Mobile computing and social networks

Technology, Mobile Phone

Mobile Computing and Social Networks Sherri White Dr. Edwin Otto CIS 500 Information System Decision Making September 9, 2012 Assess the effectiveness and efficiency mobile-based applications provide to capture geolocation data and customer data, and quickly upload to a processing server without users having to use a desktop system. Geolocation integration can be accomplished at many different points in an application requests lifecycle. To realize the greatest value across the broadest Spectrum of use cases, gathering of geolocation data is most efficiently accomplished when a request is first made for a given resource. The Application Delivery Controller is typically deployed at a strategic point in the application and network architecture: at the perimeter of the network, acting as an intermediary between clients and resources. Given this strategic location, geolocation data should be incorporated into the existing context that is already associated with every request such as IP address, user-agent, and ability to accept specific types of content. Accurate geolocation data is generally provided by an external, third-party service like Quova. These services can be billed in a variety of ways, including by the number of queries and bandwidth transferred. To minimize the capital and operational costs associated with retrieving geolocation data while maintaining the ability to share that data with the broadest number of devices and applications, centralization of the retrieval process is necessary. Centralized control has the added benefit of decreasing an organizational risk by permitting or denying access at the perimeter of the network when location is part of the authorization process. By integrating geolocation services with a unified application delivery service, it is also possible to share the data retrieved from the third-party service with all functions deployed on the Unified Application and Data Delivery platform. A unified application delivery platform shares a core, underlying traffic management system that enables the sharing of request context, including location data cross all modules that are deployed on that platform. The sharing of contextual data enables web application security, access management, acceleration, and core load balancing services on the application delivery platform to take advantage of the geolocation. Evaluate benefits realized by consumers because of the ability to gain access to their own data via mobile applications. Just as accurate geolocation data has valuable benefits in terms of security and performance of web applications and resources; it also provides greater business value and insight through enhanced visibility. Business value and insight come from discerning the client's location and from additional data provided by geolocation. For example, geolocation can be used in defined areas, such as those established by Designated Market Areas (DMAs) and Metropolitan Statistical Areas (MSAs), to derive deep demographic data that becomes part of the application request context and can be subsequently incorporated into analytical evaluation of visitor and customer web application interaction. Understanding from where clients typically access your applications can influence the placement of future data centers and co-location of CDN components to improve application performance and distribution. Accurate geolocation data can assist in prioritization of requests by aligning application delivery policies with defined demographic-based business goals. Data such as the time zone associated with visitors, available from provider Quova's geolocation data, can further assist IT in gaining visibility into use patterns based on time. This visibility affords an opportunity to understand the potential impact of leveraging cloud computing and employing a “ follow the users" strategy for improving application performance, potentially eliminating the need to provision costly CDN services. Moving the content closer to the users is still a valid strategy, but knowing the application access point for the majority of customers makes it possible to move the entire application across cloud computing environments rather than add additional complexity with a CDN service. Business analysts understand the value derived from demographics, especially those based on location. But the demographics that are typically analyzed using business intelligence tools are only for customers with known locations. However, demographics provided a geolocation for visitors can be correlated with data on known locations to provide insight as to why those visitors have not become customers. This information is invaluable to business analysts when determining, for example, which products are not selling well in a particular location but may be of interest, or in understanding the impact of location on visitor interaction with web applications. Examine the challenges of developing applications that run on mobile devices because of the small screen size. Compactness can enable a device to be used just about anywhere, but it can also work against many aspects of usability. A small screen limits the information that can be legibly displayed. While designing, text and images can quickly consume the limited screen space, causing a trade-off between content and user interactions. Smartphones are small, and tablets are in the range of netbook to laptop size. Many vendors offer both types of devices in a variety of display sizes, as shown in Figure 1. Mobile web application designs must scale to handle the wide range of displays without appearing cramped at the low end or stretched at the high end. Many popular mobile devices use touch and gestural input. While touch input can be intuitive, it is relatively imprecise. Touch targets, such as buttons, must be fairly large and widely spaced in comparison with the mouse and pointer style input in conventional installed or web applications. On phones, constrained screen sizes, coupled with large interaction targets, result in fewer controls per panel. Fingers and hands also obscure much more of the screen on a UI than a mouse pointer icon. Because mobile web applications are inherently cross-platform, the input characteristics of different types of devices also must be considered. Some mobile devices have a physical keyboard, some have only a virtual keyboard, and others have both. Some Blackberry devices use a touchpad for pointing, selection, and dragging. Both Blackberry and Android devices have dedicated, but differently ordered, physical buttons for various navigation actions. Java Script performance is improving, mobile devices still performance-challenged. They use less powerful processors and must contend with lower network bandwidth compared to laptops and desktop systems. The primary design challenge for mobile web applications is how do you create positive user experiences for an application that appears on screens measuring from a few inches square up through tablets, laptops, and devices using large displays? The responsive web is the design philosophy and set of techniques that try to address this issue. The goal of response web design is to make each website or web application appear as if it were designed specifically for each device and browser on which it's displayed.

