Mobile Networks and Applications

A Survey of Android Mobile Phone Authentication Schemes

- Published: 09 August 2018
- **volume 26**, pages2558–2566 (2021)

Abstract

The Android operating system is the most popular mobile operating system resulting in a great number of applications being developed for the platform. This makes them vulnerable to security threats such as social engineering, shoulder surfing and Malware. Therefore, Android devices require a secure authentication scheme in order to control access to the device. This paper briefly discusses the mobile security threats, the authentication protocols and Android Security. Then the paper presents an analysis of some of the authentication schemes that are used in mobile devices and some of the threats and technical issues faced. Authentication schemes discussed include password/pin, pattern based authentication, fingerprint recognition, facial recognition, vocal recognition and iris based authentication. In discussing the various authentication methods, it was observed that while biometric based authentication schemes offered the greatest level of security, there was always a trade-off between computational complexity and ease of use/implementation/cost that ensured that more traditional authentication schemes, while not as secure as biometric schemes, are still widely used in mobile devices.

1 Introduction

The Android operating system is, as of 2016, the most popular mobile operating system in the world with a market share of 87.5% [1]. As a result of the Android platform being so popular, there is a great number of applications being developed for the platform and being made available through Google Play. Some of the popular Android applications include the Weather application, those owned by Google such as Gmail, Maps, YouTube, Chrome and those owned by Facebook such as Facebook and WhatsApp Messenger. The Android platform can also be used for Internet of Things (IoT), BOYD (bring your own device) to improve work efficiency and productivity and access enterprise resources.

Using the Android platform may involve the storage of sensitive data on these mobile devices, like contacts, mail messages, phone calls, short text messages, bank information and these need to be protected for personal or business use only [2]. Most Android devices get carried around by their owners and are therefore susceptible to getting lost or stolen. Once the Android device are in the hands of an unauthorized user, sensitive data stored on the device as well as data on the cloud can easily be accessed by unauthorized users [2]. In addition, connecting the Android device to Internet presents itself to a number of security vulnerabilities such as account theft or service hijacking, data scavenging, data leakage, denial of service, customer-data manipulation, sniffing and spoofing [3]. An account theft can be performed by different ways such as social engineering and weak credentials while data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed [4]. Therefore, Android devices require a secure authentication scheme in order for the user to interact and access the device. Authentication is the process of determining whether a particular person or device should be allowed to access a system, an application, or specific data on a device [2].

Though mobile devices are more and more ubiquitous, their input methods that users can use to interact with the mobile devices are limited [5]. With the limited authentication options that are available, manufacturers of mobile devices have had to be increasingly creative as to how best to implement authentication schemes in their mobile devices. Authentication methods need to be improved upon and changed with time because attackers continually improve their attacking methods.

Of all authentication methods, password-based authentication has been one of the most popular methods [6]. In the early days of computer usage, user accounts were open to password guessing attacks due to a lack of mandatory use of strong password composition policies [6] but in recent years, there have been greater improvements in the field of authentication of users for mobile devices. This paper aims to perform a survey of some of the authentication schemes that are used in the field of mobile devices and also perform a survey of some of the fields of research that are being performed in the field of authentication on mobile devices.

This paper is organized as follows. Section 2 describes the related works in which we briefly discuss the mobile security threats, the authentication protocols and Android Security. In section 3 we discuss the authentication schemes dividing them into two categories namely the traditional authentication schemes and the biometric authentication scheme. Under the traditional authentication schemes, we have the Password/Pin authentication methods and the pattern based authentication. Under the biometric based authentication schemes, we have the fingerprint recognition, facial recognition, vocal recognition and iris based authentication. In section 4 we provide the analysis of the presented authentication schemes. Finally we conclude this paper in Section 5.

2 Related works

2.1 Mobile security threats

Authentication can be used to protect and secure the Mobile devices from security threats against confidentiality, integrity and availability of data. Attackers would like to gain access to the mobile device not necessarily to access the data on the device but in order to use the mobile device as conduit to freely access enterprise resources and other information on the cloud. Mobile security threats associated with authentication include social engineering, shoulder surfing, guessing and duplicates, Malware and broken cryptography [2, 7] [8, 9].

