

MULTIFACTOR AUTHENTICATION SYSTEM

^aFamutimi.R.F., ^bEmuoyibofarhe O.N. ^cSoriyan H.A ^dOgunbowale O. A..

^{abd}Department of Computer Science and Information Technology

Bowen University, Iwo, Osun State, Nigeria

^cDepartment of computer Science and Engineering

Obafemi Awololo University, Ile-Ife

Rffam@ymail.com

ABSTRACT

Multifactor authentication generally refers to a security authentication system in which more than one form of authentication is used to validate the identity of a user. For example, a webpage which asks a user to remit a single username/password combination may be considered a “single-factor” authentication system since it requests a single data username/password combination in order to validate a user's identity. The webpage may add additional procedures, such as checking the user's internet protocol (IP) address against a list of pre-approved IP addresses or sending a confirmation email to the user's verified email address, in order to add additional levels of user authentication, thereby implementing a “multifactor authentication” system for the webpage. Passwords alone cannot provide the kind of confidence in user authentication that is essential to security. Faced with requirements including regulatory compliance and reducing their risk of security breach, enterprises are increasingly looking to implement stronger authentication systems. Strong authentication goes hand-in-hand with additional technologies, including Grid card.

In this paper, we present a method to authenticate a user with a grid card which supports the single- sign on.. Support for multiple authentication technologies is important, particularly in information grids, where classified resources/data should enjoy fine grained protection. This paper describes our work in the design and implementation of a Grid card authentication. In our methods, a service provider challenges the user with a Grid card password. To determine the appropriate password and their order, the user needs some hint information transmitted only to her personal Grid card. The grid card serves as a second factor of authentication which was designed using C-sharp (scripting) and ASP.net (Interface) It is shown that this method can overcome threats. With the

increasing popularity of handheld devices such as tokens, smart cards, our approach can be leveraged by many organizations without forcing the user to memorize different passwords. Anywhere that there is a need to enter sensitive or private data multifactor authentication is necessary. The system is built using best-practices in system design and software development. The deliverable of this research can be used to secure systems where multifactor authentication is applicable E.g. Internet banking, web transaction etc

Keywords: Passwords, Grid Card, Multifactor Authentication, Technologies, C-sharp (scripting) and ASP.net.

1.0 INTRODUCTION

Authentication is the process used to determine whether the person or process attempting to gain access to a secure system is the person he or she claims to be. Authentication can be simply stated as a question: "Who are you, who you say you are?" Various systems have different ways of authenticating users. The word **user** will be used to denote the person trying to gain access to a system. The most popular technique is the use of a username and password combination to identify the person accessing a system. It is no longer news that the twenty-first century is deemed as the information technology age. Many of our everyday activities are now shifting from manual processes to automated systems. These includes: banking, telecommunication, sales, inventory control, education, e-governance and many more. As our dependence on these information technology systems grows; it is important to access the security risk associated with the use of these systems. We need to ask

ourselves questions like: What is the implication of someone compromising my internet banking PIN number? What is the implication of a tourist group taking control of a highly destructive nuclear weapon? Considering the possible answers to these questions will certainly remind us of the importance of information security.

Though it is often said that: "Change is the only constant thing in life." We would all agree that for every positive change there are often new challenges to tackle. One of such is the need to secure automated systems. Information technology security is on its own an area of specialty in the field of Computer Science, deserving researches, projects and intense studies. Many interesting work have been done in this field to address some of the problems we encounter from the use of automated systems, especially in the areas of preventing unauthorized persons from gaining access to a secure system.

This research is an effort to explore an area within the field of information technology security to

address the problem of authentication in a highly secure system. Usually, there is an enrollment process this is when the user is created on the system; here the user is given a username and password combination. The username is the name that the system will use to identify the user, while the password is a secret code known to the user only. For example, a user with username “Funke” could be identified by password “peaceng”. Here, only the combination of these two parameters will give Funke access to the system.

Systems that use only one technique of identify users are known as single-factor authentication systems. This means that once the user passes the only authentication test or challenge, he/she is given access to the system. E.g. your Yahoo® email box uses a single sign-on authentication method, since only your email address and password are required to gain access to the system.

