International Journal of Current Trends in Engineering & Research (IJCTER)
e-ISSN 2455–1392 Volume 2 Issue 4, April 2016 pp. 102 - 104
Scientific Journal Impact Factor : 3.468
http://www.ijcter.com

Securing the Smartphone

Virat Gandhi
Computer Engineering, C. U. Shah University

Abstract—Mobile security or mobile phone security has become increasingly important in mobile computing. Of particular concern is the security of personal and business information now stored on smartphones. More and more users and businesses employ smartphones as communication tools, but also as a means of planning and organizing their work and private life. Smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

Keywords—secure; smartphone; mobile; cell; smartphone attack

I. INTRODUCTION

Smartphone is the trend of unified communications which integrate telecom and Internet services onto a single device because it has combined the portability of cell-phones with computing and networking power of PCs. As illustrated in figure, smartphones as endpoints of both networks, have connected the Internet and telecom networks together. Another key reason for this trend is the ease and low cost of introducing new integrated Internet and telecom services. Easy service creation demands common operating systems. Because smartphones are typically as powerful as a few year-old PCs, their operating system have evolved to be rather full-fledged. [1]

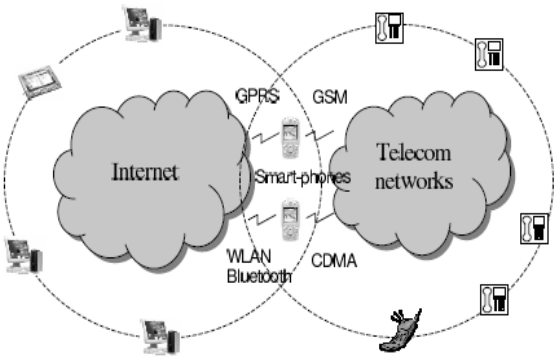

Fig.1 Smartphones become end-points of both the internet and telecom networks.

II. PREVENTING A SMARTPHONE FROM ATTACK

2.1. Use a pin, password, pattern or fingerprint to lock your phone

Now a days every smartphone comes with protection mechanism which adds a layer before getting into the device. User can set PIN, PASSWORD or some kind of PATTERN to lock the device. In some latest devices there is also a provision for fingerprint scanner which will scan your finger to lock/unlock the device.

2.2. Download apps only from trusted stores

If you're browsing for a new game or something more productive, use trusted places. Make sure you check ratings and reviews if they are available, and read the app's privacy policy to see exactly what phone features it will have access to if you download.

2.3. Back up your data

Now a days we keep our important data in smartphones for quicker access to anywhere. Not only this but there are also some other data that we don't want to loss in any case. Backing up all these data is

an important if we lose the phone or phone got damaged accidentally. There are many cloud based services available which will help you to back up the phones data.

2.4. Keep your operating system and apps updated

Smartphone users should always keep the operating system and apps updated. There are typically periodic updates to both of these that not only add new features, but also offer tightened security. Many third-party app-makers frequently update their software, adding new features and patching security holes. Keeping software up to date can help ensure you are protected from new threats.

2.5. Log out of sites after you make a payment

If you bank or shop from your smartphone, log out of those sites once your transactions are complete. Other tips include not storing your usernames and passwords on your phone and avoiding transactions while you are on public Wi-Fi.

2.6. Turn off Wi-Fi and Bluetooth® when not in use

You think of them as ways to connect to something, but thieves can use them to connect to your device and access files.

2.7. Avoid giving out personal information

That text message that looks to be from your bank may not be. If you get requests via email or text for account information from any business, contact the business directly to confirm the request. The same advice goes for tapping links in unsolicited emails or texts.

2.8. Beware of links in email, on websites, and in social posts

Phishing continues to be a major -- and increasingly sophisticated -- security problem. While some users get hacked through an active attack, many people open up their own security holes by getting caught in a phishing scam or by downloading malware from untrustworthy sites. Be smart about links in emails, on websites, and in posts, and if a link looks suspicious, don't click it.

2.9 Use public Wi-Fi with caution

If you're using a public Wi-Fi hotspot -- in a cafe, in a hotel, on a plane -- experts say it may be possible that someone is snooping on you, trying to grab your information. While some recommend that you turn off Wi-Fi and Bluetooth when out in public, that kind of defeats the purpose of having a mobile device. Most email services and e-commerce and financial sites offer secure connections by default, which provides a measure of protection when using Wi-Fi in public places, and browser makers are adding security features that will warn you when you're trying to access an insecure site. For additional security, a VPN allows you to create a private connection over a public network to send and receive sensitive data, such as credit-card information. In an Internet address, look for the "s" at the end of "http." That shows you have a secure channel over an insecure network.

2.10 Use security software

Antivirus and security software can scan for malicious apps, warn you about suspicious websites, and offer security for lost phones. Several publishers make security apps.

2.11 Do Not Save All of Your Passwords

Many users tend to save their passwords to online services and sites on their device, never once thinking about what it would mean to a person who got their hands on the phone. Avoid having all important passwords saved in your device particularly when it comes to banking or payment apps.

REFERENCES

[1] http://download.cnet.com/blog/download-blog/keep-your-android-phone-secure/
[2] https://en.wikipedia.org/wiki/Mobile_security
[3] Chuanxiong Guo, Helen J. Wang, Wenwu Zhu, Smart-Phone Attacks and Defences,