MEMORAMDUM

DATE: June 7, 2015

TO: Wendong Li

FROM: Bin Wang, Beijing University of Posts and Telecommunications

SUBJECT: **Information Security of Mobile Phones**

INTRODUCTORY SUMMARY:

The number of mobile phones tends to have an explosive growth. More and more users access to the Internet through a mobile phone. By now, the smartphone has become an essential way for ordinary people to surf the Internet. But malicious software for smart phones also become more and more, which causes a great loss of information. So there is a huge safety concerns over the personal information in mobile phones. Meanwhile, unlike the traditional PC platform, mobile phones can be carried by users easily, and can be real-time online. What's more, these mobile terminals would store a lot of sensitive data about users' privacy, especially the address book, short message and call records. On the other hand, plenty of functions and services provided by apps are involved with money. So information security is directly related to users' interests.

The category of personal information

There are several main kinds of personal information in our mobile phone, these are:

- Messages
- Important data stored by users
- Identification messages
- Call
- Mobile phone message itself
- Other kinds of messages

When we get to master the source of the personal information, we can solve the problem according to different kinds of information.

Shortage about personal information protection

The methods above can protect the personal information in a way, but still, there are some shortages.

1. There are not so effective methods to prevent the malicious software accessing the personal data, due to the openness of the Android platform itself, the information including messages, address list, even the data in the SD card can be accessed easily.

2. There is a lack of sound laws or the regulations of the related field to restrict the behaviour of the mobile companies. For example, the server to backup the personal data belongs to the company, which is not bound to protect the security of the information, so some users don't believe the service like this.

The common risks attacking our mobile phones

1. Vicious software or other vicious codes have quietly wantonly stolen mobile phone users in the personal information. Through these malicious software our mobile phones behave abnormally, such as unusual power on and off, switching on the networking services of mobile phones, sending text messages secretly and so on.

2. Users will be more and more getting used to tackle important things on smart phones for its carrying convenience, moreover, a mobile phone can be related to a PC and other mobile devices through networks, the risk will increase and spread, and most of apps are free of charge. So users can download them casually and may be less aware of its security.

3. A kind of software which looks usual seemingly but in fact a vicious software. Because Android programs is created by java, the intermediate code being compiled is realized by Java Virtual Machine. This means Android applications are easily decompiled and then changed. This kind of software is not completely finish by the original developers, but acquired by third-party vicious developers.

4. Modification or reset of the operating system of the mobile phones: by changing ROM to change the elemental settings of the phone. But the third-party ROM usually doesn't guarantee the security of the system. So some ROM makers can add ads and some malicious hidden apps, and these apps may link to the internet secretly. ROM makers have different levels, some ROM may have loopholes which may be used by the malicious software.

5. Releasing the supreme restriction: we know it as 'ROOT', in the Android system, ROOT is a super administrator, and in general, users can't have use ROOT, but now, with a lot of apps acquiring ROOT, which can cause that many vicious apps can also get ROOT, if so, these apps can not only read and write personal data, but also modify or even delete important files of other applications.

6. Free Wi-Fi: At present, many people is used to going somewhere to have a lunch or just rest, and these public places may provide free Wi-Fi, but few people are aware of whether it is safe. These networks may let your login and require you to input your account and password, and some people can get personal information through this way.

What we can do to protect our information

1. Access control: Users should avoid downloading some software which has the acquiring ROOT function. Some important information, such messages, call records and address list should be encrypted by using protection software or be equipped with password. So the most important thing is to get ROOT, when the supreme rights are got, a mobile phone can be easily attacked and spied on by other illegal software.

2. Backup of personal information: To prevent the loss or the destruction of the mobile phone, a good habit is to backing up the important data through internet. If there comes an emergency, the information can be retrieved from the cloud. The backup of the address list means that it is transformed into VCard version then uploaded to the server, since the VCard version is a common standard, so it can be used on different platforms.

Conclusion

As the development of the mobile telecommunication and network, the smartphones is becoming a terminal which will be used extensively to process data. The protection of information security will be stronger in a technical level. But, it is not enough to protect information through technology merely, we also need management. When we can combine technology and management, our personal information can be well protected, which requires the users, the mobile phone companies, application programers, and the government all to make effort.