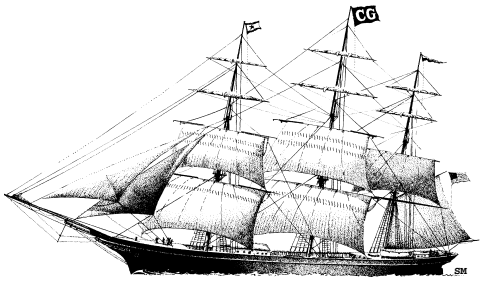
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2008046 September 22, 2008

Universal Encryption — Has it come to this? Brocade Brings a Foundation

Analyst: Robert A. Vega

Management Summary

My friends in Vermont or New Hampshire do not lock their cars. Many don't lock the doors to their homes, and some on occasion, leave purses or wallets in easy reach at their desks. If you're a city boy, you find this charming, or quaint, or wacky. If, as I, you were born in the south Bronx, grew up in Queens, and worked in Manhattan, you lock your car and put any appealing items out of sight (perhaps you also use a steering wheel lock). You have learned this, personally or through your neighbor or from your relative. Always check to see that the windows are secured and that you lock your home before you leave. Carry your wallet in your front pants pocket. If you use a purse, keep your purse on your lap when you have lunch at the fast food place (not on the floor under your seat). Life in the big city is not carefree. However, it's not paranoia or obsession if somebody out there really is trying to "get" you in some way, and we know that somebody is.

In the courts, there is the concept of the "Reasonable Man," an abstract ideal being who, among other factors, is careful to protect himself as well as others, and practices moderation in all things. We are often reasonable, and we often act accordingly, but not in all things. We try to protect our valuables, whether we leave them at home, or on the street, or carrying them with us. Sometimes we don't secure them well enough. Consider the number of laptops that are reported missing or stolen each year. In the somewhat distant past, we didn't consider the data in the enterprise as vulnerable. Traditionally, IT personnel "never lost sleep worrying about hackers breaking into systems, or tapes getting lost on the way to Iron Mountain, or laptops being stolen," as Clipper said in an earlier bulletin in reference to tape, but this was also true for all enterprise data.[1] That report continued: "It is no longer good enough to put combination locks on computer room doors or require passwords on files." This, as we know, is because there are some people eager to steal (or illegally "borrow") whatever you are supposed to protect. As a solution, maybe we should just encrypt everything! Maybe, it has come to that. In the not-so-distant future, would you like to sleep at night? Are you reasonable? Then a *universal encryption (UE)* solution may belong in your data center.

Brocade recently announced their *Fabric-Based Encryption* solution for data in connection with their introduction of the Brocade Encryption Switch and Blade product line. The Brocade Switch and Blade product, which we view as a stepping stone to UE, offers up to 16 or 32 ports at 8 Gbits/sec, up to 96 Gbits/sec of encryption processing power, high-level encryption, and secure master key storage. To find out more, please read on.

IN THIS ISSUE

[1] See **The Clipper Group Navigator** dated August 28, 2006, entitled *IBM Gives Enterprises Options for Encryption* and available at http://www.clipper.com/research/TCG2006077.pdf.

Universal Encryption Requirements

Has it come to this? In a word, yes. First, we do not have any other way to protect digital information. Second, our goals are to respect the value of the information of which we are stewards, to be aware of the dangers we now reasonably understand, and to take the appropriate action. Finally, most enterprises have "under-encrypted," primarily because of the related complexity. Of course, it's only a solution if we recognize a problem.

If you were to ask the average "man-in-the-street" (another mythical being), they would probably say that they have heard of data encryption and, increasingly, they are saying that that they expect their information to be protected by encryption. We cannot escape the growing truth that encryption is an expected cornerstone of data security. Thus, we need to figure out how to encrypt with ease and lowest unit cost.

As technology develops, we have opportunities we did not have before and we have to use them. If their data had all been encrypted, leading retail establishments and other enterprises, who demonstrated shamefully weak or non-existent defenses against hacking, would have had some measure of protection. On the other hand, encryption (even Universal Encryption) does not replace an overall data security plan that is robust, tested, and updated regularly.

Current encryption solutions don't scale well, generate significant overhead and add complexity in parts of the fabric, often are point software solutions, lack central key management, and have other negative aspects. Here are important factors we expect in such a solution.

- It should ***scale well***
- It should ***reduce complexity***, within the environment and at the edge
- It should provide a ***blanket of encryption*** capability
- It should have ***central key management***
- It should ***handle disk and tape***
- It should be ***compatible with existing and evolving virtualized environments***, so it can be introduced without disruption

However, let's not forget the user experience. Encryption should also provide the following characteristics.

