The Granular Protection Solution for Databases

Author: Ulf T. Mattsson and Ulf G. Dahl, Protegrity, Inc.

As we head into the 21st century, organizations must consider information threats. Simply, step one would be that all-sensitive data should be classified as important and relevant access restrictions and granular protection should be enforced. Or consider that all laptops, desktops, and peripherals should be physically and logically secured after business hours. Most importantly, users should be required to utilize file- or data-item-level passwords on files containing sensitive or confidential information.

Why do we need to Protect Sensitive Enterprise Information?

Corporations own many different assets, some appear on the balance sheet and some do not. Any Corporation owns valuable Information assets often stored in a computer-based environment: customer lists, personnel data, product specifications, strategic plans, financial information. These assets have been hidden within internal systems, but with the advent of networks this information becomes exposed to outside intruders as well as to unauthorized internal personnel. With information increasingly becoming a critical factor in the performance and competitiveness of most organizations, availability of that information becomes ever more important.

The technology used to manage information is changing continuously. The move towards client/server, laptops, distributed and open systems, together with downsizing and the need to introduce new systems into existing structures while maintaining an acceptable level of security, present real technical and economic challenges for Company management and security professionals.

Successfully implementing an effective enterprise-wide information security policy is difficult enough. To do it over multiple systems, databases and different platforms each with a mix of legacy and new systems in existing structures it is even more challenging. When you add multiple sites and laptops together with professional professionals it can become a real headache. These issues are just not the responsibility of the IT Department either the security of the Company sensitive information ultimately lies with the Board, which is responsible for all the company's assets, including its data. For most organizations this means that an individual's access rights are often out of control, and there is no easy way of checking who has access to sensitive information in which systems. It can also be hard to provide a new employee with suitable rights for his role, or indeed to remove someone's access rights when he leaves to company. The most common form of intrusion today is an insider compared with outside intruders.

Evaluating and Improving Information Security

Like any other significant asset, you need to protect your information. Data-level security enables you to evaluate your security controls, improving the effectiveness of security measures, and designing an effective security architecture. Data-level information security methodologies focus on the sensitive information security and on the complexities of today's emerging distributed environments including technologies such as electronic commerce, client/server, laptops, the Internet and Intranets.

Information Security Requirements for Client/Server Computing.

The move to client/server, decentralized processing environments is a change that nearly all organizations have undertaken over the past few years. At the same time, organizations struggle with finding the right mix of centralized or decentralized security administration. The conflict between the benefit of easy access to information inherent in the client/server computing environment and the need to protect and secure corporate information requires a new generation of security solutions.

These solutions must be specifically designed to function in large scale, multi-platform computing and databases environments, while providing the same level of protection and security functionality expected of mainframe-level information security. Information security is more than passwords, data encryption, and Internet fire-walls. Information security should be determined by needs of the business, not dictated by limitations of particular technology. Business managers, not just Information Technology managers, must be able to control the level of security on their systems, as well as determine the status of information security in their enterprise at any time. In the end, while there have been improvements in security administration, organizations continue to struggle with finding the right balance of centralized and decentralized security administration.

Protegrity

Client/server computing has empowered users by putting information at their fingertips. Making sure that appropriate information reaches those fingertips is the difficult challenge we all must face. The security infrastructure we have become used in centralized mainframe environments is still nascent in the distributed computing world. **Protegrity** vision is to solve this problem by providing a comprehensive information security solution for client/server computing.

Protegrity is protecting information assets on mainframes, servers including Web servers and workstations including laptops which is critical to the success and productivity of any enterprise.
The primary goal of **Protegrity** management is to provide a solution for protecting database information in a role-based distributed client/server security management which incorporates, integrates, exploits and extends the best aspects and functionality of **Protegrity**. **Protegrity** provides a granular protection of sensitive information defined initially across multiple flavors of databases. IBM Universal Data Base (Extender), Oracle 8.x (Data Cartridge), Informix Universal Server (Datablade), Microsoft SQL (Server Snap-in) will be supported by Protegrity.

