U.S. Defense Department Requirements for Information Security

Kevin J. Fitzgerald
Oracle Corporation

Wednesday, 1 May 2002
Industry Plenary: 8:00 - 8:45
Ballroom

The events of 9/11 have resulted in a heightened awareness of the importance of information security. Paradoxically, there is a greater requirement than ever before for military, intelligence, and law enforcement entities to share increasingly sensitive data, yet enforce stringent information security policies to protect their critical infrastructure. The security of these information systems must meet the technical challenges of a diverse user community: need-to-know enforcement, interoperability, secure communications, and high availability, as well as offering independent measures of assurance required by federal directives (e.g., National Security Telecommunications and Information Systems Security Policy No. 11).

The importance of information security has increased substantially in the past few years, primarily due to the growth of the Internet. The events of 9/11 have resulted in a heightened awareness of the importance of information security in several key ways.

There is a greater need for information sharing than ever before to enable disparate intelligence, military, and law enforcement groups to selectively share information, yet maintain "need-to-know" provisions required by national security. There is an increased awareness of the threats posed by information warfare; without ever firing a shot, enemy forces could launch a cyberattack on a nation's critical infrastructure, thus rendering a foe helpless.

The importance of information security to the U.S. armed forces is thus both old and new. Its importance is old in that the problems of information security are, as they have always been, related to the confidentiality, integrity, and availability of information (the "CIA" of traditional information security). Its importance is new in response to cyberwarfare threats, the sheer volume of computerized information, and the numbers of people accessing it. U.S. Department of Defense (DoD) requirements for information security include all of the following:

- Large diverse worldwide user community.
- Coalition forces' need for interoperability.
- Enforce "need-to-know" while enabling greater data sharing.
- Highly secure communications.
- Stringent auditing requirements.
- Users access to multiple systems to carry out their mission.
- Critical nature of many defense systems requires 100 percent uptime.
- Independent measures of assurance as required by federal directives.

An explanation of each information security requirement follows below.

DoD Information Security Requirements

Large User Communities

The DoD represents an extremely large diverse worldwide user community. The sheer size of the user community accessing defense systems via the Web not only increases the risk to those systems, but also constrains the solutions that can be deployed to address that risk. Moving applications to the Web creates challenges in terms of scalability of security mechanisms, management of those mechanisms, and the need to make them standard and interoperable. Whereas the largest traditional enterprise systems typically supported hundreds of users, many Web-enabled defense systems have potentially thousands of users.

> *"Without ever firing a shot, enemy forces could launch a cyberattack on a nation's critical infrastructure, thus rendering a foe helpless."*

Interoperability

Unlike traditional defense systems where a command or program owns and controls all components of the system, Web-enabled systems must exchange data with systems owned and controlled by others, e.g., other commands, suppliers, coalition forces, partners, etc. Security mechanisms deployed in these systems must therefore be standards based, flexible, and interoperable to ensure that they work with others' systems. They must support thin clients and work in multitier architectures.

Enforce Need to Know

Allowing greater access to data while enforcing need to know means that access control must be enforced on the data to ensure that the same security policy is enforced regardless of the method of data access. This requires a high degree of granularity in traditional access control mechanisms, as well as the ability to compartmentalize data access based on an application-specific security classification. (*Application-specific* meaning that organizations may have different data labeling requirements, and thus cannot necessarily use a fixed-labeling scheme across every organization that needs access to the same data). Real-time information sharing requires real-time or near real-time reclassification of data, so that, as threats change, information can be both shared and segmented among the multiple constituencies who need access to it.

Secure Communications

The sensitive nature of communications within the armed forces requires that even ordinary communications provide encryption for confidentiality and data integrity to ensure that communications are neither intercepted nor modified in transmission. Furthermore, large-scale encryption of stored data is generally a bad idea (as it does not address access control issues, gives users a false sense of security, and slows down system performance). However, there is a requirement for selective encryption of some stored data as an extra layer of protection, for *defense-in-depth*.

Stringent Auditing

The more sensitive the data, and the more users with access to that data, the greater the requirement to hold users accountable through auditing. Unfortunately, a number of serious security breaches involving national security might have been prevented had proper auditing mechanisms been enforced. Auditing must be granular enough to focus upon a particular activity, user, or object, and comprehensive enough to record *all* user activity of interest, yet have minimal impact on performance. Auditing must also be tied into an alert mechanism to provide administrators with timely information.

