Security Authentication Techniques for Protecting Data of Personal Devices

Megha D. Pradhan[1], Prof. V. B. Bhagat[2]
[1, 2] Dept of Computer Science & Engineering
[1, 2] P. R. Pote (Patil) college of Engineering & Management, Amravati

Abstract- *Internet authentication for popular end-user transactions, such as online banking and e-commerce, continues to be dominated by passwords entered through end-user personal computers (PCs). Most users continue to prefer (typically untrusted) PCs over smaller personal devices for actual transactions, due to usability features related to keyboard and screen size. With mobile devices constantly taking a bigger part in our everyday life, the convenience of accessing a bank account, paying for any services or even checking medical journals independently of current place and time is getting more and more feasible. Authentication plays a critical role in securing any online banking system, and many banks and various services have long relied on username/password combos to verify users. Memorizing usernames and passwords for a lot of accounts becomes a cumbersome and inefficient task. Our approach has been achieved good results of reliability, and validity for cloud password authentication. The experimental results show an effective level of performance*

Keywords- Authentication, security, mobile, PCs

I. INTRODUCTION

In the current Internet environment, most consumer computers are infected with one or more forms of spyware or malware. Internet connected PCs are not ‘safe’ anywhere; an improperly patched home or public computer generally survives only minutes. The need for stronger user authentication in an online banking environment has become necessary to ensure customer security, confidence, and acceptance of this widely used channel for financial institutions. Mobile devices are becoming essential tools in modern life, which seamlessly connect human beings to each other and outer world. A mobile phone (also known as a cellular phone, cell phone, and a hand phone) may be a device that may build and receive phone calls over a link whereas on the road a large geographical area. Many of these attacks attempt to extract user identity and sensitive account information for unauthorized access to users’ financial accounts; for example, user names and passwords for thousands of bank accounts have been found on an online storage site reportedly gathered by a net. There are known attacks against mobile devices but the trustworthiness of such devices is currently more easily maintained than a PC. Mobile devices such as cell phones and are becoming more sophisticated tools, with data processing, storage and communication capabilities getting closer to the functionality of desktop computers. As a consequence, the information that can be accessed through and stored on them is becoming more sensitive. This has already been witnessed with other forms of mobile device (e.g. laptops) and as a result the now represent a recognized area of risk.

II .LITERATURE REVIEW

Sullivan in 2005 introduced the beginning of the twenty first century has brought a dramatic increase in the use of the online channel for financial institutions. The number of users taking advantage of the services offered online by financial institutions continues to increase each year [1].

Ivatury and Mas (2008) predicted that poor people are more likely than rich people to use mobile phones to undertake financial transactions. People in developing countries have less options (if any) for transferring money and accessing banking services, because there is less deployed formal banking infrastructure fewer branches, automated teller machines (ATMs)generally co-located to relieve branches, and low Internet penetration. So a branchless banking channel using mobile phones could be far more preferable topoor people than the available options: traveling to and queuing at distant branches or saving in cash or physical assets[2].

Mannan and Oorschot proposed a protocol that they called MP-Auth(*M*obile *P*assword *Auth*entication), which uses a mobile device to protect user passwords from easily being recorded. In their approach, the mobile device is assumed to be free from malware as the user will enter the password into the mobile device rather than into an untrusted computer. In another approach proposed by Jeun et al [3].

Mazurek in 2015 introduced the development of smart devices is un deniably transforming the way of our daily life. Recent surveys show the great potential of loT(Internet of Things) technology (e.g., smart appliances, wearable devices, and home automation). However, these applications also present potential risks like unauthorized access. The most common mechanism to address the unauthorized access issue is the authentication. Authentication methods include PIN (Personal Identification Number) passcodes, smart cards, and biometrics (e.g., fingerprints, face recognition, and gait recognition). However, most passcodes are either simply decoded or require intentional memory[4].

Verizon in 2014 is proposed scheme that allow the username/password combo is one of the biggest data breach problems based on a report. The same report indicated that in 76% of the data breaches, attackers were able to gain accesses by using the stolen user credentials. According to the security Hold Security a cyber gang breached over 420,000 web and FTP sites to harvest more than 1.2 billion credentials; this incident could be one of the largest data breaches reported to the media[5].

