Introduction to android platform development

Business, Industries

Android is an open source platform, which means the SO can be customized by anyone. Anyone can develop for Android and all the developer tools are free to access and download. 2. 1 Android vs.. Other Mobile SO There are different types of mobile operating systems.

Android and ISO by Apple, are the two main offerings on the market today. As of 2013 over 60% of all smart phones purchased were android devices [8]. Windows is now producing a mobile SO that resembles the desktop version their users are accustomed to.

Currently, there are not many offerings for devices or applications, although it is an emerging market. The unique aspect of Android s that it is an open source operating system, which anyone with the right tools can customize. 2. 2 Android Rooting and Modification Often, individual mobile service providers and manufacturers modify the SO on the devices they offer in order to add or limit certain resources.

Tech savvy users have the ability to “ root” their devices. Rooting allows the user privileged access to features on the device. It allows the user to unlock features that can be locked such as tethering.

Losers can also modify the look and feel of the device. There are currently laws and regulations that are Ewing changed in order to prevent rooting devices. Rooting is a way to circumvent the mechanisms to protect digital rights management (DRY). In the United States, there are currently regulations against rooting, however mobile phone devices have been exempt until 2015. There are certain situations which that have been allowed for, such as when it is necessary to legally use APS and device

features necessary. Mobile devices make our lives easier. Tasks that once could only be completed while in front of a PC are now able to be addressed easily with the touch off screen. This presents a double edge sword.

Much of the data that is stored on mobile devices or transmitted over mobile devices can be sensitive data. A user can’t always be in control of access to the devices network, and something as simple as a device in the wrong hands could be detrimental. 3. 1 Device Breach If someone other than the owner has access to a device, they can retrieve important personal data.

From a business perspective, an executive who uses his mobile phone to access his company e-mail and leaves it on a restaurant table while at lunch, has now made available to anyone who picks p the device, industry information and business e-mails regarding such information. A threat doesn’t always have to be an unknown developer or attacker. Often in the world of technology we overlook or underestimate simpler means of breaching security. 3. 2 Mallard and Malicious Applications A user visits the Google Play Store, and downloads a simple game.

Assuming that because it is offered in the app store, the application is safe, the user doesn’t bother to read the permissions that the app is asking for very carefully. Once the user installs the app and clicks accept for the APS remissions, the developer can access areas of the device unrelated to the APS performance. Andrew Borg, research director for enterprise mobility and collaboration at research firm Aberdeen [8] tells of an eye opening experience at a convention. A demonstrator downloaded an application from the Google Play Store, onto a device that was just out of the box. The

application was made to look like a knock off of the popular game app Angry Birds. Once the application was deployed nothing seemed different on the device.

The demonstrator then logged onto his laptop to show how the app loud let him access a control stream that showed him all of the smartness that had downloaded the app, inspect the devices and access their emails. The demonstrator showed that he was able to put the device to sleep and control the camera from his laptop to take pictures and video from the device. Features that would normally alert the device owner that these applications were in use, such as a shutter sound, had been disabled by the mallard. Other similar APS can run hidden along with other APS in order to make unauthorized purchases. 3.

3 SO Fragmentation The ability to customize the Android SO makes it difficult to one option for securing all devices. A device that is rooted may not employ SO updates that could protect the user from identified security risks. A manufacturer may provide a solution that works for their device, but would not work on a device from another manufacturer. This make risks unique to certain devices, running specific platforms. Once these risks are identified by a malicious programmer, they can be exploited.

4. SECURITY SOLUTIONS Sec ritzy for mobile devices is twofold. One must consider the security of the device and the data. There are a variety of tools, APS, and tips that a user can employ in order to protect their device and data.

4. 1 Personal Device Sec ritzy The first means of protecting your device can be as simple as using a screen lock on the device. These vary from device to device and can be as simple as requiring a pin code to wake the phone, or recognizing the face of the device user before allowing the user to proceed. A screen lock can give you time to access accounts and clear data from the device. 4.

2 Data Loss Prevention Maintaining a backup of information is one method of protecting yourself room loss of data. Cloud storage is a good option and Google automatically updates your contacts from your phone. There are also applications which are discussed further below that aid a user in wiping data from a phone in the event the device is lost or stolen.

. 3 Mobile Security Applications Users can install an application to protect their mobile devices. Some applications are free and others offer a per month subscription. MacAfee and Norton both offer a mobile security application. Many applications offer the ability to secure the device, backup the data, back up the data and restore it ND wipe or erase data remotely on a lost or stolen device.

Lookout Mobile is one of these options. Lookout offers a free application and then also offers users more advanced features for a monthly subscription fee. There are also third-party applications that scan APS to determine if they are safe or not before installing on the device. Figure 1 4.

4 Developer Authentication One restriction that many devices have, is the ability to sidelong APS, or install applications that are not offered at the

approved app store. This can act as a line of defense from developers of malicious APS. Developers are squired to create a key for their applications and to be digitally signed with a certificate before they can be installed (See Figure 2).