- ***Transparency*** – users should not realize this superbly complex service is there
- ***Accessibility and Availability*** – the service should not deny consistent and speedy access
- ***Choice*** – it should offer the capability to encrypt some or all of the data within flowing in and through the data center
- ***Cost Effectiveness*** – it has to be affordable and in line with the risks being mitigated
- ***Reliability*** – it must work without catastrophic failures
- ***Compliance*** – it must support enterprise programs required for regulatory compliance

Is this "insurance?" Some types of insurance are mandated, e.g., in Massachusetts both health and automobile insurance are required by law. Lenders require mortgage insurance for all standardized loans. Life insurance is optional, yet is valuable protection when properly implemented. Ordinarily, insurance compensates you for a loss or damage resulting from risks that you face. We now regard the concept of encrypting all the data within the environment that you control to more valuable than insurance. This is because **encryption provides *assurance* that you have reduced your risks.** With such assurance, you have greater confidence that you are able to maintain the confidentiality and integrity of the data that you transport or store.

In Brocade's solution, all data moves through the SAN, so there is centralized management, and centralized key administration. The Brocade offering includes plug-in encryption services, "pay as you grow" scalability, and robust encryption processing power. Brocade's Data Security Services are geared up to provide security assessment, training, hardening, monitoring, and other vital evaluation and implementation support, and soon also will be offering Data Encryption Services.

In the first release, the Brocade Switch and Blade will support disk encryption, NetApp Lifetime Key Management and the RSA Key Manager (RKM), along with four industry-leading backup applications.

- IBM *Tivoli Storage Manager 5.4*
- EMC/Legato *Networker 7.3*
- Symantec/Veritas *NetBackup 6.5*
- CommVault *Galaxy Data Protection 7.0*

Pricing for customers, as determined by

Brocade distributors, should present an attractive cost and benefit scenario. We anticipate that the cost of the Brocade entry configuration solution, delivering up to 48Gbit/second of encryption processing, will compare favorably to the cost of five 2Gbit/second encryption appliances (i.e., representing a total of 10Gbit/-second), while providing up to five times the processing capability. In addition, the entry configuration can be upgraded to 96Gbit/sec processing (via software license key upgrade).

Next year, expect to see support expanded to include additional key managers, backup, and encryption capabilities as part of the offering.

Conclusion

Brocade has designed the Encryption Switch and Blade solution to provide a blanket of encryption capability, as well as robust processing (up to 96Gbit/sec), and scalability beautifully suited for a fabric-type environment. With this solution, enterprise data has a very significant layer of protection, even if system access is somehow compromised.

If you are already using a SAN environment and you want to protect your data further, or if it is your intent to evolve your enterprise's data security, then you need to give serious consideration to encrypting everything. To do this, you should consider the Brocade Switch and Blade offerings as the enabling technology. Brocade's solution can protect the data that is your main concern now, while providing a springboard to the efficient and cost-effective maximum encryption you will need. Given that you are now or soon will be expected to have Universal Encryption, isn't the time ripe to figure out how you are going to do this?

About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Robert A. Vega **is Contributing Senior Analyst for The Clipper Group.** Mr. Vega's focus is on enterprise network, data and voice transport, strategic business solutions, and trends in telecommunications. He began contributing to The Clipper Group after three decades in Telecommunications project and operations management. Positions held by Mr. Vega include: Director of the Office of Telecommunications at NYC Health & Hospitals Corporation, Consultant in the NYC office of Trecom Business Systems (now part of Fujitsu Consulting), Lead Planning Analyst at Empire Blue Cross Blue Shield, Director of Telecommunications/Information Services Projects for the SHARE Group, and Manager, Telecommunications & Systems Development, for The Presbyterian Hospital (Columbia-Presbyterian Medical Center). Mr. Vega also served in positions for New York Telephone (now Verizon), Alternative Resources Corporation, Alcatel (now Alcatel-Lucent), and Aspect Software, and has performed project work at EDS, Cedar Point Communications, Massachusetts Blue Cross Blue Shield, and Cross Country Group. Mr. Vega's writing has appeared in Network World and other outlets. Hiss presentations include conferences sponsored by The Eastern Management Group and the American Hospital Association. Mr. Vega earned a B.A. degree from Queens College, CUNY.

- ***Reach Robert A. Vega via e-mail at bob.vega@clipper.com or at 781-235-0085 Ext. 216. (Please dial "216" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group** *Captain's Log*, **The Clipper Group Voyager**, *Clipper* **Notes**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.