Implementing Secured Device Pairing for VLC Based Systems for Smartphones

H.Prabavathi[#1], M.Sathya[#2], S.Keerthana[#3], G.Sribarkavi[#4]

[#1]*Assistant Professor, A.V.C.College of Engineering*
[#2-4]*UG Students, A.V.C.College of Engineering*

Abstract— *2D barcodes have enjoyed a significant penetration rate in mobile applications. This is largely due to the extremely low barrier to adoption. As an alternative to NFC technology, 2D barcodes have been increasingly used for security-sensitive mobile applications including mobile payments and personal identification. However, the security of barcode-based communication in mobile applications has not been systematically studied. Due to the visual nature, 2D barcodes are subject to eavesdropping when they are displayed on the smartphone screens. Almost every camera-enabled smartphones can scan 2D barcodes and able to receive SMS. Text SMS have been increasingly used for security-sensitive mobile applications including mobile payments and personal identification. So, we propose QR code based authentication system for smartphones.*

Keywords— Short-range smartphone communication, key exchange, secure VLC, 2D barcode streaming, QR codes.

1 INTRODUCTION

Despite of wide use of current online banking system, it has many security holes as it's based on traditional password based model, no mutual authentication between user and bank server which leads to threats like phishing(stealing passwords and using them for transactions), intercepting communication lines, database hacking, etc.. we generate QR-code, display it on user screen and decode it with user's mobile device. QR- code is generated on server side also and QR-code generated by user device and by server are verified to proceed. User database should also be encrypted to prevent data leakage. In this paper, We design a new system that can stream QR-codes between smart phones at a throughput comparable to that of state-of-art NFC systems. Due to the inherent directionality, the visible light communication (VLC) channel of barcode exchanges yields some interesting security properties. We formally analyze the security of VLC based on geometric models and propose physical security enhancement mechanisms such as manipulating view angles and leveraging user-induced motions. Based on our security analysis, we develop three secure data exchange protocols that encode information in barcode streams. We believe such protocols are useful in many mobile applications including private information sharing, secure device pairing, and contactless mobile payment, etc.

2 SECURITY MODEL

Successful defense against eavesdropping vastly depends on careful analysis of the attack scenarios and adopting suitable protection mechanisms based on the analysis. Before presenting our secure communication schemes, we would like to build formal 2D and 3D geometric security models and study several physical protection mechanisms in this section. The 3D model reflects the situation in reality, but the 2D model is also useful and intuitive, because we can always take a projection map P : R3 ->R2 and project all the objects onto a plane.we can map any point (x; y; z) in the 3D space R3 to a point (x; y; 0) as its projection on the x-y plane, which is the plane parallel to the ground. We now present the 2D/3D geometric model of a smartphone screen. The typical screen size of a mainstream smartphone platform is between 3 and 6 inches. One important feature of a smartphone screen addressed in our model is its visible angle.

3 ENABLING THE VLC CHANNEL FOR SMARTPHONES

3.1 Channel coding scheme design

First of all, we need to enable a one-way real-time VLC channel between Smartphone. We emphasis

that all kinds of 1D and 2D barcodes can be the channel coding candidate. Our prototype adopts QR code due to its advantages over other conventional barcodes, including high information density per code and low sensitivity to varying lighting conditions and angles. The prepared barcodes are sequentially displayed on the sender's screen at a certain frame refresh rate. The receiver starts the decoding process as soon as the first barcode frame is captured by its front-facing camera. The successful barcode decoding process outputs a frame string, which is then decoded

by ECC decoded to a package. Finally, the data string is assembled from those received data chunks. System Integration determines the optimal system parameters. SBVLC uses the 8-bit binary mode (mode indicator '0100') for QR code generation. The main system parameters that need to be decided includes the QR version, error correction level and frame refresh rate. In order to determine the proper ECC level, we did statistical test from QR version 1 to 20 on iPhone 4S, Google Nexus S and Samsung Galaxy S3. The result shows that low ('L') ECC level is sufficient in our usage scenario, and there is no correlation between the barcode decoding success rate and the error correction level even for high QR versions. Hence, we pick low ('L') ECC level for better storage capacity per barcode. Each data chunk is formatted to a package by adding a 16-bit sequence number in the header.

4 CONSTRUCTING FAST QR FILTERING

Since the frame refresh rate cap is about half of the camera capture rate, it is expected to have multiple camera frame images for the same QR code. So we have to construct an efficient filter to remove duplicated QR frame images. Secondly, the filter should also be able to remove that image that does not contain a QR code before submitting them for decoding. In this section, we propose a novel fast QR filtering technique to remove those non-QR and duplicated QR frame images with only a few image pixel samples.

