Tablets Report

Prof Alexiei Dingli
Dr Lalit Garg
Dr Colin Layfield
Prof Matthew Montebello

Faculty of Information and Communication Technology
University of Malta

16th March 2015

UNIVERSITY OF MALTA
L-Università ta' Malta

TABLE OF CONTENTS

Executive Summary

In January 2014, the Government of Malta launched the 'One Tablet per Child' pilot project whose aim is to foresee the introduction of computer tablets in primary schools. An expression of interest was also published in order to test different types of hardware and software solutions with the aim of collecting feedback from educators and students.

As part of this initiative, the Faculty of Information and Communication Technology was requested to assist. In fact, an inter-departmental team was setup made up of academics from the Department of Intelligent Computer Systems and the Department of Computer Information Systems. These academics were entrusted with the task of analyzing the three major tablet platforms in order to create a coherent and impartial analysis, which can help during the selection of the ultimate platform. The result of this exercise is this document, which was presented to the committee responsible for the tablets project.

Throughout this document, one can find a thorough discussion pertaining the positive and negative aspects of each platform; be it Android, iOS or Microsoft. Whilst praising the most positive features of each platform, the document also highlights the issues, which might arise when developing content for these operating systems (OSs) and the weaknesses, which currently exist. We also examined issues, which might arise when using these platforms. In particular, our analysis also takes into consideration the fact that the usage will happen in a primary classroom setting and thus, additional issues such as sturdiness of the device had to be considered. Even though we mentioned some examples, we did not really go into the merits of particular devices because the market is so fragmented that it would have been impossible to pinpoint specific models or brands. Being a highly volatile sector means that the information presented in this document can be considered correct at the time of writing however we are expecting major changes in the coming months which will definitely change the way in which we interact with computers forever.

The document is well suited to help the committee get abreast with the latest offerings and future potential of each platform in order to allow them to take an informed decision. A decision, which will have a long lasting effect on the eventual success of the project and the ultimate wellbeing of our children.

Introduction

The tablet revolution started five years ago with the launch of the original Apple iPad. Since then, we've seen a myriad of tables flooding the market. It seems that the tablets are here to stay and in the coming years, we expect to see more powerful devices, which are even lighter, capable of communicating with wearable technologies and ubiquitous computing seamlessly.

The choice of tablets, especially for school environments, might be tricky. Experiments using technologies such as tablets should be done on a small scale at first before a decision is reached or a large investment is made. Malta is currently following a similar approach with their tables in schools initiative. The choice is between the iPad, one of the many Android tablets or a Windows model.

First of all, we need to clarify that despite the increasing capabilities of the tablets in terms of computing power; they still cannot replace a full-blown computer. Having said that, recent innovations such as cloud technologies might help to drastically reduce this issue in the coming years. The most adequate tasks for these devices include amongst others the productivity tasks (software dedicated to producing information, such as documents, presentations, worksheets, databases, charts, graphs, digital paintings, electronic music and digital video), thus tablets can be considered as being an ideal device for the classroom. Apart from this, the ergonomic benefits of tablets surpass by far those of other devices such as laptops.

A negative aspect of any tablet is the on-screen keyboard because it cannot provide the same comfort and response which one can experience from a physical keyboard. Another issue is the support for a Maltese keyboard. In fact, at the time of writing, this is only possible on Android devices. Notwithstanding this, there are various options, which one can consider to overcome these issues.

The Operating Systems

Just like any device, a tablet needs an Operating System in order to work. At the moment, the undisputed leader is the Android OS with a 64% market share, followed by iOS with a share of 29% and Windows with 7%. Whereas iOS is locked down to specific Apple hardware, Android can be found running on various hardware choices from the likes of Acer, Amazon, Asus, Samsung, and others. Windows on the other hand seems to be built around the Intel's Atom processor, which is in use, by various manufacturers. We will now explore the different aspects of the three systems mentioned earlier in order to facilitate the decision, pertaining to which tablet is adequate for the purpose of this project.

Android

Security

Android does come with a basic native security architecture which is customisable from basic to advanced, meaning that the software developer will be responsible to ensure the safety and integrity of the application and the tablet itself. Security features can be enabled and enforced in a number of ways.

- **Android Application Sandbox –** isolates data and code execution for every individual App, which can be further increased with security-enhanced Linux (SELinux) mechanisms and policies that support access control, as well as boot integrity.

- **Android Application Framework –** strong enforcement of the most effective security capabilities that include safe Inter-Process Communications (IPC), security permissions and cryptography. IPC specifically specifies the communication between different components of an Android OS using: Intents (data messages sent between components to initialise services, activities, and invoke broadcast receivers); Bundles (the actual entities that data goes through); and Binders (the entities themselves that enable references between activities and services).

- **Encrypted File System –** purposely and intentionally developer enabled for data protection on stolen or lost devices.

The open architecture of the Android OS does give rise to security preoccupations but both the default security measures and the App developers' knowledge of potential security issues and best practices make this OS as secure as any other.

Some concerns still need to be ironed out, namely:

- Upgrades of latest security patches not performed and updated regularly can lead to security holes.

- Active content like Java, JS, HTML5 and Flash can potentially allow malware and security attacks and thereby need to be kept in mind when developing or deploying Apps.

- The nature of Android's open platform is more liable to rooting whereby the user gains super rights and unlocks the access to alter the boot loader and a free hand to other OS versions and a variety of App installation.

