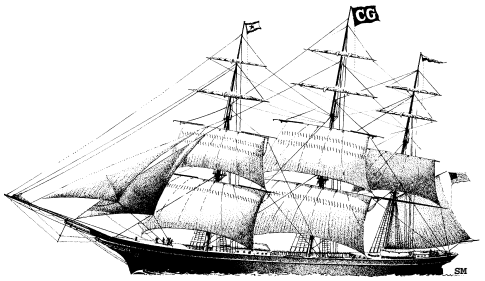
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2008015 February 28, 2008

Xceedium GateKeeper Mitigates the Risks Posed by Privileged Users

Analyst: Anne MacFarland

Management Summary

Securing the IT infrastructure that underpins business processes is, for everyone, a high priority. It is built into sourcing contracts; and it is featured repeatedly in government or industry regulations, such as PCI-DSS[1]. It is part of elementary good governance. However, as every CIO charged with securing an infrastructure knows, the challenge goes well beyond the physicality of the equipment. The applications must be secure – and the physical infrastructure must be secure from the threats that rogue applications and spyware pose. They must be secure from the threats posed by external networks and the Internet. Virtualization and application dependencies spread the domain of *mission critical* to encompass the whole of your IT environment.

However, there is still one more threat that is often overlooked. As Sir Edmund Hillary's conquest of Mount Everest would not have been possible without his Sherpas, no infrastructure would be kept up and running without its administrators, troubleshooters, and consulting engineers. These people are critical assets, but by the nature of their access, knowledge and capabilities, they are also a source of risk.

When IT came from a single data center, this risk was mitigated by the known identity of the people who worked with the system, as well as the known domains of infrastructure that they addressed. Now, however, with distributed infrastructure and multi-sourcing – factors of life at most organizations – the situation has become murky.

Business has never been free of industrial espionage. Unlike academic institutions (who have their own IT security problems, but they tend to be more localized), businesses must preemptively control IT risks – without affecting business or IT operations or the efficiencies of the personnel who tweak the infrastructure. A strategy of avoidance is not possible. The challenge is to track the changes to the IT systems in a way that discriminates between allowable actions (that must be optimized), suspicious actions (that must be delayed for analysis), and dangerous actions (that must be prevented). This is not something that can be tasked to humans. The consequences come too fast.

A Jersey City, NJ, company called Xceedium developed its Xceedium *GateKeeper* appliance to address this task. The Xceedium GateKeeper came to market in the Federal space, designed for compliance with regulations like SOX, HIPAA, CLBA, and FISM. It launched bristling with certifications – EAL2, EAL3, FIPS140 Level 2, and JTIC PKI/CAC, because its customers would not accept a security appliance without them. They have come up with an approach that can lock the gate on malfeasance while not constraining the regular operations of the infrastructure and its administration. For more details, please read on.

IN THIS ISSUE

[1] See *The Brave New World of PCI DSS - Why You May Need to Think Differently about Your Systems Architecture(s)* in the October 31, 2007, issue of The Clipper Group Captain's Log, available at http://www.clipper.com/research/TCG2007093.pdf.

The Extent of the Challenge

Risk aversion and constrained budgets have caused businesses of all sizes to reach beyond their boundaries for supplies, distribution of their products and, in some cases, outsourcing of IT functions. Corporate data is exposed on more systems than ever, and poses an attractive risk for external administrators who are now part of your infrastructure but extend beyond the domain you control.

Even within a single data center, securing IT infrastructure brings several special challenges:

- Technical staff must go where IT problems lead – and the trail is often long and convoluted – just the same kind of pattern as the behavior of malfeasance that you would like to prevent.
- You need to know everything they do to know what they have done. You need monitoring and reporting that can follow privileged users around the infrastructure. However, the plethoras of monitoring and reporting tools that exist are limited in scope. Even comprehensive tools lack the ability to capture and correlate events across systems that are the consequence of a *change* rather than an *event* (such as a fault). In most cases, the data points concerning interactive infrastructure access that are needed to provide this critical correlation are missing or woefully inadequate.
- Each point of instrumentation, and each upping of the polling frequency of that instrument, degrades the performance of the infrastructure. A heavy-handed solution is unacceptable.
- There is a large gap in vocabulary between the evidence that is gathered and an explanation of what did or did not happen that would be useful to an auditor. By allowing the aggregation of time sequenced forensics, the path of a technical user around the infrastructure becomes clear and interpretable by those without deep technical knowledge.
- Any gaps in visibility compromise the ability to validate that no risk has been incurred. *Almost good enough* security is inadequate. It is neither *good* nor *good enough*.

