Mobile Devices in the Enterprise: CTO Roundtable Overview

An overview of the key points discussed in the ACM Roundtable on Mobile Devices in the Enterprise.

Mache Creeger

The CTO Roundtable on Mobile Devices in the Enterprise focuses on the implications of the widespread use of mobile devices, such as smartphones, in the enterprise computing environment. These new personal devices have presented great challenges and opportunities for the protection of valuable information assets and creation of business value. What follows are the key points from that broader conversation. For a more in-depth understanding of what was covered in the roundtable, please read the full panel discussion.

Historically, when people considered enterprise-oriented mobile phones there was only one real choice: the BlackBerry from RIM (Research in Motion; <http://www.rim.com/>). Complaints about RIM focused on its being a full end-to-end enterprise solution. While this architecture made RIM easy to deploy and manage, critics felt it enforced a closed architecture with few external APIs, making it hard to customize for business needs and difficult and/or expensive to maintain as a fully integrated, mission-critical platform.

Today's choices are broader and along with the BlackBerry include Apple's iOS (<http://www.apple.com/ios/>) and Google's Android (<http://www.android.com/>). How Microsoft's Windows Phone (<http://www.microsoft.com/windowsphone/en-us/default.aspx>) product will fare is still an open question. While RIM's historic approach of taking care of everything has been frustrating for some, the alternative of providing functions taken for granted under RIM can also be quite challenging.

The mobile-device market is very fragmented with a lot of dumb phones, a lot of smartphones, and carriers that may may not provide data services. There are at least 18 platforms and/or operating systems available. Change in the mobile market is moving much faster than one typically sees in IT—think every 18 months you have a new Windows release. In planning to develop new application software it is important to continually ask what the market will look like in 6 to 12 months.

Don't assume a Microsoft Windows-like winner anytime soon in the mobile marketplace. If you think the world is all about iPhone and Android, just blink and it will be something else. The relatively large number of vendors offering products in the mobile space is not expected to consolidate. Your industry and application set will determine the most popular smartphone platforms for you. As the mobile-device market evolves, existing players will swap market share with each other, with perhaps one or two additions and/or dropouts. This condition will remain unless or until somebody produces a new game-changing killer device.

Because of the high rate of fragmentation and change, IT organizations wanting to gain mobile application development expertise should not try to develop it in-house. It's too hard and the chances of making rookie mistakes are too high. It is better to hire or outsource the expertise and get it right the first time.

CHOOSING THE RIGHT SMARTPHONES TO SUPPORT

The adoption of smartphones in many areas of the world is growing very fast. How a company invests to develop mobile applications is heavily dependent on the geographical areas it wishes to service. This makes the selection of smartphone platforms especially difficult. You should start by defining the key issues (e.g., functionality, security, and ubiquity) and then make every effort to define the minimum functionality that an application set must support.

To make a list of supported platforms in order of priority you must perform basic research on your user base: poll users, look at market trends, and make best efforts to forecast what phones will be popular in your business area. Don't just look at Web stats and don't just say all. You should ask:

- How quickly does a solution need to be in place?
- How many platforms must be supported?
- In what geographical areas will the mobile services be used?
- Are employees purchasing their own smartphones, or is the company supplying them? Mandated and/or company-supplied smartphones allow for better control.

If the correct choices are made, mobile devices offer the opportunity to provide information services at a huge scale. Mistakes mean fragmentation and will result in getting bogged down.

A tiered approach is recommended, with each tier representing increasing levels of device support (such as good, better, best) and/or different types of available functionality. You need to define the right functionality for each platform and the minimum functionality required for any device. Additionally, you must decide how many tiers of service will be supported and define what is in each tier. Inherently this entails compromise, and it will be impossible to make everyone happy.

For increasing levels of device support, you must be prepared to do reference ports and individual device certification by placing those devices on specific networks, doing physical testing, and then constantly reevaluating. This typically results in a three-level hierarchy of supported mobile devices:

- I know it works because I've certified it.
- I think it works because the device manufacturer that just released the device said it's totally compatible with my earlier devices.
- I have no idea if it works because there have been multiple changes.

Alternatively, or additionally, you could link business roles with specific devices. This could mean adopting a policy that lets employees use their iPhones on the internal network unless they want to use the corporate CRM application, in which case they would have to use an Android or BlackBerry. Another approach would require services that are high on the security stack to use a BlackBerry, while services further down the list would allow iPhone synchronization. For each tier, define the level of IT resource devoted to the support of each issue and the supported devices at that level. Recognize that trying to make every tier support every device at maximum level is a recipe for failure.

APPLICATION ARCHITECTURES

When designing multiplatform software, consider the following:

- Use the smallest number of APIs that you possibly can—this limits the complexity of porting the software to new devices.

- Use the oldest APIs—they have been around long enough to be supported by many different device variants.
- Use the best-tested APIs—they will be the most reliable.

