Market Roundup

July 9, 2004

On the Processor Front: I Coulda Been a Contender

By AJ Dennis

Expanding on last week's Market Roundup coverage of the launch of the Intel chip formerly known as Nacoma, we look to the impact these new processors, which use EM64 memory extensions in a compatible way to AMD's Opteron chip to ensure 64-bit compatibility, will have on Opteron future in the workstation and small-server markets.

Since its launch in April 2004, we felt the reality of Opteron was important, even with a lot of pieces of the puzzle still outstanding, setting the stage for real customer opportunity and market competition, and perhaps crafting the conversation of an easier transition to 64-bit x86 computing. We had been impressed by both the early performance results and with the slow but steady growth in vendor awareness and enthusiasm for the AMD Opteron. Among the major vendors, IBM came out early with high-performance computing servers and Intellistation workstations using the chip. After apparent angst, Sun Microsystems joined in delivering its Sun Fire servers with the chip. HP, who already uses AMD in consumer and business desktops, has recently committed to Opteron, giving AMD design contracts with three of the world's four largest server makers. (Dell, which uses only Intel chips in its computers, is not interested.) In the OS and applications space, Sun's Solaris operating system for Opteron is ready. Microsoft is in beta with its 64-bit version of Windows for the Opteron (which does not run on the Intel Nacoma) with plans for delivery in the second half of 2004. (Standard 32-bit Windows already runs on Opteron.) Versions of Linux in 64-bit mode already exist. IBM has ported a version of its DB2 database software to run on 64-bit Linux for Opteron.

Acknowledging the gains, we are still concerned that Intel has the market clout to effectively forestall Opteron's deployment beyond the high-performance computing and workstations. IBM, for instance, while an early adopter of the technology, decided to position their Opteron servers outside their mainstream x86 products (eServer xSeries) and branded them simply eServers, only marketing them through their High Performance Computing group. To maintain momentum, Opteron needs to compete in the one- to four-processor segment, a market currently dominated by Intel's current Xeon chip and the target segment for Intel to refresh with this new Xeon. Initially, we believed that IBM was the best vendor to be able to differentiate itself in the Industry Standard 64-bit x86 server space with Opteron, and overcome the inertia of Intel's incumbency within its eServer xSeries product line. But alas, IBM seems to have missed that opportunity. Now that Intel has delivered on its recently realized enthusiasm regarding 64-bit extensions to the IA-32 architecture, we believe Opteron will not have the time and attention in the xSeries to see that develop. While the various vendors, analysts, and pundits will hold forth on the issues of comparative architecture, implementation, performance, and support, we believe it will amount to mostly hand waving and background noise to the very real and very powerful impact of Intel's ability to MAKE (IA-32), FAKE (IA-64) or TAKE (64-bit x86) a market.

Copyright © 2004 The Sageza Group, Inc.
May not be duplicated or retransmitted without written permission

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Milan +39 02·9544·1646

Email: An Open Book?

By Jim Balderston

A federal appeals court in Boston ruled last week that federal wiretap rules do not apply to email messages if they are temporarily stored on a computer owned by an ISP. Federal agencies seeking to "tap" those communications will be allowed to do so without getting a court order, as required with traditional wiretaps. The ruling stems from a case in which an online bookseller offered free email accounts to booksellers and then snooped on the contents of their inboxes. One employee pled guilty to wiretapping charges in 1999; a second employee fought the charges and argued that the wiretap law did not apply because of conflicting laws offering lesser protections for stored email vis-à-vis email in transit. The Boston court agreed with that argument and it was subsequently upheld on appeal.

While it is unclear how quickly this ruling will disseminate through the legal system, in its infancy it offers the opportunity to consider what will be. Assuming that this ruling stands the scrutiny of further judicial review, its is reasonable to assume that government agencies will be taking a much more proactive stance in monitoring email as it passes through various way stations on the Internet. It is also reasonable to assume that some individuals will seek to monitor emails in efforts to gain valuable information of one sort or another. This ruling could open a whole new wave of corporate espionage efforts.

Unlike the U.S. Mail, which has a long history of enforcing violations of the chain of mail possession between the sender and the recipient, email has no such protections as it moves from one computer to another through the vast web of interconnectivity that is the Internet. This ruling would appear to give legal cover to those who wished to snoop on others people's email as it was stored on any computer, regardless if that storage time could only be measured in milliseconds. Given the fact that so much corporate communication is done via email, it is clear that significant corporate intelligence could be gleaned from monitoring email traffic. Assumptions of privacy in such circumstances are clearly inappropriate; such circumstances warrant the application of various encryption schemata to ensure privacy in an environment where an email can pass through anyone's hands before reaching its destination. The need for more prevalent encryption communications should not be viewed with alarm or concern, but merely as evidence that the Internet is striding toward maturity and assimilation.

