Group 12 - An Analysis of Various Authentication Mechanisms in Mobile Systems

Sagar Parekh [Leader]
sjparekh@asu.edu

Arvinthan Sundaram Govindaraju [Deputy Leader]
asunda25@asu.edu

Mugdha Kolhe
mkolhe@asu.edu

Achyutha Bharadwaj
asbhara2@asu.edu

Dhrumil Shah
dpshah8@asu.edu

Sai Pragna Etikyala
setikyal@asu.edu

Venkatesan Murali
vmural17@asu.edu

Prajwal Kodi
pkodi@asu.edu

Harish Ravichandran
hravich4@asu.edu

The School of Computing, Informatics and Decision Systems Engineering
Arizona State University
Tempe, AZ 85281

1. Background And Motivation:

Mobile security can be defined as the protection of portable computing devices (laptops, smartphones, tablets) from threats and vulnerabilities. With the exponential increase in organizations moving towards expanding their mobility in order to engage more customers on different platforms, mobile security has become one of the biggest challenges. There is a greater need than ever to focus on mobile security because a lot of personal information is stored nowadays on these devices and an unauthorised access would cause significant consequences. With the significant increase in development and usage of wireless communication, there is a need to focus on addressing the threats and vulnerabilities that the portable computing devices are posed with. We have advanced into a world where we have access to biometric devices, sophisticated methods to recognize spoofing attacks and with big data solutions to authentication, we have come a long way. We are now looking at adaptive authentication, risk-based authentication systems emerging, which use different forms of authentication methods like passwords, pin, Yubikey, tokens, biometrics. But this doesn't guarantee 100% secured applications, every day several applications are being hacked into and the user's sensitive data is being comprised. We definitely have more scope to better our authentication methods. There is a greater need to understand the existing solutions and innovate. Usability is another important aspect that needs to be considered on the path to making applications more secure. If the authentication process is tedious, it is going to affect the usability of the application. That is why there is a need to choose the right form of authentication methods based on user profile and the application sensitivity. We need to study existing solutions to build and compare the user profile and calculate the risk and adapt. Due to high-speed internet availability and increase in mobile storage, accessibility to sensitive data has increased. So it is necessary to have a good authentication

mechanism to prevent potential security breaches. That is why there is a great need to study and improve present-day authentication processes and methods.

2. Goals and Scope:

Smartphone devices nowadays contain sensitive data and also access external sites through Apps and APIs. It is important to protect data against unauthorized access. One way to do that is to have a foolproof authentication which identifies users who can access this data. Our goal is to understand how these authentication systems protect vulnerable data and to explore and analyze modern authentication mechanisms for mobile devices and analyze their vulnerabilities and security concerns. To understand the advantages and disadvantages of each technique and decide which technique works for a given scenario.

Scope:

1. To understand and compare different authentication techniques.
2. To explore vulnerabilities and security concerns in authentication mechanisms.
3. To study the prevention of security breaches for these authentication techniques.
4. To list out the advantages and limitations of each technique.
5. To discuss at least one case study for each technique.

3. Results:

3.1 Threat Models:

Mobile phones nowadays are powerful devices, as they can perform a wide variety of tasks such as, play music, look for directions, mobile banking, send/receive emails, SMS, MMS, play videos, scan barcodes, etc. Due to its wide variety of uses and compact/portable size, the threat model for mobile systems differs compared with others such as client/server architectures. The goals of Attackers can be divided into three major categories,

- Collecting User's Private Data
- Exploiting Computation Power of the Device
- Perform Harmful Actions

Among these, the first two goals are Covert, while the last one is Harmful. Since mobile devices nowadays have essentially become storage units of personal data such as SMS, MMS, Email, Photos, Videos, etc., a single successful attack can land all of the user's private data in the hands of the attacker compromising the confidentiality and integrity of the stored information. Furthermore, the attacker can make use of the mobile devices' basic hardware such as inbuilt mic or camera to collect additional data from the user's surroundings. For example, the attacker can turn the mobile phone into a listening device by turning on the voice recording system. In recent years, the mobile devices have come into focus for malicious exploits, such as the deployment of botnets, with aim of covertly exploiting the raw computing power in combination with broadband network access. The following are some of the attacks on mobile systems we have analyzed, **Brute Force**:

Using an automated process of trial and error, the attacker can guess the user's password, pin etc. **Weak Password Recovery Validation**: Allows an attacker to access a mobile device that provides them with the ability to illegally obtain, change, or recover another user's password. **Shoulder Surfing:** This an observation attack, attackers may steal user's sensitive information through direct observation, particularly at crowded places. **Smudge Attack:** Smudge attack is possible when latent smudges of fingerprints are visible after a user uses the smartphone to unlock it. **Spoofing:** This attack is aimed at biometric authentication systems. In this attack, the attacker tries to imitate the user by making use of fake biometric samples or some type of synthetically produced artifact. **Alteration Attack:** Alterations are applied to different biometric modalities to try and gain unlawful access to private data.