In order of preference, the three implementation choices for multiplatform smartphone applications are: a browser-based, thin-client application; a hybrid approach that has a portable application operating on a standardized execution platform such as PhoneGap (<http://www.phonegap.com/>); or a natively coded application. Because of the high fragmentation of smartphone architectures, once a minimum functionality set has been defined, the goal is to pick the technology solution that allows the program design to get as close as possible to a single application. First, work to see if the application can function in a Web browser (including HTML5; <http://dev.w3.org/html5/spec/Overview.html>) on the supported devices. Since things are happening very fast in the mobile browser landscape, if not today, can the application be supported in the future? Check W3C (<http://www.w3.org/>) and other standards bodies. If the application is not browser friendly, research whether a standardized platform is feasible before you consider developing an entirely native application.

Many people choose the BlackBerry as the base platform in developing multiplatform mobile applications. Compared with other mobile devices, BlackBerry is a relatively minimal platform, and developers target at least operating system release 4.6 because of its continued use by enterprise customers. A typical development strategy would be to target what can be done using the browser and build up from there to the Android and iPhone. Starting on an iPhone or Android and going in the other direction to BlackBerry would be much more difficult.

To protect information assets that typically reside behind a firewall, mobile developers have three choices:

- Go to a thin client and protect information in much the same way people have done with thin desktops.
- Implement a BlackBerry-specific application taking advantage of RIM's proprietary enterprise features.
- Emulate what people have done with laptops and install endpoint security products to impose control directly on the device.

For testing, while a tool such as DeviceAnywhere (<http://www.deviceanywhere.com/>) is a good start, nothing can beat placing a device on its production network and doing actual physical testing. Plan to test the application(s) comprehensively on all the different supported devices running on all the different supported carriers. It is barely good enough to buy all the devices and have one individual do basic testing on every device. To achieve adequate testing coverage, you may need to hire a third-party testing service.

While Apple tries to make it easy to move things from the Mac desktop environment to iOS, it's not the same environment, and the resulting user experience is usually poor. It is generally felt that a similar issue will result from moving desktop/server Linux applications to Android.

WI-FI VS. CELLULAR NETWORK TRADEOFFS

Using a carrier network for data transmission can be very attractive as it typically provides an easily authenticated secure channel.

In the U.S., critics charge that the availability and performance of carrier data networks is steadily degrading, making smartphone data services less useful. If not remedied, this may very well cause

subscribers to abandon carrier data networks and move to public Wi-Fi access points for network access.

Many retail businesses in the U.S. provide free public Wi-Fi service, and urban areas typically provide good Wi-Fi coverage. Practically all mobile devices support Wi-Fi, and mobile application developers should take advantage of this alternative mode of network access.

Unless the data connection is encrypted (such as VPN), use of public Wi-Fi for smartphone data services exposes your data stream to all the users of that access point.

MANAGING MULTIPLE MISSIONS

Because smartphones are personal devices, they are commonly used in both professional and personal roles. To secure the information assets for one or more roles, a user must carry at least two phones, or a single phone must have a way to compartmentalize the data and applications for critical roles.

Because of the need to manage power and other limited resources, it does not seem likely that virtualization will be a viable solution to this problem. A more likely approach will be a Unix-like method of multiple users.

REGULATORY COMPLIANCE

Many industries have explicit rules and regulations regarding the disclosure of confidential data, and mobile application developers should seek legal guidance for industry-specific security compliance requirements. As a general rule, it is important to create a culture that views security not as the enemy but as a way to enable the delivery of business value and managed risk in a sustainable way.

In finance, security compliance has been along the lines of protecting against the disclosure of sensitive customer data. To avoid triggering a mandatory client notification, the focus has typically been on being able to guarantee to some level of technical certainty that the loss of a mobile device would not result in unauthorized information disclosure.

OUTLOOK FOR THE FUTURE

In the near term, application architectures in both consumer and enterprise roles are expected to trend toward thin clients because of the popularity of public and enterprise-based cloud services and the access control they provide for data. At some point thin clients will become unattractive and fat mobile clients more desirable because:

- Available carrier network availability and bandwidth degrades to the point of not being able to support thin-client connectivity requirements.
- Storing data in public clouds becomes unattractive as a result of increased data breaches through either security failures or poor data aggregation and collection policies by service providers. This is not expected to be an issue for enterprise users of private cloud services.

Tablets will become a huge part of the mobile market over the next two to three years in both the consumer and enterprise spaces, with applications moving from the phone to the tablet. It is expected that tablets will become the primary device for media and a major platform for consumer mobile computing.

As carrier network bandwidth, availability, and cost negatively impact more mobile users, more segmentation of the mobile network space should occur. Individual devices will be able to talk

locally over a personal area network and will be able to share a single-device gateway to gain network access through MiFi, a phone on the cellular network, Wi-Fi, or whatever.

By supporting always-available personal devices, mobile platforms will fundamentally change the types of services that can be delivered to end users, provide those services more efficiently, and significantly increase the number of people who can be engaged from every economic stratum. ◻

LOVE IT, HATE IT? LET US KNOW

feedback@queue.acm.org

© 2011 ACM 1542-7730/11/0700 \$10.00