International Journal of Information Technology and Management

Vol. VI, Issue No. I, February-2014, ISSN 2249-4510

REQUIREMENT & ARCHITECTURE OF TWO WAY AUTHENTICATION

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. VI, Issue No. I, February-2014, ISSN 2249-4510

Requirement & Architecture of Two Way Authentication

Inderpal Singh Oberoi

Research Scholar CMJ University, Shillong, Meghalaya

Abstract – The ever increasing use of internet around the world has without doubt increased the usage of internet based services, e-business models, easier ways of communication and information sharing. Such drastic increase in usage of network based systems has made the current cyber security systems old dated as the hackers and attackers of networked systems is on the rise with new and modern attack methodologies. This has necessitated the need of more secure ways of communications. The issues of Confidentiality, Integrity and the Availability of systems are of prime importance and more research towards these issues has been called for around the world.

Key Words : Network, E-Business, Communication.

----------♦----------

INTRODUCTION

Dynamic password (One-Time-Password) technology is a sequence password system and is the only password system proved non-decrypted in theory. Its basic idea is to add uncertain factor in authentication so that users need to provide different messages for authentication each time. By this way, the applications themselves can obtain higher security guarantee than those use static password technology. 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:

The distributed nature of the cloud model necessarily involves more transits of data over networks, thus creating new challenging security risks. The confidentiality of the data must be assured whether it is at rest (i.e. data stored in the cloud) or in transit (i.e. to and from the cloud). It would be desirable to provide a closed box execution environment where the integrity and confidentiality of the data could be verified by its owner. While encryption is an answer to securely storing data in the cloud, it does not fit that well with cloud-based processing. This later problem occurs because generally the cloud both stores data and applications running on the cloud operate on this data. 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.

SMS GATEWAY SERVICE PROVIDER

SMS has shown significant resilience in market that is bombarded with media that all add to the clutter of daily Communications. SMS is a form of highly personal, immediate communication with high reach capability, low cost and high retention levels. With communications media converging, SMS is now accessible in many ways as a business tool. Sms Country is an SMS Gateway provider, which provides an interface between an existing systems and the SMS Messaging Gateway.

It is a lower level connectivity option, but offers the very good functionality and flexibility for the end user. With the API Sms Country can set up alert-based SMS delivery from Sms Country's server. Depending on the messaging requirements, Sms Country may find one or more of Sms Country's products to suit Sms Country needs, out of which they have opted HTTP API which is gives us the easy ways in order to connect to the Sms Country API for sending SMS.

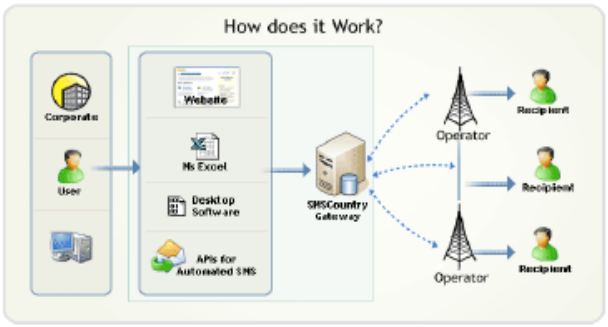

Fig 1: Sms Country API Working Process

ARCHITECTURE OF TWO WAY AUTHENTICATION

Two ways Authentication System Architecture is as below. In Two way Authentication System user submit a their credentials and that credentials goes to server which is checked that credentials after that if credentials is valid its goes to next step that is generate a code and send it to registered mobile number after and system waiting for that code to be entered. After receiving code user submit this code to system and system verified that it's the right code or not if the code is right then user get welcome page else system goes on login page.

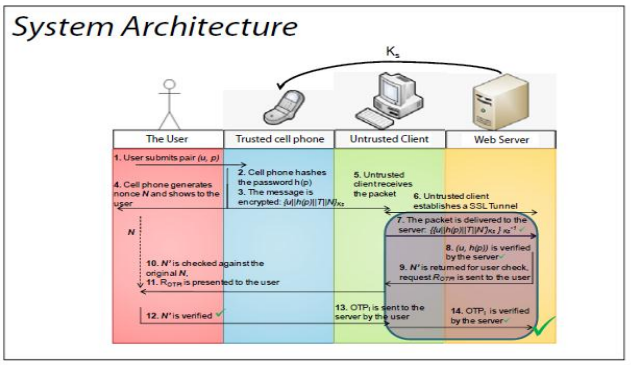

Fig 2: System Architecture of 2WAS

With the help of two way authentication we can easily able to secure our id and password from unauthorised access. Authentication scenario is as demonstrate in above diagram.

FUTURE WORK:

Probing deeper, the demo application in this paper also provide a strong foundation for future work in Two Factor authentication for security applications. Future developments include a more user friendly GUI and extending the OTP algorithm so that password can be generated based on different cryptographic functions. In addition to that we can add features such as giving as choice to the user to choose from different ways to authenticate him to the system to which he was supposed to authenticate.

REFERENCES

[1] B. Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley, 2nd Edition, 1995.

[2] Michael Pearce, Ray Hunt, Sherali Zeadally. Assessing and Improving Authentication Confidence Management, University of Canterbury, New Zealand and University of the District of Columbia.

[3] Suzumura T, Trent S, Tatsubori M, Tozawa A, Onodera T. Performance comparison of Web Service Engines in PHP, Java and C,IEEE International Conference on Web Services 2008.

[4] George Schlossnagle, Advanced PHP programming.

[5] Naphtali Rishe, Khaled Naboulsi, Ouri Wolfson, Bryon Ehlmann. An Efficient Web-based

Semantic SQL Query Generator. High Performance Database Research Center, Florida International University.

[6] Muhammad Saleem, Kyung-Goo Doh. Generic Information System Using SMS Gateway. Fourth International Conference on Computer Sciences and Convergence Information Technology 2009.

[7] Do van Thanh Jorstad, I.Jonvik, and T.Do Van Thuan. Strong Authentication with Mobile Phone as Security Token, Mobile Adhoc and Sensor Systems, 2009. IEEE 6th International Conference.

[8] Aloul F, Zahidi S, El-Hajj W. Two Factor Authentication Using Mobile Phones, IEEE/ACS International Conference on Computer Systems and Applications.