International Journal of Computer and Internet Security.
ISSN 0974-2247 Volume 5, Number 2 (2013), pp. 43-50

http://www.irphouse.com

Second Level Authentication Using QR Codes

Mukund Sarma

Dept. Of Computer Science, Amrita School of Engineering
Amritanagar, Coimbatore-641112, Tamilnadu, India.
mukundsarma9@gmail.com

Abstract

User authentication is one of the fundamental procedures to ensure secure communication and to share resources over an insecure public network channel. For this a simple and efficient authentication mechanism is required for securing a network system in the real environment. In general, a password-based authentication mechanism provides the basic capability to prevent unauthorized access. Instead of using the password file as conventional authentication systems, many researchers have tried to implement various one-time password schemes using smart cards, time-synchronized token or short message service. This helps to reduce the risk of tampering and maintenance cost. However these schemes are impractical because of the far from ubiquitous hardware devices or the infrastructure requirements. To remedy these weaknesses, the use of the QR (Quick Response) code technique can be introduced into one-time password authentication protocol. For every session, a different QR image appears on the web site by constructing the QR for the Hash Value of a Random Number, Date and Time of the access of Server, all combined. The Hash value will be unique and hence works like a One-Time Pad. Using out of Band (OOB) channel, the second level authentication happens from Mobile Scanning App for QR and using Internet/GPRS channel the server is reached from Mobile for authentication. QR code not only eliminates the usage of the password verification table, but also is a cost effective solution since most Internet users already have mobile phones. For this reason, instead of carrying around a separate hardware token for each security domain, the mobile phone makes our approach more practical and convenient.

Keywords— Quick Response (QR) code, Out of Band (OOB), IMEI (International Mobile Station Equipment Identity), IMSI (*International Mobile Subscriber Identity*), TRNG (True Random Number Generator), AES (Advanced Encryption Standard).

Introduction

With the number of people using smart phones increasing, more people are connected to the internet through mobile devices. The amount of money being transferred electronically has grown with the explosive growth of the dot com businesses. In a number of places a user has to be authorised securely for monetary, legal, social and medical services. In the age of Ubiquitous computing enabled by Internet of Things technology and Cloud computing technology, breach in cyber security can have serious impacts on the real world. The identity assurance is implemented by checking for one or more of the following three factors: Proof of knowledge; Proof of Possession; Proof of characteristics. Single level knowledge based authentication techniques that check for one of the above mentioned factors are the most popular and have been proven to be insecure and have led to security breaches. In areas where security is of prime concern, second level or multi-level authentication systems becomes mandatory.

Second Level Authentication

Authentication is the act of confirming the truth of an attribute of a datum or entity. Authentication in its most basic form is implemented in the form of user-names and associated passwords which is the most commonly seen method to confirm a person's identity on the Internet. However, a single set of values is not 100% safe and so people are looking for methods to make the authentication technique foolproof. As a result, second level authentication techniques have been developed to increase the security of accounts on the Internet [1].

Multi-factor authentication (also Two-factor authentication, TFA, T-FA or 2FA) is an approach to authentication which requires the presentation of two or more of the three authentication factors: a *knowledge* factor ("something the user *knows*"), a *possession* factor ("something the user *has*"), and an *inherence* factor ("something the user *is*") [2].

Two-factor authentication seeks to decrease the probability that the requester is presenting false evidence of his/her identity. So, for authentication the user needs to submit a set of values that the he/she knows (such as the username and password) or produce something he/she possesses (such as a token or smartcard) or something that he/she is (biometric information such as fingerprint or retina scan).

Existing systems and drawbacks:

The most popular way of providing a second level authentication is by checking for proof of knowledge and for proof of possession. Though checking for proof of characteristics through biometric authentication [8] provides greater security the cost of implementation is too high.

The most popular technology is to provide user with tokens which generate one time password based on a mathematical problem or a crypto function or by random number generation. Time synchronization between client and server is ensured and the challenge is that the password is generated by a dynamic nondeterministic system.

The password is delivered to the client by hardware or software token.

The issue with the current system is that if the token is lost, the recovery is difficult. Requiring the user to carry additional hardware decreases the suitability of the system.

Another popular technology is SMS based one-time password where the client provides a phone number at registration time to which the service provider sends a One Time Password (OTP) over SMS when the user logs in. When received by the user on the phone, the client then enters it on the PC interface. By verifying the presented OTP, the server can be confident that the user is indeed the owner of the phone and therefore the account holder. Another variation to this is where the server creates a one time phone number and presents it to the user through the PC-channel. The user then calls this number from a phone with a previously registered number. The server, by verifying that the call came from a registered number, can be confident that the user is the account holder.

SMS (Short Message Service) or telephone based methods are vulnerable to a type of attack known as the man-in-the-middle attack because of the physical disconnect between the authorised device and the authentication entity.

One of the latest developments in the industry, which is of immense interest to the developers of security techniques, is the use of QR codes in many web applications. The basic concept behind QR codes is the barcode, and has been in use in the industry since the 1970s. QR codes in their present form were developed in the recent past, when they were and are still being used in production control of automotive parts in Japan and Korea.

