



White Paper

Security at the Heart of B2B E-Transactions

“The most sensitive data for commercial web sites will usually reside in databases that exist behind the corporate firewall. Clearly, the database holds the jewels in the Web site’s vault. For this reason access to the database must be carefully controlled.”

Anup Ghosh – *E-Commerce Security; Weak Links, Best Defenses*

“Given that the majority of corporate data is stored in databases, database security weaknesses are of greater concern than operating system weaknesses. Yet most companies still do not appreciate the severity of these risks.”

Hurwitz Group, “Databases have security weaknesses too” - August 14, 1998

Executive Briefing

In the wake of disappearing Y2K concerns, companies are now facing another set of business challenges, namely how to secure their rapidly growing business-to-business e-commerce.

“The worldwide B2B market is forecast to grow from \$145 billion in 1999 to \$7.29 trillion in 2004. By 2004, B2B e-commerce will represent 7 percent of the forecasted \$105 trillion total global sales transactions.” GartnerGroup, January 2000.

Whether your company is a ‘.com’ or a more established enterprise, today’s business goal is to leverage the power of the Internet, thereby increasing your business possibilities, lowering your costs and maximizing your productivity. Of course there are associated challenges with such a transition, not least of these is the challenge posed by security concerns. If the leap from mainframe to client/server architectures provided a more flexible yet vulnerable environment, then the addition of the Internet portal provides a quantum leap in the same direction. In the B2B E-commerce world, all of your partners and customers (as well as your employees) will have on-line access to information generated by your internal systems. Security becomes of paramount concern, not just for the new e-commerce sites but also for the legacy architectures that have become ‘e-enabled’.

What are the repercussions for inadequate security in the e-business world?

-Consider the business issues facing CDUniverse after it was revealed that a hacker penetrated their site and accessed credit card numbers which were then posted publicly on the Web. ([PC Week Online](#), January 14 2000)

-*“EPA’s failures in this area have placed at risk hundreds of millions of dollars in agency computer systems and databases, the sensitive and confidential data maintained in those databases, as well as the resources and data of other federal agencies connected to EPA’s systems,”* Rep. Thomas J. Bliley Jr., Chairman of the House Commerce Committee after hearing of serious security problems the EPA’s information systems. ([USA Today](#), December 1999)

The transactions that occur over the Internet, commercial or not, are all driven by data. Whether an organization creates a new e-business architecture or integrates its pre-existing environment with the Internet, more likely than not the data source will be a relational database. This is true for a commercial transaction or for employees accessing data through the Web client of a CRM or ERP application. Security of the relational database should be a principal part of your B2B security strategy.

When considering the best strategies to secure an Internet enabled database, corporations must draw as many parallels as possible between the Intranet application and client/server or legacy applications which are being replaced or supplemented. While the Internet does pose some unique security considerations, many long held security policies already in place within the enterprise are extendible to Internet security. In fact, the strategy which is eventually implemented must be able to manage access and authorization for e-commerce as well as the ‘click and mortar’ applications that will continue to leverage the databases internally.

The B2B E-Security Market

As the B2B E-Commerce market explodes, so will the security community, in fact it is already occurring. After all, businesses and consumers will only take advantage of Web-enabled transactions if trust, integrity, availability and non-repudiation can be assured.

The information security market, or rather information security marketing, is dominated by 'hot' Internet enabled security technologies such as PKI and Directory services. In theory their ability to centrally handle authentication and access control for distributed systems provides huge advantages in the enforcement and management of security controls. In practice very few implementations have yet been completed successfully, and when they are, they will most certainly have to integrate with a number of 'point solutions' which control certain areas of the new and legacy environment and address other issues such as auditing and policy management.

Firewalls are perhaps the most mature security products that exist in this new market space. Firewalls are an important part of a company's security make-up but, in the connected world of e-business, clients and remote employees need to be *and will be* inside this perimeter control and therefore the firewall is only one of many solutions in other areas that must work in tandem. The business driver behind this requirement of flexibility and interoperability is the nature of the e-business transaction itself.

"An e-business transaction is an instance of cross-application business processes split into subtransactions, each of them running on different infrastructures," Alain Dang Van Mien – Gartner Group, "Shift in IT Security: Business Needs Secure E-Transactions", 1/11/99.

When it comes to securing today's multi-tier E-Business environments a strategy must be developed which takes into consideration all potential points of exposure. Those risks must be addressed point by point. Begin where all roads lead - the database.

Relational Databases

Ultimately, an E-Business transaction will result in a select, insert, update, or deletion in a database such as Oracle, DB2, Sybase, or MS SQL Server. The major ERP, CRM, BI, or SCM products already utilize an RDBMS to house information assets. Now EAI and E-Business initiatives are allowing applications to share information and resource access to business partners and customers.

"While Net markets make it easy for buyers to find suppliers and complete transactions online, those things do not happen in a vacuum. They are driven by data, forecasts and analyses housed in and created by ERP and supply-chain systems. That intelligence represents the true keys to the e-business kingdom". Internet Week, 1/10/2000

Enabling access to this information via the web adds a new access path additional to the client/server (two-tier) access that has and in most cases is still being used within most environments. By not properly protecting the database, the integrity of a corporation's most valuable asset is left precariously exposed.

