Developing Authentication Solutions using Quick Response (QR) Code & Near Field Communication

Divyans Mahansaria
Dept. of Information Technology
Jadavpur University
Kolkata, India
divyansmahansaria@gmail.com

Uttam Kumar Roy
Dept. of Information Technology
Jadavpur University
Kolkata, India
royuttam@gmail.com

***Abstract*— Authentication is the process to verify whether a person who is requesting access for a system or resource is a legitimate one. The commonly used methods of authentication such as use of login credentials (e.g. username and password), combination of Automated Teller Machines (ATM) Card and Personal Identification Number (PIN), One Time Password (OTP) via Short Message Service (SMS) and others are subject to a number of different types of attacks. Few of the security attacks include key-logger and asterisk-logger, eavesdropping, shoulder surfing, brute-force, dictionary attack, replay attack, Trojan Horse attack, man in the middle attack, phishing attacks, ATM card skimming, Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks and many others. Thus it has become a necessity to deploy secure authentication solution while authenticating a user to shelter the user from the exposed attacks.**

The objective of the ongoing ph.d work is to design and develop secure solutions to counter security threats during the authentication process. The scope of the work covers authentication in a wide range of applications including desktop software, web applications, mobile apps, ATM terminal and other types of electronic devices. OTP is found to be more secure than static password and it is resilient against replay attack. In our proposed solutions, we have utilized the benefits of OTP by generating OTPs on each authentication request in a novel way. In one of the proposed solution, along with OTP, Quick Response (QR) code has been used for exchanging information pertaining to authentication. Due to its short range of communication, Near Field Communication (NFC) is considered advantageous for making payments and to carry out other secure end to end transactions. To authenticate the users at electronic terminals such as ATM kiosk we have designed a solution based on OTP and NFC card emulation. Our case study analysis supports the usefulness of using QR code and NFC during authentication.

Keywords— Secure Authentication, QR Code, Near Field Communication (NFC), One Time Password, Security Attacks.

I. Introduction And Related Works

Authentication is the process to verify whether a person who is requesting access for a system or resource is a legitimate one. Some of the common methods of authentication are use of login credentials (e.g. username and password), One Time Password (OTP) via Short Message Service (SMS), biometrics (e.g. face, voice, fingerprint etc.), digital certificates, multi-factor authentication products like SecurEnvoy, RSA SecureID etc. Other authentication techniques being researched include virtual keyboard or on-screen keyboard, graphical password with challenge-response, human body characteristics based (such as haptic, gaze, handwriting, brain waves etc.) and others. Automated Teller Machines (ATM) plays a vital role in providing the people easy access to cash and carry out other banking activities. At ATM kiosk, a combination of physical ATM Card along with Personal Identification Number (PIN) is in widespread use worldwide to authenticate the users.

However, the threats on these modes of authentication have significantly increased. Some of the security attacks include key-logger and asterisk-logger, eavesdropping, shoulder surfing, brute-force, dictionary attack, replay attack, Trojan Horse attack, man in the middle attack, phishing attacks, ATM card skimming, Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, SQL Injection, physical theft of devices and many others. Thus it has become a necessity to deploy secure authentication solution while authenticating a user to shelter the user from the exposed attacks.

Decades of research work has being carried out in the area of Information Security and a lot of solutions have been proposed and some of them have been implemented to counter security attacks. However, still there are open issues that need to be addressed. The use of One Time Password (OTP) for authentication was pioneered by Lamport in early 1980s and subsequently different adaptations of OTP have been proposed. OTP is found to be more secure than static password and it is resilient against replay attack. In our proposed solution, we have utilized the benefits of OTP by generating OTPs on each authentication request in a novel way.

. Quick Response (QR) code or 2D matrix bar code can hold large amount of data in a small space. It has error correction capability and a quick response time. QR code usage has continuously increased and it is being used in many applications. In one of the proposed solution, we have used QR-code to store and retrieve encrypted confidential information which will be required to carry out authentication. Near Field Communication (NFC) enables two electronic devices (or a device and a NFC Tag) to establish communication, by bringing them close to each other. Due to its short range of communication, NFC has advantages over Bluetooth, Radio Frequency Identification (RFID) and other communication technologies to carry out secure end to end transactions. In Card-emulation mode, a NFC device behaves

like a contactless smart card. In our research we have considered electronic device (such as smart phone) in NFC Card Emulation mode to authenticate users at electronic terminals such as ATM kiosk.

