Market Roundup
August 27, 2004

## Cryptic Foundations

*By Charles King*

At the recent Crypto 2004 Conference, French computer scientist Antoine Joux reported an apparent flaw in MD5, the algorithm that serves as the basis for many popular 128-bit digital signature solutions. His findings were followed by a report from a team of Chinese researchers who released a paper detailing a method for creating two different files that shared the same MD5-based digital signature. In addition, Eli Belham and Rafi Chen from the Technion Institute in Israel discussed preliminary findings which identified potential vulnerabilities in SHA-1, a popular 160-bit output algorithm embedded in PGP and SSL, and the only signing algorithm approved for use in the U.S. government's Digital Signature Standard. If the findings are substantiated, they could potentially curtail the long-term viability of SHA-1 and drive the need for other options.

The IT industry is one where the relationship between research and commercial product development is often blurred, sometimes despite the best of intentions and sometime purposely. While much IT research is arcane in the extreme, other developments have significant and measurable impacts on the lives of IT solution customers. The Crypto 2004 findings are a case in point. Are the French and Chinese reports on possible weaknesses in MD5 a cause for concern? Sure. If you discover a crack in the foundation of your home, prudence suggests you investigate and repair the damage. Similarly, since the venerable MD5 algorithm (originally introduced by Rivest in 1991) serves as the basis for so many digital signature solutions, further investigations are warranted. But do these apparent cracks mean that any solutions using MD5 as a digital signature foundation are in danger of collapse? Well, no. For one thing, the researchers' results did not demonstrate a usable hack but a negligible vulnerability that might be conceivably be exploited. In other words, it's still a long way from here to there, though hackers taking advantage of increasingly powerful and sophisticated computing tools may have less trouble making the journey at some future point.

Most importantly, the Crypto 2004 reports did not address or discuss potential dangers to MD5 Plus-based solutions, which utilize vendor-developed technologies in addition to MD5. For example, EMC utilizes MD5 as only one naming system in the GM (GlobalMD5) solution set featured in products such as Centera Compliance Edition. Along with the MD5 128-bit name, Centera attaches a day and time (to the millisecond) stamp to documents, as well as additional encryption features that can result in a 256-bit total output. The application runs checks to ensure that original documents and their backups are the same, and also provides an option to turn off the single-instance storage feature. In order to exploit the flaws discussed at Crypto 2004 in a Centera system, a hacker would need to create rogue files produced at precisely the same time, on precisely the same nodes, and with precisely the same content as the originals. Overall, the reports of the French and Chinese researchers offer an interesting window into the way previous generations of technology are inevitably overtaken by robust newer generation solutions. Similarly, MD5 Plus offers an example of how innovative vendors can use well designed foundation technologies as a basis for their own, more formidable creations.

## To BEA or Not To BEA?

*By Jim Balderston*

BEA Systems has announced second-quarter revenues of $263.2 million, below previous estimates of between $265 and $275 million, yet on target for lowered numbers BEA circulated a week before the financials were released. While revenues were up quarter-to-quarter by some 7%, the latest financials show that this is the second straight quarter in which the company has not met projections. The company has also been hard hit by a series of high-level departures in the past few months, as well as an ongoing drop in licensing revenues. Those departing include the company's CTO, the company's chief architect for long-term initiatives, the vice president of channels and alliances, the senior vice president of marketing, and a senior director of product marketing.

While BEA officials (the remaining ones, that is) note that the company is still strong and that its soft revenues are endemic throughout the software industry, we have to suspect that something much more dire is going on within the halls and cubicles of BEA. The loss of so many key executives may indicate that they see the writing on the wall for the company, and are seeking greener pastures. As such, we suspect there is no small amount of consternation at companies partnering with BEA receiving application servers and middleware from the company. The developments at BEA are in all probability not being well received at HP or Sun, for example. Meanwhile, folks at IBM may find themselves reaping a significant windfall for WebSphere middleware sales as customers begin to raise legitimate questions concerning BEA's viability. The folks at JBoss may also be smiling, but we are not all that sure they should be, since they may end up in a head-to-head battle with IBM while being forced to fight headwinds associated with their own stature and long-term viability.

