Cyber Security and Applications 2 (2024) 100021

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

E-Brightpass: A Secure way to access social networks on smartphones

Chaitanyateja Thotadi[a], Monith Debbala[a], Subba Rao[a], Ajay Eeralla[b], Basker Palaniswamy[c], Srijanee Mookherji[d], Vanga Odelu[d], Alavalapati Goutham Reddy[e,*]

[a] National Institute of Technology, Andhra Pradesh, India
[b] AMD Inc, Austin, USA
[c] Queensland University of Technology, Brisbane, Australia
[d] Indian Institute of Information Technology Sri City, Chittoor, India
[e] Fontbonne University, St. Louis, USA

ARTICLE INFO

Keywords:
Smartphones
Social networks
Malware
Authentication
Security

ABSTRACT

Social network providers offer a variety of entertainment services in exchange for end users' personal information, such as their identity. The majority of users access social networking sites via their smartphones, which they utilize in conjunction with a traditional authenticator like a password. On the other hand, aggregators, which pull content from multiple social networks, are often used to get into smartphone apps that may involve mobile ticketing, identification, and access control. They are a potential target for malware and spyware injections due to their powerful position. Malware is capable of circumventing authentication mechanisms in order to get access to social networking services, which may result in stealing the personal information of users. To deflect any type of attack from malicious software, BrightPass [22], a malware-resistant method based on screen brightness, was introduced. Conversely, we have demonstrated that the BrightPass user's personally identifiable information, such as PIN numbers, may be recovered by evaluating the variations between the recorded input from many authentication sessions. We have then offered various enhanced BrightPass versions to address the observed vulnerability. Our enhanced BrightPass versions are both simple and secure to use when it comes to accessing social networks via mobiles.

1. Introduction

Social networking sites offer an amazing platform for people to stay in contact with family and friends. It allows conversations and interactions with individuals from all over the world, which has both advantages and disadvantages. These websites, for instance, contribute to education through exerting influence over students. On the other hand, social networking platforms have a plethora of negatives. They give rise to cybercrime types such as cyberbullying, cyber extortion, targeted phishing, social engineering, propaganda and cyber terrorism [1,2]. Social networks have exploded in popularity in recent years. With over 100 million registered users, some of the most popular social media websites include Facebook, TikTok, WeChat, Instagram, Twitter, WhatsApp, and LinkedIn [3–5]. This is evidence for the growth of social networking sites for creating large reservoirs of personal information.

Likewise, recent hardware and telecommunications improvements have enabled the development of low-cost mobile devices with a variety of sensors. As a result, in recent years, mobile devices have expanded in popularity and ubiquity among customers all around the world [6]. The mobile revolution has enabled and motivated users to move practically all of their daily activities to the mobile environment via so-called mobile applications. Mobile devices are regarded by their users as very personal tools that are largely used to assist with day-to-day tasks, but they can also be used to store sensitive information [7]. Users of mobile devices that run on a specific operating system must download a range of programs from various sources, such as the Apple App Store and Google Playstore, in order to enhance their functionality. Conversely, applications are a source of many malware, and mobile devices are vulnerable to a variety of security issues and threats, including the theft of private information [8–12].

Security is not taken seriously by everyone. It is not uncommon for people to create a social media account and never explore the settings beyond the default. Similarly, they will purchase a mobile device, or other device to access those sites and accept that it is configured in the most secure manner possible. Often, default settings are the most convenient but also the least secure. For instance, though Facebook has ensured security for its users by a password-based authentication system, it is not sufficient to protect the personal information of its users by a single factor. Generally, the default authentication systems used by social networks are insufficient to establish security. Specifically, password-

* Corresponding author.
E-mail address: gralavalapati@fontbonne.edu (A.G. Reddy).

https://doi.org/10.1016/j.csa.2023.100021
Received 21 February 2023; Received in revised form 20 April 2023; Accepted 10 June 2023
Available online 15 June 2023

based authentication is vulnerable to attacks such as brute-force and guessing [13,14].

