
- ✓ GPS Authentication
- ✓ Wifi based Authentication

VI.Biometrics based Authentication
- ✓ Finger Print Authentication
- ✓ Iris Detection

VII.Password Manager
- ✓ Firefox Authentication
- ✓ Cloud Password Manager

VIII.Federated Single Sign On
- ✓ OpenID/Facebook Connect

3.1 One Time password

One Time Password (OTP) [1,2] is a recent trend in authentication where in user enters user-id in the input form and an OTP is generated based on the hashing algorithm which is sent to mobile device as sms and email or the OTP can be a device generated. Then the user enters the OTP to get authenticated into the system. The major advantage of this kind of authentication scheme is that guessing the password is not possible as OTP is generated for every login and is always unique. Also, users do not need to remember password as it is sent to the device's sms inbox or email. It also adds advantage that physical observation attack is not possible with this kind of scheme. The downsides of the scheme includes that it is device dependent and there is a need for third party dependency for the scheme and theft of the devices facilitates the attack of user credentials which leads to breakage of the system security.

3.2 Location Based –GPS authentication

Here, the user authentication [3] is done using person's geographical location with the help of location identification sensors and other technologies like GPS, cellular network or Wi-Fi Hotspots. It combines the timestamp with location and sends the encrypted data to server. The user also receives the encrypted information as a key in the mobile device and enters the same in the server side where it is matched and authenticated. Location of the user is unique and hence not possible for the attacker to impersonate the user, easy to learn, memorization of the password is not required and also there is no dependency for third party. On the other hand, this is a new scheme and latch on to poor maturity when compared to other schemes. It lacks accuracy while locating the place due to technical issues and there is a need for special device for user authentication in this mechanism. Also, there is a pre-requirement of higher bandwidth as the location information has to be transferred between multiple devices and servers.

3.3 Scribble a secret

It is a pattern recognition system [4] in which authentication is performed based on how similar the input drawing is to a pre-registered template. It is similar to signature strokes. The major advantages include easy learning, adaptable nature and no third party dependency. Guessing attack fails in this case as attackers cannot guess what actual user have scribbled. This method is difficult to deploy and also suffers from the risk of impersonation by observing user patterns. Apart from this, it is difficult for user to remember what has been scribbled before. These schemes are most suitable for touch interface enabled devices only.

3.4 Biometric Authentication [5]

This is related to "what people possess as part of their bio system". Users themselves are the key to security and the attributes are highly natural and unique without involving any mathematical model and complex algorithms. The well known facts are:

i. No memorization issue is associated with this scheme.

ii. It is a natural and highly independent scheme where learning curve is very low.

iii. Guessing attack is highly unlikely.

Yet, biometrics possesses certain downside such as additional sensor device requirement, cost and difficulty in gathering. Poor lifetime of sensor device is also a major issue. The implementation is challenged by high rejection rate as changes in the body, for example a cut in the finger or dirt in eyes could produce false alarm, besides it is not accessible by everyone and everywhere.

The methodologies so far discussed are a few examples of authentication schemes. There are many more schemes [6, 7, 8, 9] available in literature and all of them have their merits and limitations. To summarize, it is impossible to zero in on a particular authentication mechanism that is suitable for all scenarios. Moreover, selecting a particular mechanism would have a strong coupling to the host software. Also, considering software as a service, it would be prudent to develop a ranking scheme by which an authentication mechanism could be selected dynamically at the time of user entry into the software. To implement this idea, a ranking scheme has been proposed in this paper considering the

critical limiting factors which could change from time to time due to technological advances and environmental changes.

4. PROPOSED RANKING SCHEME

The proposed ranking scheme has been arrived at using the following procedure.

1. Tabulating the issues that influence three different categories of critical factors related to Security, Usability, and Deployability [10,11,12]. These are listed in Table – 2, Table – 3 and Table – 4.
2. Mapping the issues listed in Table – 1, Table – 2 and Table – 3 with the major authentication schemes. This is required as not all the issues will be of concern with respect to a particular authentication scheme. This is shown in Table – 5 known as the Critical Factor Table (CFT).
3. An impact factor for each of the issues shown in Table – 2, 3 and 4 for the scheme has been computed based on questionnaires distributed to a variety of users. This is shown in Table – 6 known as Issue Impact Factor (IIF) Table.
4. Based on the impact factor of a specific issue and its influence on an authentication scheme, the various authentication schemes are given a score which represents its relative rank.

These steps are briefly explained in this section.