A quick response (QR) code is a two dimensional barcode that can be read on devices such as a mobile phone with camera or a laptop computer which, once accessed, allows you to complete an action such as reading some text, accessing a web site or texting a number. Mobile phone interprets the QR codes using a decoding software.

These QR codes are increasingly found in places such as product labels, billboards, and buildings, inviting passers-by to pull out their mobile phones.

The two main advantages of QR codes are

- They can hold large amounts of data (upto 4KB) as compared to bar codes which can hold only upto 20 numerical digits.
- QR codes are free to generate and read.

How QR Works

Data can be translated into a QR code by any QR generator, many of which are available for free online. Users enter the data to be translated and the generator produces the code, which can then be displayed electronically or in printed format. Any mobile camera phone that has a QR reader can decode the information. QR readers for camera phones are also available for free online. Once the software is loaded, a user points the cell phone camera at the code and scans it. The software interprets the code and the cell phone either displays the text or ask to launch a browser to display the specific web page [4].Figure 1 illustrates an example of a QR Code.

Figure 1. Example of a QR code.

Proposed system:
The user logs in or registers into a website. Now the user is required to open an application on a smart phone which is protected by a pin number and scan the one time QR code that is displayed using the phone's primary camera. The application then communicates with the server through an out of band channel and provides a proof of possession of the device. Here the user acts as the conduit between the authorised device and the authentication entity.

A new user is asked to register with the website. Theuser is asked to enter login credentials including phone's IMEI and IMSI numbers and logs in with registered credentials. The mobile application is then installed into the user's mobile. Once the mobile application is installed in the user's mobile, the mobile is registered with the server. The user has to choose a pin for further mobile authentication. Now mobile unique ID gets added to list of devices for the user account. From now onwards when the user enters the credentials in the browser, a QR code is displayed. The QR code is scanned and the mobile application PIN is entered when prompted. If the QR and PIN are valid, the user is successfully logged in. Figure 2 illustrates how Second level authentication is achieved using QR codes.

Figure 2. Second level authentication using QR codes.

Generation of Secure QR code:
A physical random number generator [3] can be based on an essentially random atomic or subatomic physical phenomenon whose unpredictability can be traced to the

laws of quantum mechanics. Sources of entropy include radioactive decay, thermal noise, shot noise, avalanche noise in Zener diodes, clock drift, the timing of actual movements of a hard disk read/write head and radio noise.

We consider the threshold noise in electronic circuits [4]. The noise is amplified and sampled. The numeric string is divided into sequences of 512 bits each. Each of this 512 bit number undergoes a Diehard test which checks for the randomness of the number. All those numbers that pass the Diehard test are stored as a bank of true random numbers in the server. These 512 bit numbers are used in generation of QR codes. An image of the 512 bit number is generated. Using the concept of image cryptography two shares of the same image is generated [5] [6]. Share 1 is kept in the server, whereas the share 2 image is used to generate the QR code (A QR code generator is used to generate the QR). This QR is then scanned using the mobile application installed in the user's phone [7]. Once it's scanned, the application returns the share 2 image back to the server along with the date, time IMEI and IMSI numbers through an Out Of Band (OOB) channel. Share 1 and share 2 images are overlapped and the noise from the image is removed and then the combined image is compared with the original image of the random number. If both the images match perfectly the user securely logs in. Each random number is used for a single session and discarded after that session. Replying to the Server through the OOB prevents man in the middle attacks. Figure 3illustrates the various steps on how the shares of a secure QR is created and overlapped.

Figure 3. Screenshot of a Window that shows how a 512 bit random number is made into share 1 & share 2. Overlapping of shares is also shown in the figure.

Sequence Diagram of the proposed idea.

Step 1:
The client machine sends a request to the server.

Step 2:
The server, when it receives the request from a client, first authenticates the client. For this, it generates a random number. This TRNG is split into two shares SH1, SH2. The SH1 is kept with the server. The SH2 along with the timestamp is embedded into the QR code and sent to the client machine and the timer is set.

Step 3:
Once the QR code is received, the user uses his smart phone which is already registered with the server and has its own customized software to scan this QR code. The user has registered his smart phone using the IMEI and IMSI number which is unique to the device. This will authenticate the smart phone. Also a four digit PIN number is used so that the user is authenticated. Only then the legal customized software can scan the QR code. The SH2 and timestamp is obtained from this QR code.

Step 4:
The SH2 and timestamp is then sent to the server through out of band (OOB) channel. The device's IMEI and IMSI numbers are also sent to the server. If this message has come within the time period the server checks the IMEI, IMSI number stored in the registry to authenticate the message. Next, the shares SH1 and SH2 are overlaid. Only if this matches the TRNG stored, the authentication is complete. Now the client and server machine can communicate securely using the SH2 as the key and any algorithm like AES, etc [8]. This way no third party key generators need to be used. Figure 4 illustrates the sequence diagram of the proposed model.