3.2 Security Models:

3.2.1 Android Security Models:

Android is built on top of the Linux kernel which is responsible for the execution of application by interacting with the operating system, development frameworks, and core libraries. As Android applications are sharing the same resources, drivers; it becomes necessary to prevent one application not to influence the execution of other application and as well as not to steal the private data. Android has already implemented a security model called Sandbox. Sandboxing is performed at the Linux Kernel Level. In order to achieve isolation, Android utilizes standard Linux access control mechanisms. Each Android application package (.apk) is on installation assigned a unique Linux user ID.

This functionality is useful for providing a secure environment for application execution but it reduces the overall application functionality. To enhance the user experience by not compromising the security, there are two mechanism implemented in android. 1. Shared User ID: It allows applications to share data and application components. The developers can bypass the isolation model restrictions by signing applications with the same private key. 2. Permissions: Each Android application can request and define a set of permissions.

3.2.2 IOS Security Models

iOS security model provides different philosophy for achieving mobile device security and user‟s protection. Each application submitted by a third party developer is sent to the revision process. which makes sure that the application is safe before it is released the application store. The iOS security APIs are located in the Core Services layer of the operating system and are based on services in the Core OS (kernel) layer of the operating system. Keychain Services API: It is used to store passwords, keys, certificates, and other secret data. CFNetwork is a high-level API: It is used to create and maintain secure data streams and to add authentication information to a message. The Certificate, Key, and Trust Services API: It is used to create, manage, and read certificates, keychain, encryption keys. Randomization Services: It is used to get cryptographically secure pseudorandom numbers.

The Linux kernel is responsible for executing core system services such as memory access, process management, access to physical devices through drivers, network management and security. This approach allows the IOS to enforce standard Linux file access rights. Since each file is associated with its owner"s user ID, applications cannot access files that belong to other applications without being granted appropriate permissions. This way an application cannot compromise system security by running native code in privileged mode.

3.3 Authentication Techniques:

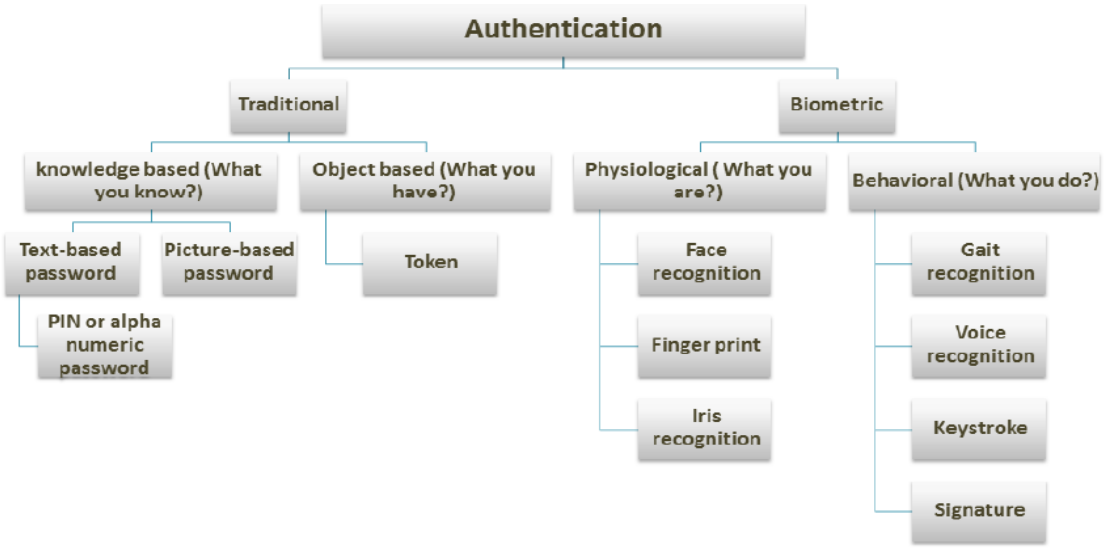

Fig. 1. classification of authentication techniques

3.3.1 Traditional Mobile Authentication Technique:

Traditionally, authentication methods are either knowledge-based or object-based authentication. Knowledge-based method depends on what the user already knows, whereas object-based method depends on what the user already has.