- Unsecured Apps that have not been tested for security issues are potentially malware that can provoke havoc throughout the OS while taking full control of the tablet.

All these concerns can be easily taken care of by knowledgeable and good-intentioned developers, administrators and providers. The list below summarizes the user benefits and the IT security impact of the latest features in Android 4.4 tablets and smart phones:

- **Certificate handling and KeyStore enhancements -** Whitelisting and Certificate Pinning ensure that only valid certificates are used, Elliptic Curve algorithms streamline strong encryption, and warnings from Certificate Authority (CA) certs added to device thwart man-in-the-middle attacks.

- **Always on listening -** Saying "OK Google" without touching anything activates the device. This feature is currently just on Nexus 5, but planned to expand. Devices may wind up recording unintended conversations and may dynamically enable or disable features based on what is said.

- **Auto add of missing content -** The automatic addition of missing contact, nearby resources, maps and location info fills in. People who work in secured facilities, or with highly security-conscious customers should not be giving away rich location-based info and must disable this feature.

- **Cloud integration -** Integration of local and cloud storage means that information can be automatically stored/ synced between the device, applications and the cloud. The use of Google Drive and third-party personal file sharing services will be native to apps and enabled through API's. IT must ensure that an enterprise-grade solution is available and enabled.

- **SMS, Google Hangouts for SMS -** While Google Hangouts is great for personal interaction, enterprise SMS must be configured and enforced for institutional communications.

Final advice regarding security of an Android OS includes:

- **Platform –** use different user accounts on a shared device.

- **Authentication –** screen should be locked and lock configured to set the passcode and PIN security with an automatic time-out on the lock, which instantly locks when powering down.

- **Encryption –** Device and Apps should be totally encrypted.

- **Cloud services –** backup to personal Google accounts should be disabled.

- **Bluetooth and Sharing –** data transfer should be disabled.

- **Network and wireless –** notifications should be provided by configuring the wireless.

- **Email –** make use of secure connections only.

- **Upgrades / Lost / Stolen –** third party or centralised backup system for each device with a facility to erase all personal data on a factory data reset.

- **Privacy –** ensure to disable any settings that collect personal and sensitive data including any diagnostics and usage data.

- **Diagnostics and developer features –** any developer enabled capabilities should be disabled including USB debugging.

- **Applications –** only from trusted or in-house sources.

Customisability

The Android platform is highly customisable as the OS developers are independent from the hardware and software developers allowing plenty of room for tweaking settings and changing things around or customising the entire hardware and software, only Android allows you to do so.

Speed and Hardware Range

The fact that Android devices sustain and handle multitasking is a sign that the OS running off a dual-core processor has more than enough power to do so. With a default multitasking panel that can easily bring up running Apps with a single tap on the screen, the Android performs very well together with a facility that provides full previews of all currently running Apps.

The Android platform is completely open to all industry collaborators making it the largest OS deployed on a variety of different hardware ranges. This could be a problem in some cases, where the hardware provision is not centrally controlled as different people in the same group can opt for different models, but in the case where all units are provided centrally, then this is no issue at all and actually turns out to be a great advantage of having so many providers offering the same platform specifications.

Software

Similar to the flexibility expressed in the hardware range section, software development and availability is even more flexible and easier adapted as it is sourced from any developer and not necessarily from a dedicated source. Over and above this, the possibility of in-house or trusted software App developers is so vast that it makes the issue of software availability for Android-based tablet practically

inexistent. Security issues still apply as discussed earlier in the document. Compatibility issues come also into play as active content mentioned earlier like Java, JS, HTML5 and Flash, if secured and within a controlled environment give the Android platform a competitive edge above other Oss.

Ease of Development

The ease of development goes hand-in-hand with the software issues mentioned in the previous section. Android SDKs are as popular as much as they are available in quantities that developers have such an ease to develop, test and deploy quickly and effectively. In-house development as well as trusted local developers are very much advanced in the Android-based Apps development than any other platform available.

Robustness

Physical endurance of Android tablets is as vulnerable as any other tablet and if dropped onto one of its four corners the screen is likely to crack. So a good case and an insurance cover is the best way forward. With regards to software robustness Android is not as stable as other counterparts but has been improving as newer OS versions adapted and optimised the deployment of Apps.

Connectivity

Wireless is obviously the natural choice for all tablet platforms, and as new standards come into play, being g, n, or ac, does not really matter, as the different platforms will quickly come up to scratch and roll out devices to take advantage of the latest and most effective connectivity standard. What Android tablets can boast about as having a competitive advantage is the availability of a USB or micro-USB connection giving the user and administrators alternative connectivity options.

iOS

The iPad is an innovative computing mobile hardware tablet which runs iOS. The user interface consists of a touch screen which includes a virtual keyboard (which does not support Maltese). The iPad is able to perform many multi-media type functions such as shoot video, take photos and play audio as well as enabling Internet connectivity to perform web browsing tasks or use email. As one knowledge gathering and sharing event on the experiences of using iPads in an educational context observed: "participants noted the physical elements of iPads enable easy portability and facilitate gesture-based approaches to interactivity more readily". Internet connectivity can be gained either through WiFi or 3G connections (3G being supported on higher end models). The iPad was the first of its kind as it is neither a tablet computer nor a smartphone but includes components of all of these technologies.