Social engineering is manipulation of people to get them to unknowingly perform actions that threaten the confidentiality, integrity, or availability of the organization's resources or assets, including information, information systems, or financial systems [7]. In the context of Mobile device authentication it is the manipulation of people to reveal confidential information like a PIN or password so that the unauthorized user can gain control of the device. Most people prefer to use a PIN or password for securing their phones and this makes them vulnerable to many security threats [8]. It is also easy to communicate PIN, password or an unlock pattern and this make them vulnerable to social engineering attack. Social engineering may also result in the exposure of an image that could be used for Face Unlock and put NFC tags at risk, because an attacker may come close enough to read the tag. Social

engineering assumes the use of human psychology, such as cognitive limitations and biases, which attackers exploit to deceive the victim so that the attacker can gain control of the Mobile device [7]. People use their mobile phones for monitoring their home appliances, checking emails, accessing web services and enterprise resources therefore access control of their device by unauthorized users might cause impact on devices, people, systems and environment [8].

Shoulder surfing is a threat where an attacker watches someone who is authenticating on a mobile device so that they can easily recognize a PIN or an unlock pattern [2]. For example, if the user PIN is 1234 it is easy for the attacker to watch and memorize it. Therefore, PIN authentication and Unlock patterns are particularly vulnerable to shoulder surfing, because as they are drawn or entered on the screen and they can be spied out even from a distance. Other authentication schemes are such as a long password or fingerprint authentication do not pose a threat when being watched by others as they cannot easily be remembered or duplicated via shoulder surfing. Guessing is some kind of brute force attack that can happen if a mobile device is stolen and in the hands of an attacker, then the attacker can attempt many trial unless the device deactivates itself or locks on many attempts. PIN and Unlock patterns may pose a threat as always the same numbers or pattern is entered which may leave a greasy residue or scratches on the touch screen that can make it easy for the attacker to guess [2]. Duplicates is a security threat where the Face Unlock and for NFC tags can be copied by the attacker by using a photo of the legitimate user.

Malware are malicious applications or hostile software created to perform a variety of attacks on Mobile devices in the form of trojan horses, spyware, worms, exploits, and viruses. Malware can gain access to the Mobile device and begin to send data streams to the attacker, for example, a fake applications can log user input from the background and send it to a server controlled by the attacker. Once authentication data is on the server and in the hands of the attacker, then the attacker can steal, encrypt or delete sensitive data from the device or even attempt to get physical access to the device [2]. Broken cryptography is the insecure usage of cryptography where a mobile application uses a process behind the

encryption/decryption that is fundamentally flawed or implement an algorithm that is weak and therefore can be exploited by an attacker to decrypt sensitive data. In the ecosystem perspective this affects customer privacy violations and can also lead to information theft, code theft, intellectual property theft and reputation damage, affecting vendors [10]. Malware and broken cryptography is a threat that can be easily exploited and hence the need to use and implement authentication protocols that have been thoroughly tested and accepted as strong by the security community.

2.2 Authentication protocols

The authentication protocols plays a critical role in information security and in particular in addressing mobile security threats. The current authentication protocols are generally divided into three categories namely identity based authentication protocol, authentication protocol based on traditional public key cryptography, and certificateless authentication protocol [11]. Certificate-based cryptosystems require that the authenticated public-key certificate of an entity be generated in large and distributed to many users in communities and verified frequently [12]. So the management of public-key certificates is cumbersome and involving. In order to avoid the shortcomings of the use of public-key certificates, researchers have proposed the concept of identity-based cryptography where the public keys directly derived from user identifiers, such as telephone numbers, email addresses, and social security number and the corresponding private key is generated by a combination of the user's public key and the system-level secret key of a central authority that is named as Private Key Generator [12]. There are a number of ID-based cryptography proposed in literature such as ID-based signature schemes, ID-based encryption schemes, ID-based key agreement schemes [12]. In the ID-based signature schemes, [12] proposes ID-based linearly homomorphic signature in which the signer can produce a linearly homomorphic signature in identity-based cryptosystems and then use bilinear groups as the underlying tool to design an ID-based linearly homomorphic signature. This scheme was proved to be secure against existential forgery on adaptively chosen message and ID attack in the random oracle model, and it combined the natures of linearly homomorphic signature and identity-based cryptosystems.