According to recent findings, single-factor authentication is no longer sufficient. As a result, two-factor authentication is created [15–17]. Most social media plat-forms, including Facebook and Twitter offer two-factor authentication as an optional security feature. When 2FA is enabled, Facebook, for example, sends a 6-digit one-time password (OTP) to the user's mobile phone. However, due to their impracticality, traditional 2FA solutions such as tokens or biometrics cannot be extended to online social networks. As a result, either OTP generated by users' smartphones or OTP received via SMS is considered a viable option.

As threats evolve, security must adapt and address them. Social media platforms frequently update their security measures in response to identified or potential security vulnerabilities. Some websites will notify you of updates and new settings, whereas others may do so without your knowledge. Given that social media requires the use of a computer or other device, you should also review how those devices are protected. Smartphones are evolving and increasingly resembling personal computers. With the advancements in smartphone capabilities, the risk of attacks from various types of malware is also increasing [18]. The malware or spyware can recover sensitive personally-identifying information including passwords, PIN numbers, and personal data [19]. And it can read SMS and send it to a remote server, where it can be sold or utilized. As a result, the attackers can read the second factor, namely the OTP given by social networks, and get access to the profiles of users. This adds to the security concerns with two-factor authentication, particularly OTP.

At present, new correspondence interfaces can be incorporated to a wide range of smartphone functions, allowing them to access and transmit security-basic tasks such as sensitive personal information in social networking apps. Such sensitive information can be misused in a variety of ways. Without a doubt, current mobile operating systems such as Android provide an ideal environment for developers to create apps and distribute them through online marketplaces such as the Google Play Store and Apple App Store. Unfortunately, these platforms allow mobile malware to infiltrate smartphones and gain root access. To access social networking platforms, the spyware can obtain sensitive information such as user authentication details. It can be done through side-channel attacks or by recording the entire authentication process as well as the user's keystrokes [20,21]. Many mechanisms have been proposed to prevent spyware from retrieving the user's credentials or launching automated attacks.

Numerous proposals have been made in response to the importance of security in the authentication process. The majority of the suggestions are aimed at preventing malware from attempting automatic authentication. Some proposals include a hidden value or a difficult cognitive intelligence test, such as CAPTCHA. Nevertheless, one of such methods is BrightPass [22], which uses the brightness of a smartphone as a tool of authentication. In this paper, we demonstrated a vulnerability in the BrightPass and proposed several improvements.

This paper's primary contributions are as follows:

1. It is demonstrated that the original brightpass method is vulnerable to recording attacks.

2. An enhanced version of brightpass method is proposed, which comprises of three different approaches that will directly contribute to the authentication times.

3. The suggested protocol is carefully analyzed to demonstrate that it may successfully prevent well-known security issues.

The remainder of the paper is divided into the following subsections. Section 2 describes the weakness of brightpass method. Section 3 presents the proposed methods. Sections 4 offer a thorough security analysis and a comparison of the proposed methods with the brightpass method. Section 5 and 6 provides the experimental evaluation and discussions. The paper is concluded in Section 7.

```
Enter the Key Captured:1138214
Enter the next Key Captured:3858174
Final Pin Code Cracked[3814]
```

Fig. 1. Cracking of PIN with two attempts.

```
Enter the Key Captured:3881144
Enter the next Key Captured:3811434
Combinations:[1144, 8144, 3144, 3844, 8114, 3114, 3814, 3811]
Enter the next Key Captured:3586814
Final Pin Code Cracked[3814]
```

Fig. 2. Cracking of PIN with three attempts.

```
Enter the Key Captured:3881144
Enter the next Key Captured:3811434
Combinations:[1144, 8144, 3144, 3844, 8114, 3114, 3814, 3811]
Enter the next Key Captured:3811459
Combinations:[8114, 3114, 3814, 3811]
Enter the next Key Captured:3818344
Final Pin Code Cracked[3814]
```

Fig. 3. Cracking of PIN with four attempts.