Additional functionality (such as games, reference, social networking tools, etc) can be enabled through the installation of apps which can be downloaded through the Apple iTunes store. Many apps are available free. With educational institutions now beginning to focus on taking advantage of new technologies in the classroom (smart boards, tablets, etc) research is now starting to take place on how best to take advantage of this. Foreshadowing for tablets in the classroom has been present for over a decade and is now being actively explored as to how it can be employed in a teaching context.

This section reviews the pros and cons of the iPad (using the iOS operating system) platform from Apple. The document is split up into several sections that will address various points.

Security

Security on the iPad is extremely important. This can range from how secure it is from outside intrusion/malware and how secure can we make the iPad with respect to what a student can see or do on it. Protection and integrity of personal data is also of concern.

Apple claims that iOS was built from the ground up with security at its core. However, this is not to say that iOS has not had its' security challenges. In February 2014 a SSL (Secure Socket Layer) vulnerability was discovered that affected all devices. This would allow hackers to intercept and, potentially, alter communications such as email messages or even login credentials (a so called man-in-the-middle attack). A patch was released to fix this flaw. In May 2014 another attack geared towards iOS devices came to light in Australia. Many apple customers reported that they were locked out of their phone and had to pay a ransom to regain access to a hacker going under the pseudoname of 'Oleg Pliss'. This was not an inherent weakness of iOS itself but rather one the victims could have possibly prevented. The perpetrators gained access by hacking the victims' email (via phishing pages) in order to determine the users AppleID credentials (this gives access

to the iTunes store as well as to the users iCloud). With this information, the hackers could then remotely lock the iPhone view the 'Find my Device' feature that is enabled through their iCloud account. This highlights that mobile devices do have vulnerabilities to attacks of various flavors and vigilance against these should be maintained. It should also be noted, certainly with respect to conventional operating systems (for example Windows) that patch maintenance (always having the latest patch/version of the OS) is often the best defense against Malware. For example, the destructive Code Red virus was largely able to propagate and cause damage largely due to lax patch management. The fix to prevent infection was available; a vast number of customers simply didn't bother to apply it in a timely fashion.

There are several types of security to consider if one were to roll out the technology in a school (enterprise) environment. These points would generally hold for any type of mobile device in an enterprise:

- **Device control -** Methods that prevent unauthorized use of the device.
- **Encryption and data protection -** Protecting data even if the device is lost or stolen.
- **Network security -** Encryption of data in transmission.
- **App security -** Enabling the apps to run securely without compromising platform integrity.
- **Internet services -** Apple's network based infrastructure for messaging, syncing and backup.

The first line of defense is a good passcode to prevent unauthorized access. As with most authentication systems, iOS allows the application of passcode policies/restrictions that can be put in place. Configuration profiles can be produced that contain device security policies, restrictions, VPN configuration, Wi-Fi settings, etc. These configuration profiles enable the iOS device to work with the existing IT infrastructure and can be configured remotely using mobile device management (MDM) solutions, thus enabling policy distribution/updates to be carried out without any action by the user.

iOS contains a great deal of technology to encrypt the contents of the iOS device. Hardware based encryption is used using 256-bit AES to protects all data on the device. Encryption is always enabled and cannot be disabled. Further protection is available to email messages and attachments stored on the device. This will use the user's unique passcode to generate a strong encryption key. Even if the device is compromised the data will be encrypted. Remote wipe and local wipe options are also available with iOS devices. Remote wipe can wipe all data from a device if it is lost or stolen. iOS also supports the "Find My iPhone" feature where the location of a device can be tracked if this was enabled.

When it comes to Apps, the OS has several features to ensure application security. There is runtime protection, which means that apps are sandboxed in such a way that their access to data from other apps is restricted. Code generation is also not allowed. Additional security can be found in the fact that all iOS apps must be signed. Apple issues a certificate for each app and runtime checks are made to ensure that an app that is being used has not become 'untrusted' in the meantime (so apps that are dangerous can be flagged as such).

Applications developed can take advantage of the built-in hardware encryption available to protect data. Developers must add entitlements to employ many features such as iCloud or background processing. Apps can't grant themselves access to data that they were not deployed with. Additionally apps must ask for permission to use features such as GPS location, user contacts information, camera or the photo library.

iOS also supports virtual private networks (VPNs), SSL/TLS security and WPA/WPA2 Wi-Fi authentication/security. With regards to Internet Security, there are several services available out of the box on Apple devices such as iMessage, FaceTime, iCloud, iCloud Backup, iCloud Keychain (for user profile information, passwords, etc.) and Siri. These employ secure handling of data when at risk of being sent over a network. The iOS technical deployment document (for iOS 7.1) goes into more detail on these features.

Customisability

Deploying a number of iOS devices can be done through various techniques that aid with account setup, institutional policies, application distribution and the application of device restorations. Users can do most of the configuration work themselves using Setup Assistant which is a built in iOS feature. After iOS devices are configured and enrolled in MDM, they can then be wirelessly managed by the IT staff directly.

Configuration can be carried out via devices connected by USB, using a mobile device management (MDM) solution or via distribution of configuration profiles via email or a web page. It can include devices security policies/restrictions, VPN configuration, email/calendar accounts, Wi-Fi settings and authentication credentials. The individual iPad's can be customized to the users content also. Whilst still adhering to any restrictions applied to the iPad via configuration the user will have great flexibility in the options they can select to personalize the iPad and 'make it their own'.