In certificateless public key cryptography the key generation centre generates user's partial private key instead of whole private key [11, 13]. Each user generates their own public key from a randomly generated secret value and encryption requires the user's public key and user's identity. Decryption requires a private key based on user's secret value and partial private key. The certificateless public key cryptography solves the key escrow problem in identity-based public key cryptography, and avoids the certificate management as well as the certificate delivery problems in the traditional public key cryptography [11]. There are many certificateless authentication schemes proposed in literature and [11] proposes a cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. The protocol ensures that no one can obtain user's real identity except for the network manager in the registration phase and in the authentication phase, the network manager cannot know the user's real identity.

To address the security threats posed by malicious application in Mobile devices a number of approaches has been proposed such as static techniques, signature based approach, permission based analysis, virtual machine analysis, dynamic techniques, anomaly based, taint analysis and emulation based. [14] Proposes an approach that extracts significant permissions from the mobile application and uses the extracted information to effectively detect Malware using supervised learning algorithms. Since the number of newly introduced Malware is growing at an alarming rate being able to detect Malware efficiently would allow analysts to be more productive in identifying and analysing them. This approach analyses permissions and then identifies only the ones that are significant in distinguishing between malicious and benign applications by applying a multi-level data pruning approach including permission ranking with negative rate, permission mining with association rules and support based permission ranking to extract significant permissions strategically. Then, classification algorithms is used to classify different types of Malware and benign applications.

2.3 Android security

The Android operating system is a Linux based operating system which is owned by Google [15]. Google provides a number of

methods of securing applications of the Android platform. These methods include the Google Play Store which allows users to download applications from a central market place and provides community reviewing of applications, application license verification, application security scanning, and other security services [16]. Other security methods offered by Google include Android Updates to the operating system, Android application services which allow applications to use cloud services to back up data and settings, continual scanning of applications on a device to better secure the device and the SafetyNet service which is an intrusion detection system which assists Google in tracking and mitigating known security threats as well as identifying new security threats [16]. Google also provides the Android Security program for the creation of a new Android release which provides components including design review which is the early phase where a security model is created; penetration testing and code review where Android-created open source components are subjected to testing; open source and community review where the code is reviewed by the Android community; and incident response where Google responds to security responses provided by the community and finally the Monthly security updates where the Android team provides an update to the application [16].

As previously stated, the Android operating system implements security on two main levels namely the kernel level and the application level [17]. At the operating system level, the Android platform provides the security of the Linux kernel, as well as a secure inter-process communication (IPC) facility to enable secure communication between applications running in different processes [16]. These security features at the OS level ensure that even native code is constrained by the Application Sandbox [18]. Whether that code is the result of included application behaviour or an exploitation of an application vulnerability, the system is designed to prevent the rogue application from harming other applications, the Android system, or the device itself. As the base for a mobile computing environment, the Linux kernel provides Android with several key security features, including: a user-based permissions model [18], process isolation, extensible mechanism for secure IPC [18] and the ability to remove unnecessary and potentially insecure parts of the kernel. As a multiuser operating system, a fundamental security objective of the Linux kernel is to

isolate user resources from one another. The Linux security philosophy is to protect user resources from one another. Android provides a set of cryptographic APIs for use by applications. These include implementations of standard and commonly used cryptographic primitives such as AES, RSA, DSA, and SHA. Additionally, APIs are provided for higher level protocols such as SSL and HTTPS. Android 4.0 introduced the KeyChain class to allow applications to use the system credential storage for private keys and certificate chains.

All applications on Android run in an application sandbox with application isolation enabled by Security-Enhanced Linux (SELinux), enhanced exploit mitigations, and cryptographic features, such as full disk encryption and verified boot [16]. An Android application by default can only access a limited range of system resources and the system manages Android application access to resources that could adversely impact the user experience, the network, or data on the device. These restrictions are implemented in a variety of different forms. Some capabilities are restricted by an intentional lack of APIs to the sensitive functionality (e.g. there is no Android API for directly manipulating the SIM card). In some instances, separation of roles provides a security measure, as with the per-application isolation of storage. In other instances, the sensitive APIs are intended for use by trusted applications and protected through a security mechanism known as permissions.