Drop a Dime on VoIP

By Jim Balderston

The IRS and U.S. Treasury Department have announced that they are beginning the process to consider whether the 3% federal excise tax on phone calls should be applied to Voice over Internet Protocol phone (VoIP) connections. The two agencies published a notice late last week indicating that the review process was beginning; an IRS spokesman said the agency was not in the process of making new rules but seeking comments on the topic. Comments will be accepted up until September 30 of this year. While consumers are beginning to make VoIP calls in increasing numbers, it is enterprises that are really taking up VoIP technology, where as many as 10% of all business calls are using the Internet as opposed to traditional switched-circuit networks. VoIP companies and vendors offering VoIP services said extending the excise tax to VOIP would stifle the fledgling market sector.

This situation should sound vaguely familiar, as we went through various proposals to tax Internet commerce just as any other retail transaction would be taxed. So far, such taxes have remained largely off the books but we suspect that situation will not last too much longer, as Internet commerce has shown itself to be a robust enough element of the economy to not be withered by the imposition of reasonable sales taxes. Given the fact that states and the federal government are facing increasingly desperate budget shortfalls, the arguments against such taxation will become harder and harder to justify. Such a scenario is likely to be followed in the present situation, with dithering back and forth on this tax despite the obvious fact that a phone call is a phone call, no matter what technology is used to make said call.

What is most amusing to us is the ongoing perception that somehow the Internet is supposed to offer lots of free stuff. Free software, free email, free phone calls, etc. While there is no question that VoIP offers a more efficient

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Milan +39 02·9544·1646

Copyright © 2004 The Sageza Group, Inc.
May not be duplicated or retransmitted without written permission

means to deliver phone calls than traditional switched circuits, what we hearing from VoIP backers is not that lower transmission and network costs can eventually bring down the cost of making phone calls; instead we hear discussions of how the VoIP market should receive a blatantly unfair exemption from an existing tax on an existing public behavior, i.e., making phone calls. In our minds the technological and economic advantages of using packet-based switching of phone transmissions over traditional circuit-based switching of calls will drive the technology deeper into the market, as carriers begin replacing aging phone switches with IP technology. Cost savings due to this technology replacement should make its way down to consumers, as a vibrant competition from traditional phone companies and other bandwidth providers will certainly ensue. So let's quit goofing around with this issue and level the playing field for all participants, and let the best technology and value proposition make its way in the market.

Virus Attacks Expected to Double in Next Ten Years

By Rob Kidd

This week European email security firm MessageLabs stated that almost 70% of European enterprises expect the number of email viruses to double over the next ten years, and 80% of respondents expect payloads to become more destructive. The survey and company data document a dramatic increase in viruses during the last several years. The MessageLabs ratio of viruses to email in May 2004 was approximately 1:11, up markedly from a year earlier (1:125) and two years earlier (1:212). In the past, most payloads have only irritated and clogged bandwidth, rather than pirated data or disrupted system functionality. However, survey respondents expect this to change quickly and dramatically with a future promise of much more destructive threats. Survey participant's perceptions come despite software developers — such as Microsoft — committing to spend greater resources to clear up existing vulnerabilities, improve coding practices, and initiate aggressive future security and best-practices programs.

Prior to the emergence of sophisticated networking technologies and the Internet, there were viruses, but their rapid spread and disruptive impact were limited. Past virus writers have unleashed viruses and worm payloads that have been disruptive and resource- and bandwidth-consuming, but fortunately, in most cases these gremlins have not been violently malicious and destructive, nor have they attempted property crimes or other criminal acts. But today the Internet has become a vehicle for nefarious endeavors and e-crime, and a sophisticated and specialized clique of virus authors that have expanded into shady business operators, common criminals, and organized crime. At the same time, the virus threat is becoming more complex and merging with other computational ne'er-do-wells. For example, a Trojan with integrated spy-ware or key-logging functionality could easily capture the information necessary to commit identity theft or perpetrate other crimes and fraud. The potential economic and personal threats of this malware are enormous and growing.

In the past security has been viewed by many as a disabler and show-stopper of cool things that can be achieved with technology (but can't be done because of security risks), but the reality is that security now has be viewed in the position of integrated enabler if the potential of the Internet is to be fully realized. But in pragmatic terms, what does this mean? Security vendors such as Symantec, McAfee, NAI, etc. will have to create countermeasures to mitigate new families of combined threats such as Bobax or those yet to emerge. Enterprises and their employees will have to create a security-aware culture focused on vigilance, best practices, and process. Government will have to focus on cross industry and end-user enterprise initiatives with enhanced cybercrime vigilance and sentences for those caught perpetrating such acts. However, harsh sentences for perpetrators alone will not be sufficient, as history has long demonstrated that it is not the severity of the sentence that deters, but rather the certainty of being sentenced. Thus, in order to counter the growing aggressiveness of the Internet club of social reprobates, it is incumbent on all of us, from vendor to user, and from CEO to facilities engineer, to take an educated, yet vigilant stand against the practices of cybercriminals by changing our own perception and user habits with respect to computer security.

Copyright © 2004 The Sageza Group, Inc.
May not be duplicated or retransmitted without written permission

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
650·390·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Milan +39 02·9544·1646