**The Appropiate Way To Handle Security For Mobile devices**

Nowadays we all use mobile phones for communicating and even entertainment. Some developed countries even being estimate each citizen has 2 mobile phones. Therefore security and privacy is becomming an issue. This article will talk about ways to handle this kind of issue.

Typical structure of traditional smart phones:

Data Storage:

* Database
* Data Folders
* Image Folders

Install Apps

Play Store

App Store

Harmony Store

**Smart Phone:**

**Andorid Devices**

**iOS Devices**

**Harmony Devices**

App

Rest APIs

Data

Modify structure of the smart phones:

App

Rest APIs

Play Store

App Store

Harmony Store

Data

Data Storage:

* Database
* Data Folders
* Image Folders

**Smart Phone:**

**Andorid Devices**

**iOS Devices**

**Harmony Devices**

The new structure of uploading and installing apps still remain the same as the traditional approach, however for the new design structure the app store not only a place to download apps, but also act as a proxy server, incoming and outgoing data are strictly controlled:

1. All android, iOS apps must be digitally signed, inorder to upload to the play store or app store.
2. It is assume all the apps are being security checked, At least no malware or viruses. We have ways to handle malware or viruses, such as we can install Norton AntiViruses for mobile.
3. It is recommend to download the apps from play store or apps store not unauthorised third party apps store.
4. All incoming data is allowed but there are strict policy for outgoing data.
5. Out going data includes:
   1. Apps data (data such as whatsapp, wechat data, banking or trasactional data, game data...etc)
   2. Personal data (phone contacts, calendar schedule...etc)
6. When upload apps to the app store, you need to provide 2 things:
   1. One is the digital signed app.
   2. The second is the data server link. After checked, this link will be used by the play store and app store to make connection to it. So the play store act as a proxy server, only valid links that are listed at the playstore proxy server are allowed to pass through (In or Out).
7. It is assume this link base on the app is strictly followed the security policy and regulation such as privacy.
8. If any violation in terms of security or privacy,the link will be removed from the play store or app store’s proxy server. By then all the devices that has install this app will not be able to make any connection or transaction untill it is fully restored.
9. Compare to outbound connection, it is assume inbound connection (in comming data) has no restriction.
10. This is the fastest way to stop an intrusive apps from operating, without uninstall the app from all devices in the world.