2. Security weakness of the brightpass method [22]

BrightPass's weakness is that the malware can recover the PIN through multiple spyware-based recording attacks. Authors [22] also mentioned that one can succeed to infer PIN digits by analyzing the differences between the recorded input from several authentication sessions. To demonstrate this attack, a simple code was executed that uses the seven-digit PIN as the input for multiple sessions. The programme is shown in Fig. 1 cracking the PIN using two session inputs, in Fig. 2 cracking the PIN using three session inputs, and in Fig. 3 cracking the PIN using four session inputs.

The PIN can be cracked using only a few mathematical operations, specifically combinations. To begin, the four-digit PIN combinations from the first session key are calculated, with a total of 35 possible combinations. Similarly, for the second session key, the combinations are calculated and sent to a matching programme, which outputs the corresponding PIN from a total of 70 combinations. The first key in Fig. 1 is 1138214, while the second key is 3858174. The BrightPass PIN 3814 is retrieved from these two session keys.

The above figures illustrate retrieving of PIN using more than two session inputs. Sometimes the user enters repeated digits from the PIN which leads to multiple combinations thereby requiring more than two session inputs. The Fig. 1, Fig. 2 and Fig. 3 show the combinations possible with the session input in every attempt.

3. E-Brightpass methods

We have proposed three methods, each of which utilizes a unique secret key that is distinct from the original PIN. Each method blurs the keypad to 80 and randomizes it to prevent spy cameras from recording input. The overview of the proposed methods is similar to that of original BrightPass[22] as shown in Fig. 4.

3.1. Method i

In this method, the secret key is obtained from a 2 x 5 matrix and is used in conjunction with the original PIN for authentication as displayed in Fig. 5. The 4-digit secret key is retrieved using the original PIN. Assuming the initial PIN is 1234, the secret key from Fig. 5 is 7582, which corresponds to the 1, 2, 3, and 4 positions. For instance, if the original PIN is 0987, the secret key is 9200, which corresponds to the positions 0, 9, 8, and 7.

Further to the calculation of the final PIN, the authentication process is identical to that of BrightPass. The final PIN must be entered in the

Fig. 4. Overview of the BrightPass [22] and the proposed methods.

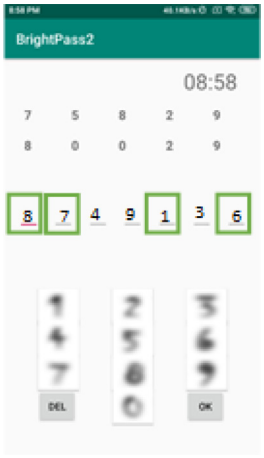

Fig. 5. Illustration of Method I.

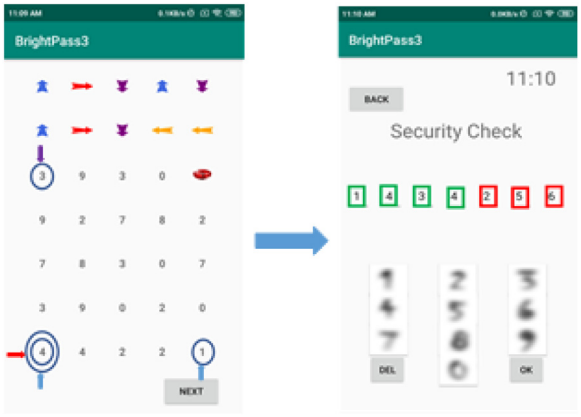

Fig. 6. Illustration of Method II.

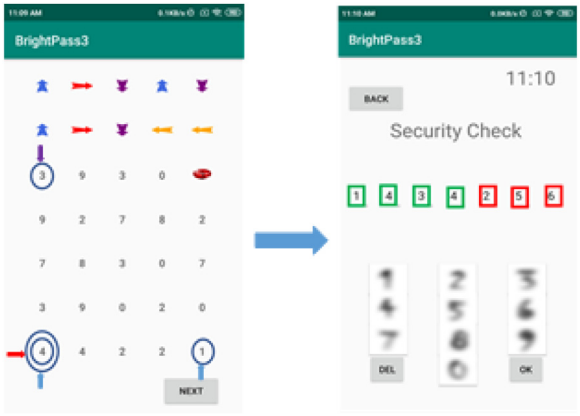

Fig. 7. Illustration of Method III.

area with the highest screen brightness and a random number in the area with the lowest screen brightness.