Speed and Hardware Range

At the time of writing, the iPad is currently in its 5th generation (the iPad-Air). Much has changed and been improved since the initial incarnation. The iPad was initially criticized due to its lack of microphone and camera to enable creativity and the ability for the student to develop their own content. With the more recent versions of the iPad, these features are now present.

The physical iPad itself lends itself quite well in the mobile eLearning domain. The height/width of iPad is similar to that of a children's book. The wide viewing angle enables different people to view content simultaneously (thus lending itself well to collaborative activities). The display has the ability to switch between a portrait and landscape mode. The combination of its size, small weight, lack of attachments and connectivity (both Wi-Fi and 3G) makes it a very portable device easy for children to hold.

Software

The variety of educational apps available for the iPad is quite large. The biggest problem may be narrowing them down to the most relevant choices required for the educational program intended. Apple makes apps available through it's iTunes App store. This is generally accessed through iTunes on a user's PC/Mac where the app is purchased, downloaded and then synced onto their device (iPad, iPhone, etc.). For a set of iPads rolled out in an educational institution, it is possible to rollout apps en-mass to the devices used. Apple also offers a volume-purchasing plan where apps can be purchased at a discount when several are being purchased. One of the drawbacks with educational apps in the iTunes store is that they can tend to run on the expensive side when the intent is to roll them out to a substantial number of devices.

Apple also has one unique distinction compared to other tablets in this area. That is access to the iTunes University content. Many colleges/schools/Universities throughout the world have uploaded high quality educational content to the iTunes University that are available for anyone to download. One simply installs the "iTunes U" app on their iPad and, with their apple ID, signs into the iTunes store. From there one can look at the iTunes catalogue/library of educational content available and download what they choose. This can include video/audio/PDF/text content. The level of material offered is very broad (from junior school all the way to advanced university level topics).

Ease of Development

Most tablet devices have a wide variety of apps available for them. Picking the correct apps to use in the class (or outside the class) is, however, another problem entirely as this can involve a substantial amount of "trial and error" as well as research into what seems the most relevant and applicable to the content being taught. It may be an option to have an individual assigned for selecting apps at an organizational level that will fit in with the educational content plan. Having the apps fit into the pedagogical model being employed in the classroom is another consideration that must be made.

Developing your own apps is always an option and with iOS this is a possibility. Most apps today tend to launch first on iOS. Ironically, this has little to do with the

hardware or operating system being remarkably better but more to do with the fact it tends to be less problematic.

If you are developing against iOS for the iPad you have, realistically, 2 or 3 models of iPad you may be targeting to roll it out on. With Android development it gets much more complicated very quickly. There are many different tablets that could potentially be supported and many variants of Android being used. Trying to develop an app to work on a wide variety of tablets can be challenging and time consuming (not to mention expensive). The advantage to developing with the iOS platform is that you tend to know exactly the hardware configuration you are targeting. In an isolated environment, such as an educational system/school board, this may be less of an issue as, presumably, the roll out of a tablet device will be fairly homogeneous in nature and this may be less of an issue in practice. Developing against a Windows device will have the same challenges as for the Android devices.

iOS apps are developed in Objective-C which is a proprietary programming language developed by Apple. You will also need access to a Apple Mac Computer of some sort (to use Xcode) and the developer will have to subscribe to the Apple Developer program (around $100) in order to create apps. Android devices can be programmed using Java (a much more widely available skill-set) but their development tools are not as sophisticated as Apple's.

Within a deployment of iPads in an educational environment you can also roll out your own apps too; they do not have to be in the App store to be utilized.

Robustness

iPads were not designed to be particularly robust. Whilst they can survive a drop and some rough treatment the best solution for this issue is to supply each iPad with a protective case (to protect from drops and physical damage) in addition to a screen cover (which will help to protect the device from scratches and generally increase it's life).

Connectivity

iOS devices have built in support for many protocols and network infrastructures. This includes the support for the following (for iOS 7):

1. Popular third-party systems like Microsoft Exchange 6.

2. Integration with standards-based mail, directory, calendar, and other systems. This includes IMAP, LDAP directory serves, CalDAV calendaring, CardDAV contacts.

3. Wi-Fi connectivity and protocols for data transmission and encryption.

4. Virtual Private Networks (VPNs). This in includes "per-app" VPN.

5. Single Sign On (SSO) support.

6. Digital certificates to authenticate both users and secure communications.

Microsoft Exchange connectivity is gained via Microsoft Exchange ActiveSync (EAS). This enables push mail, calendar, contacts, notes and tasks. iOS supports the Auto-discover service in Microsoft Exchange 2007/2010.

Several different protocols and standards are supported with iOS. This includes IMAP, SMTP, LDAPv3 corporate directories, CalDAV server synchronization (wirelessly create/accept calendar invitations, receive calendar updates, syncing of tasks with Reminders app).

iPad devices can connect to Wi-Fi or 3G (3G is available in the higher end models). 3G costs could be quite prohibitive so Wi-Fi would be the most cost effective connectivity conduit to employ. These include support for 802.11k and 802.11r. Wireless network security using WPA2 128-bit AES encryption is supported. 802.1X is supported and iOS can be integrated into a broad range of RADIUS authentication environments (including EAP-TLS, EAP-TTLS, EAP-FAST, PEAPv0, PEAPv1, and LEAP). Secure access to the school network can be achieved with iOS using established VPN protocols. Native support includes Cisco IPSec, L2TP over IPSec, and PPTP. Various third party apps also exist that can support a VPN (such as OpenVPN). Support for SSL VPN is also available. iOS supports industry -standard technologies such as IPv6, proxy servers and split-tunneling. A variety of authentication methods are available including password, two-factor token and digital certificates. Additionally in iOS individual apps can be configured to use a VPN connection independent from other apps on the device.

