International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 6, June - 2014

Mobile Device Data Security using Enhanced Application Lockbox

Ass. Prof. Dakshata Panchal
St. Francis Institute of Technology
Borivali(W), Mumbai400103,India.

Dr. A. K. Sen
St. Francis Institute of Technology
Borivali(W), Mumbai-400103,India.

Vanessa Rumao
St. Francis Institute of Technology
Borivali(W), Mumbai-400103,India.

***Abstract* - Smart phones and other mobile devices are widely used in day to day life. One of the important feature of mobile devices is mobility, which exposes them to different threat environments and excludes them from relying on external physical security. So, the security requirements for mobile devices are different from stationary machines. The enterprises, government, and military uses various productive applications. Productive applications often deal with sensitive and secret data. A risk management and security framework is required to protect applications and data on mobile devices. Application lockbox provides another layer of protection for sensitive applications and data in mobile devices. Lockbox has ability to lockout sensitive applications and data. If the lockbox is locked, applications and data inside it should be protected from the attacks on operating system and physical attacks. It will encapsulate individual applications and all their associated data to allow for access control on the application level. It can provide meaningful protection without significant changes in current technology.**

Keywords* - *mobility; security;encryption

I. INTRODUCTION

As the technology changed, the way of communication is also changed. In very early days of history, letters were used for sending messages, as the time passed, telephone came into existence and today is the era of wireless communication which gives rise to mobile phones. Mobiles are the most popular and common way to communicate now-a-days. Mobile devices have become essential to enterprise and government networks, from small organizations to large-scale agencies. Mobile devices can be a simple cellphones or it can be a smartphone. A smartphone is one device that can take care of all of your handheld computing and communication needs in a single, small package. Since the launch of smartphones and other mobile devices, they are becoming common, as the technology changes, many people changes or update their phones constantly to include new technologies. Smartphones are any mobile phones that are similar to a mini computer that can also place and receive calls. They offer a variety of features such as making calls, computing capabilities, video calling, online surfing, cameras, media players, GPS navigation units, etc.

With mobile devices such as smartphones and applications flooding the market, mobile device security is growing in importance. A Smartphone user is exposed to various threats when he uses his phone. Just in the last two quarters closing 2012 the number of unique mobile threats grew by 261% as per information available from ABI (New York based intelligence firm) report. These threats can disrupt the operation of the Smartphone, and transmit or modify the user data. For these reasons, the applications deployed there must guarantee privacy and integrity of the information they handle. In addition, since some applications could themselves be malware, their functionality and activities should be limited. For example, accessing location information via GPS (Global Positioning System), address book, transmitting data on the network, sending SMS (Short Message Service) that are charged, etc. Using a mobile device to make telephone calls is probably the primary reason for the handset; however, the applications installed on the device are a very close second. In most cases, the make-up of the installed applications differs drastically—from corporate applications that support the workplace, gaming applications for entertainment, children's applications to occupy the most demanding members of the family, to social applications to connect to friends and family. These applications, and often the people who use them, require access to different types of data. The ability to isolate these applications and the data they require is an important step.

Our phones are more than just communication devices – they're photo albums, address books, alarm clocks, wallets and more. They are, in a way, a reflection of our personal identity, housing personal details ranging from the company we keep, to the place where we bank. It's no wonder we keep these devices so closely guarded in our pockets and purses [1]. Mobile security is as critical as the pin number on your atm card or the lock on your front door. The sad truth is that there are people in this world who will exploit any security vulnerability if there's money behind the door. As mobile devices become mobile wallets, we are already seeing the rise of virtual pickpockets. It's important to secure the data that's stored on them. So, it is necessary to put the same effort into protecting the information on our mobile devices. Basically, a smartphone without proper protection puts you at risk. There are some of new security risks which have been introduced by the new smartphones. Our mobile devices are a lot more subject to loss than laptops and other devices. The data and documents residing on these lost devices are at risk. Mobile operating systems attempt to mitigate this risk by providing the ability to locate a remote device even when a device run-out of battery and to, remotely wipe-out the data on the device. The data which is being sent from our devices is transiting on public Wi-Fi and cellular networks which can

be compromised with simple equipment. The rapidly increasing usage of public networks put the data in transit at risk. The flexibility to freely download apps and content has fueled the explosive growth of smartphones and mobile applications but it has also introduced a new risk factor. Malware can mimic popular applications and transfer contacts, photos and documents to unknown destination servers. There is no way to disable the application stores on mobile operating systems. Fortunately for end-users, our smartphone are fundamentally open devices however they can quite easily be hacked. MDM(Mobile Device Management) platforms offer application validation services to ensure that the approved applications are protecting the application data. They also prevent screen capture, cut and paste operation to prevent data loss.

