



Technology Brief...

September, 2009

J.Gold Associates LLC, 6 Valentine Road, Northborough, MA 01532, USA
www.jgoldassociates.com +1-508-393-5294
Research, Analysis, Strategic Consulting

Battle of the Mobile Browsers: And The Winner Is?

There's a major battle brewing in the Mobile Browser wars (browsers on smartphones and MIDs). However the battle is all but over. And it has ramifications beyond just the browser.

The major smartphone vendors are aligning behind their favorite web-engines which they will use not only to power their web browsers, but also to enable applications and customized UI extensions. So who are the contenders? Mozilla Gecko, WebKit, Microsoft's Internet Explorer (Trident engine) and Opera Mini (Presto engine).

WebKit, like Gecko, is not really a browser - it is a rendering engine for web standards-based data (e.g., HTML, JavaScript, CSS, DOM). Trident varies in the interpretation of the DOM, which is why IE has some slight rendering differences from Mozilla-powered Firefox on web sites. Presto and Trident are both proprietary engines. WebKit was created by Apple, while Gecko was created by NetScape. Both WebKit and Gecko are now opensource.

Smartphone vendors lining up on the WebKit open source side are Apple (Safari), RIM (migrating its current browser through its acquisition of Torch Mobile), Google Chrome, Android (from HTC, Motorola, etc.), Palm Pre (WebOS), and most of Nokia's smartphone products. However Nokia is of two minds - S60 powered smartphones running Symbian use WebKit while Linux-based Maemo on Nokia's tablets uses Mozilla Gecko (derived from Maemo's Debian Linux roots), as does the Moblin OS.

Ultimately, WebKit will win the battle. Within 2 years, WebKit will be the engine of choice for 75%-85% of smartphone devices. Mobile Internet Explorer will be a minor portion of the market (as a result of Windows Mobile's falling market share) and Opera, although a capable mobile browser, will be relegated to niche status. Mozilla will remain popular with many Linux users since it powers Firefox, and so will have a major appeal to MID and Netbook users. However, although the share of Linux (and derivatives) powering smartphones will increase, Mozilla will have a minor share of that market, far behind WebKit powered devices.

WebKit, Gecko, et al are not just browser engines, but also enable a customizable UI access point to the core system as well as an app delivery platform, especially for the increasingly available cloud-based SaaS applications now being deployed. The challenge for device vendors will be making WebKit secure, as it has access to many of the core resources of the device and can therefore create OS instability

INSIDE THIS ISSUE

- 1 Battle of the Mobile Browsers: And The Winner Is?
- 2 PCs to Carry Side-ARMs
- 3 Making the iPhone More Trust-worthy Anywhere
- 4 Recent Research Reports

"...There's a major battle brewing in the Mobile Browser wars (browsers on smartphones and MIDs). However the battle is all but over. And it has ramifications beyond just the browser....."

and security risks, especially if used to power applications. Expect to see some sophisticated attacks coming in the next year as these browsers proliferate, as well as frequent SW updates.

Bottom Line: Application developers as well as web site developers who are increasingly concentrating on mobile device access must be careful to be WebKit compatible. That does not mean that designing for WebKit and Internet standards will be all that is required, as some of the “features” added-on by individual implementations could break certain user and/or display conventions. But WebKit will clearly be the core of all things smartphone where the Internet is concerned. Companies should standardize on this technology for all future deployments. Although Mozilla, Microsoft and Opera will all implement to industry standards, which should account for good compatibility, it will likely not result in 100% compatibility, much as is the case today on the Web. However, MIDs and Netbooks will still be IE and/or Gecko/Firefox centric (depending on the installed OS), much like the current PC world.

PCs to Carry Side-ARMs

The ongoing battle between Intel and AMD over supplying the brains of your PC continues unabated. While Intel clearly has the upper hand in client processors and AMD is playing catch-up, there is another battle brewing for PC processors, particularly in notebooks. This battle for the “secondary” processor will not pit Intel against AMD, but rather x86 architecture against ARM. And its not looking good for x86.

Dell recently announced Latitude ON, a feature first made available on its new Z notebook and on select E-series, but to be made available on most Latitude’s going forward. Its primary mission is to allow “instant on” access to email, calendar and web without requiring full boot-up of the machine. This is similar to Microsoft’s Windows SideShow first made available in Vista but which never went anywhere. But the features of ON take it well beyond SideShow’s, which required not only a peripheral processor but also a secondary LCD screen. ON runs a peripheral processor, in this case an ARM based chip from TI, with a Linux OS kernel and a Citrix Receiver client for application enablement, while also allowing administrators to securely access the machine resources. It runs a version of the Firefox browser for web surfing, and provides direct connection to Exchange, Groupwise or IMAP/POP3 email systems through direct memory access. Also included is a dedicated document viewer for Word, Excel, PowerPoint and PDF files, dedicated WiFi, and a VPN for secure connectivity. In essence, what Dell has done with ON is provide an embedded “smartphone-lite” device that uses the main screen, keyboard, power and memory systems.

“...The ongoing battle between Intel and AMD over supplying the brains of your PC continues unabated..... there is another battle brewing for PC processors, particularly in notebooks.....”

ON provides an interesting example of what can be added to machines to extend user convenience for relatively small cost. It’s included on Z, and a \$199 option on E4200 and E4300, but we estimate the additional cost to Dell to be \$50 - \$70. However, this capability is not new. Lenovo has offered a similar ARM-based co-processor system for about 6 months, albeit as an add-on Express Card compared to Dell’s built onto the motherboard approach. Lenovo’s Constant Connect function is similar to ON but uses a connection via Bluetooth to a BlackBerry for email, and Constant Protect is a security related enhancement that adds Yoggie System’s firewall and anti-malware/intrusion protection capabilities to monitor all incoming and outgoing traffic.

