STEPS

Solutions that Enable Phone Security

Donna Calabria

Ryan Eggert

Chang Liu

Mikel Polena

Xiajing Wang

December 2014

Current mobile phone security solutions are inadequate and underutilized.

As smart devices acquire a multitude of functionalities, increase user social interaction and enable more productivity they become more desirable targets for criminals. Once in the wrong hands, these devices remain usable and may re-enter the marketplace without major obstacles. Customers are greatly affected by financial loss as well as loss of personal data. Law enforcement is unable to track the rising numbers of these types of crimes given their limited capability and resources. Current solutions are not standardized and vary between different platforms. This creates confusion among users who often fail to take advantage of the features provided.

Adoption of security solutions increase at the time of purchase and loss.

In the continuum of “life” of a smart device two moments carry the most significant importance with regards to the user: the moment when the device is purchased and the moment when that device is lost or stolen. By framing our solutions around these two key moments, the liklihood that users will adopt STEPS is increased.

STEPS

a multilayered approach to mobile phone security with three key components:

1 Required Pins

A passcode required at set up and applied to power off, airplane mode, and lock screen. These can be configured after set up

2 Secondary Tethered Device

Another device that is “linked” to the users phone or tablet run by an app. The connecting software allows an number of security features to be used.

3 Fraud Detection

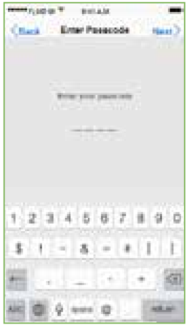
The smart device remembers the users behaviour. A warning is sent to the provider and the user when the device acts suspiciously

1 Required Pins

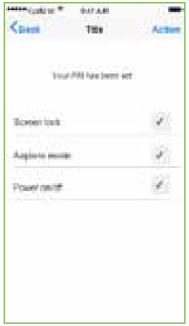
When the phone is stolen, PINs are the first line of defense. Airplane Mode and Power OFF/ON actions are logical steps that thieves follow when the stolen device is obtained. Based on recent research, it is estimated that only about 1/3 of users set-up a password on their smart device. Power off and airplane mode PINs do not even exist. This shows the importance of the required PINs.

When initially setting up the device, the user must enter a PIN. This security measure is automatically applied to putting the phone on airplane mode as well as shutting it down. Users may then change or even remove the PINs if they desire.

In addition to accessing the home screen, anytime the user decides to shut-off or place phone into airplane mode he/she would be required to enter a pin. Users may choose to have different pins for each function.



Enter your passcode

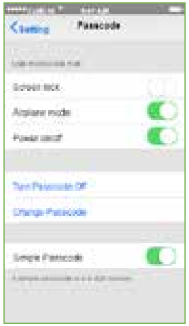


Your PIN has been set

Screen lock ✓

Airplane mode ✓

Power on/off ✓



Screen lock

Airplane mode ●

Power on/off ●

Simple Passcode ●

Benefits

Prevents thief from accessing user data

Renders phone unusable

Regulatory Considerations

Platform independent

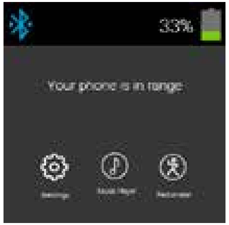
Easily implemented via software update

2 Tethered Secondary Device

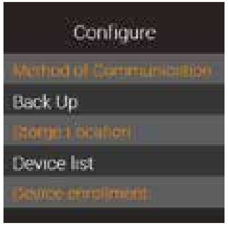
If a phone or tablet is stolen, there is no quick way to back up and or wipe the data on the device. People have to wait until they have gotten to a computer or another phone and by then the device is off and the data is stolen. In addition if the user has no knowledge of the device being left or stolen there is no way of quickly informing the owner.

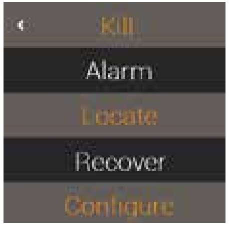
An app is installed that can add devices into its protection. These devices now sync their data into a device of their choosing or real time to the cloud. In addition a secondary device is chosen, one that will remain close to the primary.

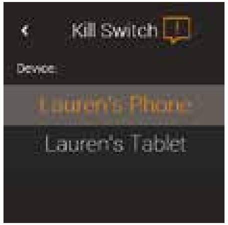
The backup of the data ensures that whether the phone is stolen or lost, the users files still exist. in a robbery situation, the secondary device will send an alert after the primary device leaves the allowed zone. Once the user knows of the incident, they can trigger an alarm on the primary device which activates the ringtone at max volume. They can also activate the kill switch from any of the devices which will wipe all data on the missing device except for the PINs.

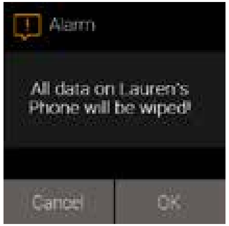


Your phone is in range









All data on Lauren's Phone will be wiped!

Benefits

Prevents data/media loss

User has control of own data.

Adds layer of security and peace of mind.

Regulatory Considerations

Tracking information cannot be accessed by Providers.

Privacy laws must apply.

3 Fraud Detection

Stolen or lost devices often never reappear. This means that somehow the device is being modified if it is being used so that it is no longer recognizable, so there is no trace of whether or not the phone was stolen.

OS is formatted to have a segment of memory dedicated to owner “activities”. This segment will not be reimaged and can only be changed with proper authorization.

If the device is ever modified so that it is gone from the network but in use, the device will remember how it used to act and will send flags to the provider indicating suspicious activity. It can also send an email to the recorded owner asking to confirm the recent actions.

Benefits

Phones will remember how they acted previously and can let providers know something is wrong even if the phone drops off the network.

Non-invasive software

Will provide useful data for phone theft

Regulatory Considerations

Providers must protect usage information that is received.

For questions & inquiries about STEPS,
we invite you to contact us.

Mikel Polena Mikel.polena@gmail.com

Donna Calabria dcalabri@hawk.iit.edu

Chang Liu cliu60@hawk.iit.edu

Ryan Eggert reggert@hawk.iit.edu

Xiajing Wang xwang191@hawk.iit.edu