User Access to Multiple Systems

Traditional mechanisms used to identify users and manage their access like granting each user an account and password on each system they access are not practical in a large interconnected environment such as organizational intranets or the Internet. It rapidly becomes too difficult and expensive for system administrators to manage separate accounts for each user on every system. There is a greater requirement for both strong user authentication – due to the increased amount of information users are able to access – and central identification and management of users due to the prohibitive cost of managing access for thousands if not hundreds of thousands of users across multiple systems. Furthermore, in the case of non-centralized account and privilege administration, shutting down or restricting a user's access in the event of a suspicious security event or security breach is time consuming. It also exposes the systems to additional breaches while the administrator is required to access and modify each separate system.

Availability

System availability is critical due to the nature of the mission of the U.S. armed forces. More than perhaps any other consumers of information technology, DoD systems require 100 percent uptime. For most commercial organizations, information unavailability during system downtime may be inconvenient and costly but not life threatening. For the armed forces, information availability may literally be the difference between mission success or failure and life or death.

Information Assurance

U.S. federal directives such as the National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, (see <www.nstissc.gov/Assets/pdf/nstissp11.pdf>) require information systems that access or manage information related to national security to have *independent* measures of information assurance, as evidenced by formal, independent (third-party) security evaluations. Acceptable criteria against which products may be evaluated include the Common Criteria ISO-15408 (see <http://csrc.nist.gov/cc/ccv20/ccv2list.htm>), the de facto worldwide evaluation criteria, and the Federal Information Processing Standard (FIPS)-140 (see <http://csrc.nist.gov/cryptval>), which attest to the correctness of cryptographic mechanisms.

> *"The more sensitive the data, and the more users with access to that data, the greater the requirement to hold users accountable through auditing."*

In the past, procurement vehicles specified formal security evaluations. Many requiring a solution compliant with the Trusted Computer Security Evaluation Criteria (see <www.radium.ncsc.mil/tpep/library/tcsec>) or an Evaluation Assurance Level 4 (EAL4), as defined in the Common Criteria, were often granted waivers for this requirement based on functionality requirements that were not supported in the evaluated versions. Procurement waivers (from NSTISSP No. 11 requirements) will likely – and rightly – be much harder to acquire in a security environment after 9/11. Security will play a stronger role in the tradeoff analysis between security and functionality.

This article describes both the appropriate technical measures as well as specific security mechanisms that can address the above requirements (in general terms). Since many Web-based information-processing systems are built on database management systems, the technical solutions will be presented in terms of the protection of information stored in database systems.

Technical Solutions

Large User Communities

Most organizations face daunting obstacles in user management. Users within an organization often have far too many user accounts, with each system that controls sensitive material having a separate authentication procedure. This problem has been exacerbated by the growth in Web-based self-service applications – every other week, users have a new user account and password to remember. Organizations who want per-user data access and accountability do not want the administrative nightmare of managing users in each database or application users access. An organization opening its mission-critical systems to partners and customers does not want to create an account for each partner in each database the partner accesses; yet per-partner privilege and per-partner accountability is highly desired.

An increasing number of products view directories as the best mechanism to make enterprise information available to multiple different systems within an enterprise. The trend toward directories has been accelerated by the growth in use of the Lightweight Directory Access Protocol. These directories contain the user's identity information, as well as their roles and privileges to perform operations. Enterprise roles, roles that are defined across an enterprise and that apply to multiple applications, enable strong centralized user authorization. Also, an administrator can add capabilities to enterprise roles (granted to multiple users) without having to update each user's authorizations independently.

Storing this information in a central repository allows the administrator to grant and remove privileges that impact all of the organizational resources. Directory information that specifies users' privileges or access attributes is sensitive since unauthorized modification of this information can result in unauthorized granting or denial of user privileges or access. A directory that maintains this organizational information must ensure that only authorized system security administrators can modify privileges or access directory information.