Securing a system is often a tradeoff among the following metrics:

- What you have? E.g. A token
- What you know? E.g. Password
- What you are? E.g. Fingerprint
- Where you are? E.g. Geo-location

The benefits of the multifactor approach are listed below:-

- It is difficult to compromise all the available authentication factors.
- This approach often uses a combination of “What you have” and “What you know”

security metrics.

- This approach can be designed as an authentication service. Thus, it is possible to meet the authentication needs of all the applications in an organization with a single installation of a multifactor authentication system.

In this approach, there is *division of concerns* amongst the interacting systems. The multifactor authentication system focuses on security while the other systems can focus on business rule/logic validation, reporting, data mining etc.

Authentication factors that can be combined in a multifactor authentication system include:

- Knowledge-based questions: the user is prompted for a set of questions he must answer correctly E.g. Where did you meet your spouse? What is your pet's name? Who was the first king of your hometown?

- Grid card challenge: here a card is given to the user consisting of rows and column values like a matrix. Thus, the user is prompted for values at specific co-ordinates when he/she tries to access the system. E.g. enter the values at location **A1**, **B2** and **C5**.

- Tokens: A token is an electronic device that is capable of generating a unique random digit every time it is pressed. Tokens are assigned to

users, in which case each user can only be authenticated by the token assigned to him/her. When the user tries to access the system, a token challenge is prompted and the user must enter the value displayed by the token at that time. Popular token vendors are RSA, VASCO, Entrust etc.

- One Time PIN (OTP): This is a variant of the username/password. However, a OTP is generated and used only once, after which it can no longer be used to gain access to the s

2.0 REVIEW OF RELATED WORKS

In times past, a recent report by the Federal Trade Commission found that 37 percent of all Internet Fraud complaints filed dealt with identity theft[1]. Additionally, Gartner research vice president Avivah Litan noted in her report "Credit Report and Internet Data Theft" results in more Fraud in 2005. From those surveyed, financial losses resulting from information stolen of the Internet was \$2.7 Billion. Although few would describe any security protocol as impenetrable, two-factor systems can decrease the likelihood of fraud by several orders of magnitude by requiring an additional form of verification, such as the presence of a physical device[2]. In the VeriSign system, this will likely

take the form of a USB key, either dedicated, or embedded as part of a flash drive. Since key and password are each useless without the other, security is maintained even if the physical drive is lost or the password is compromised[3]. Systems that use only one technique to identify users are known as single-factor authentication systems. This means that once the user passes the only authentication test or challenge, he/she is given access to the system. E.g. your Yahoo email box uses a single sign-on authentication method, since only your email address and password are required to gain access to the system.

VeriSign has announced a new consumer verification designed to "strengthen and protect consumers' digital identities"[4]. Following in the path of recommendations released by the Federal Financial Institutions Examination Council (FFIEC), VeriSign Identity Protection (VIP) is designed as a two-factor authentication system, incorporating (to no one's surprise) open standards set forth by the Initiative for Open Authentication (OATH), of which VeriSign is a member. Single-factor authenticationsuch as entering a passwordis currently the most commonly-used method of determining a user's identity in online transactions. Although convenient, this is widely regarded as as a large security hole by most experts, due to the fact that a single password can be compromised in a variety of ways, leading to identity theft.

In a February 2007 research note, Gartner offered some blunt advice: “All organizations should look to use stronger authentication in high-risk situations such as remote access now, and consider wider use of stronger authentication by the end of 2007 and plan for deployment during the following two to three years”[5]. Gartner advises that online banking and other high-value business-to-consumer services should be implementing strong authentication now, while users with lots of system privileges, such as system administrators, should have it by year-end. By the end of 2008, organizations should implement strong authentication for all business-to-business and business-to-employee remote access requirements, Gartner says. A number of factors are coalescing to drive the urgency behind Gartner's advice. A primary driver is the need to comply with regulations and standards that require controls over data access and data protection. Examples include:

The Health Insurance Portability and Accountability Act (HIPAA)[1], which mandates strict controls over privacy of patient data. That, in turn, forces healthcare companies and indeed any organization that holds potentially sensitive data on employee health to ensure that only authorized people can access patient data.

The Federal Financial Institutions Examination Council (FFIEC) guidelines on “Authentication in an Internet Banking Environment,” which like earlier

Federal Deposit Insurance Corporation (FDIC) guidelines say that user ID and password alone should not be presumed to be a sufficient form of authentication for online banking.