3.3.1.1 Knowledge-based authentication (What you know):

They include two classes: text-based and picture-based passwords. Text-based passwords include two subclasses: 1. PINs and 2. Alphanumeric passwords. PIN is also used to protect the SIM card. After 3 failed attempts to enter the PIN, the SIM locks out and the PUK (PIN UnlocK) is then requested. If the PUK is also falsely inputted for 10 times, the SIM becomes useless. On the other hand, Alphanumeric passwords make more difficult to guess and maximize the probability to accept imposters.

3.3.1.2 Object-based authentication (What you have):

Object-based authentication techniques were developed as a second factor for authentication besides the password. These techniques include Token-based authentication. The tokens are physical devices

storing passwords. Using token for authentication means that a user deals with some hardware to carry out the authentication process. This hardware contains software programs that implement a One-Time Password (OTP) algorithm to provide changed-over- time PIN (random password) which is synchronized with a server. Seed value of the PIN and timestamp are given to a token algorithm to make predicting the random password more difficult to attackers.

3.3.2 Single Sign-on and Multifactor Authentication

Single sign-on (SSO) is a technique that uses a single action of authentication to give an authorized user to access many related, but independent software systems or applications without being prompted to log in again at each of them during a particular session. The advantage of this system is to do a login for a single time for accessing multiple applications. Multi-factor authentication is a technique of using an extra level of authentication on top of an existing one. This gives an extra layer of security on top of a given method. While doing multi-factor authentication we mainly do user authentication on mobile devices: ordinary pass-words, and one-time passwords.

3.3.3 Biometric Authentication:

Biometrics technology is based on the principle of measuring and examining the biological traits of individuals, extracting the unique features from this acquired data and then comparing it with the template set stored in the biometric templates database. These unique biological traits are called biometric identifiers and can be of two types – physiological and behavioral. Some of the common biometric methods include: Face Recognition, Fingerprint technology, Voice Recognition**.** Biometric Authentication method focuses on the behavioral matrices like touch dynamics, keystroke patterns, gait features and many more. Biometric features could also be evaluated by means of the following seven characteristics: Universality: every person should have the biometrics. Uniqueness: no two persons are expected to have such identical biometrics. Permanence: the biometrics should not vary with time. Collectability: the biometrics should be easily collected and measurable. Performance: the accuracy of the biometrics should be stable under varied environmental circumstances. Acceptability: common users should widely accept the sample collection of the biometrics. Circumvention: the biometrics should be difficult to deceive and fool.

3.3.3.1 Physical Biometrics for Authentication:

With the growing number of applications using computer networks and the increasing concern for identity theft, the deployment of biometric authentication systems is becoming more and more important. Biometric authentication systems are trustworthy and secure where biometric data cannot be forgotten or divined. Biometric systems are based on two stages: Enrollment refers to the stage where biometric features are extracted and stored as a reference in the database. In the authentication stage, extracted features from query trait are matched against the reference features. Despite having these advantages over traditional authentication systems, biometric systems are not yet developed enough to

have perfect security and privacy. Thus, they can be attacked using several strategies. Alteration is one of the critical attacks against biometric systems. The impostor alters the image of the real user and he presents it as a request in order to gain unlawful access to the system. Analysis shows that both systems are vulnerable to the proposed attack and the alteration level has a serious impact on the security of biometric systems.

3.3.3.2 Unimodal and Multimodal Biometric Authentication Techniques:

Unimodal uses a single biometric trait of an individual while multimodal uses many traits – for example, fusion of face and fingerprint technology. A problem with unimodal is only one trait is used and if noise cancellation is not properly done, verification would be an issue. Multimodal technique combines 2 or more techniques like face and fingerprint techniques. Even though the multimodal technique is complex, it is more secure and with the right techniques, user experience can be improved. For instance, instead of asking the user to speak and stand in front of a camera for authentication, they can record a video which has both voice and face. Multimodal authentication has become prevalent in recent times due to its security features.

