International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 06, June 2015
Available at http://internationaljournalofresearch.org

An Alternate Approach to User Registration using QR Codes

Prof. Shiv Kumar Goel
Assistant Prof/Deputy HOD, MCA Department,

Balakrishnan Venkatachalapathi
Vivekananda Institute of Technology Collectors Colony, Chembur, Mumbai – 400074 India

Abstract

This paper outlines a password-less authentication approach with aims to replace or supplement other authentication schemes. The method focuses on solving conventional authentication pitfalls, while improving ease of use and convenience of implementation. The vast feature set and the affordability provided by the smartphones of today makes them a suitable candidate for the development of such a solution. A QR Code is presented to the user on the smartphone which contains the information required to authenticate him. The user scans the QR Code and sets off. An authentication and registration mechanism which executes in a matter of seconds. The approach also eliminates the need to enter your personal details for various services. The standardization of such an approach will result in a system which can be used ubiquitously and implemented mechanically for smartphones of all kinds.

Introduction

Registration and Authentication mechanisms have remained the same for a significant period of time, with the underlying principles unchanged. Although, the conventional system has become considerably secure over the years, it still a time consuming process to enter the personal details for every registration.

- Registration is time consuming
- Same document need to be verified
- Storage of documents

The solution proposed in this paper hopes to leverage the smartphone as an authenticating tool to negate the drawbacks of the other methods while providing comparable security. The key component of the proposed method, the QR Code can be replaced with any other medium capable of holding information which can be interpreted by the smartphone, if necessary. The functional prototype developed using the technique in this paper was effective in providing a quick and secure authentication process.

Background

A. Platform Suitability

The smartphone has come to dominate the mobile segment in the past couple of years. The extensive feature set provided by the smartphone makes it the ideal device for development. By choosing the smartphone, we aim to minimize the hardware investment encountered in other authentication techniques.

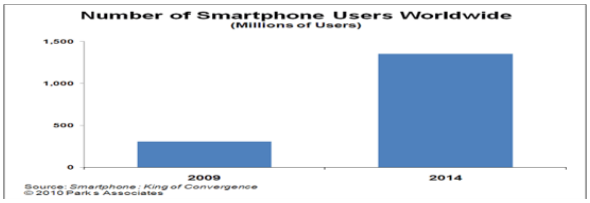

Figure 1:
Smartphone Usage Statistics

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 06, June 2015
Available at http://internationaljournalofresearch.org

With statistics indicating that smartphone penetration and popularity will increase significantly in the future, it becomes the most suited for the development of the proposed mechanism.

B. The QR Code

The QR (Quick Response) Code is a two-dimensional (2-D) matrix code that can be read by many cell phones and smartphones.

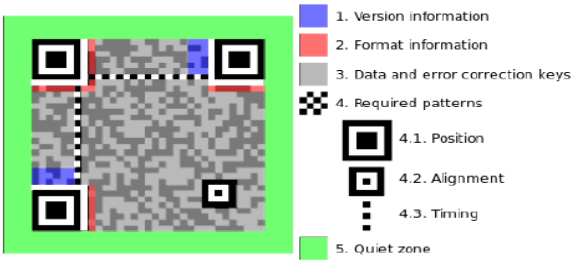

Figure 2:
The QR Code

Advanced error-correction method and other unique characteristics allow the QR Code to be read more reliably and at higher speeds than other codes. While conventional bar codes are capable of storing a maximum of approximately 20 digits, QR Code is capable of handling several dozen to several hundred times more information. Error correction mechanisms and higher content capacity of the QR code makes it favorable for this system.

C. Prerequisites

The system assumes the availability of the following.

1. A smartphone with a camera and Internet access
2. The suggested application be installed on the device
3. The user has verified his document with the verification authority

D. Methodology

Step 1: The application on the registered smartphone authenticates itself with the server of the proposed system and becomes ready to be used with other services.

Step 2: The user navigates to a web service which implements the suggested system of QR Code authentication. This can be done using any standards compliant browser on any platform. The server will now generate a QR Code using a proposed technique.

Step 3: The requester now scans the generated QR Code and derives relevant information from it. The device initiates the authentication and registration process and redirects to the required page if successful.

E. Registration Process

The mechanism requires the user to be registered with a trustworthy authority capable of providing the authentication services.

Step 1: The user registers conventionally by providing an E-Mail Address and a PIN.

Step 2: The E-Mail addresses is verified to establish the identity of the user using a verification E-Mail. The user need to submit the required document verified by verifying authority.

Step 3: A unique User Identification Code is generated for the newly registered user. A key pair is exchanged securely between the device and the authentication gateway. The PIN code is used to keep the authenticating application secure from unauthorized usage.

F. Usage

The proposed mechanism can be used by Telephone operator to get new SIM. Every time a user applies for a new SIM the person has to enter and give his details to the appropriate Telephone operator. This become a tedious job as the proof will remain the same for life time. So the activation which takes 24 hours can be completed in just 24 minutes. The verification authority plays a crucial role as the user need to do their verification and submit the required document to the verification authority.

Conclusion

The process tries to negate the vulnerabilities caused by manual input, brute forcing and keyboard cracking, shoulder surfing and password guessing. If the device is stolen, the application still remains secure due to the inbuilt pin mechanism and the ability to deactivate the lost device from the user's web interface. The technique can be easily implemented using various technique and for various personal identity authorization offering considerable flexibility. An API can be created to facilitate the implementation of this mechanism easily on various services. The future scope of such a technique would be to study the possibility of authenticating the user himself using the smartphone's feature set instead of the device alone as an authentication token.

References:

[1] M. Bishop, Computer Security: Art and Science. Pub-AW:adr: Addison-Wesley, 2003.

[2] M. L. Das, A. Saxena, and V. P. Gulati, “A dynamic ID-based remote user authentication scheme,” CoRR, vol. abs/0712.2235, 2007.Denso-Wave, “About 2d code,”

[3] FIPS, Advanced Encryption Standard (AES). National Institute for Standards and Technology, pub-NIST:adr, Nov. 2001.

[4] National Institute of Standards and Technology, FIPS PUB 186-2: Digital Signature Standard (DSS). pub-NIST:adr: National Institute for Standards and Technology, Jan. 2000.

[5] RSA Laboratories, PKCS #1 v2.1: RSA Cryptography Standard. RSA Data Security, Inc., pub-RSA:adr, June 2002.

[6] W. Stallings, Cryptography and Network Security: Principles and Practice. Pearson Education, 3rd ed., 2002.