In our mind, the source of BEA's problems is simple. The company is selling a product that is increasingly considered a commodity offering that is only a subset of a larger and more complex IT environment. At the height of the Internet boom, application servers were the hot, hot, hot technology, with dozens of innovative smaller companies bringing their products to the fore. BEA itself bought WebLogic, the maker of one such app server, and bet its future on a middleware play for partners like HP who decided such efforts were not worth the expense and time. Companies like IBM wove their application server into a broad range of in-house offerings, making it largely the glue for its other task-specific products like databases or storage products running on IBM hardware. Meanwhile, companies like Sun started giving away an app server, despite its relationship with BEA. Sun cancelled the giveaway, but the action indicates clearly that the technology itself is now a means to sell and market ancillary products, not the core offering itself. What's next for BEA? We suspect that the company will continue bravely on while seeing its market share shrink in the face of increasingly valid questions regarding the actual value-add of app servers and middleware. In all likelihood, either by partnership or M&A activity, its technology will become an element of a larger, integrated set of offerings, just like all the other leading-edge products that have drifted out of the high-tech limelight into a behind-the-scenes supporting role.

## Carcass Production

*By Jim Balderston*

HP has announced it is ending its effort to offer a new antivirus technology after finding that it had problems making the product work with computers running the Windows operating system. The product, called Virus Throttler, was designed to slow the spread of viruses by limiting the connections an infected computer could make during a fixed time after noticing different behavior on the machine after it has been infected. The product worked well in Linux and HP-UX environments, but was unable to run on Windows because it required that changes be made to the operating system. HP officials said they did not have the ability to make the needed changes in Windows because they did not own the OS.

HP has shown its Virus Throttler product to Microsoft and has deployed it on its own internal network of nearly 250,000 hosts. But it looks as though the product will not be sold or marketed in its present form in the foreseeable future since it basically would only be able to provide its protections to a subset of an enterprise network. While such protection may have some value for those machines, most viruses are written to attack

Windows machines, and the network as a whole would still be vulnerable. For the most part, security products that have out-of-the-box holes in their protection don't do particularly well in the marketplace. This one would have been no exception.

HP announced this product just six months ago at the annual RSA conference along with another security product called Active Countermeasures, a product that scans networks looking for vulnerabilities. Active Countermeasures will go into beta testing with some of HP's customers, and HP hopes to release the product in 2005. Perhaps it will fare better than Virus Throttler. One of the things that has us concerned is the fact that Throttler got as far along as it did, given the fact that anyone working on the project knew that the Windows issue was inevitable and unavoidable. HP defended its announcement of the product as a way to demonstrate innovative product development. But the old saying concerning pudding and tasting clearly apply here as the product's viability window was measured in mere months, reminiscent of the go-go days of the of the Internet boom in which innovation was the sacred mantra throughout the industry. But as the carcasses of so many "innovators" rotting across the landscape clearly show, product quality and value to the marketplace trumps vacuous innovation every time.

## Ethernet Switch Prices Rise; Current Economic Climate a Factor

*By Rob Kidd*

In contrast to historical patterns, Ethernet switch prices are on the rise, and more such devices are being purchased, according to market researcher Dell'Oro. The company says the average price of an Ethernet switch port has risen to $96, with Fast Ethernet approximately $50 per port and Gigabit Ethernet approximately $200 per port.

The "common" wisdom in the electronics industry says that cost and price of such equipment decrease over time, as volume increases. Innovation and experience in the development and production process are other contributors to this phenomenon. The Ethernet switch market seems to be operating under uncommon wisdom. IT enterprise shifts to higher speed devices, with greater functionality and intelligence, can be blamed in part for this phenomenon. For example, buyer "must haves" for layer 3 and above switches include distributed hardware based routing, wire speed switching and routing, multi-gigabit architecture, support for high-speed and -density interfaces, load balancing, and simpler device management. Higher price tags and underutilized bandwidth have not suppressed demand for these faster and more capable devices because technologies like convergence, VoIP, and wireless LANs are driving the demand for them. In the future the adoption of such technologies will continue, if not accelerate, but we expect switch price trends to return to the historical declining pattern over the long term.

Another potentially underrated factor, in our opinion, is the U.S. economic climate. The vast majority of components used in devices like switches are manufactured offshore. For the last several years the U.S. dollar has remained low against virtually all major foreign currencies fanning the flames of a tightly focused inflation furnace. Lower outsourced production costs may have been more than offset by a weak U.S. dollar against other currencies, resulting in net cost increases. This complexity is difficult to factor into production decisions such as to outsource or not to outsource, but vendors will be forced to factor the ongoing value of the U.S. dollar in making such decisions. The almighty buck is having increased difficulty filling offshore buckets.