



omobono

DIGITAL COMMUNICATION SERVICES

Mobile for B2B

Security Considerations

August 2011

Tom Millard & Rob Hurst

Intro

Mobile for B2B Series

This paper is one of a series we've written to help answer some of the questions we often hear from clients now that mobile content is firmly on the B2B marketing agenda.

Web apps or native apps? How to optimise content? What should an app look like? Why might I need an app and how can it benefit my marketing activities?

This series aims to give some useful context for anyone considering how to make the most of mobile as a marketing channel.

1. Native or Web?
2. Design considerations
3. Security considerations
4. Cross compiled apps

Introduction

Security is as big a consideration on mobile devices, as it is on any digital channel.

However, the convenience factor of a mobile app can lead people to treat it with complacency, putting less consideration on how secure the data stored or accessed via an app really is and users mostly have none of the obvious PC safeguards (firewalls, virus scanners etc.) in place.

Consequently, there's an argument that security is actually a more important consideration than on other channels. Here we highlight some of the security issues to be mindful of in two key areas – app delivery and data transfer.

For each organisation and for each app the security risks and considerations will be different – but all apps, as with any digital communication, are vulnerable to attack. Awareness of the main issues will mean you can evaluate the best approach for your needs and determine potential issues at an early stage.

Web or native?

Let's start by simply defining the two main categories of mobile apps from the point of view of some of the security considerations..

Web apps

A web app is any content developed for a mobile device but accessed directly through a browser. Consequently they are theoretically more vulnerable than native apps as they are open to the same security issues as a standard

website. It is therefore important to consider the same set of security issues as you would with any other web development project.

Native apps

Native apps, on the other hand, are downloaded from a secure location, such as the iTunes app store, and are then stored securely on your device. They can therefore often be used without a data connection and though they often connect to the web in order to access information, they do so by accessing the device's connection securely. One of the downsides of this third party delivery mechanism is that any future development that the app may require will be subject to delays during app-store approval processes, meaning that a discovered security flaw cannot be amended as quickly as with a web-based application.

Delivery mechanisms



Publishing an application through an app store can provide additional security over a web app. For example, Apple's app store requires that all applications be submitted for review, before they can be offered through the store. This means app store staff can review applications and confirm that developers are legitimately involved with a company.

It's not all plain sailing, however, as Google's Android Marketplace, which doesn't have the same rigorous approvals, has been criticised in the past for its potential security flaws, with instances cited of phishing scams being implemented in the form of fake-branded

mobile banking apps, getting users to input their personal details, which are then hijacked.

Additionally, publishing an app through a device-specific app store requires that the app be publicly visible in the store – where any user can potentially discover it. This means that any user can download the app, whether it is intended for them or not, and so security like password protection, use of a corporate login ID or account number might need to be put in place to secure any content that is not appropriate for public visibility.

Consequently native app stores do not offer a unified level of security, but can be more secure than web-based applications, hosted in the same way any website is.

Connectivity

In most cases, apps receive and transmit data to the outside world, for example accessing up to date information, search functionality or a form submission.

All out-going information, whether sent from a web-app or a device-based native app, needs to be secure, and the information that is being returned needs to be trusted. This security will scale depending on the nature of the information being sent.

So, what are the considerations you need to make?

No native app can be accessed externally unless it has been set up to do so, or given permission. Web apps, conversely are open to

attempted hacking - and this is the key difference between the two.

Native apps

Device and operating system manufacturers are aware of the potential security risks associated with apps connecting to the internet. Each manufacturer offers a stand-alone API (application programming interface) for their platform, which adds a desirable extra layer of security. Apple, for example, have a special inbuilt API which iOS developers can use to encrypt the information they are sending from the device – making it more secure.

Google's approach with Android is to run each app in something called a 'Silo' which prevents an app from accessing other areas of a device. Apps then need to be given the appropriate permission (by a pop-up warning on the device) to access anything else which it may need to use in order to function, such as GPS location data and so on. Each app is also distributed with a digital 'certificate' which contains all the details of the developer.

Other platforms have similar security measures. All of this means native apps relay information through secure connections and/or via encrypted means, keeping your customer and client data safe – a huge benefit for B2B organisations. The downside to this increased security is that each platform operates in a different way, potentially requiring separate and comprehensive development for each device.

Web apps

Speaking broadly, web apps are 'open' as they reside on the web, though of course security can be put in place.

As web apps are open, they are great to build, from a

development standpoint, but from a security point of view; they hold the same risks as any other website.

Risks could include a hacker attempting to intercept all the data passing through a network or to a particular device and analyse the contents, or trying to obtain access through the log in screen.

The danger here resides in the fact that an app is often built to replace or manage a specific function of a website, rather than recreate an entire website. Often this will be a function that involves sending or receiving private information to and from a device. As such, a hacker can attempt to hijack this individual function, rather than a website as a whole – a more targeted approach, potentially allowing for a higher success rate.

A web app can, however, be secured like any normal website using an SSL (security) certificate which is granted by a trusted provider and forces use of a secure HTTPS connection.

Conclusion

Both native and web apps have their positives, and negatives, when it comes to app security.

Native apps, whilst allowing better offline storage of information – keeping your customers details offline, are slower to develop, with a new application development needed for each platform. Web apps, on the other hand, can reside on any platform with one development – and any security concerns can be tackled much quicker, but they may lack some of the peace of mind gained with an app-store download.

It's worth noting that web apps, which have been growing in popularity against native apps

more recently, are gaining increasing numbers of advocates, especially with businesses handling potentially private data. Many businesses that handle financial transactions, banks such as HSBC and Lloyds TSB and online bookmakers such as Paddy Power and Ladbrokes are using web-apps, rather than native apps, to cater for their customers across devices.

Additionally, as mobile platform owners and manufacturers look to increase revenues from apps utilizing their platforms, this increase of web apps for transactional or paid functions is likely to continue. Apple has already announced a set of rules for 'subscription' apps that require they receive a 30% cut of the revenue.

This brings us to our final point, something which can help increase security around applications for a more targeted audience – a bespoke app store environment. Large corporations that produce multiple applications for their customers and work force are starting to make use of this approach. A notable example is the US army, whose applications are, understandably, something that the general public should not have access to. Whilst this approach is obviously very secure, it's likely to be beyond the requirement of most application developers.

Read the rest of the Mobile for B2B series.

[1. Native or Web?](#)

[2. Design considerations](#)

3. Security considerations

[4. Cross compiled apps](#)



omobono

DIGITAL COMMUNICATION SERVICES

Omobono is an award winning digital agency specialising in brand development and engagement for large corporates and government.

We believe no one has a better understanding of business audiences and how to reach them.

For more information, please contact Rob Hurst on rob@omobono.co.uk or +44 (0) 1223 307000.

© 2011 Omobono Ltd.

All ideas, concepts, brand-related names, strap lines, phrases, copy/text and creative concepts developed and contained within this document remain the intellectual property of Omobono Ltd until such time as they are procured by a third party.

Anyone viewing this document may not use, adapt or modify the contents without our prior consent.

Omobono Ltd, St Giles Hall, Pound Hill, Cambridge CB3 0AE, UK

T +44 (0)1223 307000 F +44 (0)1223 365167 E info@omobono.com W omobono.com