Perhaps the responsive web should be called the " more responsive web," because the web has always dealt with issues of displaying content in un-maximized browsers and on monitors of varying size and resolution. The smaller sizes and diversity of mobile devices has simply raised the ante. Responsive web implementation relies on the use of CSS, media queries, and JavaScript to adapt the presentation of content to devices. Media Queries, a sub-specification of CSS3, lets you associate a different style sheet with different media or display characteristics. For example, a style sheet can be selected based on the device's screen height, width, aspect ratio, and resolution. A detailed explanation of how to implement responsive designs is beyond the scope of this article. Several techniques are described in Responsive Web Design such as, what it is and how to use it and a list a part post on responsive design. The rest of this section provides an overview of some common design approaches. Sometimes, reorganizing content on the page isn't sufficient to handle the range of display sizes. You shouldn't expect to shoehorn every application into a 2 by 3 inch square and still retain usability. Usage patterns often differ between smaller and larger devices. Small devices are most suitable for brief and focused interactions; large devices are suited for longer, more intensive interactions. For example, a weather application on your mobile might contain geolocation-sensitive status on current and upcoming conditions. A desktop web version of the same application might provide more content on weather history for this and other locations, news articles or videos on weather events, and so forth. Text content can be scaled down by selectively displaying only the most important material, or by linking and moving subordinate sections onto separate pages. Images can also be responsively scaled for large and small devices. A range of approaches is possible. The simplest approach is to allow the image to rescale itself, but there are performance implications. When large images are sized down, important details can become difficult for users to see. An alternative approach is to provide thumbnail images that zoom in on touch when viewed in a mobile device but are displayed full-size on a desktop browser. . In other cases, it might make sense to create multiple images, cropped to show only the most important features, and selectively display the image appropriate to the target device resolution. Describe the methods that can be used to decide which platform to support, i. e., iPhone, iPad, Windows Phone, or Android. It's probably fair to say that most smartphone users use a single phone. On the other hand, many people use the same application on multiple types of devices. A user might access the same application on an iPod Touch, a Blackberry phone, an Android tablet, and a laptop running Microsoft® Windows. As far as the user is concerned, device types are essentially different viewers into the same content space. Multiplatform, multi device design is complicated by differences between device types. Smartphones are good for brief interactions to accomplish focused goals, anywhere at any time. Personal computers are good for extended interactions, dealing with complex information, and switching back and forth between tasks in relatively fixed locations. Tablet interactions fall somewhere between smartphones and laptops. Designing for multiple devices requires careful consideration and inevitable compromise among these competing requirements: (1) Make good use of each device's capabilities, (2) Intelligently handle each device's limitations, (3) It's probably fair to say that most smartphone provide a similar user experience on all devices. To provide a good user experience, a web application on a smartphone will often need to support different functions relative to its desktop equivalent. When displaying on a phone, you might need to remove some capabilities that make sense on the desktop, or add capabilities that make sense in a mobile context. It can be difficult to predict which functions won't be greatly missed on the mobile rendering of an otherwise complex web application. Complex layouts often work well on large displays, but they become unusable on smartphones. Conversely, extremely simple content layouts can appear uninteresting, or unreasonably tedious to read and navigate, when ample real estate is available. Many hand-held devices sense changes in orientation. Well-designed responsive content automatically adjusts its layout to fit the size and orientation of the device. One approach is to reformat multicolumn layouts to a single column layout when the device screen size and resolution become too small to support multiple columns. IPad applications sometimes exploit the familiar left pane navigation — right pane content pattern. This works well in large format screens but does not scale down to smaller, phone-sized devices. Mobile applications require high availability because end users need to have continuous access to IT and IS systems. End users require the network to be up at all times with little to no service disruption. For service providers, offering continuous network operations is a basic requirement for all applications. Residential customers require access to data, voice, and video services at all times. Enterprise business customers depend on 24-hour network operations that require strong service-level agreements (SLAs) for mission-critical applications.