What makes the Dell and Lenovo approach interesting is that: first, they utilize low cost, low power ARM-based chips adapted from the smartphone industry; second, they provide dedicated-function processing; and third, each subsystem is capable of being functionally extended, possibly even by third parties through a future API, to include additional convenience and protection capabilities. It is safe to assume that other manufacturers will follow suit and provide co-processor sub-system in business and higher end consumer machines, particularly as prices for ARM chips continue to fall. It is also highly likely that additional functionality will be added over time. Finally, it is apparent that neither Windows nor X86 will be the preferred platforms utilized by these co-processor subsystems, at least until x86 can match the low cost and low power of ARM (potentially with future Atom chips).

Bottom Line: With the potential of one or more co-processors per PC, ARM has a lucrative path in which to infiltrate the PC market - a market it has never impacted. While its unlikely that ARM will displace X86 for the core processor anytime soon, it nevertheless gives ARM a large potential market of many millions of units - a fact not lost on ARM licensees (e.g., TI, Freescale, Qualcomm, Samsung). However, the co-processing sub-systems potentially offer another point of machine failure and/or instability, especially in corporate settings where consistency, security and device management is critical. Companies should be careful when and how to deploy these co-processor enabled systems until they prove their worth.

Making the iPhone More Trust-worthy Anywhere

Many organizations are deploying the highly popular iPhone to meet end user demands. Yet, although Apple has made some progress with V3.x of the iPhone OS in implementing more enterprise-friendly security and management technology, the iPhone still does not meet many of the stringent security and compliance policies established by enterprises worried about data loss and regulatory compliance. Despite this, companies are moving forward, albeit slowly to deploy iPhones to their users. Can iPhone be brought to enterprise-level security to limit potential risks?

A number of third parties are enhancing iPhone security through add-ons. There are two primary approaches being taken. The first is through enhancing the limited and easy to defeat policy/management capabilities, especially regarding device deployment and updating. The second is to deploy secure clients to protect on-device data beyond the limited capabilities of the current iPhone iteration.

“...No doubt Apple will continue to enhance its security with subsequent revisions. However, we doubt that Apple, with its strong consumer-oriented DNA will reach the high levels of security required by many organizations. This leaves companies with a dilemma.....”

BlackBerry set the standard for both security and device management. Its BlackBerry Enterprise Server (BES) can assume total control over the provisioning and management of the device. Apple's iPhone, in comparison, has a lukewarm approach when it comes to device provisioning, policy setting, and management. To enable a more secure and enterprise friendly mode of deployment and management, and to get around the risks of “jail breaking” or end user circumvention of these policies, Trust Digital's (TD) Enterprise Mobility Management Platform provides a more robust framework for deploying and authenticating the devices and securely setting and protection on-device profiles. While ActiveSync on the iPhone provides for limited management of policies through Exchange, Apple's iPhone Configuration Utility is the primary method for set up and provisioning of the device, but is cumbersome for large deployments.

TD allows initial provisioning in an automated fashion, and further prevents end users from bypassing the settings through device resets or through “jail breaking” applications by detecting any tampering and disallowing the device from connecting to corporate services. In this way, TD provides BES-like functionality (albeit with far fewer capabilities than BES) while consolidating the Configuration Utility and ActiveSync functions in one tool. Although it requires a small app to be loaded onto the iPhone, TD does provide greatly enhanced compliance and security through monitoring of all policies and even tracking usage (e.g., keeping a backup of all SMS messages).

The iPhone’s client apps are a weak link compared to the high level security inherent in the BlackBerry and in third party email applications (e.g., Good, Sybase). To this end, iAnywhere has created its Mobile Office as an add-on application that sits in a closed and sand-boxed area of the device. It then uses the application to talk with Exchange, and protects the data in a strongly encrypted container that is separate from the native iPhone apps. While this requires a separate app and prevents users from utilizing the native iPhone tools, it has the benefit of creating an area that is not compromised by “jail breaking” or by end user tampering. Mobile Office has the further benefit of connecting to Lotus Notes for the many companies that use Domino, something the native iPhone can’t currently do.

Both approaches above are viable, indeed necessary enhancements to the iPhone for companies needing to meet the stringent requirements for regulated industries (e.g., banking, insurance, healthcare, government) as well as for companies that require a high level of data protection and management of large deployments. Of course, this is the territory that BlackBerry has staked out by defining the “gold standard” for mobile security and device management. While such third party enhancements don’t meet the integrated capabilities of BES, they do provide a much enhanced environment for corporate deployments.

Bottom Line: No doubt Apple will continue to enhance its security with subsequent revisions. However, we doubt that Apple, with its strong consumer-oriented DNA will reach the high levels of security required by many organizations. This leaves companies with a dilemma: deploy security-flawed devices, or deploy add-on enhancements to increase security and management, but at an additional cost. We believe most companies deploying iPhone’s should look at add-ons to achieve a higher level of security and manageability than is available within the native iPhone, and to prevent tampering and “jail breaking” of the devices.



J. Gold Associates, LLC
6 Valentine Road
Northborough, MA 01532 USA

Phone:
+1-508-393-5294

Web:
www.jgoldassociates.com

*Research, Analysis,
Strategic Consulting*

Recent Research Reports

Contact us if you would like to obtain any of the following research:

Major Market Studies

- Enterprise Mobile Applications: A Study of Strategies and Adoption Trends (Complete Report)
- Mobile Business Applications: A Study of Strategies and Adoption Trends (Executive Summary)

Technology Reports

- Solid State Drives in Notebooks: Cost Advantage or Cost Liability?
- Keeping Notebooks Past Their Prime: A Study of Failures and Costs
- Survival of the Fittest: Will Windows Mobile Go Extinct?