"Introduction and Limitation of 2 Wmas"

Inderpal Singh Oberoi

Research Scholar CMJ University, Shillong, Meghalaya

Abstract – Even though many organizations still rely on static ID and password authentication system, this method is getting old and there is a requirement for a better way of authentication which is required. One of the solutions for this issue is the two factor authentication technique as a fundamental security function. Our dissertation proposal explores the two factor authentication technique and implementation issues which can be used for the two factor authentication technique. We implement Two-factor authentication method in two main phases. In the first phase, the authenticator gets a request generated by the application to authenticate a specified user. When the request is received, it generates a one-time password and sends it through a SMS to a GSM cell phone registered for that specified user.

Key Words: Authentication, Password.

----------♦----------

INTRODUCTION

The typical implementation methods of OTP include Time Synchronization and Challenge/Response. No matter what methods are used to realize dynamic property of password for each authentication, the core is to ensure the randomness of factors added into the authentication. Many current OTP applications use mathematic methods like Hash function for dynamic passwords but still will suffer potential attacked risks Using static passwords for authentication, as it is commonly done, has quite a few security drawbacks: passwords can be guessed, forgotten, written down and stolen, eavesdropped or deliberately being told to other people. A better, more secure way of authentication is the so called "two-factor" or "strong authentication" based on one time passwords, instead of authenticating with a simple password. Strong authentication solutions using two identification factors require often an additional device, which could be inconvenient for the user and costly for the service providers. To avoid the usage of additional device, the mobile phone is used to receive the onetime password.

REVIEW OF LITERATURE:

In most cases the data has to be unencrypted at some time when it is inside the cloud. Some operations would be simply impossible to do with encrypted data and, furthermore, doing computations with the encrypted data would consume more computing resources (and more money, in consequence). There are recent steps towards dealing with this issue. One is the Trusted Cloud Computing Platform, which aims to apply the Trusted Computing model (developed in 2003 by Intel, AMD, HP, and IBM) to the cloud. However the scope of this initiative is to protect against malicious insiders, inside the cloud provider organization.

Another paper of the Microsoft Cryptography Group is a "searchable encryption mechanism" introduced by Kamara and Lauter in [2008]. The underlying process in this system is based on a local application, installed on the user's machine, composed of three modules: a data processor, a data verifier, and a token generator. The user encrypts the data before uploading it to the cloud. When some data is required, the user uses the token generator to generate a token and a decryption key. The token is sent to the cloud, the selected encrypted file(s) are downloaded, and then these files are verified locally and decrypted using the key. Sharing is enabled by sending the token and decryption key to another user that you want to collaborate with. The enterprise version of the solution consists of adding a credential generator to simplify the collaboration process. Other relevant papers are also being conducted. One example is a recently published PhD dissertation from Stanford University done by Craig Gentry in collaboration with IBM. This research proposes "A fully holomorphic encryption scheme". Using their proposed encryption method data can be searched, sorted, and processed without decrypting it. The innovation here is the refreshing mechanism necessary to maintain low levels of noise. Although successful, both initiatives have turned out to be still too slow and result it very low efficiency. As a result, they are not commercially

utilized yet.

RESULT & ANALYSIS

2 Way Mobile Authentication System (2WMAS) is an innovative authentication system that provides access to Web-based resources by using a two- way user authentication through the existing personal mobile phones. It is used to solve the security flaws of the web based Internet and Intranet, by involving the users to authenticate themselves using their personal mobile phones. The registration of the users has to be done in a secured manner before he can actually use the system.

It is designed to provide security to Web-based Internet and Intranet applications, and requires users to authenticate themselves with two unique criterion - a username and password, and a code which they get only during authentication before they are permitted to access a secured web resource. With 2WMAS, we can positively identify users and deliver services easily and in a most secured way to users, without having the need of an additional security system. End users can have the advantages of a very simple process that omits the need to remember multiple passwords.

