User Friendly Authentication Mechanism for Rural Communities

R. Dayarathna [1] H. Ekanayake [2]

[1] PhD Candidate,
Stockholm University,
Sweden

[2] Department of Computation and Intelligent Systems
University of Colombo School of Computing
Colombo, Sri Lanka.

E-mail: [1] rasika@cmb.ac.lk, [2] hbe@ucsc.cmb.ac.lk

Abstract

This paper proposes a simple, user friendly but more secure mechanism for user authentication. Developing countries should make necessary changes to the technologies in developed countries before using them in developing countries without blindly using technologies in developed countries. If they realize value of their cultural aspects and value systems they can have state of the art systems with fewer resources. This paper addresses how the traditional value system facilitates to have a user friendly but more secure user authentication system.

Keywords: DigiPass, User authentication, One-time Password, Cultural issues, E-Governance, Rural community, Security

1. Introduction and Motivation

Information security is based on three building blocks, namely confidentiality, integrity and availability [1]. Authentication is one of the most important aspects in providing confidentiality. Authentication verifies identity of the claimant [2]. Identity card is one method used in proving authenticity of individuals. In the digital world, authentication can be done at various levels. One level is client authentication; in this case the identity of the user is verified. Another level is device authentication which verifies the identity of the device.

There are a number of existing user authentication systems but the most popular and widely used mechanism is based on user name and password. Even though, **it's the** widely used mechanism, it has certain limitations. There is a battle between user friendliness and security in this method,. since more complex passwords are tend to be forgotten. On the other hand simple passwords are vulnerable to guessing attacks [3]. The other problem is, it is not wise to use the same passwords over and over again since it would make easy for attackers [4]. There are other user authentication systems, such as, certificate based authentication, smart card based authentication, bio-metric authentication etc.. But they are complex and very expensive in terms of setting up and maintenance.

A better mechanism, called DigiPass, which gives `one-time password`, was introduced to overcome these limitations. The proposed mechanism made further enhancements to the existing DigiPass system especially targeting at people in developing countries. It is a simple, easy to understand and user-friendly system for IT-illiterate people. The new feature of the DigiPass system called Category password facilitates to share the device with owner's close associates.

There is a trend to bride the digital divide by introducing the ICT (Information Communication Technology) to rural communities but we have to realize that, generally, people are reluctant to switch to new technology until they are confident with it. Security is one of the features people are worried about. Therefore, it is necessary to provide understandable and user friendly security mechanisms to build confidence over new IT systems [2].

Numbers of researches are being done to assess the impact of traditions, value systems and customs in communities on using ICT [5]. They reveal that It would be easy for people to understand something they have already experienced with instead of having a totally new stuff. One of the stuff people are familiar with is, keys used to access doors, boxes etc. The users of keys have realized the value of them and also established certain practices in managing their keys. Hardware token has a number of similarities to the keys in certain ways. Therefore, people would easily understand the importance of having hardware token rather than a mere password written on a paper.

People share not only tangible things but also intangible assets in order to have an overall advantage. But, no one has addressed how to share a password. Theoretically, a password should not be shared with anyone. It can be shown that sharing a password gives certain benefits to the owner. Sharing has a positive correlation with trust. The trust levels depend on various aspects such as economical, cultural values, relationships among them etc. [6]. It has shown that in India the trust level of the society is much higher than that in the USA [7]. The password can also be shared with others depending on their trust status, situations and the value of the assets accessed by the given password.

2. ICT Issues for E-Governance

The electronic money order system [8], which is an alternative to credit card payment, was introduced to Sri Lanka in 2004. Statistics reveals, this system was becoming a very popular payment method in Sri Lanka. Since this is the only option for the poor people to do business transactions over the Internet, this was known as poor man's credit card. Minimizing time and saving the cost are major benefits of the system. However, lack of IT literacy is one of the major obstacles to further progress of providing necessary ICT infrastructure [9]. Therefore, IT literate persons have to provide their assistance to others to make use of the system. But, there is a security risk in getting help from others. This enhanced DigiPass mechanism facilitates to obtain assistance from others without compromising security.