Four A's (Forays) into E-database Security - What issues should be considered when securing an e-database?

Authentication

Despite the proliferation of PKI and CA solutions in the Internet world, the relational database remains as a point of authentication for a user. All Databases have accounts that are accessible via two-tier access paths such as ODBC or the Database's own proprietary network protocol. It is vital that monitoring is carried out at the database level for both successful and unsuccessful access. When this is done, strategies for automated responses, such as disabling an ID that has accumulated numerous logfails can be enacted. (This must be done carefully however, because disabling an application ID because it has (for example) 5 logfails against it could result in a disruption of service to hundreds of users.) In all cases, some form of notification (i.e. pager email) needs to be in place to push security event information to those who need to know.

To mitigate the risk of a password guessing attack, all database passwords need to be frequently changed and well chosen. Strong authentication controls should also include a review of all user accounts, and a justification for their existence should be done periodically. For example, accounts that have never been used or have not been used in an extraordinary period of time should be disabled and possibly removed; this will reduce the number of potential attack points.

Access Control and Authentication for Applications

In 3-tier environments an application server may be used to manage application access to the database on behalf of users. This proxied access may occur via pooled processes that remain connected to the database and to which users are connected as required by the application server's transaction management features. At startup time, the application server establishes network connections to the database and in many cases the connection information (username/password) is kept in plain text within an application server startup or configuration file. It is at the application server level that the business logic, which controls the application, may be deployed and must be protected.

Authentication may also be done at the application server level, in which case yet another file or table of usernames and passwords must be maintained and protected. When authentication and access control are deployed on the middle tier, policies and procedures dealing with such things as password management and user administration must again be deployed. An application server in a 3-tier architecture provides tremendous benefit in the development, deployment and performance of the application. A breach in security at this level could cost all that and more.

Auditing

Understanding the way in which the RDBMS back-end is supposed to be accessed is vital when trying to mitigate risk: Most 3-tier architectures use transaction processing via pooled connections from the application server or middle tier to the database back-end. The resulting application "fingerprints" on the database are thus made by a single or few application IDs on behalf of the larger number of users whose transactions are being managed by the middle tier. Knowing this, a database auditing strategy, looking for activity by ID other than the application Ids, may indicate a back door attack via an access path distinct from the application. A database auditing strategy should also include checks to validate the integrity of the business rules within an application. This should also be performed on any application security tables that are maintained within the database in order to ensure that manipulation of security or business rules is not taking place via the back door.

Administration

Databases are typically accessed by administrators through the underlying operating system, yet no one person or group should be entirely responsible for database and security administration. A separation of responsibilities segregating application and database security admin. from database and operational admin. provides the necessary checks and balances to ensure that no loopholes (intentional or not) are opened. A strategy to securely delegate security administration by task (i.e. password resets), as well as by scope (i.e. the groups of users for which a given admin. can reset a password) is most likely in place for other areas of the computing enterprise. That strategy also needs to be executed at the database or application level.

The operating system platforms on which the database resides (a.k.a. Database Server) must also be evaluated for weaknesses, which could lead to unauthorized database access or manipulation. Initialization files containing database configuration information and database startup/shutdown scripts are amongst the server level resources which should be properly protected to ensure the integrity of the database environment. In some database environments, membership in certain OS groups allows complete control over the database. A justification of those users requiring membership or access to the database at this level needs to be performed regularly.

Conclusion

A relational database lies at the very heart of an e-business transaction or architecture.

Most E-business applications are extensions of client server applications that have been in use for a couple of years, and will remain in use for some time to come. Security products are required that can protect the database in existing environments as well as those that are now being opened up to E-business. The solutions need to extend to meet the additional security management requirements which e-business presents *and* allow customers to quickly deploy robust security solutions that work with existing security concepts and frameworks.

Information on BrainTree Security Software's suite of relational database products for Internet and Client/Server applications can be found on **www.braintreesecurity.com**, or may be obtained by calling +(781) 982-0200.

BrainTree was acquired by PentaSafe Security Technologies, Inc. in July 2000, and now operates as a division of PentaSafe. PentaSafe Security Technologies, Inc. provides software solutions that secure and protect key operating systems, applications and data that drive the digital economy. PentaSafe's VigilEnt Security Management Solution allows companies to audit, assess, secure and protect heterogeneous IT environments from a single point of control. Visit www.pentasafer.com for more information.



BrainTree Security Software, 200 Cordwainer Drive, Norwell, MA 02061-1671
Tel: 781-982-0200 Fax: 781-982-8076 E-mail: info@bti.com
Web: www.braintreesecurity.com or www.pentasafer.com

PentaSafe, VigilEnt, SQL<>SECURE and BrainTree are registered trademarks of PentaSafe Security Technologies, Inc.
Third Party Trademarks: * All trademarks are the property of their respective owners.