BOOK CHAPTER | One Hand – Five Fingers

Multi-Factor Authentication for Online Security of Android Devices

Benjamin Baafi
Law & IT/Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: benjaminbaafi@ymail.com
Phone: +233244058435

ABSTRACT

Digitalization decisively penetrates all the sides of modern society. One of the critical enablers to maintaining this process secure is using Authentication. It spreads many different areas of a hyper-connected world, including online payments, communications, access-right management, and others. This paper sheds light on the evolution of authentication systems toward Multi-Factor Authentication (MFA). Multi-factor Authentication is expected to be utilized for human-to-everything interactions by enabling fast, user-friendly, and reliable Authentication when accessing a service. This paper surveys how multi-factor authentication schemes can be used to secure online-android devices.

Keywords: Multi-Factor Authentication, Online Security, Android Devices, Cybercrimes

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Benjamin Baafi (2022): Multi-Factor Authentication for Online Security of Android Devices
SMART-IEEE-Creative Research Publications Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics.
Pp 77-80. www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P13

1. INTRODUCTION

Currently, MFA is expected to be utilized in scenarios where safety requirements are higher than usual. According to S.C. Media U.K., 68% of Europeans are willing to access biometric Authentication for payment transactions. Consider the daily routine of cash withdrawal using ATM services. Here, the client has to provide a card representing the ownership factor and support it with a PIN code representing the knowledge factor in accessing a personal account and withdrawing funds. This system could be more complex by adding a second channel like a one-time password to be keyed after the card and the user password was presented. It could be performed with the facial recognition methods in a more interesting scenario. Also, a recent survey discovered that 30% of companies planned to implement the MFA scheme in 2017, with 51% claiming that they already utilize MFA and 38% saying they operate it in “some areas” of operation.

This evidence supports the MFA as a promising direction of the authentication evolution. As one of the fascinating future trends, Authentication between a vehicle and its owner or a temporary user may be considered. Based on the statistics, a car is stolen every 45 s in the U.S. The current authentication method for starting and using the vehicle is still an immobilizer key. The MFA may critically improve access to most electronic devices from security and user experience perspectives.

1.1 Background to the Study

Mobile multi-factor schemes can be categorized according to (1) what is protected with the second authentication token (the OTP) and (2) how the OTP is generated. What does multi-factor Authentication protect? Multi-factor schemes are widely deployed in online banking and login authentication processes in two major application areas. Online banking applications use TANs (Transaction Authentication Numbers) as an OTP to validate transactions submitted by the clients to the financial institution. TANs are cryptographically bound to the transaction data and only valid for the given transaction. Recently, large Internet service providers such as Google, Apple, Dropbox, Facebook, etc. were also deployed multi-factor login schemes. These applications use OTPs during the user authentication process to mitigate attacks on user passwords, such as phishing and key loggers. Where are OTPs created?

OTP can be either created locally on the client-side (e.g., on the user's mobile device) or by the service provider on the server-side with an OTP transfer to the user via an out-of-band (OOB) channel link. Client-side OTP algorithms may, for example, rely on a shared secret and time synchronization between the authentication server and the client or a counter-based state that is transmitted between the client and the server. This technique allows the OTP to be generated offline, as no communication with the server is required. In contrast, server-side developed OTPs use OOB channels to share an OTP from the server to the client. The most common direct OOB is SMS messaging over cellular networks, which offers high availability for users, as usually, any mobile phone is capable of receiving SMS messages. However, SMS-based services incur additional costs. Hence, many service providers propose alternative solutions that use the Internet to transmit the OTP with no extra costs directly.

For instance, a mobile application could receive an encrypted OTP sent from the server over the Internet and then decrypt and show the OTP to the client. As a downside, internet-based OTP sharing require the customer's phone to be online during the authentication process. An alternative to an online application is an indirect OOB channel between a mobile app and a server via the user's P.C. This solution uses the P.C.'s Internet connection to transfer and encrypted OTP from the server to the P.C. and a side-channel to transfer the OTP from the P.C. to the mobile phone for decryption. The server can instantly generate and encrypt an OTP (or a nonce), share it with the P.C. in a visual cryptogram, and display it on a website. The mobile device then scans and decrypts the cryptogram to get this value. The transferred data is encrypted on the server side and decrypted on the mobile device. The P.C. cannot get it in plain text. This solution does not demand a mobile phone connected to the Internet. In practice, this approach is used by visual TAN solutions, which are increasingly gaining popularity in online banking.

2. RELATED LITERATURE

Mobile multi-factor authentication schemes Balfanz et al. aim to prevent misuse of the smartcard plugged into the computer by viruses without user knowledge. They cherish replacing the smartcard with a trusted handheld device that asks the user for permission before performing sensitive operations. Aloul et al. utilize an authorized mobile device as an OTP generator or as a means to establish an OOB communication channel to the bank (via SMS). Mannan et al. propose an authentication scheme that is tolerant against session hijacking, keylogging, and phishing.

