# Identity, Privacy, Issues, Challenges and Solutions In Mobile

Madhumay Sen* Gaurav Kumar Jain** Ravi Ranjan***

The gap between mobile phones and portable computers in shrinking, and portable computer is shrinking, and almost everyone's daily activities are highly dependent upon a device, know as mobile phone/Smart phone (sp). So mobile device security is becoming increasingly important, as business information and personal information move from the PC onto handheld storage. It is very important to do our daily activities without any problems. But what if our mobile gets stolen ? The paper describes issues and challenges in security and privacy of mobile device. The paper also proposes privacy solutions. Fingerprint sensors and face recognition are also highlighted as a growing feature in security and navigation for handsets. In this paper, we have used security password , face recognition and finger print recognition to avoid unnecessary messaging. It operates silently in the background and it should and it should be very hard to spot.

Keyword: Smart phone (sp), GPS, java mobile devices, j2ME, Face recognition technology, Fingerprint technology.

## Introduction

The gap between mobile phone and portable computers is shrinking and is being replaced advanced mobile phone as smart phone (sp). SP offers more advanced computing ability and connectivity, in addition to basic features of a mobile phone. SP provide digital voice service as well as any combination of text message, e-mail, web browsing, still camera, video camera, MP3 player, video player, television and organizer. In addition to their built-in function. SP has become application delivery platforms, turning the once single –minded cell phones into a mobile computer.

We highly depend upon mobile for various reasons. The unconventional reasons are: (a) Young generation user mobile as a total communication tool; (b) Huge demand for mobile service and mobile broadband access; (c) Availability of more CPU power; (d) Multitasking; (e) Multimedia messaging; (f) Mobile e-business; (g) Entertainment; (h)Internet access; (i)Rich call; (j) Page load timing ,great content and easy navigation; (k) Successful advertising (mobile ads are far more than online advertising); (l) Social networking interactions ; (M) Connecting with others with a style; and (n) Later and best audio, camera and video availability, etc. So mobile device security is becoming increasingly important, as business information and personal information move from the pc onto handheld storage.

In the literature survey, It has been that people are not using mobile for the conventional and the above-mentioned unconventional reasons, but they are also using mobile for the following new reasons: (a) complete healthcare (like diagnostic, treatment, patient history, billing reference, drug instruction, referrals, prescriptions, patient monitoring, laboratory services, discharge protocols, etc.); (b) travel guide (to find addresses, etc.) using GPS (Mir and Masood, 2002) system; and (c) teaching etc. It means that we are using mobile for all our daily activities. Device and data both are highly sensitive and important and so it should be highly secured. But what if our mobile gets stolen ? So security and privacy of device and data are whenever the SIM card gets changed unnecessarily (like anybody can have two SIMS and they have to change SIMS according to the work requirement), In this paper ,to avoid unnecessary messaging we have used security password, face recognition and fingerprint recognition. It operates silently in the background and it should be very hard to spot. Even it the thief spots the application, the SMS has already been set out.

If a device is lost or stolen, the entire world around that person could be threatened if those devices are not protected by password and other user-level security measures. It is very important to do out daily activities without any problems.

With the large number of application available for java-enabled device, security is of paramount importance. Applications can handle user-sensitive data such as phonebook data or bank account information. Moreover, java-enabled device support networking , which means that applications can also create network connections and send or receive data. Security in all these cases should be a major concern. Malicious code has caused a lot of harm in the computer world, and with phones having the ability to download and run application, there is an actual risk of facing this same threat. Currently, viruses for phones have started to emerge (e.g., Cabir); a number of model-specific attacks have been reported (e.g., Nokia 6210 Dos, Siemens S55 SMS, etc.), and mobile attacks and exploits are starting to get attention in the hacker community (Debbabi et al., 2005).

This paper describes the issues and challenges in security and privacy of mobile device. This paper also proposes identity privacy solutions. Fingerprint sensors and face recognition are also highlighted as a growing feature in security and navigation for handsets.