NIST Special Publication 800-63, which provides electronic authentication guidelines for federal government agencies; some levels require two-factor authentication.

Multi-factor authentication also reduces the risk from increasingly sophisticated attacks on corporate data[6]. In addition to social engineering attacks that can be highly successful in getting users to give away passwords, various forms of spyware are capable of capturing passwords and forwarding them to would-be intruders[7,8], all without the knowledge of the end user or IT department. At the same time, companies need to open up their networks to suppliers, customers and business partners. Companies involved in mergers and acquisitions, or even those with multiple divisions or business units, may be in a similar situation they need to provide access to corporate data to disparate groups. Strong, multi-factor authentication is part of a security strategy that allows them to do so while maintaining proper security posture[9,10].

Two-factor authentication is already out there in a number of proprietary forms[11]. AOL for one offers an add-on to its standard service which supplies the user with a small physical device that receives a stream of constantly updated six-digit

codes[12]. Logging into an account requires the correct current code along with the user's password.

Additionally, some banks have implemented two-factor systems for online customers, and Microsoft has announced plans to support such authentication in Vista[7,8,13]. VeriSign, however, jumps in with a large head start in infrastructure: by their own numbers the company already services almost half-a-million web sites. That means that one company has the capability to make a single key work in a significant number of transactions, and that is exactly what they plan to do: sometime in the next three months, VeriSign will begin selling authentication devices online, and SanDisk has announced the upcoming availability of flash drives with similar capability.

So far, it looks like VeriSign is headed in the right direction: they are endorsing open standards, and have lined up a number of important partners in the form of Yahoo, Motorola, eBay/PayPal, and SanDisk[15]. The VIP network also incorporates a "self-learning anomaly detection engine" to help track down any attempts at fraudulent transactions, and an intelligence sharing system is planned that will allow fraud information to be spread among network partners.

Yet, through all of this, we have a tiny, nagging concern in the back of my mind. Although trusting

our personal and financial data to large companies run by complete strangers is an unfortunate fact of modern life, we have to wonder what the consequences might be if the VeriSign system is a breakaway success...If someone carries a Visa, a MasterCard, and an Amex, not a single one of those companies has all of that person's information. VeriSign might be hired to do no more than verify identities, but it will also be maintaining a record of every transaction someone makes including banking, credit cards, bill payments, purchases, etc. Multiply that single person by millions or more and VeriSign will be in a position that perhaps no other company now enjoys. How much power does that give them? And how much power does it give the group that successfully hacks VIP?

Historically, fingerprints have been used as the most authoritative method of authentication, but recent court cases in the US and elsewhere have raised fundamental doubts about fingerprint reliability. Other biometric methods are promising (retinal and fingerprint scans are an example), but have shown themselves to be easily spoofable in practice. Hybrid or two-tiered authentication methods offer a compelling solution, such as private keys encrypted by fingerprint inside of a USB device. In a computer data context, cryptographic methods have been developed (digital signature and challenge-response authentication) which are currently not spoofable

if and only if the originator's key has not been compromised. That the originator (or anyone other than an attacker) knows (or doesn't know) about a compromise is irrelevant. It is not known whether these cryptographically based authentication methods are provably secure since unanticipated mathematical developments may make them vulnerable to attack in future. If that were to occur, it may call into question much of the authentication in the past. In particular, a digitally signed contract may be questioned when a new attack on the cryptography underlying the signature is discovered.

3.0 PROBLEM DEFINITION

There are inherent weaknesses in the use of a single-factor authentication system, especially when the critical resource is been secured. Some of the weaknesses of single-factor authentication are listed as follows: Weakness of Single Sign-On Systems. Once the username and password is stolen, the system is compromised. Users often use the same username and password for all the systems they access. Thus, compromising one system is equivalent to compromise others too. Not all username and password combinations are strong or complex enough. Password secured systems can be subject to a dictionary attack. Single sign-on systems are not suitable for some sensitive operations or environments E.g. Securing nuclear weapons, internet banking,

symmetric keys of an encrypted system. The work is aimed at the development of a two-factor authentication system using a combination of any of the methods listed above; which will be built using best-practices in system design and software development.