Devices can be remotely wiped if required. Microsoft Exchange provides features to enable this. Wiping removes all the data and configuration information from the device, the devices is securely erased and restored to its original settings. Wiping also removes the encryption key to the data (256 bit AES encryption) thus rendering all of the data unrecoverable.

Windows Platform

Microsoft Windows 8 is the most powerful operating system available for tablets today (Hardy, 2013).

In 2014, the total number of Windows tablets shipped during the first quarter was 3.4 million which was only 5.8% of total number of tablets shipped (57.6 million) during that quarter and it was third most popular OS after Android (37.9 million) and iOS (16.4 million) while during the fourth quarter of 2014 the total number of Windows tablets shipped was 5.4 million which was 7% of total number of tablets shipped (77.2 million) during that quarter with Android 66% (50.9 million) and iOS 27% (20.8 million) (King, 2015).

Windows XP Tablet PC Edition was released in November, 2002 and in August 2005 a newer version Windows XP Tablet PC Edition 2005 was released. On October 6, 2012 first Windows 8 devices were released in two different editions Windows 8 for tablets running on x86 processors and Windows RT for tablets running on 32-bit ARM processors. The recent version of Windows 8 is Windows 8.1, which was released on October 17, 2013. On January 21, 2015 Microsoft announced Windows 10 the next version of Window, which is expected to be in April 2015 and would integrate its OS for Windows phones and windows tablets and would support all devices of screen size 8 inch or less supporting greater integration through its Universal support model.

The Platform

As suggested at the Windows Store, a windows tablet provides you a tiled structure where each tile belongs to an icon for a separate app in your tablet. It permits you to have as many tiles (icons) as possible in your start screen. It has three different sizes of tiles to facilitate categorizing different applications based on their usage frequency or based on their importance or based on how much details you would like to see about the app at the Start screen of your tablet.

Microsoft claims that "*every single Windows app and game is tested and certified by Microsoft*". It also claims that it facilitates full feature trial for each paid app and game available at the Windows Store. To run on a Windows tablet, all apps require a digital signature signed by Microsoft thus making Windows tablets more secure.

Windows OS well integrates with the Windows ecosystem. A developer can use Visual Studio and/or Silverlight (codes in C#.NET and VB.NET) for developing apps for Windows tablets. User can have an option to choose auto update for installed apps. Windows OS provides developers options to either ask for all permissions from app users at the time of installation or at runtime. Windows OS has native support for the MS-Office suite.

Security

To authenticate apps, a Windows device uses OAuth and OpenID internet authentication protocols which facilitates single-sign-on to authenticate multiple Apps. Further, Windows OS has a mechanism called AppContainer which ensures each application runs in its isolated location with its defined capability (resources/ access to the device core functions) and should not affect any other application. It also implements UEFI and secure boot to ensure malware should not be introduced during the boot process and trusted boot to prevent malware from modifying operating system components and drivers during the boot process. Other security attacks such as jailbreaking, DroidDreams, Update Attacks, Malvertising are more specific to other mobile OSes. In fact, Microsoft claims that Windows OS contains less malware than iOS and Android. Further, it supports hardware-based authentication through the Trusted Platform Module. Other security features Windows 8.1 supports include Device Encryption, Binary extension scanning, Family Safety, Multi-factor authentication for BYOD (bring your own device), Picture password, Remote business data removal, Trusted Boot or Secure Boot (protection against low-level exploits and rootkits and bootloaders), Early Launch Anti-Malware (ELAM), Windows Defender (defense against malware and spyware) and Windows SmartScreen (protect against web and social engineering threats and malicious downloads).

Hardware Range

Popular Windows tablets are
Microsoft: Surface RT, Surface Pro 3.
Acer: Aspire Switch 10, Iconia Tab 8 W/ W4.
HP: Stream 7"/ 8", Pavilion x2.
ASUS: T100, Transformer Book T90 Chi/ T300 Chi.
Asus: VivoTab Note 8.
Toshiba: Encore Mini 7", Satellite Radius P55W-B5224/ WT310/ Click 2 Pro.
Lenovo: Yoga Tablet 2/ 3 Pro, ThinkPad Yoga 14/ Helix, IdeaPad Miix 10.
Panasonic: Toughpad FZ-G1.
Dell: Venue 11 Pro, Latitude 10, XPS 18.
Other: Sony Tap 20, Nokia Lumia 2520, Samsung Ativ Q, Linx 8.

Connectivity

For Wi-Fi-connections a Windows tablet uses Extensible Authentication Protocol (EAP) - Transport Layer Security (TLS) and EAP-Tunnelled Transport Layer Security (TTLS) wireless, certificate-based authentication. It also supports IKEv2, IPsec, and SSL for a secure VPN connection (Microsoft, 2014e).

It not only automatically connects to the wireless networks you already connected earlier (which is also available with iOS or Android) but also, (depending on settings you selected) connects to other new networks automatically providing acceptance of terms and conditions and also filling additional information. Even you can seamlessly

share your password protected Wi-Fi network with your trusted contacts but without actually sharing your passwords. Further, it supports mobile broadband tethering facilitating you to use your tablet as a wireless hotspot to seamlessly share your 3G/4G network with your trusted contacts. It also initiates automated VPN connection with the organization's (as defined in Workplace) VPN network wherever available.
It also support setting up a 'HomeGroup' to connect other devices to communicate and share data.