4.1 Issues in major categories

Table – 2: List of Security Issues

CODE	DESCRIPTION
S1	Impersonating the user by physical observation or with personal details.
S2	Guessing the password or credential details because of poor constraints imposed by the verifier or by applying brute force attack.
S3	Impersonating user by intercepting user input from user device or eavesdropping on text communication or by other malware programs.
S4	Probability that one verifier/provider is fraud and can help the attacker to attack other sites.
S5	Attacker simulates the verifier /provider to get credentials and use those to attack actual verifier.
S6	Theft of a device to facilitate attacker to attack the system.
S7	Attacking the trusted third party with which actual provider/verifier is prone to be attacked.

Table – 3: List of Usability Issues

CODE	DESCRIPTION
U1	Scalability Issue
U2	Memorizing/ Forgetting Issue
U3	Need for Physical object to be carried
U4	Difficulty in learning/Poor Learning curve
U5	Rejection for a Genuine User
U6	

Table – 4: List of Deployability Issues

CODE	DESCRIPTION
D1	Expensive
D2	Compatibility Issue with existing password server
D3	Browser Compatibility Issue
D4	Low Maturity
D5	High Bandwidth Requirement.
D6	Special Ambiance/Environment Requirement

4.2 Mapping of issues to Authentication Schemes

To map the issues to the authentication scheme, CFT has been constructed which is a matrix of authentication scheme and its associated critical factors. To simplify the contents of table, codes from Table – 2, 3 and 4 have been used in the CFT. The values for matrix are filled with a Boolean value viz., Yes/No that indicates the presence of an issue in the authentication scheme. For instance, U3 against sms OTP is "Yes", which means that the Usability Issue "Need for physical object" is an issue associated with sms OTP authentication scheme. The CFT for Usability, Deployability and Security Issues is shown in Table – 5.

4.3 Determination of Issue Impact Factors

Issue Impact factor (IIF) is a constant numeric value assigned to each issue based on which the overall score for each authentication scheme is calculated. IIF gives the degree to which, a particular issue affects the authentication scheme. IIF could be computed from various sources like feedbacks from users and developers, conducting a survey, data mining and other analytics technique. In this paper, survey has been conducted to derive the constant value. A set of questionnaire for usability and deployability issues have been prepared to conduct the survey. Fifty hard copies of usability questionnaires [Appendix -1] had been distributed among different age people and also an online survey had been conducted using web portal. Online survey of deployability questionnaires [Appendix - 2] had also been distributed to developers of various software organizations in India and USA. Approximately, 300 survey results were collected and based on the percentage of options voted by different user for the presence of a particular issue, IIF value has been calculated by converting the percentage into decimal values. Similarly, Verizon DATA Breach report [13] of 2013 has been used to obtain the security attack percentage with which the constant impact factor value has been calculated for security related issues.IIF for issue j has been referred as W_j in the following sections.

Table – 5: Critical Factor Table

Issue -> Scheme	D1	D2	D3	D4	D5	D6	D7	U1	U2	U3	U4	U5	U6	S1	S2	S3	S4	S5	S6	S7
Simple text password	No	No	No	No	No	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No
One time Image	No	No	No	Yes	No	Yes	No	Yes	Yes	No	No	Yes	No	No	No	No	Yes	No	No	Yes
Sketching Authentication	Yes	No	No	Yes	No	Yes	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	Yes	No	No
Sms OTP	No	Yes	No	Yes	Yes	No	No	No	No	Yes	No	Yes	No	No	No	Yes	Yes	No	Yes	Yes
Email OTP	No	No	No	Yes	Yes	No	NO	No	No	No	No	Yes	No	Yes	Yes	Yes	Yes	No	No	Yes
OTP Separate Device	Yes	No	No	Yes	No	No	No	No	No	Yes	No	Yes	No	No	No	No	Yes	No	Yes	No
Recent Message	No	Yes	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	No	Yes	No	No	Yes	No
GPS authentication	Yes	Yes	No	Yes	No	Yes	Yes	No	No	Yes	Yes	Yes	No	No	Yes	Yes	No	No	Yes	No
Finger Print Authntication	Yes	No	No	No	No	Yes	Yes	No	No	Yes	No	Yes	No	No	No	Yes	No	No	No	Yes
Firefox Pass Manager	No	No	Yes	No	Yes	No	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	No	Yes
OpenID SSO	No	Yes	No	Yes	Yes	No	No	No	No	No	Yes	No	No	Yes	Yes	Yes	Yes	No	No	Yes

Table – 6: Issue Impact Factor Table

Usability		Security		Deployability	
CODE	**IIF VALUE**	**CODE**	**IIF VALUE**	**CODE**	**IIF VALUE**
U1	2.85	S1	3.85	D1	7.05
U2	4.15	S2	18	D2	5.0
U3	5.265	S3	17.86	D3	5.87
U4	3.38	S4	14	D4	5.43
U5	4.51	S5	22.33	D5	6.59
U6	3.38	S6	2.8	D6	4.57
-	-	S7	15	D7	3.92

4.4 Ranking of Authentication Schemes

CFT shown in Table – 5 represents only the association of critical limiting factor with each scheme, but to rate and rank each of the authentication schemes, a concrete weighted score is required. To compute the score, two novel techniques have been proposed.