Their system relies on a trusted mobile device to perform security-sensitive computations. Starnberger et al. propose an authentication technique called QR-TAN, which belongs to the class of visual TAN solutions. It demands the user to confirm transactions with the trusted mobile using optical Q.R. barcodes. Clarke et al. propose using a trusted mobile device with a camera and OCR as a communication channel to the mobile. The Foolproof phishing prevention solution utilizes an authorized user's cellphone to generate a supportive token for online banking transaction authentication. All these remedies assume that the user's mobile device is trustworthy. Attacks on SMS-based TAN authentication Mulliner et al. Analyze attacks on OTPs sent via SMS and describe how smartphone Trojans can intercept SMS-based TANs.

They also describe countermeasures against their attack, such as dedicated OTP channels, which regular apps cannot easily block. Their aggression and countermeasure assume that an attacker has no root privileges, which we argue are not sufficiently secure in the adversary setting nowadays. Schartner et al. present an attack against SMS-based TAN remedy for the case when a single device, the user's mobile phone, is used for online banking. The proposed attack scenario is relatively straightforward as the assumption of using a single device eliminates challenges such as cross-platform infection or mapping of devices to a single user.

Many banks already acknowledge this vulnerability and disable TAN-based Authentication for banking app customers. Cross-platform infection. The first malware spreading from smartphones to P.C. was discovered in 2005 and targeted Symbian O.S. Infection occurred as soon as the phone's memory card was plugged into the computer. Another example of cross-platform infection from P.C. to the mobile phone is a proof-of-concept malware that had been anonymously sent to the Mobile Antivirus Research Association in 2006. The virus affected the Windows desktop and mobile operating systems and emerged as soon as it detected a connection using Microsoft's ActiveSync synchronization application. Another well-known cross-platform infection attack is a complex worm, Stuxnet, extending via USB keys and targeting industrial software and equipment.

3. RESEARCH GAPS/FINDINGS

The paper revealed that Authentication is now very critical more than ever. In the digital era, most client will rely on biometrics concerning application security and validation to complement the traditional passwords. Not regarding privacy, security, usability, and accuracy concerns are still in place. MFA has become an application that promises the security and ease of use needed for modern users while acquiring access to sensitive data. Undoubtedly, biometrics is one of the critical layers to help the future of multi-factor Authentication.

This feature is often regarded not as standalone but adds to conventional authentication schemes like passwords, smart cards, and PINs. Adding two or more authentication mechanisms is expected to provide a higher level of security when verifying the user. The predicted evolution towards MFA is based on the synergistic biometric application that permits significantly improved client experience and MFA system throughput, which would benefit various applications. Such systems will intelligently couple all three-factor types: knowledge, biometrics, and ownership.

4. CONCLUSION AND RECOMMENDATION FOR POLICY AND PRACTICES

This paper provided a systematic overview of the state-of-the-art in both technical and usability issues and the significant challenges in currently available MFA systems. In this study, I discussed the evolution of Authentication from single- through two- and towards multi-factor applications. I focused on the MFA factors constituting the state-of-the-art, possible future directions, respective challenges, and promising solutions. Institutions that transact with their customers or clients on mobile devices strengthen the transactional security with their customers. Having a higher-level multi-factor scheme for data and transactional protection is the best and most secure means to enhance mobile online mobile security.

6. DIRECTION FOR FUTURE WORKS

Therefore, a promising direction of MFA development is neural networks and Big Data. Several successful applications have been known to the community for more than a decade. Usage and implementation of neural networks for the next-generation biometrics is the most feasible way to proceed due to presently high levels of analysis complexity. In summation, biometric technology is a prominent direction driven by the mobile device market. The number of smartphones sold only in the U.S. is expected to reach 175 million components by 2018, with the corresponding market to exceed $50.6B in revenues by 2022. It is believed that a strong push toward the usage of biometrics in many sectors of life is essential since most of the flagman devices are already equipped with fingerprint scanners and facial recognition technology in supplement to convention PIN codes.

REFERENCES

[1] J. Azema, and G. Fayad, "M-Shield Mobile Security Technology: making the wireless secure," www.ti.com/m-shield, [Mac 2011, 2008].

[2] D. Balfanz and E. W. Felten. Handheld computers can be better smart cards. In USENIX Security Symposium - Volume 8. USENIX Association, 1999.

[3]. Carlos Castillo, McAfee. Android banking Trojans target Italy and Thailand. http://blogs.mcafee.com/mcafee-labs/android-banking-trojanstarget-italy-and-thailand/, 2013.

[4] Carlos Castillo, McAfee. Phishing attack replaces Android banking apps with viruses. android-banking-apps-with-malware, 2013

[5] Ometov, A.; Orsino, A.; Militano, L.; Araniti, G.; Moltchanov, D.; Andreev, S. A novel security-centric framework for D2D connectivity based on spatial and social proximity. Comput. Netw. 2016, 107, 327–338. 209.

[6] Yang, C.C.; Chang, T.Y.; Hwang, M.S. A(t,n) multi-secret sharing scheme. Appl. Math. Comput. 2004, 151, 483–490. 210.

[7] Dehkordi, M.H.; Mashhadi, S. An efficient threshold verifiable multi-secret sharing. Comput. Stand. Interfaces 2008, 30, 187–190. 211.

[8] Smart, N.P. Secret Sharing Schemes. In Cryptography Made Simple; Springer: Berlin, Germany, 2016; pp. 403–416.