III. RELATED WORK

The authentication schemes and attacks introduced in the article represent the standard of knowledge discussed in various publications dealing with user authentication.1 However, most of them provide just an overview of schemes and corresponding attacks and don't attempt to draw a security landscape by relating them to each other in a sensible way.[6]Gorman categorized user authentication into three categories: knowledge-based (e.g., a password), object-based (e.g., a car key-less entry), and ID-based (e.g., a fingerprint). Brainard et al. explored a fourth factor which is based on the concept of vouching for somebody you know. Recently, the authors in [3] proposed a secure authentication scheme using dual channels in rogue access point environments [7].

Different from existing works, we exploit dynamic authentication credentials along with user-centric access control to solve the static credential problem. Our approach is to introduce one-time usernames utilizing user's smart devices and cryptographic primitives such as encryption, digital signature, and hashing. The goal is to create a unique username and password set for each session such that various security vulnerabilities in conventional, static username and password systems can be tackled [12].

The approach that was examined in his study relied on the human ability for memorizing and processing to solve the simple challenges. Since then, other researchers and practitioners have also proposed and developed various graphical password schemes. Graphical passwords attempt to leverage human memory for visual information with the shared secret being related to images .This capitalizes on the natural human ability to remember images, which is believed to exceed memory fort ext. However, graphical passwords are not immune to security attacks. For example, graphical password schemes may suffer from shoulder suffering attacks where credentials are captured through direct observation of the login process, or by recording the process using a recording device [13].

The username/password combo is one of the biggest data breach problems based on a report from Verizon in 2014 The same report indicated that in 76% of the data breaches, attackers were able to gain accesses by using the stolen user credentials. According to the security firm Hold Security a cyber gang breached over 420,000 web and FTP sites to harvest more than 1.2 billion credentials; this incident could be one of the largest data breaches reported to the media. All previously mentioned breaches, attacks, and issues could lead to a serious problem called the domino effect of password reuse. A domino effect is the result of one password file falling into the hand of a malicious user, who can then use it to infiltrate other online accounts [8].

IV. PROPOSED WORK

In Proposed System, An efficient and practical user authentication scheme using personal devices that utilize different cryptographic primitives such as encryption, digital signature, and hashing. The technique benefits from the widespread usage of ubiquitous computing and various intelligent portable and wearable devices that can enable users to execute a secure authentication protocol.

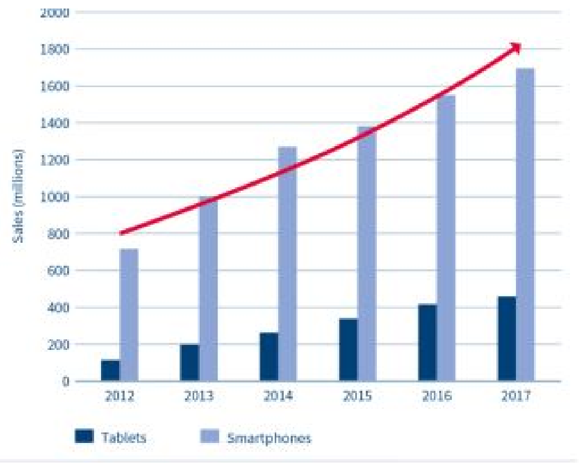

Fig.1.1 Mobile Device Growth Trend

The number of mobile devices on the market is steadily increasing with tablet sales rising23.9% and smartphone sales growing 39.2% in 2013. Looking ahead, growth forecasts remain positive. In recent years, mobile devices have become more and more intelligent as computing functions and applications move from laptops and PCs to smaller, smart devices such as phones and tablets. As smart devices become the most important entry point to a wide variety of data ranging from private photos to large data sets required for different applications, both the end user and the providers of services that can be accessed via these devices have an increasing interest in protecting this data. Increasingly popular in the enterprise and government context, these applications use large volumes of data, some of which is extremely sensitive. Typical applications that require high levels of security include corporate, payment and health systems. Here, loss or theft of confidential information could have serious implications.