Protegrity provides a highly secure approach to accessing and segmenting sensitive data. Using Role Based Access through to the Data Element Wrapper down to data element level, **Protegrity** takes a granular approach to information security that is not limited to protecting groups of data or transactions, but can also actually secure the individual pieces of data. This approach prevents penetration, internal or external wherever data is stored.
The **Protegrity** solution allows dynamic and real-time management of the Security System providing full database protection at a Data Item level across major platforms.

Protegrity brings together existing security systems and databases through database exits, providing a single or a multiple point of security administration and control(Central Security Consoles) which is independent of protocols, databases and platforms used.

The Solution Provides - Key features:

- Allows you to implement a comprehensive, consistent security policy across your enterprise using a role-based access control model.
- Enables easy implementation of enterprise-wide security policy and rules.
- Single or multiple point of security administration and control via a central security console. This gives security administrators the ability to administer users across disparate computer platforms, and it provides network-wide identification and authentication, and allows users to sign on to the network and automatically gain secure access sensitive information.
- Flexibility to centralize or selectively distribute security administration tasks in a protected environment to target systems.
- Homogenous auditing and revision of all target system defined with sensitive information --lets administrators tailor the optimal audit trail to meet their needs. Administrators can select events and information resources they want to audit, as part of the security policy, and what log: only successful resource access and/or system log-in attempts, only attempted violations, or both. **Protegrity** complements its compressed detail logs with tamperproof and encrypted information

and an interactive tools, letting authorized auditors analyze the audit data easily and effectively. In addition, **Protegrity** Management system protects its own audit files and security parameters by encryption and unauthorized modification, ensuring the reliability of the audit trail.

- Ensures Integrity of all Database Information.
- Uniform, protected and consolidated compressed logs selectively from target systems across all platforms
- State of the Art, Graphical User Interface with drag and drop facilities.
- Automatic transfer of **Protegrity** security parameters to the target systems.
- Trusted Programs. **Protegrity** provides Protection against virus and unauthorized programs and versions.
- Ability to selectively Encrypt Information with the Data Element Wrapper level through the Crypto-Conductor process.
- Distributed Key Management System. Key management, Generations of keys and exchange of key parts of encrypted keys.
- Super-ordinate and uniform logic. The independence of the **Protegrity** logic from target systems enables the definition and realization of a comprehensive, enterprise-optimal security strategy.
- Controlled centralized and/or distributed administration. Security administration tasks are carried out in the optimal place from the enterprise point of view: decentralized within departments, or centrally through the central security console. Discrepancies are eliminated and acceptance is raised. The central security console is protected by encrypted databases.
- Multiple client capability. Precise separation and optimization of security administration for different organizations through the multiple client capability from **Protegrity**.
- Users group and group hierarchies and User role models. With grouping and modeling functions and create roles or roles in processes, **Protegrity** allows for the definition and realization of organization, rule based and/or process/function oriented information access and protection concepts. An economic and flexible security policy is realized independent of the connected security system, databases and according to the requirements of the company.
- Models for resources, resource groups and target systems. Through the security administration of resources and target systems according to pre-defined models, the time consuming repetition of entering the same definitions and security parameters is avoided.
- Initial load. The automatic integration and transfer of security definitions from productive security systems with **Protegrity** enables the flawless transition to security administration by **Protegrity**.
- Postponed events. The timely execution of security administration activities guarantees the flawless and punctual granting and revoking of information access rights.
- Consistency maintenance. Possible inconsistencies of security definitions between **Protegrity** and the administered access control system are tracked down up to the user level, and, according to the setting are either documented or corrected.
- Generators for the integration of new target databases. The **Protegrity** supports the quick integration of other standard target databases and customer-specific homemade developments in the complete solution by using pre-processors.
- System-wide reporting. **Protegrity** enables the person responsible for revision and auditing to have a complete and flawless overview of users, access rights, selected sensitive information and resources at any time.
- Internal **Protegrity** security mechanisms. The different security levels of **Protegrity** guarantee consistent and controlled security definitions for all integrated target systems at all time through the run time applied to the target system.
- Openness for the exchange of data with personnel systems. Users defined in the company personnel system is a customized option in **Protegrity** and automatically passes on to and added to **Protegrity**.
- Openness for the integration of single sign on and password synchronization systems. The combination of the best software solutions available in the market and **Protegrity** offers a highly effective security mechanism, especially in heterogeneous and decentralized environments
- Trojan Horses Protection. **Protegrity** prevents, in real time, attacks such as Trojan Horses or back doors. **Protegrity**, with the Trusted programs function, intervenes before execution of any