Solution have been developed with the help of mobile applications development language, j2ME (Jonathan and Sing, 2005). This paper is divided into the following sections: section 2 describes different issues and challenges in security and privacy of mobile device. Section 3 talks about identity privacy solutions. Finally, the paper ends with a conclusion and future prospects.

## 2. Issues and challenges

After going through the literature available on websites, the following few issues and challenges in security ad privacy of mobile devices are found to be more critical:

### 2.1 Major Issues

- No single security solution will work in the given nature of the mobile environment. And just extending the existing security infrastructure for mobile device, simply is not practical, enterprises must treat mobile security as an independent task. And as a independent task, mobile-usage-specific security policies must be created and implemented. A comprehension risk analysis of the potential security hazards associated with the use of mobile devices should be the first step along the path of mobile device security policy creation.
- Note that the strength of a password is a function of length, complexity and unpredictability. Mobile password (PIN) or security password should be strong and safe and such that nobody can able to detect it.
- Battery power is a critical issue. Any mobile device will be ' ON/Active ' during certain interval of time depending upon its use. Power conservation is mobile devices is of paramount concern. If the device life can be prolonged, the user can be more productive and more satisfied with the use of this device.
- The privacy of mobile location information. Privacy is a serious concern for many emerging applications in wireless network, whereas mobile privacy protection is a complicated issue. On the one hand, location tracking capability provided by modern technologies makes mobile users uncomfortable. On the other hand, location management for mobile device, which helps direct incoming calls and supports mandatory location services required by governments in the case of emergency makes mobile terminals vulnerable to revelation of location information. Any mobile privacy protection mechanism has to address these seemingly contradictory requirements ( Applewhite, 2002).
- Esay to use. A mobile with strong security and privacy techniques shoukd be user-friendly. This is required because not all the person are technically strong and have time.

### 2.2 Major Challenges

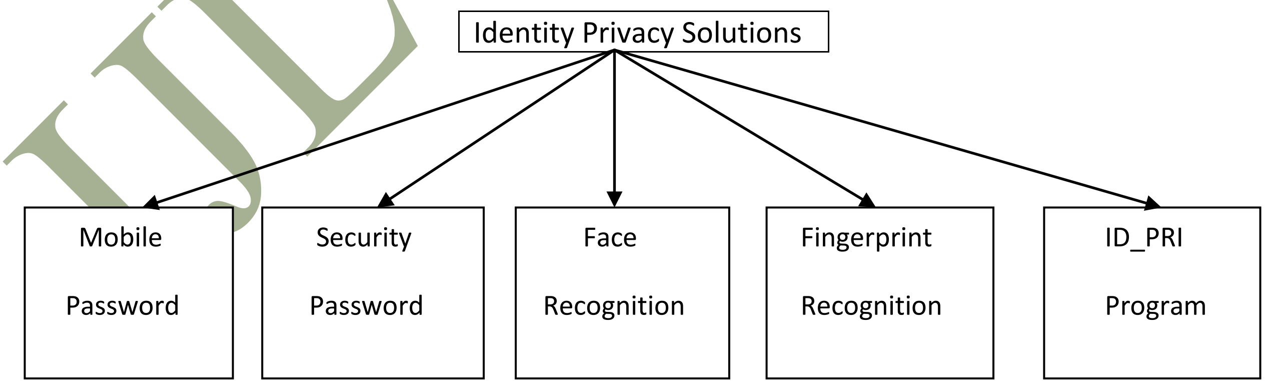
- User standard security controls on mobile devices . Mobile device are often exempted from the security control routinely applied to desktop computers for fear of interfering with the actions of traveling users. These devices are much more likely to be stolen or attached to a hostile wireless network than desktops that are stored securely in a corporate office behind several layers of perimeter protection. So stronger controls should be there in such system that go on the road. It is also wise to make sure that these devices have current software firewalls, patch management, antivirus and antispyware software.