The specific challenges and importance of the challenges did not change significantly from year to year, but the overall number of IT professionals facing security concerns as well as the number concerned about particular items, has increased across the board [10].

Security Analysis:

1.Keep your device up to date: This means you can take advantage of the latest device security technologies.

2.Can trust any external device you're connecting the device to: When connected to another device (e.g. with a USB cable), the device should prompt you to trust it before syncing data. Similarly, if your device has Bluetooth, be careful what devices you pair with. For example, don't accidentally synchronies all your contacts to a hire car over Bluetooth.

3.Don't disable any of the security features that come with your device: Even if apps ask you to do this. Similarly, don't enable developer mode, debug mode, or 'jailbreak' or 'root' your device as these will often disable securityfeatures as part of the process.

Look for the padlock symbol when making transactions on the Internet: Make sure that you're using the legitimate website of the company you're trying to visit when banking, shopping, or any time you type in passwords or payment details. Make your own way to websites using addresses you've entered yourself, or from search engines.

Take care using public Wi-Fi networks: Get Safe Online has some advice on protecting yourself when using public Wi-Fi networks. Follow this guidance when you have to connect to a network you don't fully trust.

Disable any services and uninstall any apps you don't intend to use: Apps that come with the device will likely communicate with online services. Disable or uninstall ones that you won't use, as this will prevent any data leaking through these routes.

High-Level Threats and Vulnerabilities:

Mobile devices typically need to support multiple security objectives. These can be accomplished through a combination of security features built into the mobile devices and additional security controls applied to the mobile devices and other components of the enterprise IT infrastructure. The most common security objectives for mobile devices are as follows:

1. Confidentiality—ensure that transmitted and stored data cannot be read by unauthorized parties
2. Integrity—detect any intentional or unintentional changes to transmitted and stored data
3. Availability—ensure that users can access resources using mobile devices whenever needed

User and Device Authentication

Require a device password/passcode and/or other authentication (e.g., token-based authentication, network-based device authentication, domain authentication) before accessing the organization's resources. This includes basic parameters for password strength and a limit on the number of retries permitted without negative consequences (e.g., locking out the account, wiping the device).

1. If device account lockout is enabled or the device password/passcode is forgotten, an administrator can reset this remotely to restore access to the device.
2. Have the device automatically lock itself after it is idle for a period (e.g., 5 minutes).
3. Under the direction of an administrator, remotely lock the device if it is suspected that the device has been left in an unlocked state in an unsecured location.

The following figure give an overview of the potential specific mobile device threats which will be faced by mobile device users and manufacturers and how these threats may be addressed. These three areas impacts are fall in impacts– Authentication, Platform Security, Application Security all of which will face an even higher number of skilled attacks in the future[11].

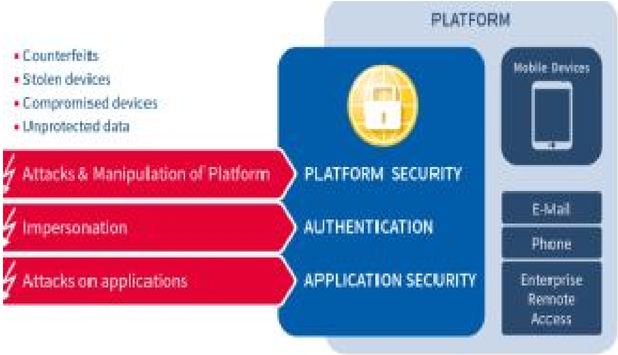

Fig.1.2 Secure Mobile Platform Challenges

Authentication:

Companies and government bodies need strong authentication functionality to ensure that only legitimate employees access internal networks or specific applications. To avoid the perils of password-based authentication (including the risk of password loss and theft), enterprises have increasingly moved to multi-factor authentication. Multi-factor authentication is generally performed by adding another element to the traditional user name and password or pass phrase. The new FIDO Universal Second Factor (U2F) protocol and Universal Authentication Factor (UAF) standards offer improved protection, especially when implemented in hardware. When authentication is needed, the user is prompted to swipe their finger and/or enter a password. This triggers the phone to perform a cryptographic authentication.