As the Web-based Internet becomes the most important tool for financial transactions, the level of security becomes a major concern in an organization's transaction system. Transactions in these days are secured using passwords. Institutions spend huge amounts of money on secure SSL solutions to make sure the passwords are not tracked. But, in majority of cases security violations occurs above the reach of PKI and SSL solutions.

FEATURES OF 2 WAY MOBILE AUTHENTICATION SYSTEMS

Double-criterion to check the identity of the User : It provides a cost-effective solution to provide the web resources with a double- criterion authentication system. Through a browser, a user requests permission to access a Web resource which needs an additional authentication code required for the Web Application. It then generates a one-time access code and sends it to the mobile phone registered to the user by an SMS text message. The user has to enter the access code into the Web-browser to finish the authentication. After the user enters the authentication information, the system determines if the information submitted is valid or not. If valid it goes ahead with the Web Application thereby allowing the user to perform the necessary transactions, otherwise not .By separating Web Application with Authentication server, we can also divide the responsibilities to decrease the internal fraud.

LIMITATIONS ON 2 WAY MOBILE AUTHENTICATION SYSTEMS

1. 2 Way Mobile Authentication cannot solve the problem of phishing (phishing is defined as a process of gathering personal data such as credentials, information of the credit cards and other sensitive data by impersonating as a trusted party through electronic communication).

2. A user cannot login to the system if the GSM gateway service provider's servers are down where he could not receive the OTP even though he is a genuine user.

3. This system cannot be used when a user's mobile network service provider terminates the connection due to the delay in bill payments and also poor signal of the network.

CONCLUSIONS:

In our study we found that one of the major areas of security improvement is the way in which authentication of users is carried out. Even though many organizations still rely on static ID and password authentication system, this method is getting old and there is a requirement for a better way of authentication which is required. One of the solutions for this issue is the two factor authentication technique as a fundamental security function. Our thesis proposal explores the two factor authentication technique and implementation issues which can be used for the two factor authentication technique.

We implement Two-factor authentication method in two main phases. In the first phase, the authenticator gets a request generated by the application to authenticate a specified user. When the request is received, it generates a one-time password and sends it through a SMS to a GSM cell phone registered for that specified user.

REFERENCES:

[1] Y. Kim, IL. Moon and S. Cho: A Comparison of Improved AODV Routing Protocol Based IEEE802.11 and IEEE802.15.4", Journal of Engineering Science and Technology Vol. 4, No. 2, 2009, pp. 132 - 141

[2] V. Talooki and K. Ziarati, "Performance Comparison of Routing Protocols For Mobile Ad Hoc Networks" Asia-Pacific Conference on Communications, APCC, 2006.

[3] A. Wierman and T. Osogami "A Unified Framework

for Modeling TCP-Vegas, TCP-SACK, and TCP Reno", Technical Report CMU-CS-02.133, School of Computer Science Carnegie Mellon University Pittsburgh, May 2003.

[4] S. A. Kulkarni and G. R. Rao, “Mobility and Energy –Based Analysis of Temporally Ordered Routing Algorithm for Ad Hoc Networks, IETE Technical Review, Vol. 25, Issue 4, 2008.

[5] A. Zahary, A. Ayesh, “Analytical Study to Detect Threshold Number of Efficient Routes in Multipath AODV Extensions”, proceedings of International Conference of Computer Engineering and Systems, ICCES, 2007.

[6] Stajmenovic Ivan, “Handbook of Wireless Networks and Mobile Computing”, Wiley Publications, India, 2002.

[7] S.Capkun, L.Buttyan and J.-P. Hubaux, “ Self-organised Public- Key Management for Mobile Ad-Hoc network”, IEEE transactions on Mobile Computing , Vol.2 , pp. 52- 64,2003.

[8] Z. J. Haas, J.Deng, B. Liang, P.Papadimitratos and S. Sajama, “ Wireless Ad-Hoc Networks” in Encyclopedia Of Telecommunications. John Willey, 2002.