In this work, we will propose an alternative approach to authenticating secure systems which will consist of the following approaches such as :- The multifactor authentication approach. Here, users are prompted for more than one security challenge before they are given access to a secure system. Also, The number of challenges and the complexity of each challenge depends on the criticality of the resource been secured. The convention “n-factor authentication” means the n (a positive numeric value) is the number of tests or challenges a user must pass before he can be given access to the system. However, in most systems a Two-factor authentication system is sufficient to secure the resources in question.

3.1 AUTHENTICATION FACTORS THAT CAN BE COMBINED IN A MULTIFACTOR AUTHENTICATION SYSTEM INCLUDES;

Passwords: A password or personal identification number (PIN) is the most common form of authentication. Used by itself, even a long, complex password is not considered a form of strong authentication. But it can be a crucial component of a two-factor authentication system.

Knowledge-Based authentication (KBA): KBA tests the user's ability to correctly answer “personal” questions, such as favorite color, place of birth or even highly personal financial data such as mortgage payment size for authentication. This is commonly deployed to help protect online applications as a secondary form of authentication.

One-Time Password Tokens: These devices generate a unique password every 60 seconds or so. Users must enter a password matching the one generated by the synchronized password server for authentication. While highly secure, these systems have a few drawbacks, including the need for users to carry devices and to enter the password quickly enough. They can also be expensive in widespread deployments, especially as users lose or break them.

Digital Certificates: Digital certificates are the electronic IDs used in public key infrastructure (PKI) systems. Typically implemented on smart cards or USB keys, they can also be implemented directly in software on a user's computer. PKI systems provide a highly reliable authentication infrastructure suitable for widespread deployments in virtually any type of environment. When implemented in software or on a USB device, digital certificates require no dedicated reader, although readers are required for smart cards. Both USB and smart card versions do require users to have the device with them at all login

times, however; they also require the IT department to manage the devices, including the ability to disable and re-issue a lost or stolen device. Implementing digital certificates in software directly on the user's computer addresses those issues, but makes the certificate less versatile, as it can only be used for the one computer.

Grid Cards: Each user is provided with a personalized matrix of numbers and letters[7,8,14]. During authentication, the user is challenged to input entries from particular cells on their Grid. If these responses match the known, assigned Grid entries, the user is authenticated. Grids are desirable for their low cost and flexibility; grids can have dedicated cards, be printed on credit cards or easily distributed via email or fax.

Out of Band Authentication : This emerging technology leverages devices users already have, such as a cell phone, Blackberry or even their computer instead of dedicated one-time password tokens. For example, a one-time password is generated and sent via text messaging to the user's Blackberry or the user is called on their cell phone to enter their PIN.

Biometrics : This category includes fingerprint readers, face topology and eye scans. These systems are generally highly secure because biometric features are unique to each individual. Biometrics do not require the user to remember anything and are considered fairly

difficult (although not impossible) to spoof. On occasion, valid users will encounter false negative readings, such as when their appearance is altered for whatever reason. Less expensive alternatives rely on behavioral, rather than physical, features such as the unique rhythm to the way each user types in their password

Risk-Based Authentication :An emerging authentication technology relies on a number of passive factors, including geography and usage patterns, to assess the degree of risk associated with a login. High risk logins will trigger the application to challenge users for a second form of authentication. For example, a user typically logs in to his bank account from his home computer between 7 p.m. and 10 p.m. If a login to his account is attempted at 3a.m. from a computer in a foreign country, that red flag would prompt an additional level of authentication.

Device ID :Leverages the user's computer as a secondary attribute by which to identify the user. When a user authenticates for the first time, a “snapshot” of publicly available device information is taken such as Internet browser type and version. Should the user login from a device varying significantly from their stored profile, the user will be prompted with an additional layer of authentication. In most instances, one of these authentication methods will be used along with a traditional password or PIN, thus providing for two-factor authentication.

That is particularly true for the token-based schemes. Because tokens can be lost or stolen, it's especially important to have the second authentication method as a backup. It is not necessary to implement strong, multi-factor authentication for all users at the same time. With the proper identity and access management solutions in place, organizations can support a mix of authentication methods, as well as smooth transitions from one to another when requirements dictate. Policy-based management makes it simple for organizations to match the level of authentication to the level of risk associated with different applications. For example, a smart card may be required to access high-risk applications, while a simple login and password is sufficient for certain low-risk applications.