II. Proposed Solution Using QR Code

The first-time user needs to register with the authentication system to setup the authentication credentials. The registration process is similar to sign-up process of most of the existing websites that use login credentials. An additional hardware device such as smartphone capable of decoding a QR code is required to carry out the authentication. This device is provisioned with the authentication server and a custom authentication application present in this device facilitates the exchange of confidential information through the use of QR code.

In order to gain access to various systems and resources a user needs to be authenticated. During authentication process, information exchange takes place between the authentication server and the user in order to verify the identity of the user. On receiving an authentication request the server validates the request and generates a QR code having some unique information pertaining to the particular authentication request. The QR code is transmitted to the system from where the authentication request was generated. The QR code at the receiver's end needs to be decoded using the custom authentication application present in the QR code scanner device. The validity of the QR code is for a preset time duration within which it needs to be decoded. This would reveal partial information stored in the QR code to the user. The use of QR code facilitates information sharing in a convenient manner in between the authentication server and the user. Now using the received information the user needs to derive an OTP based on his/her actual password. The unique information present in the QR code changes on each authentication request and thus an OTP is computed by the user based on the registered static password. The computed OTP, QR code and provisioned device information is send to the authentication server for verifying the identity of the user. Based on the correctness of the information either the user is successfully authenticated or else the authentication request is rejected. Also there is an upper bound in time duration, to complete the authentication process from the time the authentication request was generated. If the time exceeds the authentication is invalidated.

The analysis of the proposed scheme of authentication illustrates the usefulness in countering different kinds of security breaches during the authentication process. Recently compromises have been reported in SMS based plaintext OTP which is widely used. Mobile phone malware capable of receiving SMS can transmit the plaintext OTP to a malicious entity and delete it from the mobile device. In the proposed authentication solution plaintext OTP is not transmitted by the server. The solution is resistant to phishing attack and replay attack as unique QR code with a preset validity duration is used. Other forms of security breaches like Shoulder Surfing, Brute-force and dictionary attack, SQL Injection and others can also be controlled using the proposed solution.

III. Proposed Solution Using NFC

In this solution a device, such as smartphone, which supports NFC is required to carry out authentication. A custom authentication app on the device is used to provision the device with the authentication server and to carry out NFC related operations. The first time users of the system need to register with the authentication server and setup a static PIN to authenticate into the custom authentication app before using it. After authenticating into the app the user requests for an OTP from the server. The sever validates the request, generates a long OTP and transmits the OTP in a secure way to the requestor app. The OTP is stored in the Secure Element (SE) of NFC via the app. The OTP has a preset time duration during which it needs to be used to perform authentication. When the NFC device is read by a NFC reader the information (i.e. the OTP) is transmitted to the NFC reader for further processing. In our proposed system, an additional NFC reader connected to the ATM terminal reads the information present in the NFC device. The read information is send to the authentication server for further processing. If the information is validated to be correct the user is successfully authenticated or else the authentication request is rejected. Also, there is an upper bound in time duration to complete the authentication process from the time the OTP request was generated. If the time exceeds the authentication is invalidated.

We have used secure channel to make the NFC communication safe. The NFC device communicates with the electronic device such as ATM terminal via NFC channel. As stated earlier the communication distance and the lifetime of a NFC channel are short and thus making it difficult to be compromised by an attacker. Moreover, using the proposed scheme ATM skimming can be controlled. It is a faster alternative to the existing physical ATM card and PIN based solution of authentication at ATM kiosk.

IV. Conclusion

The security attacks on different authentication mechanisms are increasing to an alarming extent. Thus, it has become essential to deploy necessary mechanisms while authenticating a user to protect from the vulnerable attacks. ATM machines are deployed worldwide and it is a convenient means to meet the banking needs of the users so it is essential that the ATM transactions are safe and quick. In our research we have explored a one-time QR code based authentication solution to counter the security attacks. Also, another solution has been designed which uses NFC card emulation feature to authenticate at ATM kiosk. This solution has been explained from the perspective of ATM but it is extendable to other applications as well. The analysis of our proposed solutions illustrates its significance over existing authentication methods.