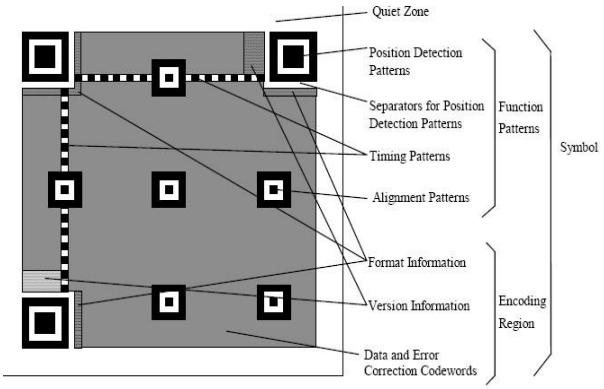

Fig.1: Structure of QR-code

5 SYSTEM ARCHITECTURE

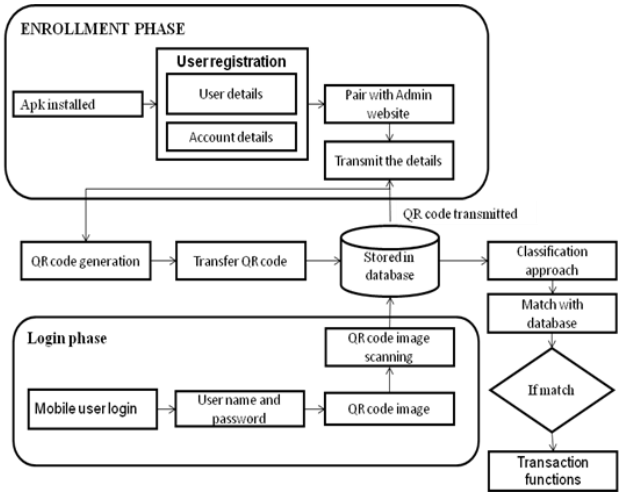

Fig.2: System architecture

6 IMPLEMENTATION

The server is designed as a web site that is made to serve all client data. Server can be in charge of keeping up all data without spilling data of other client. Server is used for login purpose and designed using PHP. Customers are considered as client in the system .Customer can be enrolled with their KYC details .These details are created as QR code QR code details are stored in the form of square matrix. QR codes are two- dimensional barcodes, so that they can be read from any direction in 360. It can put away to 4,296 alphanumeric characters. Produced QR codes are transmitted from server to client as QR image. Mobile user enters into the system utilizing two components. One is user name and password, another one is QR code based authentication. QR code image can be scanned by admin and extract the details and match with database. If the match is found means, authorized user can entered into the

system and performs basic transactions operations.

7 SYSTEM ADVANTAGES

The QR codes are only readable by the machine so untrusted person cannot understand what is inside the QR code. QR code can store up to 4000 alphanumeric characters so we can store more complex password which is not easily breakable. Time stamp provides more security. QR code can readable when it is partially damage.

8 FUTURE SCOPE

When user uses the mobile application the user need to enter the password that time size of mobile keypad is small so it may get difficult to use for some user so we can establish numeric keyboard or to use pattern authentication.Also system can provide different method forauthentication. Also we can use QR code in many applications and give them a more security.

9 CONCLUSION

Now a days, use of online banking application are increased. Security is an important issue for handling such services. We propose online banking authentication system using QR-code and OTP. The bank generates the QR-code using user input transfer information and then user need to recognize as to read the code using their mobile phone, after generate the OTP code using transfer information and the hashed user's mobile device number in their mobile phone. Finally, terminate the transfer by user typing of generated OTP code. Thus this system can be used for private information sharing, secure device pairing and secure mobile payment, etc. To our best knowledge, this work is the first one that formally defines and studies the security of a smartphone VLC system. It serves as a milestone for further development in secure VLC systems for smartphones. We will also extend our system to support other mobile and portable devices, e.g. laptops and tablets.

10 REFERENCE

[1] B. Zhang, K. Ren, G. Xing, X. Fu, and C. Wang, "SBVLC: secure barcode-based visible light communication for smartphones," in IEEE
Conference INFOCOM 2014, 2014, pp. 2661–2669.
[2] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical relay attack on contactless transactions by using nfc mobile phones," ePrint Archive, Report 2011/618, 2011.
[3] M. Allah, "Strengths and weaknesses of near field communication (nfc) technology," GJCST, vol. 11, no. 3, 2011.
[4] T. Hao, R. Zhou, and G. Xing, "Cobra: color barcode streaming for smartphone systems," in MobiSys, 2012
[5] S. Perli, N. Ahmed, and D. Katabi, "Pixnet: interference-free wireless links using lcd-camera pairs," in MobiCom, 2010.