Original PIN: 1 2 3 4

Secret Key: (+) 7 5 8 2

Final PIN: 8 7 1 6

The above method is resistant to multiple recordings because the matrix generates a secret key using the original PIN and then uses the secret key in conjunction with the original key to compute the final PIN. There are 840 possible secret keys in a session, which reduces the likelihood of recovering the original PIN.

3.2. Method II

The secret key is obtained using this method via a graphical password-based interface. The graphical user interface is composed of a 7X5 matrix containing a mixture of directions and numbers. The first ten cells contain random directions, while the following twenty-five cells contain random numbers ranging from 0 to 9.

The secret key is retrieved by entering the original PIN and following the on-screen instructions provided by the graphical password-based interface. Fig. 6 illustrates how this method works. The graphical password-based interface has a randomly generated start that varies between sessions. Assuming the PIN is 1234, the directions in positions 1, 2, 3, and 4 of Fig. 6 are used to locate the secret key. From the start position, the directions are followed, and the secret key is memorized. As a result of the image, the secret key associated with the original PIN 1234 is 1434. The secret key serves as the final PIN in this method. The second image in Fig. 8 illustrates how the final PIN for the lie sequence 1,111,000 is entered. The authentication process is complete after a successful attempt.

The method described above is resistant to multiple recordings because the final PIN is generated by the graphical interface using the arrows in the 2 x 5 matrix in conjunction with the original PIN. It generates 840 possible arrow combinations for locating the final PIN. To begin an attack, the attacker requires the original PIN in order to determine the required directions, which yields the final PIN.

3.3. Method III

This method, like Method II, employs a graphical user interface. The distinction is that this method does not require a second step, as authentication occurs entirely within the graphical password-based interface as portrayed in the Fig. 7. For instance, suppose the original PIN is 1234 and the generated sequence is 1101001, which indicates that the screen brightness is increased when1ı́s are used and decreased when0ı́s are used. The user selects the number from the start position in accordance with the directions specified in positions 1, 2, 3, and 4, as our original PIN is 1234. This is the tricky part; when the screen brightness is low, the user chooses any direction in order to make an error, and when the screen brightness is high, the user follows the directions mentioned.

Because the directions derived from the matrix and original PIN are used in conjunction with the screen brightness, the method described above is resistant to multiple recordings. When the screen brightness is low, the user can move in any of the four directions, which occurs three times during a session due to the low brightness. As a result, the chances of recovering the original PIN are extremely slim to non-existent.

4. Security analysis

This section examines the proposed methods' security against brute force, dictionary attacks, side channel attacks, spyware-based recording attacks, and smartphone theft.

Proposition 1. *The Proposed Methods Prevents Brute Force and Dictionary Attacks*

When a user attempts to access a social network using the proposed methods, each login generates a random lie sequence. By including the secret key and missing digits in random positions in the final PIN, the password space is significantly increased. Typically, these attacks will conduct an exhaustive search, iterating through every word in the dictionary or checking every possible combination of passwords. The probability of obtaining the final or original PIN, on the other hand, is extremely low, as only one password combination can be attempted at a time. The user has three tries to enter the correct password. As a result, attackers will struggle to obtain both the final PIN and the initial PIN (excluding the lies). The application will be locked if more than three attempts are made.

Proposition 2. *The Proposed Methods Prevents Side-Channel Attacks*

The methods proposed include the use of a secret key in conjunction with randomization, i.e. (including misleading digits in random positions), and communication with the user via screen brightness. Due to the fact that screen brightness is used as a security measure, malware may target the sensors on the smartphone. Smartphones of the modern era incorporate light sensors. As a result, a test is designed to assess BrightPass's resistance to these side-channel attacks. Almost certainly, the malware will use the light sensor as a backdoor to obtain the final PIN. This test makes use of the brightness values recorded by the light sensors during authentication sessions. This test was performed on a Xiaomi Redmi 4A smartphone. The examination takes place in a dimly lit room. While the brightness of the screen changed (from high to low), the light sensors recorded ambient light rather than the brightness value. The test returns zeros, indicating that ambient light, rather than the brightness value, is considered. As a result, the malware is unable to determine the final positions of the PIN digits. Even if the malware exploits a side channel other than the light sensor, it will be unable to compromise the smartphone due to the presence of the bogus digits alongside the original PIN and secret key. As a result, the available password space increases significantly.