Whether you use your smartphone to find time-fillers on the internet or save time and energy by shopping and banking online, there's always a door open to malware and hackers. They could steal your personal data and use it to their benefit. Also, the fancier phones get, the bigger the temptation to steal them. In other words, the precious information you carry around with you is increasingly vulnerable to being misused by strangers. Mobile device security for the enterprise is essential because smartphone users can now easily access corporate e-mail. Employees are using these devices not just to check e-mail but also to check the latest company news on the intranet, watch company videos, update intranet blogs, and also access applications like SAP and Oracle. It is therefore not just corporate e-mail that ends up on modern mobile devices, but a lot more content. Unfortunately, consumers aren't the only ones making the shift to mobile devices. Malicious hackers and identity thieves are following close behind. As more and more people use their smart phones and other mobile devices to do online banking, pay bills, and store critical personal and business information, more and more bad guys are trying to crack into this mobile gold mine.

II. RELATED WORK

There are number of security mechanisms have been developed to provide data security in mobile devices. An Application Sandbox[2], which is able to perform both static and dynamic analysis on Android programs to automatically detect suspicious applications. In the static part, the sandbox decompresses installation files and disassembles corresponding executable. So, Static analysis scans the software for malicious patterns without installing it. In Dynamic part, android emulator is used, which is normally used for testing and debugging ordinary Android applications. The android application is installed to the emulated and isolated environment.in a fully isolated environment. After that, applications are executed and can be used within the sandbox for performing behavioral analysis.

Physical attacks have been proved effective in breaking some well-designed ciphers in practice. Unfortunately, it is challenging to designers to theoretically investigate the robustness of a cipher scheme against various physical attacks. A novel data encryption and a storage scheme called self-encryption is proposed to address this problem. Self-encryption (SE) scheme[3] treats the data as a binary bit stream, and generates a keystream by randomly extracting bits from the stream. Based on the user security requirements, the length of the keystream changes. The bit stream is encrypted and the ciphertext is stored on the mobile device, whereas the keystream is stored separately. This makes it computationally not feasible to recover the original data stream from the ciphertext alone.

The most common mechanism is password protection enforced by the operating system. If the operating system itself is compromised, then no protection is afforded. It only provides superficial protection on the interface level. Mobile operating systems are relatively easy to circumvent [4]. Hardening the mobile operating system will not work. Attackers can also disassemble the device and read directly from the storage media [5]. Password protection can deter common thieves. Sophisticated and resourceful attackers will be able to circumvent it once they gain physical possession of the device. This is especially problematic in the military context where soldiers could be captured along with their device and forced give up the password.

In Location dependent data encryption there are two phases: register and operation phases. Firstly, a mobile client requests a random seed and a MAC function C from the information server in the register phase. The information server records the issued random seed and the function C for each individual client. They are very important for ensuring data security in the operation phase. So, they must be transmitted under a secure channel, such as Intranet or VPN (virtual private network). The random seed is the initial value of one-way hash function, such as MD5. A series of session keys is generated according to the random seed. When the mobile client is moving under an insecure channel in the operation phase, the mobile client submits a target coordinate before message transmission. The information server sends the message encrypted by using the coordinate and a specific session key. The session key is changed for every session. Since the information server and the mobile client own the same set of session keys, a key synchronization process is also designed for information server to identify the correct session key. When a secure channel is available for a mobile client, the client can request a new random seed and MAC function C. The proposed approach can provide a novel location-dependent data encryption for mobile information system.