Mobile phone subscribers expect to be able to make calls and access data services at all times. Best-effort service is no longer an option for most of today's applications. As service providers converge to a single, packet-based Carrier Ethernet network providing residential, business, and mobile services, network elements must be built for continuous system operations to meet these demands. In addition to node-level resiliency, service providers require network resiliency in order to provide service delivery even when network nodes or links fail. The primary design objective for a resilient, highly available Carrier Ethernet system is to gracefully handle both planned and unplanned downtime with minimum service disruption. Planned downtime typically consists of software and hardware maintenance tasks such as adding new features and services and performing configuration and policy changes, error corrections, and system upgrades. Unplanned downtime is generally the result of a software or hardware failure, configuration error, out-of-resource violation, security violation, or even natural disaster. The critical design concept used in creating a high-availability infrastructure is to minimize and protect against single points of failure. Modularity is an important attribute when preparing for planned events and guarding against unplanned ones. To protect against unplanned downtime, most current-generation routers offer hardware redundancy, fault handling, and failover features. However, because they do not support continuous system operations during maintenance cycles, these routers can create service downtime and add to operational expenses through time-consuming tasks. Modern network operating systems require millions of lines of code to implement protocol stacks, management interfaces, control-plane features, file systems, device drivers, and other critical services and features. To minimize the effect that failure in any of these processes can have on other processes, each process must execute in its own protected memory space, and communications between processes must be accomplished through well-defined, secure, and version-controlled application programming interfaces (APIs). To support continuous system operations, allow for In Service Software Upgrades (ISSUs), and ensure quick recovery from process or protocol failures with minimum disruption to customers or traffic, every process in the system must be capable of restarting while minimizing effect on services. Granularity of process restart during software upgrades allows system operators to restart perhaps a few thousand lines of code instead of the millions that might comprise the entire operating system. The Cisco IOS XR Software distributed and modular microkernel operating system enables process independence, restart ability, and maintenance of memory and operational states. By providing protected memory space for system processes such as the TCP/IP stack, file system, device drivers, and routing protocols, Cisco IOS XR Software offers granular support of fault handling and upgradability. Although the quantity of faults can be reduced through quality design, the nature of unplanned events makes fault handling a reality of network operations. To prepare for these conditions and maintain low MTTR, a high-availability infrastructure must provide rapid and efficient response to single or multiple system component or network failures to minimize service outage. When local fault handling cannot recover from critical faults, the system should offer robust fault detection, correction, failover, and event management capabilities. Discuss ways of providing high availability. Over the last fifteen years, mobility solutions have evolved from cell phones and pagers to platforms for wireless email and mobilizing business applications. Today's road warriors depend on their mobile devices for fast, reliable, easy access to applications and corporate data. Mobile solution downtime can adversely affect customer service, productivity, sales, and revenues. Availability means that people can use their applications and receive results within an acceptable time period. If users can't get their work done on time, the system is down. Because downtime must be avoided and minimized, next-generation routers must be designed with mechanisms to support planned maintenance tasks such as adding and replacing hardware, installing new features or services, and applying patches or upgrades to software, without affecting the routing system, customers, peers, or traffic. Server virtualization is a hot trend in the IT world because of the many business and technical benefits it can provide over the near and long term. There are many types of virtualization that can be utilized in the datacenter, but for the purpose of this paper, we will focus on server virtualization, storage for server virtualization, and storage virtualization. Server virtualization is increasingly becoming a more important tool for reducing cost, increasing availability, and enhancing business agility. By enabling organizations to run multiple operating systems and applications on a single physical server versus multiple physical machines, server virtualization can help organizations reduce hardware, energy, and management overhead significantly. From an application perspective, server virtualization enables organizations to consolidate workloads. This