1. 0/1 Score Calculation
2. Probabilistic Score Calculation

0/1 Score Calculation:

Score Value SVi for Authentication Scheme i can be given by,

$$SV_i = \sum_{k=0}^{n} W_i \; b_{i,j}$$

…… eqn (1)

Where,

j is the issue from set belongs to = {U, D and S}

W_j is IIF value for an Issue j

bi, j = {0, if j is applicable for i
1, if j is not applicable for i}

Here $b_{i,j}$ value is identified from CFT (table – 5)

2. Probabilistic Score Calculation:

Score Value SVi for Authentication Scheme i can be given by,

$$SV_i = \sum_{k=0}^{n} W_i \; P_{i,j}$$

……..eqn(2)

Where,

j is the issue from set belongs to = {U, D and S}

W_j is IIF value for an Issue j

$P_{i,j}$ is the probability of the issue j occurring in the

scheme i.

The 0/1 Score calculation method for an authentication scheme could be used when the associated issue has complete impact on the scheme whereas the probabilistic score calculation method could be used when the associated Issue has a part effect on the scheme or when there is a need for more precise result. Depends on the requirements and type of issue, the choice could be made between two different approach. These methods give the approximate degree of which the scheme may be subjected to get affected by the issue j at a particular instance of time around the globe. The score value SV for scheme i is inversely proportional to ranking of the scheme. Higher the score for scheme i, lower its ranking on the list and hence the score is a critically influencing factor for the authentication scheme.

5. EXPERIMENT RESULTS

Based on the survey conducted, the IIF value W_j has been computed and shown in Table – 6. Then, the 0/1 score calculation formula as in equation (1) is applied considering the calculated constant value W_j for each issue j and the overall score SV_i has been arrived at to rank the scores. Lower the score value SV_i signifies that the authentication scheme – i is better. Accordingly, the schemes considered in CFT (Table – 5) have been ranked based on sorted order of score value SV obtained and displayed in Table – 7. Result shows that OTP separate device authentication scheme scored the lowest value of 28.823 among other schemes and hence obtained the rank one. It signifies that OTP could be the better scheme to use in the application based on the attributes, technology and other factors considered at the time of calculation of the score.

Table 7: Calculated rank for authentication schemes

Scheme Name	Score	Rank
OTP Separate Device	28.823	1
Recent Message	39.367	2
One time Image	41.51	3
Finger Print authentication	44.189	4
GPS Authentication	54.412	5
Firefox Pass Manager	55.956	6
Sms OTP	61.137	7
Sketching Authentication	63.19	8
OpenID SSO	73.792	9
Email OTP	74.422	10
Simple text password	83.04	11
New Scheme2	91.685	12

6. CONCLUSION & FUTURE WORK

Security and privacy are inevitable when it comes to the architecture of any software application deployed in the service computing environment. In this paper, a ranking model is proposed that analyzes the authentication scheme based on the certain limiting factors like device dependency, need to remember password etc to prioritize various authentication mechanism used in the security layer of application's implementation. The outcome of such a ranking model is a list of authentication schemes ordered according to the overall applicability of the issues associated with the scheme. Quantitative research methodologies like surveys have been used to derive the weightage value (IIF constant) with which the score is calculated for the scheme. This work gives the application users and service seekers to select a particular mechanism at the time of using the application based on the ranking given. Hence, this gives a distinct advantage of dynamism in security environment which is the need of the hour. In addition to surveys, analytics techniques like data mining, big data, and feedback system could also be used to derive the IIF constant. On the other hand, Cloud is emerging and enables us to provide anything and everything as a service. Deploying such a proposed ranked authentication model as a separate layered service into service computing environment like cloud could be the future extension of this paper which can eliminate the need to develop the authentication layer for each and every software application resident in the cloud.

7. ACKNOWLEDGMENT

This work has been supported by the faculty members in various departments of PSG College of Technology, Coimbatore and also the employees of several software industries who have participated in answering the questions of survey.

8. REFERENCES

[1] Weaknesses and Improvements of a One-time Password Authentication Scheme Mijin Kim, Byunghee Lee, Seungjoo Kim, and Dongho Won, International Journal of Future Generation Communication and Networking Vol. 2, No. 4, December, 2009.