Internet Explorer 11

Internet Explorer 11 is the default browser for the Windows tablet, which is a more secure version than previous Internet Explorer versions.

Mobile Workplace

The most important and interesting feature of the Windows 8.1 for our project is built-in mobile device management (MDM) support through Microsoft Intune, which provides better control on the use of the tablets by the students. It not only facilitates Assigned Access but also facilitates remotely controlling users' / students' Windows devices, collecting data (including personal information), modifying or deleting contents or changing settings even remotely resetting tablet/OS, changing or disabling app features, remotely disabling apps (including built-in apps) and remotely preventing from installing particular new apps (through Windows store app whitelists and blacklists). It also facilitates preventing user from removing Workspace account. It also facilitates creating a Workspace hub to keep all work related data in one place (similar to share access cloud). Windows 8.1 also provides remote assistance, remote lock, remote ring and remote hardware or software reset, remote passcode reset, remote wipe (removing all data personal and business) and remote business data removal (remote device retirement or partial wipe). Such features are not well supported by other mobile OSs. Microsoft Enterprise Mobility Suite (EMS) facilitates cloud based secure management of not only Windows tablets and other windows devices but also facilitates management of iOS and Android based devices. However, it better integrates with Windows tablets and other Windows devices due to obvious reasons.

Cortana

Cortana is an intelligent personal assistant, which is similar to Siri in iOS or Google Now in Android. It integrates very well with Bing for web search. It uses machine learning to learn about the user and customize its answers/settings. Cortana does not support an always-listening mode but it well supports geo-fencing and many reminders, which are not yet available with Siri or Google now. Other features supported include quite-hours, appointments scheduling, alarm setting, weather information, news, notebook, directions, reading messages, other voice based commands and operations. It also provides an option to give written commands instead of voice and has a Narrator to read text aloud which is especially helpful for

visually impaired and also for children who are developing reading proficiency. It is only available for tablets having the preview edition of Window 10.

Action Center

The action center is considered feature rich and more customizable than its iOS or Android counterparts. It also facilitates setting quick actions (setting templates), which one can turn on and off quickly.

Conclusion

This document went through the different features of the various OSs. In synthesis, Android offers an incredible choice of hardware from different manufacturers. It is aimed at maximum configurability and top systems run fast and smooth. Since Google is behind the Android OS, it offers seamless integration with its applications such as Gmail, Google Maps and Hangouts. Apart from these, the Play store offers an incredible selection of apps. However, you're likely to have more problems getting high-quality apps for different Android tablets. The same tablet can also be shared amongst different people because the OS supports multiple logins.

The strength of the iOS lies in the clean and intuitive interface. It also boasts a wide selection of Apps as can be seen from the diagram below. The app store is well curated and monitored, offers a deep selection and includes every popular app you can think of. However you are locked-in with regards to the hardware and development tools. This is not necessary a negative thing because it can offer a lot of stability which comes at the price of sacrificing some configurability.

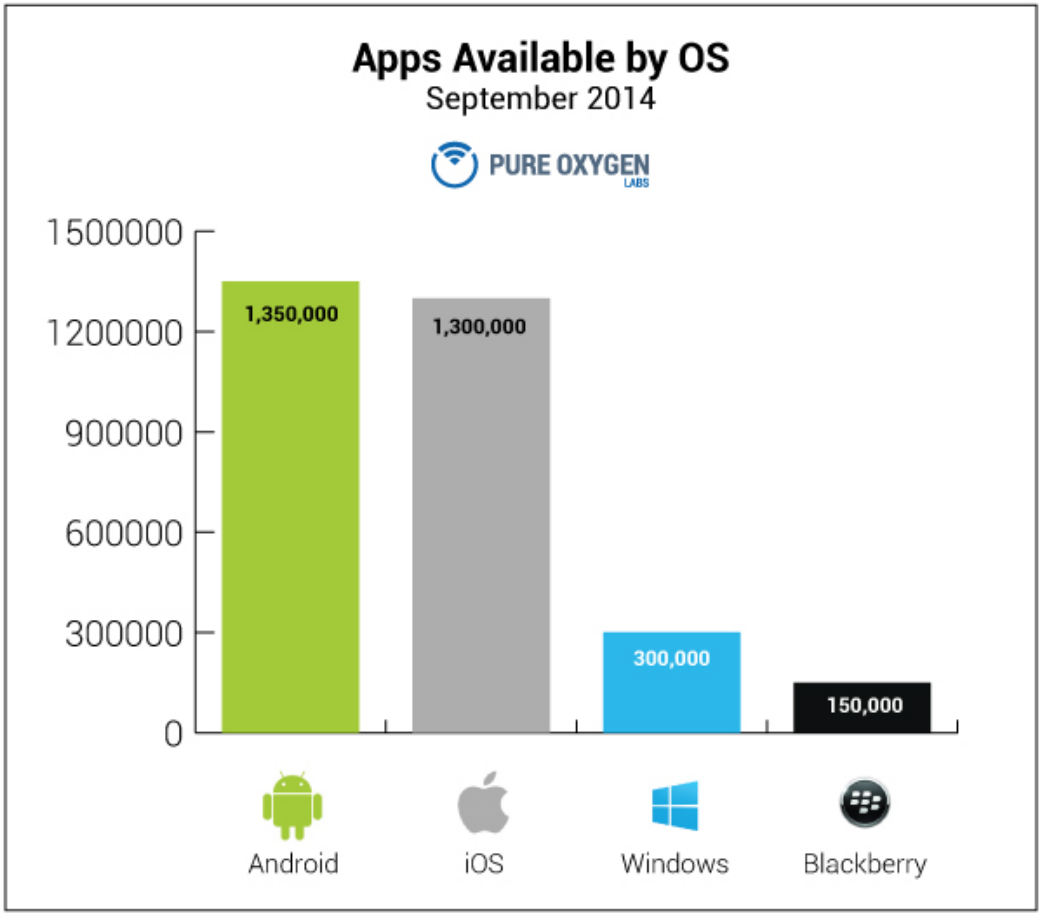
Windows on the other hand offers a traditional computing experience with full support for Windows software (Including Microsoft Office). Also, connectivity options and hardware add-ons for Windows models are typically more plentiful than with other tablet types. The amount of apps on the app store is much limited than other platforms and this is one of the reasons why it is less popular. Notwithstanding this, the tablet can also run all of the standard Windows-compatible programs.