3. DigiPass Framework

3.1. What is DigiPass?

DigiPass is a hand-held electronic device, having a keypad and a display in its face as depicted in Figure 1. A user can feed values to the device. The device then uses its embedded algorithms to process the input and finally gives a 'one time password'.

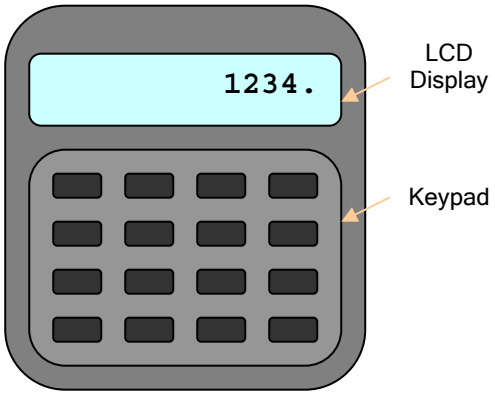

Figure 1: The DigiPass Device

3.2. DigiPass Mechanism

Categorizing User Transactions

Today, citizens interact with their government institutions and other private agencies via electronic means, such as visiting their web sites, participating in eDemocratic processes, paying for various services provided by those agencies etc.. These transactions do not require the same level of security for users' data. Therefore, it's possible to divide transactions into different categories according to their severity, for instance, paying fees for a service provided by an agency requires higher security than visiting a web site for gathering information. Based on that, different security levels could be assigned to these categories. Table 1 gives some identified transaction categories, the associated security levels and instances for each category.

Transaction Category	Security Level	Transaction Instances
Logging in to websites to get information	1	Getting applications for a driving license, passport etc.
Viewing details of utility bills	2	Viewing outstanding amount of water bills, electricity bills, etc.
Getting bank balance	3	Getting bank balance of saving's accounts, current accounts
Paying utility bills	4	Paying a telephone bill, water bill, electricity bill etc.
Transferring money among owner's accounts	5	Transferring money from a saving account to a current account etc.
Transferring money to a third party account	6	

Preparing with the DigiPass

A user is given a DigiPass with a default master password for the device. As soon as the user gets the device, the default password must be changed to a new password. This password is called master password which is a 4 digit number. Once the initial password is changed, a notice must be given to the issuing agency. Until the notice is given, the device cannot be used. The master password of the device is required to assign category passwords. If the owner forgets the master password, there is no way to retrieve the lost password. Then the device must be discarded and a new device be obtained from the issuing agency.

Once the master password has been set up, the device becomes ready to use. Now the owner could login to the device using the master password and setup category passwords for different transaction categories. It is not necessary to set up category passwords for all categories at the same time; passwords can be assigned when necessary. After category passwords are setup, there are two options to set the life time of the password. One option is to limit the life time for a given period of time varying from one minute to a number of days. In this case, the assigned password is valid only for a given period of time. Another option is to restrict the lifetime to a number of attempts. The process of setting category passwords is depicted in Figure 2 and 3.

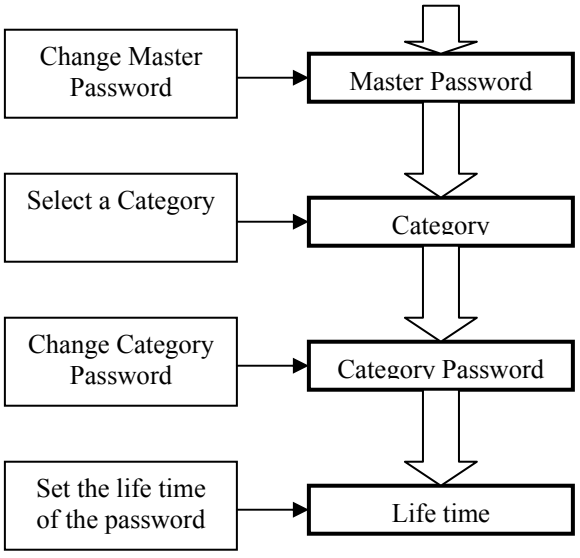

Figure 2: The owner has to first change the master password of the DigiPass, and then he changes category passwords and their life times.