III. PROPOSED METHOD

Several techniques such as self-encryption, Application Sandbox were implemented to protect the mobile devices from adversaries. Still Security remains a significant obstacle in mobile devices. They have used cryptographic techniques to secure the data. In above techniques data encryption done

on mobile device, keys are also stored on mobile devices. In some cases encrypted data sent to client by server and client will only decrypt the data. In case mobile is lost there are chances of data hacking. By using above concept we propose application lockbox concepts for data security in mobile device . In Application lockbox secure data stored in separate memory space[6]. In this encryption and decryption keys stored on server, the user is authenticated by considering three parameters such as password, location parameter and time. To
develop a risk management and security framework that compartmentalizes sensitive applications and data. Supports fine-grained access policies. The physical security of mobile devices can change access control should be managed according to the threat level. Location based application locked (Applications deemed too risky for the current physical environment should be locked) Eg. Some application should only run while the device is in the office or secured area. office data we can access only in the office not outside the office. Sensitive application that is not actively being used should be automatically locked. Application lockbox concepts are used Keys, location parameter & time will stored on server side only. Sensitive application and data to be already locked. when the enemy or a thief captures the device. Applications should be able to run inside application lockbox without modification.

The workflow of the proposed system is as shown in the figure 3.1. For file encryption first, the user has to unlock the lockbox using graphical password. After unlocking lockbox user needs to select the file for encryption and also check for location and time parameter. Encryption key is generated. Encryption key, file name and location all this parameters are stored on server. At the time of decryption, user first has to unlock the lockbox using graphical password. After unlocking user has to enter the key and also has to check for location and time parameters. If all the conditions are satisfied the file will be displayed to user.

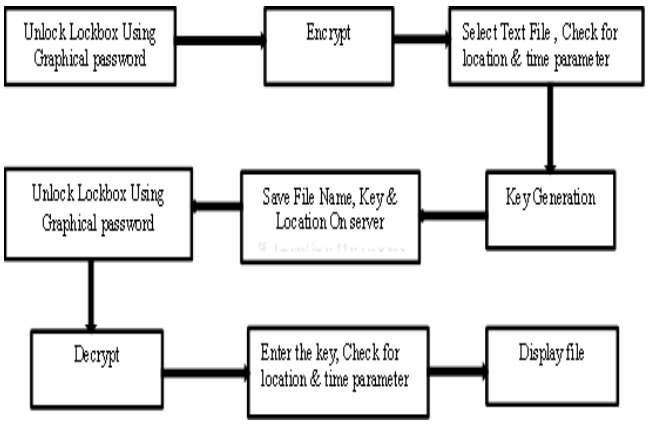
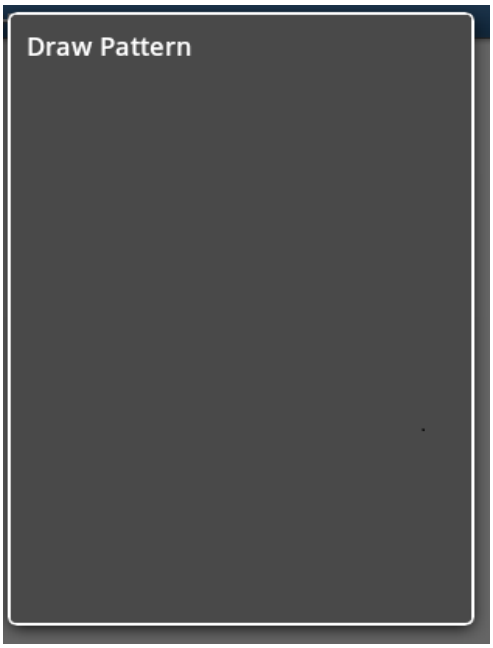


Figure 3.1.Proposed System

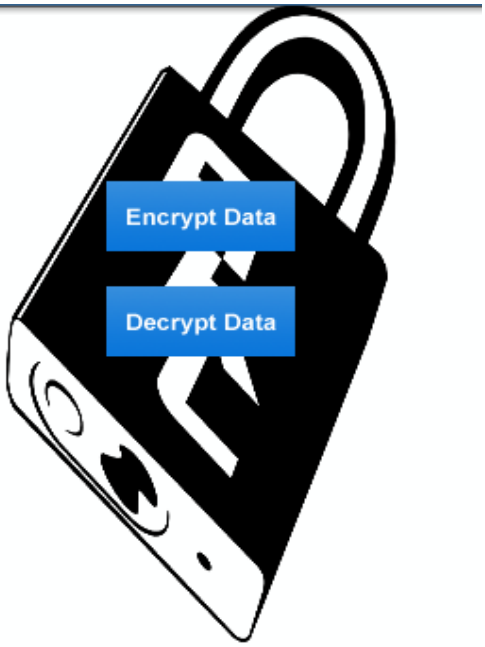
The following steps shows the workflow of the proposed system:

Step 1: Switch on mobile device and click on the created application.