- Legally and explicitly define explain security and privacy policy. As with any security issue, the foundation of a good response is solid, clear policy that is effectively communicated to all stakeholders. Ensure employees understand what constitutes appropriate and in appropriate use of enterprise information assets and the consequences of failing tp comply.
- Know where the data lives and take backup automatically (this facility should be provided by service provider or mobile device manufacturer with the consent of user) within certain interval of time to avoid the loss of data.
- To develop and maintain 100% secured wireless word.
- Energy is a scarce resource and all types of service stop when the device runs out of power.
- What to hide and what to provide with respect to the privacy of mobile location information.
- To provide location-based services with the option that full services will be available anywhere, anytime on demand (Campadello, 2004).
- Security and privacy solution should be such that it is easy to use but difficult to guess.

## 3. Identity Privacy Solutions

The parts of identify privacy solution are summarized in figure 1. The name of the full project was identity privacy solutions.

Figure 1: parts of Identity privacy solutions



The whole idea e, mentioned above was coded and implemented as a project. The project. The project started with comparing different platform for development application on mobile appliance. We chose J2ME because we know java and many devices support MIDP(Debbabi et al., 2005). The software we used are JDK 1.6.0 and NETBEANS 6.9.1. Minimum hardware requirement are 128 k RAM and 192x264 display screen. J2ME is a collection of techniques and specifications to create a platform for mobile device that fit the requirement for mobile devices such as consumer product, embedded device and advanced mobile device.

ID_PRI is a program for mobile phones that works as a safe protection from being misused, mishandled, lost or stolen, it starts automatically as the phone is turned on, and then always keeps checking whether the phone is in safe hand or SIM card has changed. There are two types of password and two types of mode. Two passwords are- mobile password and security password. Security password is required in the following condition: (a) when SIM has been changed; (b) when an unidentified user (who knows the mobile password) is trying to use this phone. User identification can be done automatically by two technologies; face recognition; (Voth, 2009) and fingerprint recognition (Saropourian, 2009), two types of mode are; user mode and guest mode. In guest mode, guest cannot access any mobile data. He can only dial those numbers which he remembers or he can receive calls. When phone is turned on, it will ask for mobile password; if it is ok, then authentic user can this mobile in user mode; Otherwise, It will work it guest mode. Algorithm of ID_PRI program is summarized below.

```
/*phone is turned on */
Step 1: I=0
Step 2 print "enter  password"
Step 3: Input password,
Step 4: If (password=systpd) then  /* systpd is the password stored in the system*/
Step 5: If (SIM changed)
Step 6:             then print "Enter security password"
Step 7:             If (security password is valid) then go to step 18.
Step 8:             else I=I+1
Step 9:             if (i<=3) then go to step 6
Step 10:                        else automatically send SMS containing location, person's identification (image, finger print details etc.) to the previously specified number (at least two from the recipient list), go to step 20,endif, endif.
Step 11: else
Step 12: check user identification via face recognition or finger print recognition.
Step 13: If (user is not authentic) then
Step 14: mobile will be working in guest mode
Step 15: print “enter securited password /*if guest want to change the mode */
Step 16: If (security password is not valid) then go to steep 14.
Step 17:        else go to step 18 endf
Step 18: else user will be working is user mode endif, endif
Step 19: else I=I+1
Step 20: If (I<=3) then go to step 2 else go to step 21 endf, endif
Step 21: turned off/stop
```