3.3.4 Transparent and Oneshot authentication:

Transparent authentication is a kind of authentication where a user using the phone is continuously verified as the owner of the mobile device in a non-intrusive manner. One-shot authentication is a kind of authentication where the users are authenticated once before a session. This involves methods such as a passcode or a lock pattern found in typical smartphones. Transparent authentication is used to solve the drawbacks of one-shot authentication.

3.3.5 Continuous Authentication :

Once a user has logged into his mobile, we are not sure if it is the owner who is still using the device or an impostor. To overcome traditional authentication issues, both biometrics and security research communities have developed techniques for continuous authentication on mobile devices. Continuous authentication systems essentially make use of physiological and behavioral biometrics, using built-in sensors and accessories such as the gyroscope, touch screen, accelerometer, orientation sensor, and pressure sensor, to continuously monitor user identity. For example, the front camera of a phone can capture images of the user and continuously authenticate the user. This ensures that the person using the device is actually the owner and not an impostor.

3.3.6 Adaptive Authentication:

Adaptive authentication helps us secure the authentication process by identifying any anomalies in the attribute factors from the context information. Adaptive authentication is helpful in avoiding high risk and suspicious login attempts. Adaptive authentication enables customization of an authentication process for a user based on certain login attributes like location, proximity to devices and various other

parameters. Nowadays services are adopting authentication which is less intrusive like keystrokes dynamics, gait recognition, user voice etc. But there is no one-size-fits-all type of authentication and where adaptive authentication plays an important role. We need to sense the environment and customize our authorization for more usable, secure systems.

4. Tasks Summary:

4.1 Task Progress Table:

Task Name	Start Date	End Date	Status	Tentative Meeting Dates
Read the paper and provide the proposal	1/14/2019	1/20/2019	Completed	1/14/2019
Distribute the topic, do the initial proposal and 1st group of summaries	1/21/2019	1/27/2019	Completed	1/21/2019
2nd group of summaries and list of references	1/28/1019	2/03/2019	Completed	1/28/1019
3rd group of summaries	2/04/2019	2/10/2019	Completed	2/04/2019
4th group of summaries	2/11/2019	2/17/2019	Completed	2/11/2019
5h group of summaries and preparation of interim report	2/15/2019	2/24/2019	Ongoing	2/15/2019
6th group of summaries and submission of interim report	2/25/2019	3/03/2019	Upcoming	2/25/2019
Spring break	3/04/2019	3/10/2019	Upcoming	3/04/2019
7th group of summaries and preparation of final report	3/11/2019	3/17//2019	Upcoming	3/11/2019
8th group of summaries and preparation of final report	3/18/2019	3/24//2019	Upcoming	3/18/2019
9th group of summaries and preparation of final report	3/25/2019	3/31/2019	Upcoming	3/25/2019
Finalizing of final report	4/01/2019	4/07/2019	Upcoming	4/01/2019
Preparation of presentation	4/08/2019	4/14/2019	Upcoming	4/08/2019
Preparation of presentation	4/15/2019	4/21/2019	Upcoming	4/15/2019
Finalizing ppt and presentation	4/22/2019	4/28/2019	Upcoming	4/22/2019

4.2 Individual Progress:

Name	References Read	References to be read
Sagar Parekh	[87][61][28][1][74]	[64][11][86][59]
Arvinthan Sundaram Govindaraju	[6][65][31][47][34]	[34][9][8][19]
Mugdha Kolhe	[21][42][75][22][23]	[56][81][24][43][27]
Achyutha Bharadwaj	[30][54][49][70]	[5][76][20][53][37][16]
Dhrumil Shah	[39][77][78][31][40]	[45][46][44][79]
Sai Pragna Etikyala	[51][12][15][65]	[3][4][13][65]
Prajwal Kodi	[68][71][80][72]	[73][10][55][47][7]
Venkatesh Murali	[67][25][17][14][85]	[84][33][62][26]
Harish Ravichandran	[50][58][44][31][65]	[32][87][83][60]