Even if the malware intercepts keystrokes as the user enters the PIN, it will be unable to differentiate between the lies and the final PIN, as the lie sequence and secret key are constantly changing. Assume the malware records multiple authentication sessions and performs statistical analysis in order to determine the final PIN. This, however, is not possible because each session has its own final PIN and secret key. These tests establish that the proposed methods are sufficiently resilient to side-channel attacks.

Proposition 3. *The Proposed Methods Prevents Spyware based Recording Attacks*

The malware is capable of capturing screenshots of the authentication session or even recording the entire session, as well as collecting keystrokes from multiple authentication sessions. The proposed methods communicate with the user via the brightness of the screen, more precisely low and high. Because the malware does not capture the change in brightness values as the PIN is entered, the malware's sessions or screenshots do not contain enough information to obtain the original PIN. The malware is unable to obtain the PIN because the recordings maintain the same brightness level throughout the session.

Malware may launch multiple recording attacks, collect keystrokes from multiple authentication sessions, and cross-reference them to obtain the original PIN. This assault on the original BrightPass will be successful. This, however, is not possible in the environment of the proposed methods due to the addition of a secret key. As a result, the proposed techniques are resilient to spyware-based recording attacks.

Proposition 4. *The Proposed Methods Prevents Data Leak in case of the Theft of Smartphone*

The proposed methods are not intended to allow attackers to steal users' PINs, but rather to provide secure social network access authentication. The applications are sufficiently robust against a wide variety of attacks. Even if the device is stolen, successful authentication is impossible without knowledge of the device's original PIN and secret key. If an attacker obtains the PIN for one session, the PIN will be invalid for subsequent sessions. Thus, the security mechanisms underlying the proposed methods are sufficiently secure in the event of smartphone theft.

Proposition 5. *The Proposed Methods Prevents Data Leak in case of the Theft of mi-croSD*

The microSD card on which the applications are stored is designed to be adoptable, which means that it will not be detected by other smartphones. If the attacker attempts to modify or decrypt the data, the data on the microSD becomes corrupted, necessitating the attacker to format the microSD; otherwise, the aggregate data is unrecoverable. As a result, the secure element's security is superfluous.

5. Experimental evaluation

This section discusses the experiments conducted to enhance the application's security and the results of user testing. The tests are conducted to determine the proposed methods' authentication time.

5.1. Adoptable storage

e-BrightPass used a MicroSD card in conjunction with Adoptable Storage, rather than a predefined secure element. Android has always been receptive to external storage adapters. Nonetheless, due to their inherent impermanence and the inadequacy of data security provided by standard external storage, these devices have historically been limited to primary file storage. External storage media can now be used as internal storage in Android 6.0.

External storage media is formatted and encrypted in such a way that it can be used by only one Android device at a time. Due to the close connection between the storage media and the Android operating system, it is capable of securely storing all applications and private data for all consumers. The framework generates and stores encryption keys for each adopted device in the internal storage of the Android device. It secures the media effectively in the same way that internal storage is secured. Keys are associated with the adopted GUID partitions. If the system's internal storage is encrypted using File-Based Encryption (FBE), adoptable storage encrypts both the file system and the metadata. Unless specified otherwise, adoptable storage utilizes Full Disk Encryption (FDE).

Android 6.0+ is required to run the applications (Marshmallow). Adoptable storage was introduced in Android 6.0, allowing the use of an external MicroSD card as internal storage if the microSD card is class 10 or higher. This adaptable storage is critical to the security of applications. Adoptable storage is supported by the majority of Android 6.0+ builds. However, in some cases, smartphone manufacturers disable this feature by layering their OS on top of the Android platform. To enable adoptable storage on such smartphones, xda-developers collaborated with numerous Android developers to create the "aftiss toolkit."