Another element to take into consideration is the screen size. These tablets all come in small and large-screen iterations starting from gigantic smart phones, which would fit in a pocket up to the larger models. Screen resolution is particularly important too, especially for eBook reading and Web surfing. Right now, the sharpest display available is the 2,560 by 1,600 pixels on the Amazon Fire HDX 8.9", the Asus Transformer Pad TF701, the Samsung Galaxy Tab S 10.5 and the iPad Air 2 and the iPad mini 3 with their 2,048-by-1,536-pixel Retina displays. The tablet's weight is also a big advantage when compared to other mobile devices such as laptops. However, they're still substantially heavier than a smartphone. In fact, you cannot hold one in your hand for more than half an hour without getting tired.

Cloud storage is an option for many tablets and it is becoming even more important, but when it comes to on-board storage, more is always better. When combining all those apps with multimedia content such as music, video or photos, they tend to use a lot of space. Storage normally tops the 128GB flash-based memory for the high-end models but most of the tablets either come in 16, 32, or 64GB varieties. Many non-Apple tablets have micro SD memory card slots that let you expand storage.

Finally, we have to keep in mind that when a new technology is brought into the classroom, there will always be technical challenges to be aware of and prepare for

in advance. Almost all of the literature examined mentions this and it should be considered as a real concern if we want this project to be a real success.



Source: Number of apps available for different mobile OS platforms (Klais, 2014)

Sources

- Government of Alberta, “iPads : What are we learning ?” Government of Alberta, Tech. Rep., 2011.

- S. Henderson and J. Yeow, “iPad in Education: A Case Study of iPad Adoption and Use in a Primary School,” in 45th Hawaii International Conference on System Sciences. Ieee, Jan. 2012, pp. 78–87. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6148617
- R. Chargel, “Tablets Are Back : Light and Fun,” TechKnowLogica, p. 2000, 2000.

- L. Barack, “Is the iPad Fit for School?” School Library Journal, no. May, 2010.

- (2014, February) Major apple security flaw: Patch issued, users open to mitm attacks. [Online]. Available: http://www.zdnet.com/ major-apple-security-flaw-patch-issued-users-open-to-mitm-attacks-7000026624/

- C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 4th ed. Prentice Hall, 2007.

- J. Andress, The Basics of Information Security, R. Rogers, Ed. Syngress, 2011.

- (2014, June). [Online]. Available: http://www.ibtimes.co.uk/ russian-hackers-behind-oleg-pliss-iphone-ransom-scam-australia-arrested-1452186

- M. Erbschloe, Trojans, Worms, and Spyware. Elsevier, 2005.

- P. Gupta, “10 Tips For Smart iPad Security in Schools,” 2014. [Online]. Available: http://www.teachthought.com/technology/ 10-critical-tips-secure-ipads-education/

- (2014, September). [Online]. Available: http://en.wikipedia.org/wiki/IPad

- C. C. Chou, L. Block, and R. Jesness, “A Case Study of Mobile Learning Pilot Project in K-12 Schools,” Journal of Educational Technology Development and Ex- change, vol. 5, no. 2, pp. 11–26, 2012.

- (2013, August). [Online]. Available: http://mashable.com/2013/08/16/ ios-android-development/

- Apple, iOS Deployment Technical Reference, Apple, May 2014.

- iOS Education Deployment Overview, Apple, 2014.

- Gartner (March 3, 2014) Gartner Says Worldwide Tablet Sales Grew 68 Percent in 2013, With Android Capturing 62 Percent of the Market, Egham, UK. Available online at http://www.gartner.com/newsroom/id/2674215 (Accessed on November 15th, 2014)

- Hugo Gascón, Daniel Arp (n.d.) Smartphone Security, Computer and Network Security, Computer Security Group, GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN. Available http://user.informatik.uni-goettingen.de/~hgascon/docs/Smartphone_Security_2013.pdf (Accessed on November 16th, 2014)

- David Gewirtz (July 24, 2014a) Six Clicks: Six ways Windows Phone is better than iPhone, Tapping M2M: The Internet of Things, ZDNet, CBS Interactive. Available online at http://www.zdnet.com/six-clicks-six- ways-windows-phone-is-better-than-iphone_p4-7000031939/#photo (Accessed on November 16th, 2014)

- David Gewirtz (August 18, 2014b) Windows Phone: The final review, Mobility, ZDNet, CBS Interactive. Available online at http://www.zdnet.com/windows-phone-the-final-review-7000032692/ (Accessed on November 16th, 2014)

- IDC (2014) Smartphone OS Market Share, Q2 2014, International Data Corporation (IDC), Available online at http://www.idc.com/prodserv/smartphone-os-market-share.jsp (Accessed on November 15th, 2014)

- ITU (20 June 2014) World Telecommunication/ICT Indicators database 2014 (18th Edition) June 2014 Edition. International Telecommunication Union, Geneva, Switzerland.