4.3 Distribution of References into Set of Summaries:

Sets of Summaries	Reference No	Status
1st Group of Summaries	[87][6][21][30][39][][50][67][68]	Completed
2nd Group of Summaries	[60][18][41][53][77][51][58][17][71]	Completed
3rd Group of Summaries	[62][65][74][49][78][12][44][62][80]	Completed
4th Group of Summaries	[1][31][22][70][5][15][31][26][72]	Completed
5th Group of Summaries	[74][47][23][5][40][65][59][86] [38]	Completed
6th Group of Summaries	[63][34][55][76][55][3][32][85][73]	Upcoming
7th Group of Summaries	[84][9][80][20][45][4][11][84][10]	Upcoming
8th Group of Summaries	[17][][24][53][52][13][83][17][55]	Upcoming
9th Group of Summaries	[33][8][42][37][42][65][60][33][47]	Upcoming
10th Group of Summaries	[25][19][27][16][79][][][25][7]	Upcoming

5. References:

1. Z. Hills, D. F. Arppe, A. Ibrahim and K. El-Khatib, "Compound Password System for Mobile," 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Glasgow, 2018, pp. 1-4.
2. OpenSpan."Adaptive Authentication Superior User Experience and Growth Through Intelligence Security".(2018).
3. "Kim, Jae-Jung, and Seng-Phil Hong. "A method of risk assessment for multi-factor authentication." Journal of Information Processing Systems 7.1 (2011): 187-198.
4. OpenSpan."Adaptive Authentication Superior User Experience and Growth Through Intelligence Security".(2018).
5. Bassi, M. and Triverbi, P., 2018, March. Human Biometric Identification through Brain Print. In *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 1514-1518). IEEE.
6. Y. Li, H. Hu, G. Zhou and S. Deng, "Sensor-Based Continuous Authentication Using Cost-Effective Kernel Ridge Regression," in IEEE Access, vol. 6, pp. 32554-32565, 2018.
7. Ghasemisharif, Mohammad et al. “O Single Sign-Off, Where Art Thou? An Empirical Analysis of Single Sign-On Account Hijacking and Session Management on the Web.” USENIX Security Symposium (2018).
8. G. M. Parimi, P. P. Kundu and V. V. Phoha, "Analysis of head and torso movements for authentication," 2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA), Singapore, 2018, pp. 1-8.
9. M. Smith-Creasey, F. Albalooshi and M. Rajarajan, "Context Awareness for Improved Continuous Face Authentication on Mobile Devices," 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Athens, 2018, pp. 644-652.
10. Aaron Dale SANDERS ,COMPARTMENTALIZED MULTI - FACTOR AUTHENTICATION FOR MOBILE DEVICES in United States
    (12) Patent Application Publication Jan 4 ,2018
11. A. Bianchi, I. Oakley and H. Kim, "PassBYOP: Bring Your Own Picture for Securing Graphical Passwords," in IEEE Transactions on Human-Machine Systems, vol. 46, no. 3, pp. 380-389, June 2016.
12. Arias-Cabarcos, Patricia, and Christian Krupitzer. "On the design of distributed adaptive authentication systems." (2017): 1-5.
13. "Jagadamba, G., and B. Sathish Babu. ""Adaptive Security Schemes based on Context and Trust for Ubiquitous Computing Environment: A Comprehensive Survey."" Indian Journal of Science and Technology 9.48 (2017)."
14. Sharma, Manisha, Raju Baraskar, and Shikha Agrawal. "A Comparative Analysis of Unimodal and Multimodal Biometric Systems." International Journal of Advanced Research in Computer Science 8.5 (2017).

