FCC TAC – Cybersecurity Working Group

Simplifying Smart Phone Security Sub-Working Group

Security Wizard Requirements

Contents

Purpose of this document

This document is intended to help facilitate the creation of an app or apps commonly known as a wizard that would help guide the consumer through the process of securing their smartphones. Smartphones today offer a wide array of features and functionality which had previously not been accessible in such an easy to use and ubiquitous device. However, with the addition of those features and functionality there is also an addition of security related issues that the consumer faces.

Although, there is a lot of security built into the smartphones, and into the networks they connect to and traverse, consumers must also take steps to protect their data, their privacy and the smartphones themselves. The FCC wishes to have an app, like a wizard that can walk the consumer through the settings necessary to secure their smartphones, educate the consumer on the best way to use their devices securely, and to reduce the possible impacts of these security threats.

This document is not intended to be an all-encompassing set of requirements as the various smartphones from various manufactures; with different Operating Systems (OS) with varying degrees of complexity all have different approaches to implementing security. Instead, this document should be a basic set of security steps a wizard should address and leave the exact steps to the application developers who will be creating these wizards for specific smartphones.

Background

Revision History

Author	Date	Version	Revision Comments
Renato Delatorre	05/11/2015	1.0	Initial Draft
Katrin Reitsma, Renato Delatorre,	06/12/2015	1.5	Revised based on feedback

Securing the Device

This section describes specific actions the consumer should take with guidance from the security wizard.

Screen lock – Pins, Passwords, Biometrics and Patterns

All smartphones today, have the ability to lock the start screen with the use of a pin or a password, and many also have the ability to use biometrics, such as fingerprint readers, face recognition as well as the use of patterns. All of these options present differing levels of security from medium to high, but in all cases the consumer is better off employing a locking mechanism then not. If the device is lost or stolen, this will become the first line of defense in protecting their data and privacy.

The wizard should educate the consumer of the differences between each available option and have the consumer select the type and level of security they wish to use then walk them through the process.

Ensure that your device locks itself automatically – Screen timeout

Screen timeout is also part of the first line of defense in that if the user walks away from their device the lock out time of the screen is the window of opportunity for someone to take control of their device. Timeouts typically start at 15 seconds to as long as 15 minutes.

The wizard should instruct the consumer to set the time out to the least amount the user can tolerate. Longer timeouts leave the device open longer thus widening the window of opportunity that someone can take advantage of.

Backing up your Data

Backing up the device is key in a recovery effort so that valuable data is not lost. There are many options for this, but all major OS have this function built in. There is also a wide array of options provided by the OEMs and third parties to choose from.

The wizard should educate the consumer of the importance of backing up the data and allowing the consumer to choose an option and walk them through setting up a backup mechanism.

Remote Lock, Wipe, Locate and Alarm (LWLA)

Locking a device remotely is essential to protecting a consumer's data if the device is lost or stolen, as is wiping that device if the device cannot be located. This feature, once activated will delete all data from the device and in some cases from the SD card as well. Remote locate is also an essential component in recovery of the device as it will query the device and give the user an area to look in. With the addition of an alarm that can be heard from some distance away, finding the device can be accomplished.

However, none of this is possible unless the consumer takes the steps in setting up the Lock, Wipe, Locate and Alarm features. There are also many options to choose from. Again, many OS's have these features built in, and the OEMs and Carriers also provide these capabilities.

The wizard should educate the consumer of the importance of setting up LWLA and present the options so that it can walk the consumer through the process

Update your device's OS and applications

Updating the OS and applications is essential to maintaining the proper level of security. Therefore, the wizard should educate the consumer to always accept these updates and walk them through setting up automatic updates.

Set your Wi-Fi hotspot to the best available security setting

Many smartphones today have the capability to also function as a Wi-Fi hotspot that other devices can connect to. Just as with Wi-Fi routers at home, the same security vulnerabilities exist. The SSID and password should be changed from the default and the highest level of encryption available should be used. In addition, if the device has WPS available it should be disabled.

The wizard should educate the consumer on why these steps are necessary and walk them through the process.

Enabling Whole Device Encryption including the SD Card

Most OS's also have the capability to encrypt their entire file system, and in many cases also encrypt the SD card. Encryption protects privacy of data in case the device is lost or stolen."