[2] oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012 651

[3] Using Geographical Location as an Authentication Factor to Enhance mCommerce Applications on Smartphones, Torben Kuseler & Ihsan Alshahib Lami,International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (4) : 2012

[4] D´ej`aVu: A User Study Using Images for Authentication_, Rachna Dhamija, SIMS / CS, University of California Berkeley

[5] Comparing Passwords, Tokens, and Biometrics for User Authentication Lawrence O'Gorman Avaya Labs, Basking Ridge, NJ, USA, Proceedings of the IEEE, Vol. 91, No. 12, Dec. 2003, pp. 2019-2040 ã 2003 IEEE.

[6] J. Goldberg, J. Hagman, and V. Sazawal. Doodling our way to better authentication. In Proc. of Ext. Abstracts CHI 2002, pages 868{869, New York, NY, USA, 2002. ACM Press.

[7] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C.Mitchell. Stronger password authentication using browser extensions. 14th Usenix Security Symposium, page 1732, 2005.

[8] The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes, Cormac Herley, Microsoft Research, Redmond, WA, USA.

[9] Computationally Efficient PKI-Based Single Sign-On Protocol PKASSO for Mobile Devices Ki-Woong Park, Student Member, IEEE, Sang Seok Lim, Member, IEEE, and Kyu Ho Park, Member,IEEE

TRANSACTIONS ON COMPUTERS, VOL. 57, NO. 6, JUNE 2008

[10] J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password memorability and security: Empirical results. IEEE Security and Privacy, 2(5):25{31, 2004.

[11] Password Management Strategies for Online Accounts, Shirley Gaw, Symposium On Usable Privacy and Security (SOUPS) 2006, July 1214, 2006, Pittsburgh, PA, USA.

[12] Revisiting Defenses against Large-Scale Online Password Guessing Attacks Mansour Alsaleh, Mohammad Mannan, and P.C. van Oorschot, Member, IEEE.IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 1, JANUARY/FEBRUARY 2012

APPENDIX-1

[RF Q1]A. Questionaries' for Survey:
Questionnaire on Usability of authentication: (Tick) - Staff/ students/ others

1. Which of the below Authentication scheme do you mostly use for login websites? Please Tick
    1. Simple Username Password
    2. One-time Passwords
    3. Picture based
    4. Biometrics

You're Option: _____

2. Do you use same password for every website or different password for every website?

Same for all: Different for all:
One for a set of website:

3. Do you forget your password(s)?

Yes: No:
Sometimes: Never:

4. If your answer for the above question is "Yes" or "Sometimes", choose the reason.

Different Passwords for different sites.

Complex Password Pattern (E.g. Alpha Numeric)

Age Problem

Others – Specify ----------

5. Have you used mobile phone for logging into the websites? E.g. SMS OTP, Google Authentication etc.

YES NO

6. If your answer is yes, give your opinion about carrying a device for authentication always.

It is annoying that I always need mobile with me for login.

It is alright except when my mobile battery goes down or signal lost.

I have absolutely no Issues.

Others, Specify _____

7. How easy it was or it would be for you to adapt to the following scheme.

Simple username password: (Tick on the scale. For e.g.)

				✓	

Easy
Moderate Difficult

OTP:

Easy
Moderate Difficult

Picture based:

Easy
Moderate
Difficult

Biometrics:

Easy Moderate Difficult

Password manager:

Easy Moderate Difficult

8. How often you are rejected for authentication while login into your most widely used site?

Rarely:

Never:

Sometimes:

Very frequently:

Every time I login:

9. Was it easy for you to recover the password on averagely used websites?

Yes, Easy

Moderate

Difficult

Never

10. Tick the following category of website you often login to use.

Social Networking

Online Banking/ Mobile Banking

Academic Websites

Emails

Cloud based Drop box, SkyDrive etc.

Others – Specify_____

11. Your Age:

Between 15-20:

Between 21-35:

Between 36 -50:

Above 50:

Your feedback or other opinion about authentication usability, if any:

_____

APPENDIX-2

[Rf Q2]B. Questionnaire on Deployment of authentication:

1. Rank the below Authentication scheme based on the ease of development and deployment.

   1. Simple Username Password

   2. One-time Passwords

   3. Picture based

   4. Biometrics

2. Have you ever faced browser compatibility issue when developing your authentication scheme?

   Yes: No:

3. Give your opinion about using a new scheme that has very low maturity such as location, Otp etc.

   It is unreliable

   Organization lead may not accept.

   Highly Risky

   User may not be satisfied

   Others, specify _____

4. What percentage of development cost is allocated for security in a project on average?

   1 – 10 %

   10 -25 %

   25 – 40 %

   Above 40 %

   Please mention the type of the project
   ._____

5. Tick the following Issues in terms of deployment in your project or other projects you have heard of.

   Bandwidth requirement

   Special Ambience/ environment

   Browser compatibility

   Need for third-party support

   Expensiveness

   Others, Specify_____

6. How was the support from a third-party when you included a third-party, when you included a third party in your project?