15. Misbahuddin, Mohammed, B. S. Bindhumadhava, and B. Dheeptha. "Design of a risk based authentication system using machine learning techniques." 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). IEEE, 2017.
16. Yamagami, R. and Yamazaki, Y., 2017, November. Biometric Bit String Generation from Handwritten Initials on Smart Phones. In Computing and Networking (CANDAR), 2017 Fifth International Symposium on (pp. 516-521). IEEE.
17. Khamis, Mohamed, et al. "GazeTouchPIN: protecting sensitive data on mobile devices using secure multimodal authentication." Proceedings of the 19th ACM International Conference on Multimodal Interaction. ACM, 2017.
18. V. Patel, M. Burns, R. Chandramouli, R. Vinjamuri, "Biometrics based on hand synergies and their neural representations", IEEE Access, vol. 5, pp. 13422-13429, 2017.
19. R. Kumar, P. P. Kundu, D. Shukla and V. V. Phoha, "Continuous user authentication via unlabeled phone movement patterns," 2017 IEEE International Joint Conference on Biometrics (IJCB), Denver, CO, 2017, pp. 177-184.
20. Jamdar, C. and Boke, A., 2017, August. Multimodal biometric identification system using fusion level of matching score level in single modal to multi-modal biometric system. In 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS) (pp. 2277-2280). IEEE.
21. Z. Akhtar, A. Buriro, B. Crispo and T. H. Falk, "Multimodal smartphone user authentication using touchstroke, phone-movement and face patterns," 2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Montreal, QC, 2017, pp. 1368-1372.
22. T. Enamamu, N. Clarke, P. Haskell-Dowland, and F. Li, "Smart Watch based Body-Temperature Authentication", ICCNI 2017: International Conference on Computing, Networking and Informatics (IEEE).
23. M. Argyriou, N. Dragoni, and A. Spognardi, "Security Flows in OAuth 2.0 Framework: A Case Study", 2017, SAFECOMP 2017 Workshops, LNCS 10489, pp. 396–406.
24. Y. Balaj, "Token-Based vs Session-Based Authentication: A survey", 2017.
25. Parkavi, R., KR Chandeesh Babu, and J. Ajeeth Kumar. "Multimodal biometrics for user authentication." Intelligent Systems and Control (ISCO), 2017 11th International Conference on. IEEE, 2017.
26. Gofman, Mikhail I., et al. "Multimodal biometrics for enhanced mobile device security." Communications of the ACM 59.4 (2016): 58-65. 2017.
27. Victor Sucasas, Georgios Mantas, Ayman Radwan, Jonathan Rodriguez, "An OAuth2-based protocol with strong user privacy preservation for smart city mobile e-Health apps", May 2016.
28. Toan Van Nguyen, Napa Sae-Bae, Nasir Memon,DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices,Computers & Security,Volume 66,2017,Pages 115-128.
29. A. Bianchi, I. Oakley and H. Kim, "PassBYOP: Bring Your Own Picture for Securing Graphical Passwords," in IEEE Transactions on Human-Machine Systems, vol. 46, no. 3, pp. 380-389, June 2016.

30. Corpus, K.R., Gonzales, R.J.D., Morada, A.S. and Vea, L.A., 2016, May. Mobile user identification through authentication using keystroke dynamics and accelerometer biometrics. In Mobile Software Engineering and Systems (MOBILESoft), 2016 IEEE/ACM International Conference on (pp. 11-12). IEEE.
31. Buriro, Attaullah et al. “Hold and Sign: A Novel Behavioral Biometrics for Smartphone User Authentication.” 2016 IEEE Security and Privacy Workshops (SPW) (2016): 276-285V. M. Patel, R. Chellappa, D. Chandra and B. Barbello, "Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges," in IEEE Signal Processing Magazine, vol. 33, no. 4, pp. 49-61, July 2016.
32. Stylios, Ioannis & Thanou, Olga & Androulidakis, Iosif & Zaitseva, Elena. (2016). A Review of Continuous Authentication Using Behavioral Biometrics. 10.1145/2984393.2984403.
33. Reich, C. "Continuous and transparent multimodal authentication: reviewing the state of the art." (2016).
34. S. Sarkar, V. M. Patel, and R. Chellappa, “Deep feature-based face detection on mobile devices,” in Proc. IEEE Int. Conf. Identity, Security and Behavior Anal., 2016.
35. V. M. Patel, R. Chellappa, D. Chandra and B. Barbello, "Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges," in IEEE Signal Processing Magazine, vol. 33, no. 4, pp. 49-61, July 2016.
36. Waggett, Peter. "Risk-based authentication: biometrics' brave new world." Biometric Technology Today 2016.6 (2016): 5-7.
37. Singh, S., Singh, A. and Kumar, R., 2016, March. A constraint-based biometric scheme on ATM and swiping machine. In Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 International Conference on (pp. 74-79). IEEE.
38. Yohan, Alexander et al. “Dynamic multi-factor authentication for smartphone.” 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (2016): 1-6.
39. Meng, Weizhi et al. “Surveying the Development of Biometric User Authentication on Mobile Phones.” IEEE Communications Surveys & Tutorials 17 (2015): 1268-1293.
40. Temper, Marlies et al. “Touch to Authenticate — Continuous Biometric Authentication on Mobile Devices.”
41. 2015 1st International Conference on Software Security and Assurance (ICSSA) (2015): 30-35.
42. H. Sun, K. Sun, Y. Wang, and J. Jing, "TrustOTP: Transforming Smartphones into Secure One-Time Password Tokens", 2015 ACM. ISBN 978-1-4503-3832-5/15/10
43. K. Krol, E. Philippou, E. De Cristofaro, M. Angela Sasse, “They brought in the horrible key ring thing!” Analysing the Usability of Two-Factor Authentication in UK Online Banking, USEC ’15, 8 February 2015, San Diego, CA, USA
44. Saevanee, Hataichanok & Clarke, Nathan & Furnell, Steven & Biscione, Valerio. (2015). Continuous user authentication using multi-modal biometrics. Computers & Security. 53. 10.1016/j.cose.2015.06.001.
45. Murmuria, Rahul et al. “Continuous Authentication on Mobile Devices Using Power Consumption, Touch Gestures and Physical Movement of Users.” RAID (2015).
46. Hoang, Thang et al. “Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme.” International Journal of Information Security 14 (2015): 549-560.

