

## **Security and iPhone OS 4 Multi-Tasking: Does It Really Matter?**

As the iPad and Mobile OS 4 for the iPhone family are readied for release in the coming months, the rumor mill is chock full of ‘multi-tasking’ talk. Yet there has been little discussion of what multi-tasking really means to the average user. Does OS 4 multi-tasking help the enterprise that wants to securely integrate the iPhone family into their network? Does iPhone multi-tasking affect the carrier who would dearly love to reclaim much of the abused bandwidth of the last mile, which is filled with 80+% junk email?

First of all, the iPhone already does multi-task. It listens for incoming phone calls or texts, and allows music to be played at the same time while awaiting notifications about updates. The iPhone OS 3 already uses the same preemptively multitasking Mach/BSD kernel as Apple's desktop Mac OS X. However, users think of multi-tasking as the experience of running more than one third party application at the same time as they do on laptops and desktops.

From the conventional security perspective, extensive multi-tasking is required. While a Word document or PowerPoint presentation is being prepared, in the background, a large variety of security processes share the memory and CPU resources as well as consume valuable power. Anti-virus and anti-spam software run ‘continuously’ while a personal firewall and VPN aid in perimeter security of the device.

Some users and enterprises run multiple versions of security software from different vendors in order to maintain the highest detection rate of hostile code or activities. All the while the user is chatting, typing, downloading and viewing rich content.

From a security viewpoint, OS 4 multi-tasking gives the false appearance of being critical to Apple’s tens of millions of iPhone customers. It really doesn’t matter.

Apple could open its entire kimono, much like Android and Windows Mobile, allowing any piece of software to run at any time the user wishes, inviting the same suite of system performance and conflict problems found on ‘regular’ computers. Since Apple’s proprietary A4 processor has up to four cores, OS 4 could manage some of the internal system processes on one core and allow other cores to share the overhead of third party applications.

Another potential view of OS 4 multi-tasking could be to allow, say, native Safari and mail to run concurrently. Then they might permit two, or three, or some number of Apple approved apps to run at the same time, with some form of Command-Shift for switching applications. The definition of multi-tasking does not have to mean “As many as apps as I want.” Building in reasonable restrictions to maintain a positive user experience is certainly one approach I would consider if I were designing a mobile operating system.

But then what about security? Smart phones are just small computers, subject to the same inherent weaknesses and vulnerabilities as any other computer – and I am not even addressing iPhones that have been jail broken.

Assume for a moment that Apple chooses to allow an unlimited number of security apps to run at the same time (multi-task). This would emulate the current state of

security where the onus is on the user to manage them and every security application is loaded onto and run from the endpoint. Users need security, enterprises demand it for compliance, but the conventional approach to security, even in a limitless multi-tasking OS 4 environment presents a number of conundra:

- How much processing power and storage are required to match a best-practices level of security?
- What happens to battery life, even on the iPad, if countless security applications are loaded and run continuously?
- With preemptive multi-tasking, which processes take precedence over others, potentially affecting both performance and security.
- How much knowledge will the user require to download, install, configure and manage the security applications?
- Security needs to be running 24/7. Do we expect users to turn on every security service each time they turn their iPhone on? In OS X, users can choose applications to autostart in “login items”, which requires a broad method multi-tasking.
- Using Time-Based Security equations, how will the last mile performance be affected as richer content and security are handled at the smart phone endpoint rather than in the cloud?
- How often is ‘often enough’ to update security profiles, signatures and alerts when resources are far more limited than on a ‘real’ computer?
- What happens when the smart phone is turned off for the night and then turned on in the morning? The user only wants to check his email or read an RSS feed, but the multi-tasking iPhone needs to first perform a series of security actions.

Apple’s approach, based upon available intelligence, is going to favor the user experience as it does in Expose, allowing easier switching between applications. Does that mean that the user can watch a You Tube video and really quickly switch over to email, essentially pausing the You Tube experience in favor of email? One could easily argue that this is multi-tasking, managed by the kernel. However, this approach would still not allow the current traditional methods of computer security to be implemented.

No matter which multi-tasking approach Apples chooses to introduce into OS 4 or beyond fails to solve security problems using conventional approaches. Whether it’s iPhone OS 3, 4, or X, or the multi-tasking Windows Mobile, Android or Symbian, it is quite clear that relying upon the smart phone vendor for security is not the answer just as it has not been the PC vendor’s concern for nearly thirty years. To properly secure all of the current and future iterations of foreseeable smart phone technology means creating a truly integrated secure mobile architecture and framework that functions in the cloud.

From a security standpoint, it really doesn’t matter how Apple chooses to define multi-tasking for the iPhone OS 4. The user experience comes first, and in most cases the user puts security near the bottom of the list of what he wants to do when he wakes up.

What happens in 2013 when more than 2 billion smart phone users chose not to secure their experience? That's something I hope we never have to find out.