The process of sending involves the following steps: (a) a mobile user creates a message on the user mobile device; (b) the user mobile sends the message to an SMS server, known as Short Message Service Center (SMSC) of the required mobile service provider; (c) SMSC receives the message and saves a copy of this message to the user mobile. If the user mobile is not reachable, SMSC waits until the user mobile is available; (e) user mobile sends an acknowledgment to SMSC. The whole process of sending can be summarized thus: The phone will automatically send message to the list of recipients (at least two) to inform that phone is lost. At the same time, this message will contain the new SIM umber, location and identity (image, fingerprint details, etc.) of the person where phone is currently available. It will send three message one after another within a specified interval of time, so that during that duration police or anybody can trace it. ID_PRI will be in attack mode when thief change the SIM and could not provide security password (at most three times); this requires power off or rebooting the mobile phone.

```
Public SMSSend()  { smsport=getAppProperty(“SMS-port”);

Display= Display.getDisplay(this);

DestinationAddressBox=new TextBox(“Destination addrss?mull,256,textfield PHONENUMBER);

DestinationAddressBox.addCommand(exitCommand);

DestinationAddressBox.addCommand(okcommand)

DestinationAddressb.setCmmmand(this)

ErrorMessageAlert= new Alert(“sms”,null,null,AlertType.ERROR);
ErrorMessageAlert.setTimeout(10000);

SendingMessageAlert=new Alert("SMS", .null, null .AlertType.INFO).

sendingMessageAlert.setTimeout(10000);

sendingMessageAlert.setCommandListener(this);

sender=new SMSSender (smsport,  display, destinationAddressBox.sendingMessageAlert);

resumeScreen=destinaionAddressBox;)
```

we also have to create one user interface which will be presented at the time of installation of software that will ask the user to save recipients mobile numbers. The concept of push registry and timer control are used, so that after installation of software if will run in the back ground. After creating a jar file we have to sign for being trusted.

## Conclusion

This paper describes the issues and challenges in security and privacy of mobile device. This paper also proposes privacy solutions. Since data stored in the mobile is very important, so it should be highly secure. We should not depend upon device security itself. For better security , mobile company and service provider should come together. If these two can provide the facility of talking backup automatically after every particular interval of time, then user data will be more secure. Future work be done on this for better safely.

Acknowledgment: the author would like to thank Nandkishore Kumar Singh. Jayprakash kumar, Kamlesh Kumar , Apurva Chitram and Suvrakanti Guharoy for help in the coding and implementation part of this project.

References

1. Applewhite A (2002), "What Knows Where You Are ?" , Pervasive Computing , IEEE, Vol. 1 , No. 4 pp. 4-8, Digital Object Identifier: 10.1109MPRV.2002.1158272.
2. Caimu Tang and Wu D O (2008) , " Mobile Privacy in Wireless Networks-Revisited ", IEEE Transaction on Wireless Communication, Vol. 7, No. 3, pp. 1030-1042, Digital Object Identifier: 10.1109/TWC.2008.060802.
3. Campadello S (2004), " Peer_to_peer_security_in_mobile_devices;_a_user perspective " , Fourth International Conference on Peer –to –Peer Computing, pp. 252-257, Digital Object Identifier: 10.1109/PTP.2004.1334954.
4. Debbabi M, Saleh M, Talhi C and Zhioua S (2005), "Java_for_mobile_devices:_a security _study ", 21st Annual Conference on Computer Security Application, pp. 10 and 244, Digital Object Identifier: 10.1109/CSAC.2005.34.2.
5. Jonathan Knudsen and Sing Li (2005), Beginning J3ME: Form Novice to Professional, 3rd Edition, A press.

6. Mir W and Masood W (2002), " GPS Technology", Proceedings of IEEE Student Conference, Vol. 2, pp. 27-39, Digital Object Identifier: 10.1109/ISCON.2002.1214579.
7. Saropourian B (2009),"A New Approach of Finger-Print Recognition Based on Neural Network", 2nd IEEE International Conference on Computer Science and Information Technology, pp. 158-161, Digital Object Identifier: 10.1109/ICCSIT.2009.5234593.
8. Voth D (2009), " Face Recognition Technology", Intelligent Systems, IEEE, Vol. 18, No. 3, pp. 4-7, Digital Object Identifier: 10.1109/MIS.2003.1200719.