47. Ye, Quanqi et al. “Formal Analysis of a Single Sign-On Protocol Implementation for Android.” 2015 20th International Conference on Engineering of Complex Computer Systems (ICECCS) (2015): 90-99.
48. D. Crouse, H. Han, D. Chandra, B. Barbello, and A. K. Jain, “Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data,” in Int. Conf. Biometrics, 2015, pp. 135–142.
49. Lafkih, M., Lacharme, P., Rosenberger, C., Mikram, M., Ghouzali, S., El Haziti, M., Abdul, W. and Aboutajdine, D., 2015, November. Application of new alteration attack on biometric authentication systems. In Anti-Cybercrime (ICACC), 2015 First International Conference on (pp. 1-5). IEEE.
50. Alotaibi, Saud nejr & Furnell, Steven & Clarke, Nathan. (2015). Transparent authentication systems for mobile device security: A review. 406-413. 10.1109/ICITST.2015.7412131.
51. Bakar, Khairul Azmi Abu, Nor Izyani Daud, and Mohd Shafeq Md Hasan. "ADAPTIVE AUTHENTICATION: ACase STUDY FOR UNIFIED AUTHENTICATION PLATFORM.(2015)"
52. Saevanee, Hataichanok et al. “Text-Based Active Authentication for Mobile Devices.” SEC (2014).
53. Eastwood, S.C., Shmerko, V.P., Yanushkevich, S.N. and Drahansky, M., 2014, August. Biometric intelligence in authentication machines: From talking faces to talking robots. In Advanced Applied Informatics (IIAIAAI), 2014 IIAI 3rd International Conference on (pp. 763-768). IEEE.
54. Galbally, J., Marcel, S. and Fierrez, J., 2014. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. IEEE transactions on image processing, 23(2), pp.710-724.
55. Chhatwani, Rinky G. and Dr. D. G. Harkut. “Implementation of Single Sign-On Mechanism for Distributed Computing MS .” (2014).
56. K. Gibbons, J. Raw, and K. Curran, "Security evaluation of the OAuth 2.0 framework", Vol. 22, No. 3, December 2014, ISSN: ISSN: 0968-5227.
57. Atwater, A., Khan, H., Hengartner, U.: POSTER: when and how to implicitly authenticate smartphone users. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security,pp. 1415–1417. ACM, Scottsdale, Arizona, USA(2014).
58. M. Tanviruzzaman and S. I. Ahamed, "Your Phone Knows You: Almost Transparent Authentication for Smartphones," 2014 IEEE 38th Annual Computer Software and Applications Conference, Vasteras, 2014, pp. 374-383. doi: 10.1109/COMPSAC.2014.60
59. Khan, Hassan & Atwater, Aaron & Hengartner, Urs. (2014). Itus: An implicit authentication framework for Android. Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM. 10.1145/2639108.2639141.
60. Xu, H & Zhou, Y & Lyu, M.R.. (2014). Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones. Proc. SOUPS. 187-198.
61. Amin, Reham & Gaber, Tarek & Eltaweel, Ghada & Hassanien, Aboul Ella. (2014). Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues. 10.1007/978-3-662-43616-5_16.
62. Aronowitz, Hagai, et al. "Multi-modal biometrics for mobile authentication." Biometrics (IJCB), 2014 IEEE International Joint Conference on. IEEE, 2014.