5.2. User test results

The proposed methods are implemented using the following development tools: An-droid Studio 3.6.1, the Android SDK 7.0, and Java

Table 1
Comparison of the Security Parameters.

Security Parameter/Method	BrightPass	Method I	Method II	Method III
Resists side-channel attacks	yes	yes	yes	yes
Resists one-time recording attacks	yes	yes	yes	yes
Resists multiple recording attacks	yes	yes	yes	yes
Reveal of PIN using multiple recording attacks	no	yes	yes	yes

Table 2
User test results for the existing methods.

Method	Authentication time (sec)
BrightPass	6.73
Method I	9.88
Method II	11.35
Method III	10.35

1.8.0 are required. The testing apparatus consists of a Redmi 4A smartphone (Android v7.1.2, 1.4 GHz Cortex A53 processor, 3 GB RAM) and a SanDisk 32GB MicroSD class 10 card that serves as a secure element.

The study surveyed 40 users between the ages of 19 and 25. The procedure is explained to users, and they are given sufficient time to familiarize themselves with the applications. Each user validated the method ten times and kept track of their own authentication times. As a result, each authentication method received 400 authentication sessions in total. It is calculated the time interval between pressing the first key and the successful screen pop-up. Table 2 contains the user's test results. Due to the highly variable nature of the secret key, the probability of recovering the original PIN is extremely slim to non-existent. As a result, the methods are highly secure and scalable.

6. Discussions

This research has the advantage of proposing three alternative methods for mitigating the vulnerability mentioned in [22] and detailed by us in Section 2. Among the proposed methods, method I is the quickest to authenticate. On the other hand, every method is resistant to well-known attacks. All the proposed methods have the disadvantage of requiring slightly more time for authentication than the original BrightPass. When additional security is required, however, performance is always compromised. While all three of our methods increase authentication time, the first method is the quickest. As a result, our first method can be used when authentication time is critical. The study's limitation is that BrightPass is not supported by all mobile operating systems. As a result, our findings are limited to operating systems that utilize BrightPass for authentication.

7. Conclusion

Many users are required to add another layer of protection known as 2FA in order to safeguard sensitive data. However, the current two-factor authentication mechanisms are deemed insecure for use due to the threat of highly advanced malware and spyware. The majority of this malware targets smartphones, as almost everything is now accessible via them. In this work, we detailed a security weakness in the BrightPass that can be perpetrated by the recording attack. To bootstrap the security flaw, we presented three authentication methods by considering some merits of the BrightPass. Our security solutions are robust towards various known attacks. But the performance of the four methods is lower than the original BrightPass. Particularly, the three methods consume more authentication time than the traditional BrightPass authentication. When the security is of the BrightPass is of high priority, its performance is insignificant.

Declaration of Competing Interest

I am enclosing herewith a manuscript entitled "e-BrightPass: A Secure Way to Access Social Networks on Smartphones" for possible publication in Cyber Security and Applications.

With the submission of this manuscript, we would like to undertake that:

- We do not have any conflict of interest.
- All authors of this research paper have directly participated in the planning, execution, or analysis of this study.
- All authors of this paper have read and approved the final version submitted.
- The contents of this manuscript have not been copyrighted or published previously.
- The contents of this manuscript are not now under consideration for publication elsewhere.
- Our Institutes are fully aware of this submission.

Submitted manuscript is a Research Article and the corresponding authors are Dr. Vanga Odelu and Dr. Alavalapati Goutham Reddy.

Acknowledgment

This research was supported by the Fontbonne University, St. Louis, USA.