Secure Communications

Communication mechanisms must support both confidentiality and data integrity requirements. It is important to secure the communications against network snooping and data replay or modification (altering data on the wire or removing information during transmission). Network encryption, including both confidentiality and integrity algorithms, is a standard method for ensuring secure communications.

In the case of client-server Web-based applications, it is important to support encryption from the client browser to the middle-tier Web application server. Using Secure Sockets Layer Version 3 (SSL V3) has become accepted technology for this purpose. SSL provides authentication, integrity, and encryption services using public-key encryption.

It is also important to support encryption from the middle tier to the database. This can be provided through a variety of mechanisms, including both native encryption technology in database products and using SSL. Because different algorithms provide different features and assurance, it is important to support a variety of industry-standard encryption algorithms to protect the confidentiality of data: for example, the Data Encryption Standard (DES, see <www.itl.nist.gov/fipspubs/fip46-2.htm>); triple DES (see <http://csrc.nist.gov/cryptval/des.htm>); and RC4 (see <www.rsasecurity.com/rsalabs/faq/3-6-3.html>). Also, use integrity algorithms to verify that data have not been modified, including Secure Hash Algorithm (SHA)-1 (see <http://csrc.nist.gov/cryptval/shs.html>) and MD5 (see <www.rsasecurity.com/rsalabs/faq/3-6-6.html>).

The Federal Information Processing Standard (FIPS) 140-1, Security Requirements for Cryptographic Modules, was established to validate encryption products purchased by the U.S. government. Products are validated against FIPS 140-1 at security levels ranging from level one (lowest) through level four (highest). A FIPS validation ensures that the implementation of an encryption algorithm has been properly tested.

Auditing

A critical aspect of any security policy is maintaining a record of system activity to ensure that users are held accountable for their actions and that they do not abuse their privileges. Auditing implementations can and do vary by vendor; the following describes Oracle's auditing capabilities. Auditing options need to be highly granular to target the user actions of interest, to minimize the performance overhead of auditing, and to avoid analysis paralysis, in which there are too many auditing records to facilitate meaningful inspection. Ideally, audit records include enough granularity that an administrator can determine what the user requested as well as what was returned to the user at the time of the original request.

A robust database audit facility will allow organizations to audit database activity by statement, by use of system privilege, by object, or by user. One can also audit only successful or unsuccessful operations. For example, auditing unsuccessful SELECT statements may catch users on fishing expeditions for data they are not privileged to see. Database system logs that capture all changes to the database (required for recoverability of data) can be accessed for this purpose. The granularity and scope of these audit options allow customers to record and monitor specific database activity without incurring the performance overhead that more general auditing entails.

A needed auditing capability is one that enables organizations to define specific audit policies that can alert administrators to misuse of legitimate data access rights. What is desired is the ability to define audit policies, which specify the data access conditions that trigger the audit event and are tied to a flexible event handler to notify administrators (e.g., via a page) that the triggering event has occurred. An Oracle implementation of this feature captures the exact text of the statement the user executed in audit tables. In conjunction with other database features that reconstruct the result of a query at a past time, this auditing capability can be used to recreate the exact records returned to a user. A flashback or temporal query allows the recreation of the data a user accessed at the time of the original operation. This is an important feature for customers who have especially sensitive information they wish to share that requires strict accountability such as federal organizations selectively sharing information for counterterrorism purposes.

Many three-tier applications authenticate users to the middle tier, and then the transaction-processing monitor or application server connects as a super-privileged user and does all activity on behalf of all users. The user on whose behalf the middle tier is operating needs to be known to the database system. This allows the database to authenticate the real client, enforce access control based on least privilege, and audit actions taken on behalf of the user by the middle tier. To provide full accountability, the audit records should capture both the logged-in user (e.g., the middle tier) who initiated the connection and the user on whose behalf an action is taken. Auditing user activity, whether users are connected through a middle tier or directly to the data server, enhances user accountability and thus the overall security of multitier systems.

Need-to-Know Protection

The U.S. armed forces, as with many military and intelligence organizations, has a requirement to separate unclassified (but sensitive) information from classified information and to compartmentalize access to classified information. This includes the ability to limit data access based on an arbitrary, hierarchical data level (e.g., Secret, Top Secret), compartments (e.g., Project X), and control of its release (e.g., Releasable to United Kingdom).

