Research Article Impact Factor: 0.621 ISSN: 2319-507X
Akash Wadate, IJPRET, 2014; Volume 2 (9): 755-760 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

USER AUTHENTICATION ON MOBILE DEVICES

AKASH J. WADATE[1], PROF. N. R. CHOPDE[2]

1. M.E, Computer Science & Engineering Department, G. H. Raisoni C.O.E.T., Amravati, MH, India.
2. Information Technology Department, Faculty of Engineering G. H. Raisoni C.O.E.T., Amravati, MH, India.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Security of mobile devices is very essential point as the amount of threats and vulnerabilities are increasing every day. There is huge increase in the number of threats to mobile devices and hence the security to those devices needs to be increase .The security to the data stored in or accessed by the mobile devices needs to be protected from mobile attacks and threats. So various methods are implemented to provide security solutions for sensitive data accessed by those devices, one of them is the authentication method which restricts the amount of access to the sensitive information stored in or accessed by the mobile devices. This paper focuses on the challenges and new strategies to authentication methods performed on mobile devices.

Keywords: Mobile Attacks, Mobile Devices, Threats, Vulnerabilities, Authentication.

PAPER-QR CODE

Corresponding Author: MR. AKASH J. WADATE

Access Online On:

www.ijpret.com

How to Cite This Article:

Akash Wadate, IJPRET, 2014; Volume 2 (9): 755-760

INTRODUCTION

Authenticating users on mobile devices can be challenging, and many solutions currently being used by mobile applications either compromise security or usability. Two common solutions that are often used are:

- Requiring the user to enter a password every time the application is started [1]. Complex passwords are difficult to enter on mobile devices, and requiring frequent password entry typically results in users either saving the passwords on their devices in plain text files, or in users choosing weak passwords that they can easily enter on their devices.
- Requiring the user to enter a password once, and storing it on the device for subsequent authentication[1].

This paper compares various approaches for authenticating users on mobile devices and highlights their pros and cons in terms of security and usability. The paper do not advocate any particular solution here because the best solution depends on your application’s requirements.

AUTHENTICATION OPTIONS

Mobile applications that require users to authenticate either need to authenticate the user to a server, or need to authenticate the user locally before allowing the user to access data stored on the device. The list of authentication options in this section is not meant to be exhaustive; only twelve common options are discussed here.

1. Require User to Enter Strong Password: this approach presents a unique challenge for mobile devices: it is difficult to enter complex passwords on mobile devices. It is Secure if device is borrowed or stolen[2] .

2. Require User to Enter Weak Password: Although having a password policy that permits weak passwords is generally considered poor practice, it can be used in specific ways where it may pose an acceptable level of risk.

3. Image Based Authentication: This patented authentication scheme offered by Confident Technologies2 [2] requires the user to remember visual categories chosen by the user during an initial setup process instead of passwords. Based on the categories chosen by the user, a 3x3 or 4x4 grid of images is presented to the user when authentication is required, and the user needs to select 3 or 4 images that are related to the previously chosen categories[3].

4. Retrieve Password Stored on Device: This is an approach that applications often use; they will ask the user to enter his/her password the first time the application is started, and will store it on the device for subsequent authentication (either in the clear, or encrypted using a key stored on the device). This approach is easy to implement and typically does not require any server-side changes. It is also easy to use for end users who just have to authenticate to the application the first time they use it from the mobile device.

5. Retrieve another Secret from Device: This option is a variation of the approach 4 however, instead of storing the password on the device, another secret is stored on the device by the application. The secret can be a random ID, a cryptographic key, the user's password encrypted using a key stored only by the server, etc. Some of these approaches are safer than others; however, in all cases, the idea is that if the user's device is compromised, the attacker cannot obtain the user's password.

6. Retrieve another Secret from Device (Revocation Capability): it adds the ability to revoke the secret stored on a device such that if the user realizes that his/her device secret has been stolen (e.g. in the case of a lost/stolen device), he/she can sign into a web application using his/her password (or call a customer service line) to revoke the secret stored on the device. Depending on how the web application is implemented, this can give users good visibility into and control over the device(s) that they have registered with the application.

7. SMS One-Time-Passwords: This authentication scheme leverages short messaging service (SMS) to deliver a one-time-password (OTP)[4] to a configured device. An application may require an OTP for performing highly sensitive operations such as performing funds transfers. The OTP is valid for only one use, and can be combined with other authentication approaches.

8. Device-Generated One-Time-Passwords: These are One-Time-Passwords (OTPs) generated by software running on a mobile device. A software token application on the device is responsible for generating OTPs that the user can use to authenticate to an application.

9. Out-of-Band Authentication (Phone Call): Out-of-Band authentication[5] uses a separate channel from the one that is being used for general communication to authenticate a device. SMS OTP discussed in Section 7 is a type of out-of-band authentication. Out-of-band authentication can also be performed using a phone call. When a user attempts an operation that requires out-of-band authentication, the server automatically calls the user's registered mobile phone.