Platform Security:

User data should be protected through volume encryption in order to prevent data from being easily read and stolen by a third party. In order to prevent dictionary attacks, devices should be equipped with brute force protection. A secured boot process and continuous device compliance checks (runtime integrity) can monitor the device's integrity prior to use. This information can help service providers to notify the user or restrict access if the device is compromised.
All smartphone apps run on an underlying platform comprising the operating system and hardware. Building security into apps has little benefit if the platform is not secure enough. Attackers who break the platform have broken all the apps. There are various ways to improve platform security thus help to protect the apps.

Application Security:

Consumers and corporate users employ a wide variety of apps on their phones. Most of these apps can benefit from greater hardware security. Commonly used apps are listed in the following along with a description of how they can benefit from more effective hardware security measures

Secure Communication:

In phone conversations, lines can be very easily tapped and sensitive content overheard. In order to prevent this, secure voice protocols such as SRTP and MIKEY can be used to allow encryption, message authentication and integrity. Many VoIP clients and servers support these protocols – but even that is not enough. The VoIP client also needs to be configured to use a private key that is stored in secure hardware.

V. CONCLUSION

In this system, protect the data of personal devices by using Strong authentication. The authentication schemes are Platform security, Authentication, Application security. Also we used secure communication for secure the personal devices like smartphone, mobile ,PCs.

VI. ACKNOWLEDGMENT

The author would like to present their sincere gratitude towards the, Prof. V. B. Bhagat (Guide) thanks for their extreme support to complete this assignment.

REFERENCES

[1] S. Fox and J. Beier, "Online Banking"2006: *Surfing to theBank, Pew Internet and American Life Project,* June 2006.

[2] Mazurek, M.L.; Komanduri, S.; Vidas, T. Measuring PasswordGuessability for an Entire University.In Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany,4–8 November 2013; pp. 173–186.

[3] Ivatury, Gautam, and Ignacio Mas,"The EarlyExperience with Branchless Banking." *Focus Note 46.Washington,* D.C.: CGAP, 2008.

[4] M. Mannan and P. C. van Oorschot. "Using a personal device to strengthen passwordauthentication from anuntrusted computer", *Financial Cryptography,* volume 4886 of *Lecture Notes in Computer Science,* pages 88 Springer, 2007.

[5] *Verizon Data Breach Investigations Report (DBIR),* Verizon EnterpriseSolutions, Inc., Basking Ridge, NJ, USA, 2014.

[6] L. O'Gorman, "Comparing passwords, tokens, andbiometrics for userauthentication," *Proc. IEEE*, vol. 91, no. 12, pp. 20212040, Dec. 2003.

[7] Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, ``Fourth-factorauthentication: Somebody you know,'' in*Proc. 13th ACM Conf. Comput.Commun. Secur.*, 2006, pp. 168178.

[8] A. Moshchuk, T. Bragin, S. D. Gribble, and H. Levy,"A crawler-based study of spyware in the web" *NDSS'06*, San Diego, CA,USA, Feb. 2006.

[9] I. Jeun, M. Kim, and D. Won, "Enhanced password-based user authentication usingsmart phone", In R. Li, J. Cao, and J. Bourgeois, editors, *GPC*, volume 7296 of*Lecture Notes in Computer Science,* pages 350{360. Springer, 2012.

[10] Infineon Technologies AG, "Need for a secure mobile platform", *infineon* 2015.

[11] Infineon Technologies AG, estimation based on: Gartner; Janessa Rivera and Rob van derMeulen, "Gartner SaysWorldwide Traditional PC, Tablet, Ultramobile and Mobile PhoneShipments", *infineon* 2014.

[12] Chow, Y., Susilo, W., Au, M. Ho. & Barmawi, A. Moesriami, "A visual one-time password authentication scheme using mobiledevices",*In L. C. K. Hui, S. H. Qing, E. Shi & S. M. Yiu (Eds.), Proceedings of the 16th International Conference on Information andCommunications Security* (ICICS 2014) (pp. 243-257). Switzerland: Springer International Publishing.

[13] Abdulrahman Alhothaily, Chunqiang Hu, "A Secure and Practical Authentication SchemeUsing Personal Devices", *in proc IEEE Digital object identifier* 10,1109/access 2017. 2717862.