privileged program and verifies that the program can be trusted and has not been tampered with in any way. By using a random cryptographic checksum on the program load module any suspicious change, known and unknown virus or tamper attacks, will be detected. **Protegrity** prevents its execution, locks the untrustworthy program out and send alarms immediately to the security console. The Detection process can be automatically programmed into each target system and be executed flexible.

The Granular Protection Solution for Databases

Using Role Based Access to the Data Item, level, **Protegrity** takes a granular approach to information security that is not limited to protecting groups of data, but can also actually secure the individual pieces of data or requests. This function is called The Data Element Wrapper and will provide the ability to a granular protection of data Item, groups of data, SQL queries and WEB actions. This approach prevents penetration, internal or external, wherever data is stored or transported.

How does the solution work ?

Protegrity's secure.manager runs on an NT server in a separate protected environment from your target systems (application servers).
Its open architecture allows for the full integration to defined sensitive information in your existing databases or files, without modifying the target applications themselves. This integration is done through certified procedure, Informix Datablade, Oracle Datacartridge and IBM Universal Database. Its main advantage is that it consolidates all security maintenance and activities into one unique protected environment. Initially extracting all security-related parameters into your application systems, **Protegrity** will pilot all activities on defined sensitive information. The Data Element Wrapper, contains manages all security parameters information on how to provide a granular protection of information using Data Authentication Code or the Crypto Conductor for Encryption when stored in the database or transported on the net.

Single Set of Rules Enterprise Wide

The role-based access functions in **Protegrity** have a set of characteristics and set of functional requirements. The characteristics are actions that can be placed on data or systems (verify, log, change, administrate, identify, search, update, create). The functional requirements define a users profile (identify, safety, level, enterprise level, ownership, status, relation to roles/views, authority(role), profile(role)).

Central Security Console Administration

The Central Security provides a single or multiple point of control for selected security related activities throughout any given Enterprise. It provides full management control over authentication, authorization, encryption and data access, as well as advanced control of all security parameters and transactions.
Having built up a set of security rules and activities, **Protegrity** automatically creates the definitions appropriate for each connected target server systems, and securely passes these definitions over to them for execution (runtime). The individual target systems own security facilities and know the rules then carry out the access control as normal.

Protegrity Secure Audit

Protegrity provides comprehensive customized audit reports and logs, imported from target system **Protegrity** databases. **Protegrity** consolidates logs selectively from each target system and provides compressed log information including read accesses. All log and journal files are produced and encrypted locally on each target system. All operations from the Central Security Consoles are included in the log files which provides a full range of reports identifying control weaknesses, security breaches attempts, checking consistency of sensitive information in target systems. And providing users, resources and authorizations to assist security professionals in their daily work.

Protegrity Security Tasks

Protegrity provides a common security administration for different databases on various platforms. **Protegrity** produces a standard administration structure that would not require the security administrators to have specialized knowledge of these systems with exception for integration with database field descriptions. **Protegrity** enables expandability to new databases and security systems and assure extensive automation and standardization on administration procedures.

Protegrity Benefits to The Business

There is a number of technical solutions that makes networks and operating systems more secure. But information security cannot be achieved by technical measures only. Security begins with measures of organization such as control of authorities and access rights, deputation rules and rules on using passwords. Organizational measures also include responsibility to outside networks. Different security standards applied to different areas within the enterprise defeat the purpose of some of the investments made in security of the network.
Security can only be achieved with interplay between the human being and the technology and, with regard to the network environment, can only be seen as a whole. Partial solutions cannot achieve the desired success.

Through the ability to apply a consistent security standards and information protection across the whole organization.