increases resource utilization and lowers capital and operational costs. In addition, server virtualization can help organizations improve application performance, availability, management, and agility. The more agile the IT environment is, the more an organization is able to meet changing business and application requirements. However, server virtualization changes the accompanying storage requirements. Organizations are unable to realize the full benefits of server virtualization without optimizing and virtualizing their accompanying storage environment. For example, many of the additional virtualization benefits, including built-in, cost-effective HA and DR, require external shared storage with a comprehensive feature set to support them. Mobile devices are subjected to hacking at a higher rate than non-mobile devices. Discuss methods of making mobile devices more secure. High availability is designed to protect mobile users against both planned and unplanned service interruptions. Unplanned service interruptions are typically triggered by technical problems within the system. Planned service interruptions, such as upgrades, are often necessary for maintaining peak performance and service. According to Patrck Traynor, the assistant professor in the School of Computer Science at the Georgia Institute of Technology, " Traditional cell phones have been ignored by attackers because they were specialty devices, but the new phones available today are handheld computers that are able to send and receive e-mail, surf the Internet, store documents and remotely access data -- all actions that make them vulnerable to a wide range of attacks. " December 2011 around 33 million people carried out shopping, e-banking and other transactions via Wi-Fi, cloud networks, or SMS. In future this number is going to make a tremendous rise by 230 million. There are reports that social networking apps are more under risk than other finance apps. Thus in order to keep your phone safe here are some methods which Smartphone users need to follow: * Keep Bluetooth switched off when not necessary As every Smartphone consist of a Bluetooth facility they should be switched off when not necessary and switched on only while transferring information or data. A device who's Bluetooth remains on have a tendency to get virus from other external sources or devices. * Keep changing passwords on frequent basis Protect your phone with minimum two layers of passwords so that hackers find it difficult to hack your phone. Set password locks for your SIM and you're mobile so that in case of phone theft the cell phone will ask for password if a new SIM is inserted. Also after a few trials of wrong password insertion the phone will automatically get locked. A password for screen locking too would prove to be beneficial. * Make use of secure connections As there are lots of unsafe networks available which phone users connect to incase of emergency which can be very dangerous. As unsafe networks always gives space for virus and other suspicious malware to enter your phone. Enabling remote services on phone and installing reliable security software will always keep your phone secure. * Take back-up of all your phone data Many people use their phones as a storage device thus every Smartphone these days offers a data back-up service which can be used in case of data loss. All phone users must take back up of their phone regularly. Users can do it by connecting their phone to a computer or by software that allows copying of all phone data to the PC. This again is very helpful in case of phone hacking or burglary. * Watch out for a reliable website There are many security software's available on the internet but people always look for a free software so in case of downloading a free software form the internet users must make sure they are clicking on the right URL because there are many fake sites where fake security applications are available. References “ ASR 9000 Series High Availability: Continuous Network Operations. " Retrieved on September 7, 2012 from http://www. cisco. com/en/US/prod/collateral/routers/ps9853/white_paper_c11-501797. html Leintz, J. (2012). “ Developer Works". Retrieved on September 7, 2012 from http://www. ibm. com/developerworks/web/library/wa-interface/index. html. MacVitto, L. (2010). “ Geolocation and Application Theory. " Retrieved on September 7, 2012 from http://www. f5. com/pdf/white-papers/geolocation-wp. pdf. “ Making Mobile Devices, Cellular Devices More Secure. " (November 8, 2009). Retrieved on September 7, 2012 from http://www. cc. gatech. edu/news/making-mobile-devices-cellular-networks-more-secure “ Oracle is the Information Company". Retrieved on September 7, 2012 from http://www. oracle. com/us/products/database/mobile-infra-using-bdb-066489. pdf “ Providing High Availability and Disaster Recovery in a Multi-Site Virtual Environment". Retrieved on September 7, 2012 from http://www. google. com/url? sa= t&rct= j&q=&esrc= s&frm= 1&source= web&cd= 10&ved= 0CHcQFjAJ&url= http%3A%2F%2Fdownload. microsoft. com%2Fdownload%2FD%2FC%2F7%2FDC719273-5979-4212-B889-7D42CB83E5AF%2FHP_P4000_HA_DR_Blueprint-Final. doc&ei= W5tJULGzMoL10gGP_YBw&usg= AFQjCNGhE4f55kJdOoLQyS_omMc99TMt6g&sig2= WJ51LVhclDhZp-NcCzmOmw Ricci, L. “ Making Mobile Secure. " Retrieved on September 7,

2012 from http://www. google. com/url? sa= t&rct= j&q=&esrc= s&frm= 1&source= web&cd= 6&ved= 0CFYQFjAF&url= http