3.2 GUIDELINES FOR DEPLOYMENT AND MANAGEMENT OF STRONG AUTHENTICATION

The tools you use to manage your authentication infrastructure and the policies you put in place to dictate who can access which resources are as important as your chosen authentication technologies.

Strong authentication deployments require multiple components to function effectively as a whole. These components include the enterprise directory and access management system, an authentication server, multiple authentication

technologies and devices as well as tools for provisioning and de-provisioning credentials to the myriad applications that users ultimately need to access. Given all these moving parts, a comprehensive management infrastructure is crucial. A key discipline to keep in mind is user credential lifecycle management. That means managing authentication credentials for employees (or business partners, customers, etc.) from the time they join the company, through their inevitable role changes, to the time they leave. Below are some of the functions that an effective strong authentication management system should handle.

Defining who is authorized to access which resource, using which forms of authentication, requires construction of policies that cover each circumstance. Some of the criteria to consider include:

Equate Authentication, to Risk If a user is logging in at an odd time, or from a new location, it may warrant more suspicion. In such instances, your policy could dictate that such users be asked for an additional level of authentication, such as answering a KBA question.

Make Them Flexible In an ideal world, security should never prevent a user from being productive. Flexible policies help make sure that doesn't happen. For example, you can build fallback mechanisms into your policies such that if a user forgets his smart card, he can use a

login/password combination to access limited resources until he can be fully authenticated.

Support Multiple Authentication Types Users with similar relationships to or function in an organization will likely need to access using similar authentication methods. For example, a role-based policy could define that all "high net worth" financial customers, have the option of accessing their online accounts using a one-time password token.

3.3 POTENTIAL EFFECTS OF TWO FACTOR AUTHENTICATION

In the short term, two factor authentications will cut down the phishing and other online banking attacks. By adding the second factor of authentication, attackers will have a more difficult time trying to grab the full credentials from unsuspecting victims. This is the primary benefit that everyone expects when implementing two factor authentication. The early adopters of an extra factor in authentication will see a drastic decrease in attacks simply because the attackers just move on to attack the weaker ones.

With the increasing electronification of business, it is easier than ever to obtain another person's identifying information, and perpetrate identity fraud. To detect fraudulent or stolen identities and stem the increasing tide of losses due to identity fraud, financial institutions need to employ

systems that will enable them to stay one step ahead of potential frauds. Implementing a multi-factor authentication process, performed upon the opening of a new account, can help to accomplish this. Multi-factor authentication consists of verifying and validating the authenticity of an identity using more than one validation mechanism.

Generally, this is accomplished by verifying:

- Something you are, in the form of identifying information, or biometric identification, such as an iris scan or a fingerprint.
 - Something you have, for example a driver's license, or a security token.
 - Something you know, such as a password or pin number.

This is not a new concept-it has been a cornerstone of cryptography for centuries. Today, multi-factor authentication is used in numerous applications, from ATM cards that are secured by Personal Identification Numbers (PINs) to websites that are protected by digital certificates and passwords.

Many institutions use an automated system to validate and verify applicants' identifying information. This is a highly effective means of mitigating fraud risk, but as fraudsters become more sophisticated, the means of detecting and preventing identity fraud need to keep pace. An example of multi-factor authentication at the new accounts desk would include performing the

following:

Credential validation - The ability to read and validate information encoded within the magnetic stripe and barcodes of government issued identification.

Identity screening - A system to perform positive and logical verification of furnished customer data.

Fraud detection - Comparing customer information to negative files, both internal and external from across industries, which represent known and/or attempted frauds. By employing multi-factor authentication, financial institutions can lessen vulnerabilities in the account opening process, making it more difficult for those with fraudulent intent to access our nation's financial system.