Xceedium GateKeeper

The Xceedium GateKeeper is designed to sit in every data center behind the firewall. The GateKeeper can impose granular access controls on both activities within the data center and those invoked by remote privileged users. The agents can enforce black/white lists of actions or destinations that may or may not be acceptable in strategic places, including virtual machines and fan-out locations, like *Citrix Presentation Server*.

Xceedium has a customer base that spans many industries. A considerable portion of its customers is in the U.S. Federal Government. Xceedium is just beginning to build its channel for indirect sales.

Data Center Level Controls

- GateKeeper authenticates technical users of the data center. They get unique IDs, where otherwise they might share an administrative account. Shared accounts limit forensics on the actions of an individual.
- GateKeeper denies to all users visibility of systems to which they do not have access, via a *Deny All Permit Exceptions* security model. This is better than a simple *need to know* principle of least privilege, which does not work well with technical users whose need to know depends on the nature of the problem they are solving.
- Complete monitoring and tracking of all user activity is supported. This includes CLI session recording. It can include capture of both unidirectional keystrokes, and bi-directional keystrokes and standard output.
- GateKeeper supports a centralized audit of all technical user activities. Activities can be sorted in many dimensions including by time (which is the most critical for nefarious actions).
- In addition, GateKeeper can support encryption of all interactive connections including serial and KVM systems. It can, using *Reversed Encrypted Tunneling Methodology*, secure communications from legacy devices, such as point-of sale systems, which by default, transmit in clear text. Due to their lack of programmability, such devices cannot encrypt, nor can they support an agent.

The Particular Peril of LeapFrogging

Single Sign On capabilities were a significant step forward in computer systems. But their prevalence means that if a privileged user can get access to an authorized element of an infrastructure, he or she can leverage that privilege to move about the infrastructure, bypassing local access controls. Xceedium GateKeeper'

Gatekeeper and the Special Perils of PCI-DSS

Xceedium Gatekeeper can help nail down some of the more difficult aspects of the U.S. PCI-DSS regulations that mandate security for credit card information and other forms of customer data.

- **REQUIREMENTS 2 AND 8** (disable defaults of system passwords and security parameters) is met by Gatekeeper's more granular, unique IDs.
- **REQUIREMENT 4** (transmission of customer data across networks) is addressed by its ability to encrypt clear-text transmissions when accessing remote devices.
- **REQUIREMENTS 6 AND 7** (separation of duties and restricting knowledge to need to know) are met both by Gatekeeper's DAPE security structure and by its *LeapFrog Prevention* technology.
- **REQUIREMENT 10** (tracking and monitoring) is what Gatekeeper addresses.

Source: Xceedium

patent-pending, socket-level *LeapFrog Prevention* controls prevent this by checking all requests for socket access that involve leaving the authorized element against a list of acceptable users and actions. With LeapFrog Prevention, even users with higher authorization levels cannot move beyond the systems relevant to their assigned duties.

The Challenges of Outsourcing

A service provider or service bureau that outsources the business applications for multiple business clients has the challenges described above multiplied. As customers become more aware of the dimensions of malfeasance, and of the ramifications of regulations, such as DSS (as shown in Exhibit 1, above), they may want a GateKeeper on the systems that support their business processes. Most service providers will wish to deploy them more generally, to ascertain what their technical users are doing to which systems.

Conclusion

Data Leakage is a growing problem for businesses. Whether you own a large data center with its own support staff, own a data center but hire people to come in and troubleshoot when something goes wrong, or outsource to a service provider, the privileged users that take care of your systems represent a substantial risk – and one that cannot be met by limiting their capabilities. Only by monitoring their actions and having the local power to enforce policy in context can this risk can be addressed most effectively. Consider your situation, and the risks that you run. Xceedium GateKeeper may address exactly those who worry you most.

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

Anne MacFarland **is Director of IT Architectures and Strategies for The Clipper Group.** Ms. MacFarland specializes in strategic business solutions offered by enterprise systems, software, and storage vendors, in trends in enterprise systems and networks, and in explaining these trends and the underlying technologies in simple business terms. She joined The Clipper Group after a long career in library systems, business archives, consulting, research, and freelance writing. Ms. MacFarland earned a Bachelor of Arts degree from Cornell University, where she was a College Scholar, and a Masters of Library Science from Southern Connecticut State University.

- ***Reach Anne MacFarland via e-mail at Anne.MacFarland@clipper.com or at 781-235-0085 Ext. 128. (Please dial "128" 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*, **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.