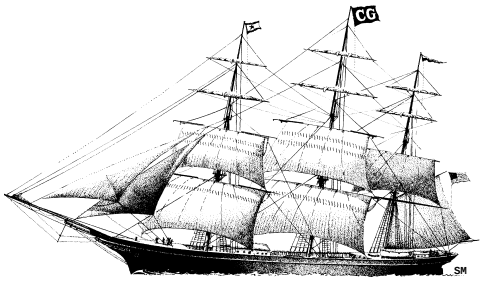
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2005034 June 1, 2005

IPLocks Polices Database Data Usage

Analyst: Anne MacFarland

Management Summary

When you are insulating a house, more is better, but cost/benefit and human quality-of-life issues usually dictate a solution that falls short of all that is possible. The same pragmatism also drives security risk management, but glaring risks should not be ignored just because they are hard to address, like enormous expanses of windows in houses in cold climates. Consider your enterprise information. You may think that intellectual property is a thing of formulas and a small collection of files. You may be focused these days on your email and whether you can discover and ameliorate all of the related risk exposures. **Nonetheless, your most externally valuable assets, and therefore your largest vulnerability, are the customer and production information in the databases of your enterprise. This is not information that can be protected by sequestering it from widespread use, for it is the widespread use that drives the productivity of the enterprise.** The speed of response time in normal use cannot be slowed too much, or that productivity will diminish. The information is much more granular than a file environment, and security features like encryption and digital rights therefore impose a larger performance penalty. Moreover, databases, unlike file-based kinds of enterprise information that gels to static information rapidly, are active in many dimensions. Users change, permissions change, new procedures are created and the data itself is constantly changing.

These inherent database characteristics make keeping up with vulnerabilities a continuous, rather than periodic, job. It starts with securing the physical environment, firewalls, and intrusion detection. Authentication and authorization strategies, a well as encrypting data both in motion and at rest, add robustness to the security strategy. Vigilant discovery of sloppy device and network configurations close down still more intrusion opportunities.

All these efforts do not and cannot address a significant source of risk – the opportunity for *authorized users* to misuse or misappropriate information. This kind of theft happens frequently, and represents, in insulation terms, not just a large window, but also a large window thrown wide open to the howling winds of winter. Most cases of theft of this type are not publicized, for the publicity would cost the enterprise far more than the money stolen off the books or the facts leaked to competitors. It is only when personal information is exposed and personal privacy is compromised that the story hits the news. Such cases are appearing in the news more frequently. It is past time to address the risks that authorized users pose to the enterprise.

One way to address this risk is by establishing patterns or profiles of authorized users, and then looking for breaks in the pattern. This profiling is what your credit card company does with your account to spot fraud expeditiously. IPLocks, a privately-held company based in San Jose, California, has focused its *Information Risk Management Platform* on addressing the risks to database information from both system vulnerabilities and authorized users. If, your processes depend on databases, this kind of security is an operational imperative. Read on for details.

IN THIS ISSUE

Database Vulnerabilities to Malfeasance by Users

It is difficult to address malfeasance by authorized users while maintaining the usefulness of the system. Writing – and administering, and evolving – policies to address the idiosyncratic work habits of individual users is not feasible in today's opportunistic work environments. Digital Rights Management can constrain use to what is reasonable, but can be circumvented by a determined, authorized miscreant. It is only by determining what is normal in reality, not in theory, and then alerting for deviations against that observed normalcy, that malfeasance can be promptly discovered. IP Locks cannot prevent malfeasance – only personal morality will do that. Nevertheless, it can discover it in near real-time, and the knowledge that discovery will be prompt is a great deterrent.

The Information Risk Management Platform

IPLocks' *Information Risk Management (IRM) Platform* integrates assessment of vulnerabilities, monitoring of user behavior, and auditing and analysis of logs. The platform includes the following:

- A content monitor, to alert for data corruption,
- A metadata monitor, to track structural changes and alert on vulnerabilities,
- A privilege monitor, to track invoked changed in privilege, and
- A transaction monitor, with drill-down capabilities, to track, alert, and explore suspicious transactions.
- An analytic engine to compare historical and current data, identifying anomalies, and to compare operations against best practices. This engine allows administrators to run SQL queries on the audit logs.

No matter how vigilant your database administrators, if your organization is constantly tweaking its databases, or many different populations are using the same database, it makes a lot of sense to have an independent check of these and other vulnerabilities on an ongoing basis. IP Locks has Vulnerability Assessment software to do just that, without impeding or impairing access to database data. The assessment looks for things like:

- Authentication and authorization loopholes.
- Orphaned privileges and surplus permissions.
- Inappropriate hardware configurations.
- Variably configured database instances.
- Inconsistent or inadequate patch levels.
- SQL injection attacks via stored procedures.

IPLocks' *User Behavior Monitor* collects the data needed to compile a profile of data usage by each authorized user. The monitor learns the vagaries of business cycles and employee roles, keeping an updated profile of what is normal for this person, in this role, at this point in the business cycle, for this organization. IPLocks can also extract data from older log files, even archived log files. The IPLocks-generated profiles become the standard for detecting unusual behavior as it happens, when counter measures may be effective.

IPLocks' *Audit Log Analysis* of the detailed monitoring gathers all the transactions related to an incident[1] (for malfeasance comes in many steps, as well as many forms). Together, these capabilities allow the full extent of damage to be known and addressed. Rules can be linked, and associated with actions, to give a chain of appropriate responses where needed.

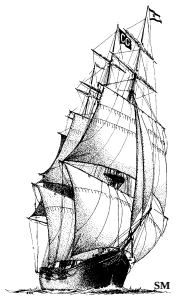
IPLocks' *IRM Platform* works with Oracle, IBM's DB2, Microsoft's SQL Server, Hitachi's HiRDB, and databases from Sybase and Teradata. Version 5.0 features a high-speed data collector to capture more information about user activities, a command line interface capability to allow secure implementation of unattended automated operations, and enhanced support for Teradata environments.

IPLocks early clients have been, not surprisingly, in the Financial Services industry. It has channel partnerships with BMC, Hitachi, NEC, and Unisys. It has technology partnerships with IBM, Oracle, Sybase, and Teradata.

Conclusion

IPLocks can protect against data corruption as well as data theft, and adds another much-needed layer to your enterprise's protection of database data. Its capabilities meet the needs of many government regulations, and ease a significantly difficult area of corporate governance. The detailed analysis it allows can be helpful in optimizing partner and supplier relationships.

Constant vigilance against external threats and consistent profiling of authorized usage is a complete strategy to allow an enterprise to get the most out of information assets without exposing them to flagrant opportunities for misuse. IPLocks' profiling might be just the thing you need to complete your database security strategy.



[1] If data is copied, that is documented. If data is altered, the extent of the alterations made at a particular session, or by a particular user, can be known.

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 Infrastructure Architectures and Solutions 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*, **The Clipper Group Voyager**, 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.