3.4 USING GRID CARD CHALLENGE IN MULTIFACTOR AUTHENTICATION SYSTEM

A Grid is a collaboration of computational resources, applications, and data that spans multiple domains and institutions. This results in a Virtual Organisation (VO) where users are able to gain access to resources across multiple domains from anywhere on the Internet. The existing middleware developed by the Grid community mainly relies on digital certificates for user authentication. It does not support more advanced authentication techniques such as smart cards, smart tokens, and biometrics. In the

Grid environment, it is expected that scientists or researchers will gain access to Grid resources not only through wired devices such as desktop machines and home computers, but also through wireless devices such as laptops, PDAs and smart phones. This poses problems of supporting user mobility and of secure management of the private keys associated with the certificates. Current Grid Authentication requires that a user's digital certificate be present on each and every device that is used to access the Grid ultimately, this expose the certificate's private key on multiple locations and is considered as a security weakness. Additionally, when a certificate expires, is revoked, or for any reason needs to be updated or removed, the changes would have to be replicated on every device that is used by the user, and this is often a costly and time-consuming process. The use of Remote Repositories manages to solve a part of this problem by having an on-line credential repository for storing the certificates and private keys. Currently, the My Proxy [3] on-line credential repository is used to provide access to Grid resources via Grid

An Authentication Strength Linked Access Control Middleware for the Grid portals. The biggest disadvantage of using Grid portals is that it only allows accesses through a Web browser, thus limiting the types of authentication methods that can be used. Furthermore, 'Smart' devices such as Personal Digital Assistants (PDAs) and smart

phones may not have the computational resources to manage digital certificates. Therefore, alternative, preferably less expensive, authentication techniques should be supported. Other proposed projects, such as Grid Logon often use the Pluggable Authentication Module (PAM) which allows a user to be authenticated with a variety of mechanisms. Our aim is to not only support a variety of mechanisms for authentication, but also to derive authentication strength, or the Level of Assurance (LoA), from the authentication method(s) used. The LoA can be fed into an authorization engine to derive an authorization decision based upon appropriate access control policies. Our work will be based upon an implementation of the recently standardized Web Service Resource Framework (WSRF) specification..

4.0 THE RESEARCH METHOD AND DEVELOPMENT PLATFORM

Before designing the system, it is no gain saying that proper understanding of the overall need and objective of the system be known. As explained the background to the project, a two-factor authentication system can make use of many different security mechanism or factors namely, token-based authentication, grid card, knowledge-base question and answer, biometrics and secret sharing amongst others.

The proposed deliverable of this project is a two-

factor authentication system with the following features:

1. A first factor based on conventional username and password authentication.
2. A second factor based on Grid Card authentication.

4.1 PROCESS FLOWS

The process flow for the proposed application is described below

User Enrollment

1. First Factor User Authentication
2. Second Factor User Authentication

User Enrollment

This process is broken down as follows:

- Administrator logs into the system
- Administrator initiates action to create a new user
- Administrator enters user information E.g. Username, email, password etc
- Administrator generates a grid card to be associated with the user's profile
- Administrator prints the user's Grid Card and hands it to the user

First Factor Authentication

This process is broken down as follows:

- User initiates action to log into the system
- User is prompted for username and password
- Client application captures user response
- Client application makes call to Authentication service

- Client application waits for response from Authentication service
- Authentication service validate the username and password
- Authentication service response with either a VALID USER or INVALID USER feedback (with reason if the feedback is invalid)
- If VALID USER, client application authenticates the user for first factor and then prompt user for second factor challenge.
- If INVALID USER, client application doesn't grant the user access to the system.

Second Factor Authentication

This process is broken down as follows:

- Client application makes call to Authentication Service for a Grid Challenge for the current user
- Authentication Service response with a grid challenge for the current user
- Client application captures the user's response.
- Client application makes call to Authentication Service to authenticate user
- Authentication service response with either a VALID USER or INVALID USER feedback (with reason if the feedback is invalid)
- If VALID USER, client application grants

user access to the system

- If INVALID USER, client application does grant user access to the system

A typical workflow of the process is shown below:

USER
SCREEN

LOGIN

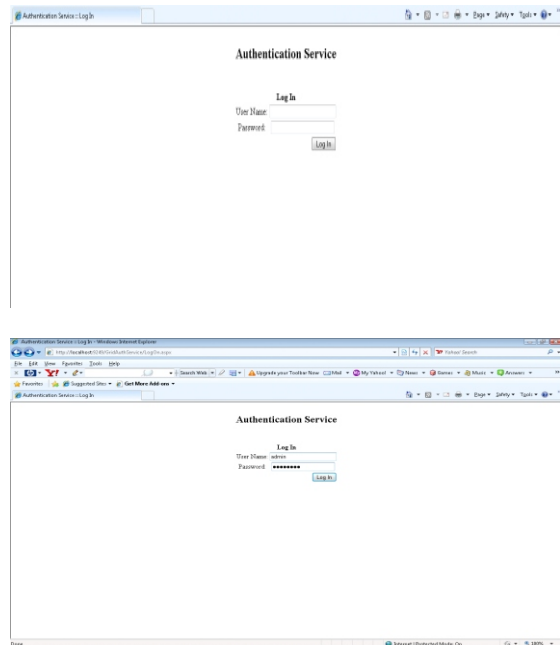


Fig 1.3 User sees in interacting with the application
Fig. 1.4 User enter login details

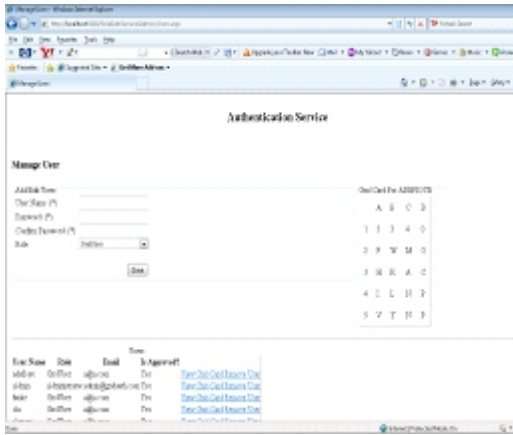


Fig 1.7 Administrator view user “the Grid Card”
Fig1.8 newly created user log into the system.

First Factor: User name and password challenge

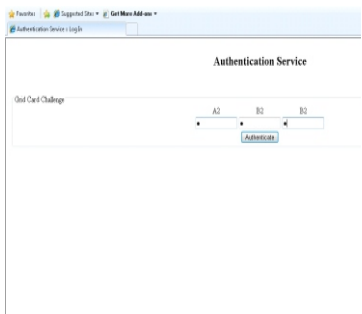


Fig 1.9 The second factors Grid card challenge after passing the first factor challenge.

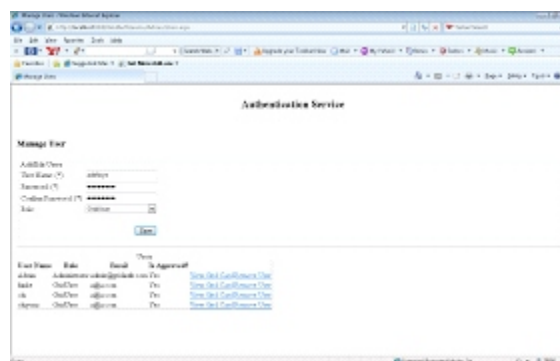
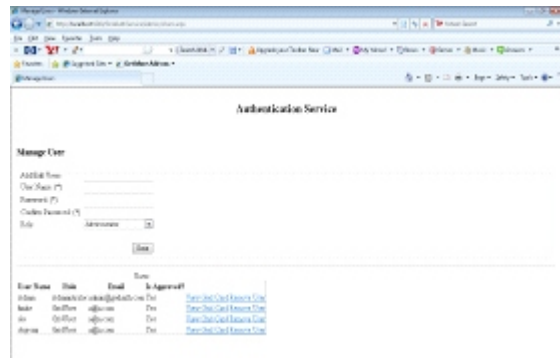


Fig 1.5 create users, edit users and remove users
Fig.1.6 A new user with user name: Adefoeye

.0 CONCLUSION AND CONTRIBUTION TO KNOWLEDGE

Computer Security is an expert area of Computer Science in itself involving extensive research and development. Recent advancement in technology and application accessibility via the internet, mobile devices and other channels have increased the rate at which these application can be compromised by malicious users. Thus, the need to raise the bar on security of the applications we use in our everyday life.

Strong authentication using a multifactor authentication system is one of the approaches that can be adopted for solving the problem of security compromise in most applications. It involves adding another layer of authentication to user profiles, in addition to the tradition Username\Password combination commonly used in most systems.