A list of Android Security Issues and threats which include: *Information Leakage*: occurs when application users grant permissions to applications without any restrictions from the android OS [18], *Privilege escalation:* escalation of privileges/permissions because of kernel vulnerabilities, *Repackaging of Applications:* Where applications may be reverse engineered by attackers and re-packaged to attack unsuspecting users [18], *Denial of Service (DoS) Attack:* applications may be designed to overload a smart phone and restrict the use of other services [18] and *Colluding:* users deploy a group of applications having the same certificate and grant various permissions that grant access to their resources and permissions by taking advantage of the shared UID [19].

A good way of ensuring security in mobile environments is to make sure that data is secured in the process of transmission. This is especially true in mobile environments that require transmission of data over mobile networks. One way of ensuring security in data transmission is to make sure that data that is transmitted over mobile networks is encrypted [20]. The encryption of data ensures both privacy and security for mobile application users.

3 Authentication schemes

3.1 Traditional authentication schemes

3.1.1 Password/pin code authentication

The most popular authentication methods that exist by far are the PIN/Password, biometrics and the unlock pattern authentication [21]. A major difference in authentication between desktop and mobile environments is that mobile users are not bounded to a particular location and settings, therefore, the users are free to utilize their mobile devices to access and use password-protected services (e.g. online banking, email services, etc.) anytime and anywhere [6].

As easy as these methods are, they are prone to classic attacks such as guessing attacks and attacks such as “shoulder surfing” [21].

A suggested way of further strengthening the pin method is the DRAW-A-PIN authentication method [22]. In this authentication method, a user, instead of simply typing out their pin code, needs to draw the pin code on their device screen as shown below (Fig. 1):

Fig. 1

DRAW-A-PIN Authentication method [22]

Full size image

The advantage brought forth by this method of authentication is that on top of recognising the pin entered by the user, the scheme also offers better security by utilizing drawing traits or behavioural biometrics as an additional authentication factor beyond just the secrecy of the PIN [22]. The DRAW-A-PIN algorithm has two phases namely the enrolment phase and the authentication phase.

In the enrolment phase, the algorithm prompts the user to choose a pin that they will use for authentication several times to begin building a bank of the users writing biometrics. The system then extracts metrics such as coordinate data, finger pressure and size of touch area from the user's input and stores it on the device [22].

In the authentication phase, the user is prompted to enter their credentials on the devices lock screen. When a pin is drawn, the system will first verify the digits being entered and will then proceed to observe the behaviour that was employed in entering the pin. Only when both are verified will the system authenticate the user [22]. The full process is shown in the figure below (Fig. 2).

Fig. 2

DRAW-A-PIN phases [22]

Full size image

3.1.2 Pattern authentication

Pattern based authentication is also a very popular form of authentication on many mobile devices today [21]. These authentication methods involve a user entering a pattern in order to authenticate themselves. On the Android operating system, this usually involves swiping a pattern connecting dots to complete a pattern as shown below (Fig. 3):

Fig. 3

Pattern unlocking on Android [21]

Full size image

If the wrong pattern is entered, the device will not authenticate the user and if the pattern is increasingly incorrect, the device uses a push-back for them to re-try entering the password after an increasingly longer period of time. There are a number of rules that need to be observed when using this method including: (1) a pattern must consist of at least four dots; (2) each dot can only be visited once; and (3) a previously unvisited dot will become visited if it is part of a horizontal, vertical or diagonal line segment of the pattern [23].

Technical issues

One great technical issue found with the pattern authentication method is that it is liable to being exploited by an attacker by analysing the smudging that are left on the screen as the user types [22]. This method also dealt a great blow in terms of security in 2017 when researchers were able to successfully crack this password by deducing the pattern code from a video of a user entering the pattern on their mobile phone [23]. In the technique, the five steps involved are: (1) filming and video pre-processing, (2) tracking fingertip locations (3) filming angle transformation, (4) identifying and rank candidate patterns and (5) testing of candidate patterns.