The wizard should educate the consumer of the importance of whole disk encryption and guiding them through the process of setting that up.

Bluetooth configuration should be set to Non-Discoverable

Bluetooth technology has been around for a long time Most of the security issues that had been associated with Bluetooth have been addressed in the current versions. However, Bluetooth can still be a conduit for malware if the right precautions are not followed. To prevent Bluetooth from becoming the conduit you simply need to not broadcast your availability to connect with devices that you do not intend to pair with.

The wizard should educate the consumer on the risks associated with publicly broadcasting the devices Bluetooth signal and walk them through making that the default setting if it is not already the default.

Secure Behavior – Educating the Consumer

This section discusses educational awareness around certain consumer behavior that may lead to a less secure device. The wizard would be used to present the consumer with this information as part of the process but not necessarily have the user do anything. This can be accomplished in many ways, but a simple webpage that pops up is sufficient.

Be careful about rooting or Jailbreaking your smartphone

Do not alter security settings for convenience. Tampering with your phone's factory settings, jailbreaking, or rooting your phone undermines the built-in security features offered by your wireless service and smartphone, while making it more susceptible to an attack.

Only install apps from trusted sources

Before downloading an app, conduct research to ensure the app is legitimate. Checking the legitimacy of an app may include such thing as: checking reviews, confirming the legitimacy of the app store, and comparing the app sponsor's official website with the app store link to confirm consistency. Many apps from untrusted sources contain malware that once installed can steal information, install viruses, and cause harm to your phone's contents.

Understand app permissions before accepting them

You should be cautious about granting applications access to personal information on your phone or otherwise letting the application have access to perform functions on your phone. Make sure to also check the privacy settings for each app before installing.

Accept updates and patches to your smartphone's software

You should keep your phone's operating system software up-to-date by enabling automatic updates or accepting updates when prompted from your service provider, operating system provider, device manufacturer, or application provider. By keeping your operating system current, you reduce the risk of exposure to cyber threats.

Be smart on open Wi-Fi networks.

When you access a Wi-Fi network that is open to the public, your phone can be an easy target of cybercriminals. You should limit your use of public hotspots and instead use protected Wi-Fi from a network operator you trust or mobile wireless connection to reduce your risk of exposure, especially when accessing personal or sensitive information. Always be aware when clicking web links and be particularly cautious if you are asked to enter account or log-in information.

Wipe data on your old phone before disposing of it

Your smartphone contains personal data you want to keep private when you dispose your old phone. To protect your privacy, completely erase data off of your phone and reset the phone to its initial factory settings. Having wiped your old device, you can donate, resell, recycle or otherwise properly dispose of your phone.

Report a stolen smartphone.

The major wireless service providers, in coordination with the FCC, have established a stolen phone database. If your phone is stolen, you should report the theft to your local law enforcement authorities and then register the stolen phone with your wireless provider. This will provide notice to all the major wireless service providers that the phone has been stolen and will allow for remote "bricking" of the phone so that it cannot be activated on any wireless network without your permission.

Change all of your passwords in the case where the device is stolen

If your device is ever stolen or has been missing for some time, you should consider changing all the passwords to accounts you used on the device. Not just those for the app stores but also for all the accounts on apps that you used on that device.

Turn off Bluetooth, NFC, Location Services and Wi-Fi when not in use

When not in use you should turn off the Bluetooth, NFC, Location Services and Wi-Fi radios to prevent them from being abused, and to conserve battery power.

Log out of sites after you make a payment or other financial transaction

Just as with a personal computer you should always log out and close the browser once you have completed your transactions. This will prevent a hacker from stealing your session and reestablishing the connection to the webserver you were just connected to.

Avoid giving out personal information via Text messages or email

Many scams are perpetrated via email or SMS text messaging asking that you supply sensitive personal information. You should research the sender or institution asking for this information and ensure that they are who they say they are.

Avoid clicking on links in email or Text Messages

For the same reason above, you should never click on a link that is in an email or SMS text message even if you think you know the person who sent it to you unless you are sure that it's legitimate. Many scammers count on the fact that you might know the sender to get you to click on the link.