THE CLIPPER GROUP

Explorer™

Navigating Information Technology Horizons℠

Published Since 1996 Report #TCG2004071 August 29, 2004

Storage Security — Where Are Your Vulnerabilities?

Analyst: Michael Fisch

The Security Drumbeat

You have heard the growing and relentless drumbeat about the importance of storage security – from the press, vendors, analysts, and fellow IT professionals. The reasoning goes like this.

- Information is a critical business asset, and storage is where it resides,
- Theft, loss, and unavailability of information can have terrible consequences,
- Threats come from many sources, both outside and inside the enterprise, and can be directed at multiple points of vulnerability,
- Networked storage (SAN and NAS) brings greater efficiency but also additional vulnerability points,
- Therefore, it is imperative to take active and sufficient measures to secure storage.

What storage security measures must an enterprise take? The answer depends on the value of the information and the ways in which it is exposed. These factors are unique to each enterprise. **Finding an appropriate security solution requires analyzing the information and vulnerability points of an enterprise.**

Chinks in the Armor

When analyzing storage vulnerabilities, consider the following areas.

Keys to the Castle

Those who have the keys can come and go and they please. In this case, the keys to the castle are *management access*. **As the point of total control, it is critical to protect management access points by regulating *who* has access and *how* access occurs.** First, only give access to trusted IT administrators. It is also best to assign roles that limit privileges to their respective areas of jurisdiction. For instance, the storage administrator in one department does not need control of another department's storage. Network traffic traveling between the management console and the device under management should be private, especially if the console is remote, as well as checked for data integrity. (See *No Peeking* and *The Genuine Article* below.)

Compartmentalization

To protect its secrets, the CIA is known for rigorous *compartmentalization* of information. A person must have a "need to know" to access to a particular file. This is because a mole or leak can turn up anywhere, and compartmentalization limits the damage one can do and keeps the list of suspects short. Similarly, **enterprise clients (i.e., application servers and end users) ought to**

have access only to data they need to perform their respective tasks – also known as *selective presentation.* For instance, the marketing department should not have access the R&D files because they don't need to see the source code to create presentations and literature. Or, an e-mail application should not be able to see storage volumes belonging to a database server, lest it be tempted to use the volumes and overwrite transaction data. In a SAN or NAS environment, compartmentalization also limits the impact of error traffic or the equivalent of *broadcast storms.* In short, this technique prevents data corruption, snooping, and theft – whether intentional or advertent. Storage-related technologies for compartmentalization include LUN masking, zoning, file access privileges, virtual private networks (VPN), and firewalls.

No Peeking

Like a celebrity in disguise, ***encryption* keeps information private – even if it falls into the wrong hands.** When sending data over a public network like the Internet, the need for encryption is obvious. Enterprises do not want proprietary information moving openly in a public forum. Prying eyes could steal it and use it against the enterprise and its employees and customers. When data travels over a commercial or even private WAN link, the possibility of hacking still exists and encryption is a smart choice. How about within the confines of the corporate data center? Is data safe when traveling over a SAN or at rest in a storage array, if good compartmentalization is in place? Not necessarily. (See *Barbarians Inside the Gate*.)

The Genuine Article

No one wants to make a $10,000 deposit and have it appear on the next monthly statement as merely $1,808 because a bit flipped in the stored figure. So, *data integrity* is important. **An enterprise must be confident that data an application sends over a SAN is the same when it is stored – that it does not morph in flight.** When the application retrieves it a year later from disk or tape, the data must still be the same. There are effective techniques and algorithms for ensuring data integrity. They should be an integral part of storage networking and the storage devices themselves.

Members Only

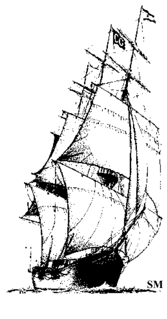
Related to compartmentalization is *authentication* – the means to ensure a person or device is who or what it claims to be. When users and administrators log in, they must provide a username and password or other proof that they are indeed that person. Similarly, **devices should be required to authenticate themselves before connecting to the storage network, whether servers or network devices.** Authentication prevents someone from connecting a rogue device to the network in order to gain access to data. It also prevents unintentional but nonetheless disruptive misconfigurations.

Barbarians Inside the Gate

When people think of IT security, they often think of preventing an evil computer genius from launching electronic attacks and viruses on an enterprise from a faraway location. But, in fact many, if not most, security breeches come from within. Disgruntled employees, unscrupulous persons with access to your facilities, and thieves breaking in the old-fashioned way are serious threats. These barbarians inside the gate can snoop the network, copy data onto a CD, or just walk out the back door with disk drives and tapes. **The only way to guard against the bad guys is to encrypt all data, whether on the network and at rest on storage devices.** So, even if they manage to steal important data, like all of your customer's credit card numbers, they cannot read it without the encryption keys. The good news is that technologies are available now that offer this level of real-time encryption.

Conclusion

With a realistic assessment of where vulnerabilities lie, one can then plug the holes, fill the gaps, and otherwise safeguard the crown jewels of enterprise data and storage. **And you will sleep better knowing that the risk of data exposure or loss has been minimized. More importantly, the enterprise will be free to pursue its strategic objectives without the hindrance of an exposed flank.**



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

***Michael Fisch* is Director of Storage and Networking for The Clipper Group.** He brings over eight years of experience in the computer industry working in sales, market analysis and positioning, and engineering. Mr. Fisch worked at EMC Corporation as a marketing program manager focused on service providers and as a competitive market analyst. Before that, he worked in international channel development, manufacturing, and technical support at Extended Systems, Inc. Mr. Fisch earned an MBA from Babson College and a Bachelor's degree in electrical engineering from the University of Idaho.

- ***Reach Michael Fisch via e-mail at mike.fisch@clipper.com or at 781-235-0085 Ext. 25. (Please dial "1-25" 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*, 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.