3.2 Biometric authentication schemes

In the field of biometrics, there are seven basic criteria that are considered to make a secure biometric system namely uniqueness, universality, permanence, collectability, performance, acceptability and circumvention [24]. For a biometric system, these criteria are essential otherwise there is a great danger of compromising a system's security. The two aspects of biometric security are physical access control which control covers identity authentication processes which require users to provide physical characteristics and logical access control which refers to a process of a scheme control over data files or computer programs [24]. In order for biometric systems to be effective, the system has to accomplish requirements including usability (ease of use is key),

security (imposters must not be able to gain access to a system) and availability (should be used on the go) [25].

On the mobile front, biometrics for mobile access control has been established as the most significant development in the field of biometrics in mobile devices [25]. The field of biometrics in mobile devices has become more popular in recent years as it can be used in applications such as mobile payment of law enforcement [25]. Fingerprint authentication, facial recognition, vocal recognition and iris recognition are the biometric fields that will be discussed in this section:

3.2.1 Fingerprint authentication

Authentication via fingerprints works because our fingers are made of a number of ridges and valley on the surface of a finger that is unique to each human [24]. It is this uniqueness of fingerprints that make the use of fingerprint scanners a viable biometric to be used. Touch-screen devices such as smartphones and tablets make the option of using fingerprints or at least measure the size and shape of any portion of fingers in contact with the screen as an authentication method [26]. While biometric methods such as face, fingerprint, iris, voice, and palm print are widely used, fingerprint biometric authentication has attracted the most attention and is mostly deployed in mobile devices [27]. This may be because of the practical nature of fingerprint authentication.

Threats and technical issues

Though fingerprint authentication is a convenient technology, it is not without its flaws. One of the greatest of these is the faking of the fingerprints. For instance, Matsumoto et al. [28] performed an experiment where the fingerprint authentication was bypassed by using gummy (gelatine) fingerprints. To overcome such flaws, other factors such as the measurement of sweat diffusion pattern over time along the ridges of the fingerprint are used [29]. On this front, some observations that can be made include: (1) in live fingers, perspiration starts from the pores, either completely covering them or leaving the pore as a dry dot in the centre of the sweating source. (2) Second, the sweat diffuses along the ridges in time, making the semi-dry regions between the pores moister or darker in the image. Unless the skin is extremely dry, the pore

region remains saturated while the moisture (sweat) spreads towards drier parts. (3) The perspiration process does not occur in cadaver or spoof fingers [29].

3.2.2 Facial recognition

Faces are the most recognisable features of the human biometrics. Aside from being one of the most recognisable features of the human body, facial features can be used in biometric security systems in the process of user authentication [24]. Facial recognition is popular because the hardware needed for facial recognition is relatively cheaper than other biometric technologies such as iris scanning which makes it a viable authentication technique for mobile devices. Earlier on, effectiveness criteria including usability, security and availability which are criteria that facial recognition meets. Facial recognition is easy to use and understand, has a relatively high rate of recognition and does not need intense hardware in order to be utilised [25]. Facial recognition though, as convenient as it may be, is liable to some attacks. For example, an attacker may simply use a users' photo or video of the person that they are seeking to attack and may gain unauthorized access to the users' device. This threat is increased with the availability of photos from social networking sites like Facebook and Twitter [25]. Other problems with facial recognition include issues such as the difficulty of facial recognition due to exposure conditions such as the day-night cycle or changes in the environmental lighting, distance between the person and camera, and the way different camera sensors operate in the same or different spectral bands [30]. To alleviate such problems, proposals have been made to use facial recognition on not only the visible spectrum but also performing the facial recognition on the invisible spectrum such as the ultra-violet and infra-red.

Facial recognition algorithms

When it comes to facial recognition algorithms, there is an inherent trade-off between accuracy and computational complexity of the facial recognition algorithm especially on mobile devices which typically have lower computational power than that of their desktop counterparts [31]. To counter this, the algorithm that is used is very important. For instance, colour segmentation

techniques can be used to make the process of facial recognition work. Dave, Chao and Sriadibhatla proposed a facial recognition algorithm illustrated in Fig. 4.