Step 2: Using graphical password user has to unlock the application.



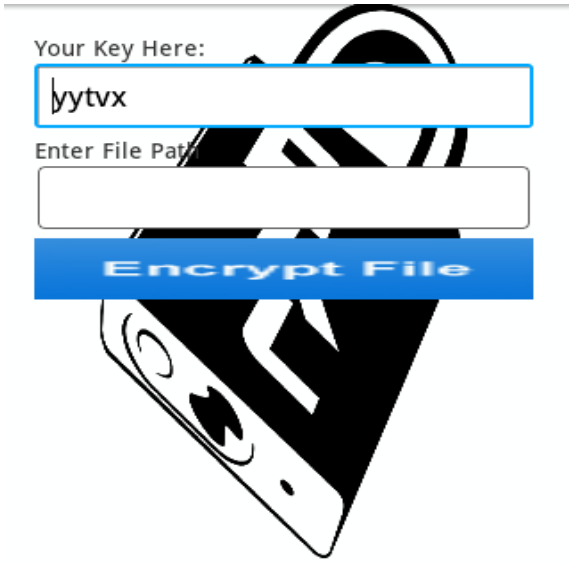
Step 3:Once unlock the lockbox user need to choose an option of either encryption or decryption.



Step 4: For encryption user has to choose either of the following option.

Step5 : If user selects an option of Important Data then user will get the following screen. User needs to fill three fields encryption key, file name and data. It will also check for the time and location parameter. If user wants to encrypt office file then it will check that, that file will open only during office timings and also only at the particular office location.

Step 6: If user selects an option of files then user will get the following screen. User needs to fill two details, encryption key and file path.



Step 7: At the time of decryption user needs to provide same encryption key and it will also check for the time and location parameters. If all the parameter matches then the file will be decrypted.

IV. CONCLUSION

Due to extremely high demand of mobile phones among people, over the years there has been a great demand for the support of various applications and security services. Using application lockbox, we are locking the data and application. Mobile device access, data access, data storage & data transmission are the various parameters that will be analyzed. Using password, security for mobile device is provided. So, it is essential to analyzed that unauthenticated user doesn't get access of the phone. Also, it will be analyzed that unauthenticated user is not able to access the data. In Application lockbox secure data stored in separate memory space. It will be analyzed that the application lockbox provides location and time based application locked. Eg. Some application should only run while the device is in the office or secured area and also between during the office time only.

REFERENCES

[1] http://www.huffingtonpost.com/drew-hendricks/mobile-security_b_2280915.html

[2] Blasing, T. ; Batyuk, L. ; Schmidt, A.-D. ; Camtepe, S.A. ;Albayrak, S. ,"An Android Application Sandbox system forsuspicious software de tection", *Fifth International Conference on Malicious and unwanted Software*, pp 55 – 62, Oct. 2010

[3] Yu Chen ; Dept. of Electr. & Comput. Eng., SUNY - Binghamton, Binghamton, NY ; Wei-Shinn Ku " Self-Encryption Scheme for Data Security in Mobile Devices," *Consumer Communications and Networking Conference*, pp 1-5 Jan.2009.

[4] T. Stevens. "iPhone vulnerability leaves your data wide open, even when using a PIN," 10/12, 2010; http://www.engadget.com/2010/05/27/iphone-vulnerabilityleaves-your-data-wide-open-even-when-using/

[5] S. Jacobsson. "iPhone security flaw: Using a PIN won't help," 10/12, 2010; http://www.msnbc.msn.com/id/37400086

[6] Jim Luo ,Myong Kang , "Application lockbox for mobile device security", *Eighth International Conference on Information Technology: New Generations* ,pp 336 – 341, April 2011.