During the 1990s, many vendors delivered products that provided multilevel security (MLS): the ability to enforce mandatory access control based on the comparison of a user's clearance to a label on the data. For example, a database containing products required for a joint military exercise with coalition partners could contain data that were viewable only by the United States, particular coalition partners, or all parties. The database would both separate the data and control access based on user clearance. However, MLS systems had a very low rate of adoption even among the user communities (DoD) who had the requirement for such systems.

At the same time, MLS systems were failing to be adopted by the markets that had demanded them; commercial organizations were taking advantage of the accessibility of the Internet to become e-businesses. Many commercial companies that wanted to open mission-critical systems to partners and customers over the Internet had an increased requirement for granular access control to the user or customer.

Companies offering application-hosting services also faced unique security challenges such as keeping data from different hosted user communities separate. The simplest way of doing this is to create physically separate systems for each hosted community; the disadvantage of this approach is that it requires a separate computer with separately installed, managed, and configured software for each hosted user community, providing little economies of scale to a hosting company. Business-to-business exchanges also faced requirements for both data separation and data sharing.

To address both the Internet requirements for data separation and data sharing and government requirements for granular access control, Oracle introduced the ability to provide programmable row-level access control. This capability called Virtual Private Database (VPD) is server-enforced, fine-grained access control together with a secure application context, enabling multiple customers and partners to have secure direct access to mission-critical data. VPD enables, within a single database, per-user or per-customer data access with the assurance that enforcement is not able to be bypassed. The result is lower cost of ownership in deploying applications since security can be built once in the data server rather than in each application that accesses the data. Security is stronger because it is enforced by the database: No matter how a user accesses data, security policies cannot be bypassed.

VPD can be built upon to support specific application policies. One such policy implementation developed by Oracle addresses the DoD and intelligence community requirement to automatically provide labeled data management and enforce label-based and compartmentalized data access. This policy implementation allows organizations to assign sensitivity labels to information, control access to that data based on those labels, and ensure that data are marked with the appropriate sensitivity label. For example, a counterterrorism application may separate data for "need-to-know" purposes based on selected agencies or groups within agencies (e.g., Secret: CIA, Defense Intelligence Agency). The ability to natively manage labeled data is a tremendous advantage for organizations managing data of different sensitivity levels by being able to provide the right information to the right people at the right level of secure data access.

Standards

The existence of and adherence to standards enable stronger security of an integrated system. Security standards are especially important since security generally needs to be integrated to work; there are very few security bolt-ons that can enhance or enable security that do not already exist in the underlying components. Security standards also facilitate the secure integration of disparate technology components.

Standards also usually result in a lower cost of ownership because integration costs are lower (more things work together out of the box), and component costs are generally lower if the products are differentiated on something other than proprietary, lock-in technology. In general, the price is high, and the quality (especially security, which tends to be costly to build) is lower in a monopoly or near-monopoly market.

It is especially important for the DoD to ensure interoperability between entities within one of the armed forces, among the various armed forces, and with coalition partners' systems.

Another benefit of standards is that there tends to be less security by obscurity; the security mechanisms, if they comply with a standard, are well-known rather than hidden and can also be certified or evaluated against the standard, thus providing consumers with confidence in the security of the resulting products.

Standards can include two types of technical interfaces. The first is the Public Key Certificate Standards (PKCS, see <www.rsasecurity.com/rsalabs/pkcs>), and Public Key Infrastructure X.509 (PKIX, see <www.ietf.org/html.charters/pkix-charter.html>). Second, are the independent measures of assurance for security components such as FIPS-140, which speaks to cryptographic module validation and the international Common Criteria, which is a formal security evaluation standard.

> *"... a counterterrorism application may separate data for 'need-to-know' purposes based on selected agencies or groups within agencies ..."*

Public Key Infrastructure

In an effort to provide more secure computing environments, many customers are pursuing rapid adoption and deployment of public key encryption technologies. Public key infrastructure (PKI) describes the application of public key technologies to a computing infrastructure to ensure data privacy and to protect systems from unauthorized access.