Fig. 4

Block diagram of the Face Recognition system [31]

Full size image

In this algorithm, the first step that is carried out is facial detection which is then followed by facial recognition. To perform this facial detection algorithm, Dave, Chao and Sriadibhatla [31] use colour segmentation, morphological processing and template matching algorithms. In order for the user's photo to be processed by the algorithm, the following conditions need to be met: (1) The face is centred and takes a big part of the image, since the photo is shot closely, (2) The illumination conditions are correct and (3) The user

is facing the camera [31]. Factors used for facial detection are (1) colour segmentation to find skin pixels, (2) morphological operations to eliminate isolated pixels and finally, (3) template matching to extract only the face, which we will use for face recognition [19].

3.2.3 Vocal recognition

Vocal recognition is also an authentication device that may be used in the authentication on Android devices. There are two main factors to be considered for vocal recognition to be used in authentication which are the physiological component which is known as the voice tract and the behavioural component which is known as the voice accent [24]. Advantages of vocal recognition include the relative ease of installation and the minimal requirements (hardware and software) in order to use it. The only special equipment needed for this to work is a microphone. In order for vocal recognition to be of higher quality and secure, factors such as performance of users when they record their voices and the possibility of authorized users' recorded voices may be used to try and bypass a vocal recognition system being used [11].

Vocal recognition algorithm

One way of making vocal recognition more secure is the use of a vocal challenge to the user in order to try to verify the user. For instance, the use of a vaulted voice verification protocol to perform a challenge-response approach to authentication to increase the security of a system [32]. The figure below illustrates the process of vaulted voice verification (Fig. 5).

Fig. 5

Vaulted voice verification protocol [32]

Full size image

In this model, users will make a claim of identity to the vocal recognition system which the system challenges by asking the users to state phrases that are generated by the system. This method makes it difficult for attackers to use recorded clips of the user to bypass the system since the word challenges are generated dynamically.

3.2.4 Iris recognition

Iris recognition is a biometric form of recognition where the iris of an individual is scanned in order to verify a users' identity. This is made possible because like fingerprints, the iris has a unique pattern for every individual and also because characteristics of the iris are extremely complex and random [33]. Another advantage of iris recognition is that the iris is relatively unaffected by the effects of aging which makes if a very viable form of authentication.

On mobile phones, iris recognition is different from that of conventional iris recognition in that once iris recognition is being performed on mobile devices, factors such as computational power of the mobile device and the space for placing the Near Infrared LED illuminator and the iris to be authenticated come into play [34]. Such issues can be alleviated in a number of ways such as the use of fast eye detection algorithms and the use of dedicated hardware to better detect the iris. Mobile iris recognition systems can be divided into three main categories namely: systems using dedicated devices to perform the iris recognition, systems connecting additional hardware to the mobile device, and systems

attaching a Near-Infrared (NIR) cameras with illuminators [34]. These Near-Infrared (NIR) cameras are powerful devices which can capture iris images with sharp spectral patterns even from dark coloured irises [35].

4 Discussion

Authentication schemes discussed in this document are password/pin, pattern based authentication, fingerprint recognition, facial recognition, vocal recognition and iris based authentication. Of the authentication schemes discussed in this paper, the most user friendly authentication methods are those which require the least amount of interaction from the user i.e. the methods that cost the least amount of effort from the user. For instance, practical ways and methods of making text based authentication stronger is by using random characters for the password but the use of such complicated passwords is often off-putting to a user of a mobile device. In general, the four barriers to adoption of strong authentication are the cost of the authentication methods, ease of use of the authentication method, the security provided by the authentication method and the privacy offered by the authentication method [36]. As a result, the authentication method that employs all of these to the best degree is a better method. Given this criteria for a good authentication scheme, the table below shows how the authentication schemes perform relative to one another:

From Table 1, it is observed that more traditional based authentication schemes such as password/pin and pattern based authentication have the lowest cost while offering medium security. It can be argued though that these authentication methods are less secure because users tend to use simpler passwords in order to remember their authentication keys. For instance, a user will try to use a password that is easily remembered or a pin they can easily remember or even a pattern that is simple and quick to enter. Fingerprint and iris based authentication on the other hand, while being relatively expensive, offer the highest level of security. These methods of authentication do not suffer from the password/pin flaw of users using easy-to-remember passwords. Biometric authentication systems also offer the highest level of privacy to the user in that the user need not worry about anyone

peaking while they enter their credentials. It can also be noted from Table 1 that fingerprint authentication is more likely the next most popular authentication method especially as the technology becomes more prevalent in the mobile computing space.