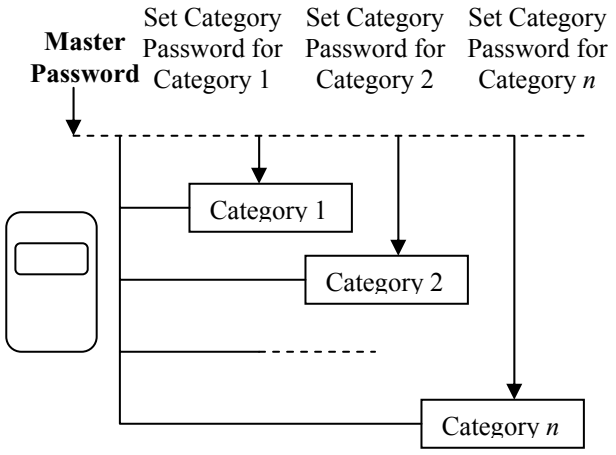

Figure 3: The owner uses his master password to log into the DigiPass and sets category passwords for transaction categories.

Using the DigiPass

After setting up category passwords, the device becomes ready to be used by either the owner or a legitimate holder nominated by the owner. If in the case of a legitimate user, the owner must define the lifetime of the category password(s) or number of valid attempts before giving it to the holder. By restricting the life time, the owner can assure that the holder cannot use the device for any unauthorized category or exceed the limits set by the owner in the case of authorized category.

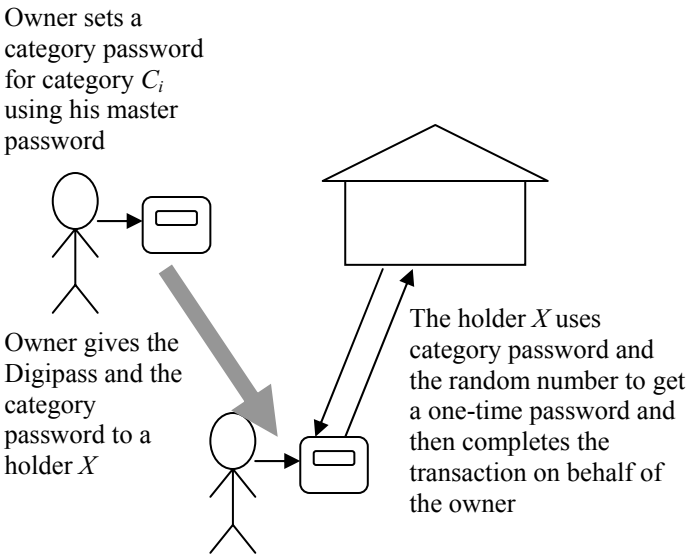

Figure 4: A holder completes a transaction on behalf of the owner.

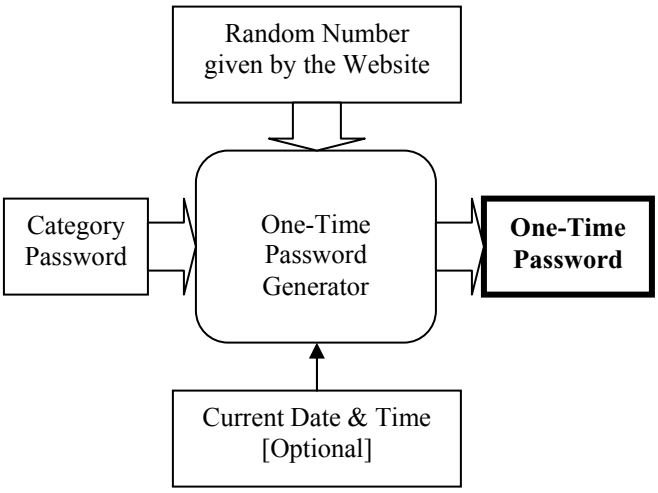

Figure 5: One-time password generation process.