63. "Bakar, Khairul Azmi Abu, and Galoh Rashidah Haron. ""Adaptive authentication based on analysis of user behavior."" Science and Information Conference (SAI), 2014. IEEE, 2014.
64. S. Indu, T. N. Sathya and V. Saravana Kumar, "A stand-alone and SMS-based approach for authentication using mobile phone," 2013 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2013, pp. 140-145.
65. Bakar, Khairul Azmi Abu, and Galoh Rashidah Haron. "Adaptive authentication: Issues and challenges." Computer and Information Technology (WCCIT), 2013 World Congress on. IEEE, 2013.
66. M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, “Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication,” IEEE Trans. Inform. Forensics and Security, vol. 8, no. 1, pp. 136–148, 2013.
67. Rastogi, Vaibhav, Yan Chen, and William Enck. "AppsPlayground: automatic security analysis of smartphone applications." Proceedings of the third ACM conference on Data and application security and privacy. ACM, 2013.
68. Polla, Mariantonietta La et al. “A Survey on Security for Mobile Devices.” IEEE Communications Surveys & Tutorials 15, (2013)
69. Aly, Ola M., et al. "Multimodal biometric system using iris, palmprint and finger-knuckle." International journal of computer applications 57.16 (2012).
70. Paul, S., Gupta, D. and Tiwari, A., 2012, September. Indexed search strategy for an automated biometric identification system. In Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the (pp. 1-6). IEEE.
71. V. Radhaa, D. Hitha Reddya, A Survey on Single Sign-On Techniques, aInstitute for Development and Research in Banking Technology,Road #1, Castle Hills, Masab Tank, Hyderabad – 500 067 (A.P), INDIA, 2012.
72. Corella, Francisco and Karen P. Lewison. “Strong and Convenient Multi-Factor Authentication on Mobile Devices.” (2012).
73. Carullo, Giuliana et al. “Towards Improving Usability of Authentication Systems Using Smartphones for Logical and Physical Resource Access in a Single Sign-On Environment.” (2012).
74. P. Tanvi, G. Sonal and S. M. Kumar, "Token Based Authentication Using Mobile Phone," 2011 International Conference on Communication Systems and Network Technologies, Katra, Jammu, 2011, pp. 85-88.
75. B. Cha, N. Kim, and J. Kim, "Prototype Analysis of OTP Key-generation based on Mobile Device using Voice Characteristics", 2011
76. Omelina, Ľ. and Oravec, M., 2011, June. Universal biometric evaluation system: Framework for testing evaluation and comparison of biometric methods. In Systems, Signals and Image Processing (IWSSIP), 2011 18th International Conference on (pp. 1-4). IEEE.
77. Maiorana, Emanuele et al. “Keystroke dynamics authentication for mobile phones.” SAC(2011).
78. Li, Fudong et al. “Behaviour Profiling for Transparent Authentication for Mobile Devices.” (2011).

79. Niinuma, Koichiro et al. “Soft Biometric Traits for Continuous User Authentication.” IEEE Transactions on Information Forensics and Security 5 (2010): 771-780.
80. Marise-Marie and D’Costa-Alphonso. “The adoption of single sign-on and multifactor authentication in organisations: a critical evaluation using TOE framework.” (2010).
81. Y. Lee, H. Lim, H. Lee, "A study on efficient OTP generation using stream cipher with random digit", Advanced Communication Technology (ICACT), 2010 The 12th International Conference on, Volume: 2
82. Riener, Andreas. (2011). Continuous Authentication based on Biometrics: Data, Models, and Metrics. 10.4018/978-1-61350-129-0.
83. Nathan Clarke. 2011. Transparent User Authentication: Biometrics, RFID and Behavioural Profiling (1st ed.). Springer Publishing Company, Incorporated.
84. Kang, Byung Jun, and Kang Ryoung Park. "Multimodal biometric authentication based on the fusion of finger vein and finger geometry." Optical Engineering 48.9 (2009): 090501.
85. Snelick, Robert, et al. "Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems." IEEE transactions on pattern analysis and machine intelligence 27.3 (2005): 450-455.
86. Bigun, Josef, et al. "Multimodal biometric authentication using quality signals in mobile communications." null. IEEE, 2003.
87. Parreno Centeno, Mario & van Moorsel, Aad & Castruccio, Stefano. (2017). Smartphone Continuous Authentication Using Deep Learning Autoencoders. 147-1478. 10.1109/PST.2017.00026.
88. Delac, G., Silic, M. and Krolo, J., 2011, May. Emerging security threats for mobile platforms. In 2011 Proceedings of the 34th International Convention MIPRO (pp. 1468-1473). IEEE.