Table 1 Authentication schemes perform relative to one another
Full size table

Of these authentication schemes, the most practical scheme for users is the fingerprint sensor which offers very high security and privacy while having low user effort to use it. The one barrier that has held up this authentication scheme is the cost of implementing it. This barrier is also shared by other biometric authentication methods except voice recognition. As a result, the most commonly used and readily implemented authentication methods are pin/password, pattern based schemes and vocal recognition.

5 Conclusion

This paper began by introducing mobile security threats and then proceeded to discuss authentication protocols and Android Security. The main section discussed in this paper were the various authentication schemes that are used in the mobile computing such as the Android devices. Authentication schemes were divided into two main sections namely traditional authentication schemes and biometric authentication schemes. The traditional authentication schemes that were discussed include the password/pin number authentication schemes and the pattern matching schemes used especially in Android-based authentication schemes.

The biometric authentication schemes that were discussed included fingerprint authentication, facial recognition, vocal recognition and iris-based recognition. Biometric schemes are, generally, more secure than the traditional authentication methods mostly because metrics used in biometric authentication cannot easily be replicated. These metrics such as iris detection and fingerprints are unique to one individual per set. While biometrics offer a more secure way of authenticating, the cost of the biometric devices and the computational cost of the algorithms used in biometric authentication make it rather expensive to outrightly migrate to using biometric authentication exclusively.

References

1. Kharpal A (2016) Google Android hits market share record with nearly 9 in every 10 smartphones using it. [Online]. Available: https://www.cnbc.com/2016/11/03/google-android-hits-market-share-record-with-nearly-9-in-every-10-smartphones-using-it.html. [Accessed: 13 May 2018]

2. Schlöglhofer R, Sametinger J (2012) Secure and usable authentication on mobile devices. In: Khalil I (ed) Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia (MoMM '12), p 257–262

3. Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB (2013) An analysis of security issues for cloud computing. J Internet Serv Appl 4(1):1–13

   Article Google Scholar

4. Nagpal D, Sharma D (2016) Survey on threats attacks and implement ation of security in cloud infrastructure. Int J Res Comput Appl Robot 4(5):55–61

5. Patel SN, Pierce JS, Abowd GD (2004) A gesture-based authentication scheme for untrusted public terminals. In: Proceedings of the 17th annual ACM symposium on User interface software and technology - UIST '04

6. Maydebura SV, Jeong DH, Yu B (2013) Understanding environmental influences on performing password-based mobile authentication. In: 2013 IEEE 14th International Conference on Information Reuse & Integration (IRI), p 728–731

7. Greitzer FL, Strozer JR, Cohen S, Moore AP , Mundie D, Cowley J (2014) Analysis of unintentional insider threats deriving from social engineering exploits. In: Proceedings - IEEE Symposium on Security and Privacy, vol. 2014–January, p 236–250

8. Chantal M, Lee SW, Kim KH (2017) A security analysis and reinforcement design adopting fingerprints over drawbacks of

passwords based authentication in remote home automation control system. In: Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications - IEEA '17, New York, New York, USA, p 71–75

9. Singh V, Sharma K (2016) Smartphone security. In: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies - ICTCS '16, New York, New York, USA, p 1–3

10. Krupskiy A, Blessinga R, Scholte J, Jansen S (2017) Mobile software security threats in the software ecosystem, a call to arms. In: International Conference of Software Business. Springer, Cham, pp 161–175

11. Shen J, Gui Z, Ji S, Shen J, Tan H, Tang Y (2018) Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. J Netw Comput Appl 106:117–123

Article Google Scholar

12. Lin Q, Yan H, Huang Z, Chen W, Shen J, Tang Y (2018) An ID-based linearly homomorphic signature scheme and its application in Blockchain. IEEE Access 6:20632–20640

Article Google Scholar

13. Al-Riyami SS, Paterson KG (2003) Certificateless public key cryptography. Springer, Berlin, Heidelberg, pp 452–473

MATH Google Scholar

14. Li J, Sun L, Yan Q, Li Z, Srisa-an W, Ye H (2018) Significant permission identification for machine learning based android malware detection. In: IEEE Transactions on Industrial Informatics. IEEE. https://doi.org/10.1109/TII.2017.2789219