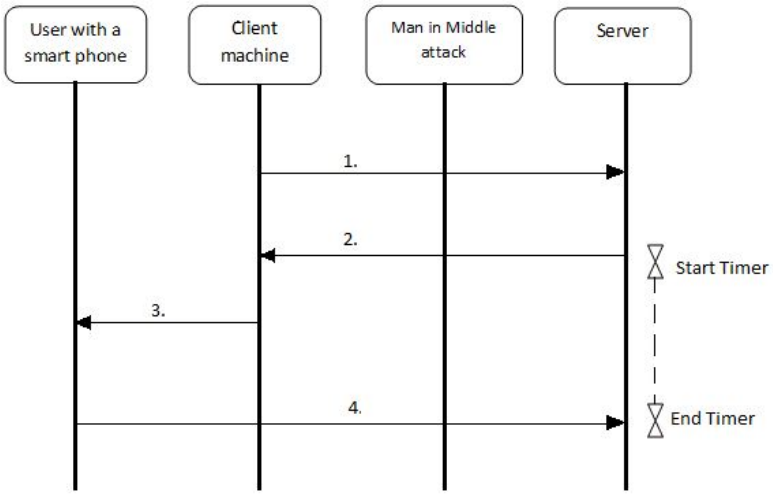

Figure 4. The sequence diagram of the proposed model.

Advantages in using the proposed idea:

Robustness:

- Can be made available in all mobile platforms.
- Secure handover to new phone in case old phone was lost /changed.

Secure:

- The shares are made using highly impregnable visual cryptography algorithms.
- No scope for Man in the middle attacks.
- User authenticated to server via mobile internet/GPRS different from original Server to PC QR origination channel, resulting in enhanced security.
- The QR codes are generated based on TRNG which are always unique and random.
- QR codes are 2D matrix codes with high encryption and decryption speeds, can store large information and feature high error correction ability.

Convenient:

- No need for complex, tricky usernames and passwords.
- Mobile phone more ubiquitous-almost everyone carries one already-compared to other second factor tokens and hardware.
- Zero incremental hardware cost, unlike other alternatives.
- Easy to integrate and easy to use.

Conclusions

This idea can be implemented to achieve security to a great extent in applications such as Net Banking, Online Shopping, detecting Counterfeit products etc. The usage of true random numbers in the generation of QR codes itself makes it very unique and secure. The highlight of this technique is that there is no necessity for carrying external hardware such as tokens and smartcards. These features make it a very attractive option for second level authentication in future projects.

References

[1] Anna Vapen and NahidShahmehri, 2011. 2-clickAuth: Optical Challenge-Response Authentication Using Mobile Handsets.*International Journal of Mobile Computing and Multimedia Communications.* Volume 3, Issue 2, 1-18. DOI:10.4018/jmcmc.2011040101URL:http://dl.acm.org/citation.cfm?id=2440583.2440584&coll=DL&dl=GUIDE&CFID=372999437&CFTOKEN=54817096

[2] Gregory D. Williamson, 2006. Enhanced Authentication in Online Banking.*Journal of Economic Crime Management.* Volume 4, Issue 2.

[3] Vittorio Bagini and Marco Bucci, 1999. A Design of Reliable True Random Number Generator for Cryptographic Applications. Cryptographic Hardware and Embedded Systems, First International Workshop, CHES'99 Worcester, MA, USA, August 12–13, 1999 Proceedings. *Springer Berlin Heidelberg.* 1717: 2014-218 DOI: 10.1007/3-540-48059-5_18 URL: http://link.springer.com/chapter/10.1007%2F3-540-48059-5_18

[4] Michael Epstein, Laszlo Hars, Raymond Krasinski, Martin Rosner and HaoZheng, 2003. Design and Implementation of a True Random Number Generator Based on Digital Circuit Artifacts. Fifth International Workshop, Cologne, Germany, September 8–10, 2003. *Springer Berlin Heidelberg.* 2779: 152-165 URL: http://link.springer.com/chapter/10.1007%2F978-3-540-45238-6_13#page-1

[5] Wen-Pinn Fang, 2011.Offline QR Code Authorization Based on Visual Cryptography. Seventh International Conference. *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP).* 89-92. DOI: 10.1109/IIHMSP.2011.10 URL:http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6079541&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6079541

[6] Jonathan Wei and WeiQi Yan, 2012. Authenticating visual cryptography shares using 2d barcodes. IWDW'11 Proceedings of the 10th international conference on Digital-Forensics and Watermarking. *Springer-Verlag Berlin, Heidelberg.*7128: 196-210. DOI: 10.1007/978-3-642-32205-1_17 URL:http://link.springer.com/chapter/10.1007%2F978-3-642-32205-1_17

[7] RishabhKulshreshtha, AyushiKamboj, Sanjay Singh, 2012. Decoding robustness performance comparison for QR and data matrix code.*CCSEIT '12 Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology*.722-731. DOI: 10.1145/2393216.2393337 URL:http://dl.acm.org/citation.cfm?id=2393216.2393337&coll=DL&dl=GUIDE&CFID=372999437&CFTOKEN=54817096

[8] P. Preneel, V. Rijmen, and A. Bosselaers, 1998. Principles and Performance of Cryptographic Algorithms, " *Dr.Dobb's Journal*, Volume 23: 126 – 131. URL:http://www.drdobbs.com/algorithm-alley/184410756