at&t | EMERGING DEVICES

12.2.2009

Wireless Network Development Considerations

Development Brief

Wireless Network Development Considerations

Development Brief

An Introduction to Wireless Network Development

A mobile device is not a desktop PC. Although this statement may seem obvious, application developers may try to treat them as essentially the same platforms, an approach which can cause serious problems. Many development tools make it possible to create an application for a desktop and port it to a mobile device, but the result is not likely to be a good wireless application unless care is taken to customize it to the target delivery environment.

This development brief describes the key differences between mobile devices and PCs, and between wireless networks and the wired Internet, as they relate to the development of mobile applications.

Service Considerations

Personalization. Personalization increases the value of content and services to users, which is important in the mobile environment because of the extra effort required to find relevant content and to interact with applications, and also because of the limited output capability of mobile devices. In the PC environment, users have a variety of input methods and controls, making it easier to input personalizing information and surf to the desired content. Also, they can more easily scan a large amount of content to find the parts that are relevant to them. Therefore, mobile application developers should set the goal of including automatic personalization and easy-to-use methods for input of personalizing information.

Privacy. Related to personalization is the need to protect the user's personally identifiable information from malicious attacks (eavesdropping or tampering) over the Internet. The efficiency of methods for personal information security in the mobile environment must be more carefully considered. To ensure privacy and information accuracy, developers should use only trusted information and protect any personally identifiable information, especially user identifiers or keys to user identity. Privacy considerations apply to PC-based applications as well; however, in the mobile case additional options, such as operator-certified user identity, are typically available for protecting access to trusted personal user information.

User awareness and control of automatic behavior. In the mobile environment, automatic application behaviors can present more substantial risks to security, privacy and service cost. Applications should ensure that the user is notified when a function will access sensitive information, and if possible give the user a means to control the function. Examples of such functions include those that use personal information stored on the device (such as a contact list) or obtained through the device (such as user location or photos/videos), and automatic network traffic.

Conservative use of network traffic. In mobile networks, the amount of network traffic that applications generate can have a significant impact on service cost, especially for applications that automatically interact with network-based services. These costs may be borne by the user and/or network service provider.

Users with usage-based service plans can find themselves responsible for huge charges. Network service providers can choose to bear these costs for users that subscribe to "bucket" or unlimited service plans, and as a result may only recommend or support efficient applications for use with such plans. In either case, mobile application developers need to consider the efficiency of content and automatic application behaviors.

Network Considerations

Network sharing. Wireless networks are shared by customers within a particular cell. This means that one customer's use of an application can impact other customers in the cell. Also, because of user mobility, the number of customers provided service by any given cell site at a particular time is dynamic; this is a fundamental difference with wired networks.

Network availability. Wireless connections are not always available to a user, and can be lost in the middle of transactions. Also, various network types may be supported in mobile devices, with varying support for services, so it is not always possible to rely upon any available network connection.

Roaming. Wireless network service costs can vary widely in roaming environments. Applications may need to be roaming-aware, and be able to suspend automatic operation when roaming to avoid unexpected data charges.

Throughput. Although today's 3G networks have broadband capability, the actual throughput a customer will obtain depends on several factors, including network loading and signal quality. In addition, 3G devices can use slower networks (such as 2.5G) when needed, so applications may need to be aware that the currently serving network may not support 3G speeds.

Security. Wireless networks handle security differently from wired networks. Securing wireless devices and applications involves user authentication and protection against eavesdropping, as well as protection against threats (such as viruses) and device loss. Mobile applications are more likely to require certification by a code signing authority to gain access to sensitive device functions (for example, network access, user data, and GPS). This certification helps ensure overall security, privacy, and reliability of network services for users. Restrictions on specific types of data traffic (such as direct peer-to-peer data exchange across the mobile network) may be necessary to ensure the stability and reliability of public mobile networks.

User Interface Considerations

Presentation. Due to their typically smaller screen size, mobile devices are significantly limited compared to the PC in terms of content presentation, especially in the following ways:

- Content context and overview are constrained
- Greater dependency on scrolling
- Higher screen usage for images and navigation links
- Overall lack of application/content cohesiveness due to fragmentation of display and application structure, resulting in more difficult site navigation

Interaction. The user input options of mobile devices are severely constrained, relative to the PC, by small or non-QWERTY keyboards. Furthermore, mobile users often interact with their devices using only one hand. As a result, the user's data input capability is limited, meaning that application flows and the presentation of data must be carefully designed for the particular devices on which the application will be used. Some examples of interaction limitations for mobile devices include:

- Limited keypad (for example,16-key), leading to difficulty in selecting characters and the need for application help in selecting the input character type
- Dynamic variations in key layout; for example, for devices with both a phone keypad and QWERTY keypad
- Physical difficulty in keying due to small key size
- No pointing device, or one that is more difficult to use
- Variations in pointing methods (for example, joystick, keys, and touch screens)
- Variations in softkeys for navigation and local application menus

Communication channels. Mobile devices provide several different types of communication channels, including voice capability, messaging, location-based

information, and video. The best mobile applications integrate these capabilities to optimize how users interact with data.

Platform and Device Considerations

Variety of platforms and devices. There is no dominant operating system or device in the wireless space, in contrast to the "Wintel" platform (Microsoft Windows OS and Intel chipsets) that has a greater than 80% share of the PC market. Several different mobile operating systems from several device manufacturers are in use, and none of these has greater than a 30% market share. As a result, developers must create for multiple operating systems to cover the broad range of devices available to customers. Furthermore, the capabilities of these devices vary widely. These factors imply the ability of an application to identify the model of device on which it will be run, and to have access to a device capability database that aids in content/service adaptation for the device.

Memory management. Although the amount of memory in mobile devices is increasing, it is still severely constrained compared to a personal computer. A mobile application will need to make extremely efficient use of available memory on the mobile device if it is to perform well.

CPU speeds. The slower processing speeds of mobile devices demand that developers create the most efficient applications possible.

Power management. Mobile devices have a limited battery life. Mobile applications must be able to accommodate a finite battery life as well as recover from a sudden loss of power.

Device lifecycle. Mobile devices have a relatively short lifetime. Developers must decide if their application will be designed to work on a device that may shortly be obsolete.