15. Schmidt A, Schmidt H, Clausen J, Camtepe A, Albayrak S (2008) Enhancing security of linux-based android devices. In: Proceedings of 15th International Linux Kongress

16. Android Open Source Project (2017) Android open source project. [Online]. Available: https://source.android.com/. [Accessed: 13-May-2018]

17. Smalley S, Craig R (2013) Security Enhanced (SE) Android: Bringing Flexible MAC to Android. 20th Annual Network and Distributed System Security Symposium, vol. 310, p 20–38

18. Rashidi B, Fung C (2015) A survey of android security threats and defenses. JoWUA 6(3):3–35

Google Scholar

19. Ahmed O, Sallow A (2017) Android security: a review. Acad J Nawroz Univ 6(3):135–140

Article Google Scholar

20. Cai Z, Yan H, Li P, Huang ZA, Gao C (2017) Towards secure and flexible EHR sharing in mobile health cloud under static assumptions. Clust Comput 20(3):2415–2422

Article Google Scholar

21. Harbach M, De Luca A, Egelman S (2016) The anatomy of smartphone unlocking. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16, New York, New York, USA, p. 4806–4817

22. Nguyen TV, Sae-Bae N, Memon N (2017) DRAW-A-PIN: authentication using finger-drawn PIN on touch devices. Comput Secur 66:115–128

Article Google Scholar

23. Ye G, Tang Z, Fangy D, Cheny X, Kimz KI, Taylorx B, Wang Z (2017) Cracking android pattern lock in five attempts. In: Proceedings 2017 Network and Distributed System Security Symposium 2017 (NDSS'17), Reston VA

24. Uddin MN, Sharmin S, Hasnat A, Ahmed S, Hasan E (2011) A survey of biometrics security system. IJCSNS 11(10):16–23

Google Scholar

25. Vazquez-Fernandez E, Gonzalez-Jimenez D (2016) Face recognition for authentication on mobile devices. Image Vis Comput 55:31–33

Article Google Scholar

26. Jakobsson M, Shi E, Golle P, Chow R (2009) Implicit authentication for mobile devices. USENIX Association

27. Khan MK, Zhang J, Wang X (2008) Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. Chaos, Solitons Fractals 35(3):519–524

Article Google Scholar

28. Matsumoto T, Matsumoto H, Yamada K, Hoshino S (2002) Impact of artificial 'gummy' fingers on fingerprint systems. In: Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677, p 275–289

29. Derakhshani R, Schuckers SAC, Hornak LA, O'Gorman L (2003) Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. Pattern Recogn 36(2):383–396

Article Google Scholar

30. Bourlai T, Hornak LA (2016) Face recognition outside the visible spectrum. Image Vis Comput 55:14–17

Article Google Scholar

31. Dave G, Chao X, Sriadibhatla K (2010) Face recognition in mobile phones. Department of Electrical Engineering Stanford University, USA

32. Johnson RC, Scheirer WJ, Boult TE (2013) Secure voice based authentication for mobile devices: vaulted voice verification. Proceedings of SPIE 8712, Biometric and Surveillance Technology for Human and Activity Identification X, 87120P. https://doi.org/10.1117/12.2015649

33. Gragnaniello D, Sansone C, Verdoliva L (2015) Iris liveness detection for mobile devices based on local descriptors. Pattern Recogn Lett 57:81–87

Article Google Scholar

34. Kim D, Jung Y, Toh K-A, Son B, Kim J (2016) An empirical study on iris recognition in a mobile phone. Expert Syst Appl 54:328–339

Article Google Scholar

35. Jung Y, Kim D, Son B, Kim J (2017) An eye detection method robust to eyeglasses for mobile iris recognition. Expert Syst Appl 67:178–188

Article Google Scholar

36. Nok Nok Labs, Four barriers to adopting strong authentication. [Online]. Available: https://www.noknok.com/sites/default/files/whitepapers/4barrierswhitepaper_0.pdf. [Accessed: 20 Jun 2017]