10. Hardware Tokens: At least two types of hardware tokens can also be used for authentication:

- Hardware tokens that generate one-time passwords such as RSA SecurID, VASCO, SafeNet SafeWord, Authenex A-Key, SecureMetric SecureOTP, ActivIdentity OTP Token[6], etc.

- Hardware tokens that perform cryptographic operations and connect directly to the device authenticating the user, to transmit the result of a cryptographic operation to the server

11. Biometrics: Since biometric verification is not exact, biometrics are generally not used as a sole authentication mechanism; they are generally used in conjunction with a password/PIN. Biometric based authentication[7] holds the greatest promise for mobile devices in the long run. It can be used in conjunction with a weak password to strongly authenticate users without causing usability problems.

12. Rely on another Application for Authentication: This is not an authentication solution in itself; this mechanism delegates user authentication to another application. Several options are available:

- A standard mechanism such as OpenID can be used where an application trusts an identity provider to authenticate a user.
- Some vendors have recently created solutions that wrap applications and allow them to be used only after the user authenticates to a management application on the mobile device.

DESIGNING A SOLUTION

Combining the authentication methods properly for an application is a non-trivial exercise. Always consult a security expert when designing and implementing your mobile application. To illustrate the point, we will analyze three ways of combining some of the authentication mechanisms

Let’s consider a hypothetical mobile banking application. It stores a token on the device that it uses to authenticate the device. Additionally, if the user wants to perform a transaction, the user has to enter a PIN from a hardware token. As we will discuss below, different choices have different security properties and there are tradeoffs to be made.

- **Initial authentication and with device and biometrics: step up authentication with OTP:** The application starts with an authenticated device using the technique discussed in Section 6. It then uses the user’s voice as an additional authentication factor when the application is started. When the user chooses to transfer funds to another user’s account, he/she enters an OTP generated by hardware token as discussed in Section 10. The application ensures that both the device and the user are authenticated before permitting the potentially high-risk transaction. One potential problem in this scenario is that if the device is infected, the malware can modify the beneficiary account number and transaction amount to transfer funds into the attacker’s account.

- **Initial authentication and with device and biometrics: Step up authentication and transaction verification with OTP:** The application starts with an authenticated device using the technique discussed in Section 6[8]. It then uses the user's voice as an additional authentication factor when the application is started. When the user chooses to transfer funds to another user's account, he/she enters an OTP generated by hardware token as discussed in Section 10. Part of the OTP generation process requires the user to enter the beneficiary account number and transaction amount into the hardware token.In this case, malware cannot modify the beneficiary account number or transaction amount.
- **Initial authentication and with device and biometrics: step up authentication with OTP and transaction verification with Biometric:** Both of the above options suffer from one potential problem. If a user loses his/her device and hardware token while he/she is authenticated to the application, an unauthorized user may be able to perform transfers on the user's behalf. If we reorder the authentication steps, we can help mitigate this issue. This option uses voice authentication in a different way to solve the problem of what happens if a user loses his/her hardware token and device while authenticated to the application[8].

CONCLUSION

As is clear from the above discussion, combining authentication approaches is not a trivial task. To keep it simple, the above discussion skipped over many implementation details that will have a real impact on security. For example, the token stored on the device by the server could be used in several ways:

- It can be transmitted with the authentication request.
- It can be used as part of a challenge-response protocol.
- It can be used to encrypt a counter value and send it to the server each time it needs to authenticate to the server. This will require the server to maintain a counter value for each device that connects to it. In this case, once the token is provisioned on the device, a network-based attacker cannot access it. The attacker will only see the encrypted counter values. This approach has the potential advantage that if the

There are many other design choices that have various pros and cons, and combining them in various ways leads to thousands of possible implementations. Designing an authentication mechanism for mobile applications is a non-trivial exercise. Although here several options are discussed in this document, there are too many combinations and design/implementation choices possible to define.

REFERENCES

1. GAO-12-757," INFORMATION SECURITY: Better Implementation of Controls for Mobile Devices Should Be encouraged",2012, [Online].Available: http://www.gao.gov/648519.pdf

2. Norton, "Norton Mobile Security Lite,"2011.[Online].Available:http://us.norton.com/mobile-security/

3. Sophos, "Security Threat Report," 2010. [Online]. Available:http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf

4. Wikipedia,"Whitelisting",2014.[Online].Available:http://en.wikipedia.org/wiki/Whitelisting

5. "Security solutions available and proposed",2014.[Online].Available: http://www.zdnet.com/search?q=security+solutions+available+and+proposed.

6. Wikipedia,"MobileSecurity",2014. [Online].Available: http://en.wikipedia.org/wiki/ Mobile_security

7. "McAfee Labs 2014 Threats Predictions ",2014,[Online].Available:http://blogs.mcafee.com/consumer/mcafee-labs-2014-threats-predictions

8. Lookout, "Lookout Mobile Security,"2011.[Online].Available: https://www.mylookout.com