Figure 4 depicts how the holder completes a transaction on behalf of the owner and Figure 5 depicts the one-time password generation process. Once the holder informs his intention to make a particular transaction with an agency, for instance, paying a utility bill, the agency presents a random number associated with the particular transaction on the web page. The holder enters the category password, given by the owner, and the random number displayed on the web site to the DigiPass device. The DigiPass then generates a 'one time password'. This one-time password permits the holder to proceed and complete the requested transaction.

The following steps summarize the process of doing a web-based transaction using the enhanced DigiPass.

1. The customer gets the login page of the web site.
2. The customer selects the transaction category given in the web page, e.g.
    a. View the account balance
    b. Pay utility bills
    c. Transfer funds
3. The web server generates a random number and displays it to the customer.
4. The customer enters the category password, followed by the random number appearing on the web page to the DigiPass device. Consequently the DigiPass device generates a one time password to do the requested transaction.
5. The customer feeds the user name and the generated password to the system through the web page.
6. The web server responds to the customer by displaying the status information of the transaction.

4. Digital Exposure through DigiPass: Advantages

The proposed system has a number of advantages for people in developing countries. Researches have been conducted worldwide, especially in developing countries, with a view to identify better ways of using the ICT in their countries, since technologies in developed countries cannot be applied in developing countries "as is" basis [8]. These modified technologies and policies have to be amended to suite with economical, political and social structures of developing countries. Our approach is an attempt to modify and improve one of the existing technologies in developed countries to make it suitable for developing countries.

There is a struggle between security and usability of a system [3]. If the security is high, then the system becomes less user friendly and vice versa. In conventional systems, it is highly advised not to share one's password with someone else. In addition, there are guidelines for a good password, such as, a password should have a minimum length, contain numeric and special characters etc.. These measures are good precautions to keep a system in a secure state; however it drastically reduces the system's usability, since it creates a lot of hardships to users. Many people tend to forget their password and as a result they request new passwords [3]. This incurs cost to individuals, since their transactions get delayed for some period and on the other hand the issuing agency has to generate a new password and inform it to the user. Further researches should be conducted to identify the correct balance of security and usability.

Societies where people trust each other gain certain advantages over the rest. People in trusted societies do not paranoid about their security or privacy very much [7]. As a result people do share their belongings with others, since that would make their life easier. Another advantage is, they can save money otherwise would have been spent on providing additional security and privacy. Trust also varies with cultural, social and economical aspects.

Lack of access to the Internet is a major problem in developing countries. Over the past few years many cyber cafés, which provide access to the Internet, have been established to bride the digital divide. Since, most agencies tend to provide their services on line, it enables people to get things done by visiting a cyber café without going to agencies. However there is another problem to be considered, which is the cost and the time taken to visit a cyber café. For instance, if a family of four members want to do a transaction, each one has to visit a cyber café by himself/herself. In paper based system, if someone wants to get his account balance checked, he could give his pass book to his close associates and ask him to visit the bank to get the balance of his account. However, the same

method cannot be generalized for electronic transactions. In the digital world, everything is in digital format and people are given passwords to access different services. In some situations, a single password is given to access all services offered by an agency. For instance, one password may give access to get one's account balance, pay his utility bills or transfer money to a third party account. To avoid a single sign on password which is vulnerable to many attacks, some financial institutions have introduced two passwords, one for sign-in and one for other transactions.

It is not wise to give one's single sign on password to another person since that may cause a number of problems, such as the second person may use it without the knowledge of the owner, or the second person may use it for unauthorized transactions. In a manual system, one could give his passbook to another and may ask him to get his balance since he knows that the agent cannot do anything other than getting the account balance. In a single sign on system giving that password to someone else is not a good idea, since that person might use that opportunity to transfer money to his own account.

The proposed system is more advantageous than the existing single sign on system or dual password system where it generates one time passwords for a single transaction. It requires the owner to have a single master password, and the owner can get independent passwords for every transaction. The owner sets a password for each transaction category and this category password combined with the on-line random number generates a 'one time password' for a given transaction. Each time the user wants to do an electronic transaction, a different random number is given by the server, which in combination with the category password generates a one-time password.