References

[1] Social take over social media security, 2021, Accessed on July 20, 2021, Available[online]: https://www.zerofox.com/resources/social-takeover-social-media-security/.
[2] R. Alguliyev, R. Aliguliyev, F. Yusifov, Role of social networks in e-government: risks and security threats, Online J. Commun. Media Technol. 8 (4) (2018) 363–376, doi:10.10007/1234567890. Springer, Heidelberg (2016)
[3] Global social networks ranked by number of users, 2021, Accessed on July 20,2021, Availa-ble[online]: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.
[4] B. Dean, Facebook demographic statistics: how many people use facebook in 2021?, 2021, Avilable [online]: https://backlinko.com/facebook-users.
[5] Social media statistics, 2021, Accessed on July 20, 2021, Available[online]: https://www.oberlo.in/blog/social-media-marketing-statistics.
[6] Statista, smartphones-statistics and facts, statista, hamburg, germany, 2020, Available[online]: https://www.statista.com/topics/840/smartphones/.
[7] B. Guo, Y. Ouyang, T. Guo, L. Cao, Z. Yu, Enhancing mobile app user understanding and marketing with heterogeneous crowd sourced data: a review, IEEE Access 7 (2019) 68557–68571.
[8] D. He, S. Chan, M. Guizani, Mobile application security: malware threats and defens-es, IEEE Wireless Commun. 22 (1) (2015) 138–144.
[9] G. Delac, M. Silic, J. Krolo, Emerging security threats for mobile platforms, in: Proceedings of the 34th International Convention MIPRO, IEEE, Opatija, Croatia, 2011, pp. 1468–1473.
[10] S. Mavoungou, G. Kaddoum, M. Taha, G. Matar, Survey on threats and attacks on mobile networks, IEEE Access 4 (2016) 4543–4572.
[11] D. Mikhaylov, I. Zhukov, A. Starikovskiy, S. Kharkov, A. Tolstaya, A. Zuykov, Review of malicious mobile applications, phone bugs and other cyber threats to mobile devic-es, in: in Proceedings of the 5th IEEE International Conference on Broadband Network & Multimedia Technology, IEEE, Kyoto, Japan, 2013, pp. 302–305.
[12] A.K. Jain, D. Shanbhag, Addressing security and privacy risks in mobile applications, IT Prof. 14 (5) (2012) 28–33.
[13] V. Odelu, A.K. Das, A. Goswami, A secure biometrics-based multi-server authentication protocol using smart cards, IEEE Trans. Inf. Forensics Secur. 10 (9) (2015) 1953–1966.
[14] A.G. Reddy, E.J. Yoon, A.K. Das, V. Odelu, K.Y. Yoo, Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment, IEEE Access 5 (2017) 3622–3639.

[15] N.L. Clarke, S.M. Furnell, Authentication of users on mobile telephones-a survey of attitudes and practices, Comput. Secur. 24 (7) (2005) 519–527.
[16] N.L. Clarke, S.M. Furnell, Authenticating mobile phone users using keystroke analysis, Int. J. Inf. Secur. 6 (1) (2007) 1–14.
[17] E. Ikhalia, C.O. Imafidon, The need for two factor authentication in social media, In Proceedings of the International Conference on Future Trends in Computing and Communication-FTCC 15 (1) (2013) 11.
[18] R.A. Botha, S.M. Furnell, N.L. Clarke, From desktop to mobile: examining the security experience, Comput. Secur. 28 (3–4) (2009) 130–137.
[19] S.M. Dye, K. Scarfone, A standard for developing secure mobile applications, Comput. Standard. Interfac. 36 (3) (2014) 524–530.
[20] A.J. Aviv, B. Sapp, M. Blaze, J.M. Smith, Practicality of accelerometer side channels on smartphones, in: In Proceedings of the 28th annual computer security applications conference, ACM, New York, NY, USA, 2012, pp. 41–50.
[21] L. Simon, R. Anderson, PIN Skimmer: Inferring PINs through the Camera and Microphone, in: In SPSM' 13: Proceedings of the Third ACM Workshop on Security and Privacy in Smartphones & Mobile Devices, ACM, New York, NY, USA, 2013, pp. 67–78.
[22] M. Guerar, M. Migliardi, A. Merlo, M. Benmohammed, F. Palmieri, A. Castiglione, Using screen brightness to improve security in mobile social network access, IEEE Trans. Dependable Secure Comput. 15 (4) (2016) 621–632.