- Peter King (January 30 2015) Global Tablet OS Market Share: Q4 2014, Strategy Analytics. Available online at https://www.strategyanalytics.com/default.aspx?mod=reportabstractviewer&a0=10546 (Accessed on March 9th, 2015)

- Adrian Kingsley-Hughes (July 14, 2014) Why Windows Phone is barely making a dent in the market, Mobility, ZDNet, CBS Interactive. Available online at http://www.zdnet.com/why-windows-phone-is-barely- making-a-dent-in-the-market-7000031543/ (Accessed on November 16th, 2014)

- JM Kizza (2013) Mobile systems and their intractable social, ethical and security issues, Ethical and Social Issues in the Information Age, Springer London. 281-297. DOI 10.1007/978-1-4471-4990-3_14

- Brian Klais (September 25th, 2014) Research: How Many Apps Are in Each App Store?, Pure Oxygen Lab, Available online at

http://pureoxygenlabs.com/how-many-apps-in-each-app-store/ (Accessed on November 14th, 2014).

- Ed Hardy (June 26, 2013) How to Choose the Right Tablet Operating System, TabletPC ReviewTM, TechTarget. Available online at http://www.tabletpcreview.com/howto/how-to-choose-the-right-tablet-operating-system/ (Accessed on March 16th, 2015)

- Paul Krill (April 2, 2014) One Windows, all devices: The new Microsoft app strategy unveiled, InfoWorld. Available online at http://www.infoworld.com/article/2610769/microsoft-net/one-windows--all-devices--the- new-microsoft-app-strategy-unveiled.html (Accessed on November 15th, 2014)

- Microsoft (2014) Windows Phone Apps+Games Store, Available online at http://www.windowsphone.com/en-us/store/overview (Accessed on November 16th, 2014)

- Microsoft (2014a) Use Wi-Fi Sense to get connected, Windows Phone 8. Available online at http://www.windowsphone.com/en-us/how-to/wp8/connectivity/use-wi-fi-sense-to-get-connected (Accessed on November 16th, 2014)

- Microsoft (2014b) Notifications and quick actions, Windows Phone 8. Available online at http://www.windowsphone.com/en-us/how-to/wp8/settings-and-personalization/notifications-and-quick- actions (Accessed on November 16th, 2014)

- Microsoft (2014c) What is a workplace account? , Windows Phone 8. Available online at http://www.windowsphone.com/en-us/how-to/wp8/accounts-and-billing/what-is-a-workplace-account (Accessed on November 16th, 2014)

- Microsoft (2014d) Use Narrator on my phone, Windows Phone 8. Available online at http://www.windowsphone.com/en-us/how-to/wp8/settings-and-personalization/use-narrator-on-my- phone (Accessed on November 16th, 2014)

- Microsoft (April 2014e) Windows Phone 8.1 security overview. Available http://www.microsoft.com/en- us/download/details.aspx?id=42509 (Accessed on November 16th, 2014)

- Microsoft (2015) Compare Windows 8.1 Editions, Windows 8.1 Enterprise, Windows. Available online at https://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/windows-8-1/compare/default.aspx (Accessed on March 16th, 2015)

- Matthew Miller (September 24, 2014) Android and Windows Phone have unique capabilities, but the Apple iPhone 6 Plus is still best, Mobility, ZDNet, CBS Interactive. Available online at http://www.zdnet.com/why-windows-phone-is-barely-making-a-dent-in-the-market-7000031543/ (Accessed on November 16th, 2014)

- Brad Molen (April 14, 2014) Windows Phone 8.1 review: Microsoft's mobile OS finally feels whole. engadget, Available online at http://www.engadget.com/2014/04/14/windows-phone-8-1/ (Accessed on November 16th, 2014)

- Terry Myerson (September 30, 2014) Announcing Windows 10, Blogging Windows, Windows, Microsoft. Available online at http://blogs.windows.com/bloggingwindows/2014/09/30/announcing-windows-10/ (Accessed on November 16th, 2014)

- Larry Seltzer (October 28, 2014) Mobile app permissions: Who does it right?, Security, ZDNet, CBS Interactive. Available online at http://www.zdnet.com/why-windows-phone-is-barely-making-a-dent-in-the-market-7000031543/ (Accessed on November 16th, 2014)

- Simon Thomas (August 21, 2014) Windows Phone 8.1 vs Android KitKat, InfoWorld. 3G.co.uk, Available online at http://www.3g.co.uk/PR/August2014/windows-phone-8-1-vs-android-kitkat.html (Accessed on November 15th, 2014)

- Wikipedia (12 November 2014) Windows Phone. Available http://en.wikipedia.org/wiki/Windows_Phone (Accessed on November 16th, 2014)