Since the DigiPass uses 4 digit passwords it is not that difficult to keep them in mind, and furthermore risk is very less since the owner has a hardware token. Consider an ATM account which has four digit numbers. Even though the password is very short, it provides enough security since the ATM card must be presented before doing any transaction.

This solution enables one to share his passwords with others while keeping control over his passwords. If something happens to his property, he knows the person who had the key and can identify the wrongdoer. The holder of the key also knows that if something goes wrong, he is responsible for that. The proposed mechanism uses this concept in sharing passwords. In this case, if a DigiPass is given with a password for a particular category, if something goes wrong in that category, the holder is responsible for it. For instance, if one is given a DigiPass to pay utility bills with the category password and if he has used it to pay more than the outstanding amount or paid twice, the owner can easily identify the person who was having the device when the particular transaction took place.

IT literacy is low in developing countries, therefore, it is difficult to educate them how to use a password and how to keep it secure. They might not realize its value and as a result they may write it on a piece of paper. They may reproduce it or write it down elsewhere. On the other hand, it would be easy for them to understand something they are familiar with. People are familiar with tangible keys and they have already realized the value of tangible assets, especially reproduction cost. Therefore, they would easily realize the value of the tangible DigiPass device.

There is no risk in showing a category password to a third person who loves to assist, if the password is set only for a single session. The third party cannot use again even though he has the device since the device is locked after the initial transaction. It also protects the people who use computers at cyber cafes. There might be key loggers or spy-ware programmers installed in the machines. Not like the single sign-on password, this is not vulnerable to spy-ware or key logger attacks since the system uses one time passwords.

While this facilitates sharing passwords it also prevents sharing of low sensitive passwords. The low sensitive passwords are used for accessing electronic journals, magazines, newspapers etc.. These passwords are used to protect commercial interest of the content providing agencies rather than protecting subscribers. Therefore, the subscribers are not reluctant to share these passwords unless they respect the intellectual rights of the content providers. This reduces cost for subscribers since one subscription is enough for many readers. But this practice makes huge losses to the content providers. The proposed mechanism does not solve this issue completely but it makes difficult to share passwords. Since, every time a unique and distinct password is required to access a web site and it is not convenient to contact the holder every time to get the right password for a particular session.

5. Conclusion and Future Work

This password generation process can be implemented as a separate unit or embedded in mobile phones. Implementing it as a separate unit adds an extra cost to the users and is also an extra burden for him to take it every where he goes. It gives a number of advantages if this mechanism is embedded in a mobile phone. In this case, it costs a very minimal amount and no extra burden is involved in carrying it since the mobile phone is always with the user. All mobile phones do not facilitate but fortunately upcoming mobiles do support third party programmes.

References:

[1] "Web Site Privacy with P3P" Helena Lindskog, Stefan Lindskog. Wiley publishing Inc 2003. p 17

[2] "Web Site Privacy with P3P" Helena Lindskog, Stefan Lindskog. Wiley publishing Inc 2003. p53

[3] "Password memorability and security: Empirical Results," J. yan et al. Sept./Oct. 2004 IEEE Security and Privacy.

[4] "Customers, Passwords and Web Sites" B.Schneier, July/ Aug. 2004 IEEE Security and Privacy.

[5] http://www.sida.se/Sida/jsp/polopoly.jsp?d=321
"Sida- ICT in Developing countries" last accessed on 15/08/2005

[6] "Contracting on the Internet – Trends and Challenges for Law**"** Christina Ramberg
Law and Information Technology. Swedish Views 2002 *Information and communication technology commission. p 109*

[7] "Privacy In India : Attitudes and Awareness" Pnnurangam Kumaraguru and Lorrie Cranor

[8] eMoney Order System: The Smart way to Pay Online, IICT 2003

[9] ICTs, e-Governance and Rural Development, ICEG 2004