Protegrity is flexible enough to allow the administration of specific roles and or processes to be devolved to local business unit or a data item. This means that business areas can control their own users with a distributed central security console without requiring technical knowledge of underlying security mechanisms, or weakening the overall information security.

Protegrity helps reduce business risk through inadvertent or malicious damage to business critical systems, information and resources. The use of **Protegrity** for administration across all systems and databases minimizes the possibility of unauthorized access; for example by a contractor or end-user who may already left the company. Likewise, where a user changes business roles, **Protegrity** will ensure that their information authorization also instantly changes to reflect their new role or roles. Security features currently supported on all platforms such as multiple signatures can be implemented across all systems. End-users can quickly be given the freedom to access company sensitive information they need to use to carry out their jobs. **Protegrity** enable this while remaining completely transparent to them.

Protegrity Administration

The global rules structure only needs to be defined once and there is no data re-entry needed. This reduces the overall administrative burden supporting security on multiple systems and databases at multiple sites. **Protegrity** manages all the corporate sensitive information from one screen, the central security console, so you only need to learn the one system. Through this central security console administration and control and the time closure of security actions you do not need to remember to close them.

In these times it seems that everyday their are new security products and databases on the market. When your organization and security needs to grow, **Protegrity** will grow with them. **Protegrity** have a close partnership with IBM, Informix, Oracle and other key vendors and future development of

Protegrity will concentrate on integrating new target platforms, supporting **Protegrity** to additional platforms and adding functionality.

Protegrity increases Internet security, in real time, attacks such as Trojan Horses or back doors. **Protegrity** role based access intervenes before execution of any privileged user access or application program and verifies that the user or the program can be trusted and has not been tampered with in any way. If any suspicious access or change in the program is detected **Protegrity** prevents its execution, locks the user from accessed information and the untrustworthy program out and sends alarms immediately. **Protegrity**, Data Element Wrapper, provides a light firewall for each defined sensitive data item, SQL request or WEB action and protects information wherever it is accessed. The Data Element Wrapper also has the ability to provide information protection utilizing The Chrypto-conductor for encryption or data authentication. Selective encryption down to the data item level is an option that **Protegrity** can provide if your demands for extended security is a need.

Intranet

The Intranet is just now a revolution for internal communications within Europe's largest corporate. The Intranet delivers, on the promise of client/server computing, information to the individuals that need it irrespective of platform or geography. For large multi-national corporations improved internal communications translates directly into the bottom line. The Potential of the Intranet as a platform for the rapid development and deployment of group-ware applications was widely recognized amongst the companies. The key advantages cited were the openness and flexibility of the Intranet platform as both group-ware. Intranets are proving to be increasingly popular means of communicating and distributing information throughout the organization. As more and more organizations create and piece together the infrastructure for these types of networks, it is likely that concern regarding network issues will remain at high levels. **Protegrity** enables organizations to enforce the same security level on sensitive information on The Internet or on Intranet solutions.

Protegrity Protecting WEB-servers

Securing systems and data in a distributed world is an increasingly complex issue, and software products alone are not sufficient. An effective information security solution also must manage WEB server security, control access, detect intruders, protect information, and administer all kind of users such as customers, partners e.g. The operating systems of most distributed computing platforms and most third-party products generally address only some of this needs. **Protegrity** will provide centralized robust security management both for heterogeneous and non-heterogeneous environments in a client/server and WEB server-computing environment.

The **Protegrity** has together with Netscape developed functions that create a high level of security needed for company sensitive information.

The WEB server protection is a part of the growing requirements for comprehensive security solutions for the enterprise. **Protegrity** addresses the growing requirements for comprehensive security solutions as organizations migrate from centralized, proprietary computing platforms distributed to client/server environments.

Protegrity Central Security Console, features

Client Information, integration to customer systems

Organization and Geographics, Role based information, organization and company information

Configuration, **Protegrity** target systems

Smart card administration

Certification Security Administrators, **Protegrity** IAM

Integration Access Control Facility systems and **Protegrity**

Data **I**tem Protection in target databases

Trusted Programs in target systems

Log and Alerts from target systems

Reports and Agreements from target systems.

###