The additional layer of security can be one of many authentication factors name: Tokens, Grid Cards, Biometrics, Knowledge-Based Questions and Answers, One-Time Password (OTP), Personal Verification Number (PVN), Personal Identification Number (PIN) and many more.

This work has proposed a model that uses a Username\Password authentication as the first factor and a Grid Card challenge as second factor. The implementation uses a simple Service-Oriented Architecture (SOA) with a decoupled design of the client application from the

authentication service. Thus, making it possible for any client application to reuse the authentication service for security as its functions. The application is written entirely in the C# programming language. The client application is a web based system that depicts the process of creating users and generating grid cards. Users are able to login and pass through both the first factor and second factor authentication before accessing the system.

In this paper, we propose a new authentication scheme based on Grid card and multi-factor authentication. Our approach can be effectively and securely used as user-friendly authentication mechanism for public and un-trusted terminals. Our proposed solution is unique in many ways which are:

We never assume the handheld device is trusted and our method doesn't need a "familiarization" or a lengthy "password setup" process.

We can apply our system to more than just Authentication mechanisms: our system is applicable anywhere that there is a need to enter sensitive or private data.

REFERENCES

[1] Butler R, Welch, V.; Engert, D.; Foster, I.; Tuecke, S.; Volmer, J.; Kesselman, C(Dec. 2000,) "A national-scale authentication infrastructure", Computer Volume: 33 Issue: Page(s): 60-66. 12

- [2] Chiasson S, Biddle R, and Oorschot P. C. (2007,),"A second look at the usability of click-based graphical passwords," in *Proceedings of the 3rd symposium on Usable privacy and security* Pittsburgh, Pennsylvania, pp. 1-12.
- [3] Czajkowski, K., Ferguson, D., Foster, I., Frey, J., Graham, S., Sedukhin, I., Snelling, D., Tuecke, S., Vambenepe, W. 2004. The WS-Resource Framework.
- [4] Dhamija R. and Perrig A. (2000), "Déjà Vu: a user study using images for authentication," USENIX Association Berkeley, CA, USA, pp. 4-4.
- [5] Foster, I. Kesselman, C., and Tuecke, S. (2001.)The Anatomy of the Grid: Enabling Scalable Virtual Organizations. International J. Supercomputer Applications, 15(3), 200-222
- [6] Geer D, (2005). "Security technologies go phishing,"*Computer*, vol 38, pp. 18-21
- [7] Goble, C.A , Pettier S, Stevens R. and Greenhalgh C., (2003) Knowledge Integration: In silico Experiments in Bioinformatics in The Grid: Blueprint for a New Computing Infrastructure Second Edition eds. Ian Foster and Carl Kesselman, Morgan Kaufman,.
- [8] Graham J.A., Tom Maguire E.R, David Snelling Steve Tuecke,(03/05/2004) From Open Grid Services Infrastructure to WS Resource Framework: Refactoring & Evolution.
- [9] Klein D. V,(1990) "Foiling the Cracker: A Survey of and Improvements to, Password Security," Proceedings of the USENIX UNIX Security Workshop,(Portland)
- [10] Kumar M, Garfinkel, D and Winograd, T.(2007) "Reducing shoulder-surfing by using gaze-based password entry," *Proceedings of the 3rd symposium on Usable privacy and security*, pp. 13-19
- [11] Mannan M. and Oorschot P. C. van,(2007.) "using a Personal Device to Strengthen Password Authentication from an Untrusted Computer," Financial Cryptography and Data Security (FC'07)
- [12] Pering T, Sunda M, and Want R ,(2003) "Photographic authentication through untrusted terminals," *Pervasive Computing, IEEE*, vol. 2, pp. 30-36
- [13] S. G. M Wu, Miller R (2004)"Secure Web Authentication with Mobile Phones," in *DIMACS Workshop on Usable Privacy and Security Software*
- [14] Wiedenbeck S, Waters J, Birget C, Brodskiy A, and Memon N (2005.)Design and longitudinal evaluation of a graphical password system," *International Journal of Human-Computer Studies*, vol. 63, pp. 102-127
- [15] Zhang N, Chin J., Rector A, Goble C, Y. Li, (September 2004.)"Towards an Authentication Middleware to Support Ubiquitous Web Access", In proceedings of the 28th Annual International Computer Software & Applications Conference.