PKI itself is a basic encryption technique that has many important applications for secure systems. One application is SSL. For example, a secure implementation of SSL requires at least a server-side certificate attesting to the identity of the server with which a user is attempting to connect. PKI can also enable strong client authentication, provided that the PKI credentials themselves are securely contained and accessed (for example, via a smart card).

PKI is also very scalable technology; in theory, a user who has been given a set of PKI credentials attesting to his/her digital identity can authenticate to servers and systems that he/she has never connected to before because the user's identity can be validated through PKI mechanisms. While this portability of credentials has limited practical application in many commercial organizations (realistically, Bank A will not accept user credentials issued by Bank B), the applicability within DoD is much more apparent. Each service member has precisely one identity as far as the U.S. armed forces is concerned. Once credentials are issued for that identity, they can be reused in multiple DoD systems.

The following are features that are important in database products to support PKI Infrastructure implementations:

- Client-based authentication using X.509 certificates stored in PKCS No. 12 containers. PKCS No. 12, titled Personal Information Exchange Format, specifies a standard for the transfer of identity information including private keys, certificates, etc.
- Wallets (PKI credential container) interoperable with third-party applications and portability across operating systems.
- Support for multiple certificates for each wallet, including Secure Multipurpose Internet Mail Extensions (S/MIME, see <www.rsasecurity.com/standards/smime>) signing certificates, S/MIME encryption certificates, and code-signing certificates.
- Client authentication using SSL.

Since PKI at best provides a single set of credentials, but not single sign on, it is helpful to use PKI in conjunction with single sign-on services as described below.

Single Sign On

In client-server database applications, strong authentication, and single sign on (SSO) are important features. A variety of different user authentication mechanisms are used depending on the application requirements. These can include user passwords, smart cards, token cards, and biometric authentication devices. SSO is provided by technologies such as Kerberos (see <http://web.mit.edu/kerberos/www>), Distributed Computing Environment (see <www.osf.org/dce>), and SSL.

Web-based SSO encompasses a different set of security issues than client-server SSO due to the stateless nature of Web-based connections. One approach to dealing with this problem is to use a centralized server to authenticate and pass authenticated identity securely to partner applications. With this approach, a log-in page is displayed to the user requesting a username and password. Once the user has done so, his/her password is verified and an SSO cookie is set in the user's browser. The client sends this encrypted cookie along with all subsequent HTTP interactions to the partner applications, authenticating the client with the centralized authentication server and avoiding the need for the client to re-authenticate as long as the cookie is valid.

Coupling this authentication technology with PKI allows a user to strongly authenticate to the centralized authentication server via SSL while obtaining the benefit of Web-based SSO after PKI-based authentication.

Availability

Databases and the Internet have enabled worldwide collaboration and information sharing by extending the reach of database applications throughout organizations and communities. This reach further highlights the importance of high availability in data management solutions. Small businesses and global enterprises alike – let alone the U.S. armed forces with their obvious need for high availability to support national security missions – have users all over the world requiring access to data 24 hours per day. Data availability includes the capacity to recover from unplanned outages, allow planned database maintenance while the database is in production and available to users, improve system manageability and serviceability, and provide enterprise-class disaster planning. Highly available solutions have three basic characteristics:

- Reliability: Reliable solutions are made of components that seldom fail.
- Recoverability: In the event a component does fail, a highly available solution quickly recovers without human intervention.
- Continuous Operation: Highly available solutions continue to provide service, even during maintenance activities.

Each component in a system should be designed to provide high availability, which means each component is reliable. In addition, each component must be able to recover from failures of supporting components in the stack. The frequency of failures and the speed of recovery determine the amount of unplanned downtime and application experiences. However, unplanned downtime is not the complete story. Each component must be able to provide continuous operation to meet an acceptable planned downtime target. This may require designing and building the system so that preventative maintenance can be performed while the application is online and users are accessing data. It is also important to plan for unforeseen incidents such as earthquakes and power outages that may prevent recovery for an extended period of time.

One of the true challenges in designing a highly available solution is examining and addressing all the possible causes of downtime. It is important to consider causes of both unplanned and planned downtime, including middleware, application, and network failures. Unplanned downtime can include component failure; hardware failures include system, peripheral, network, and power failures. Human error, a leading cause of failures, includes errors by an operator, user, database administrator, or system administrator. Another type of human error that can cause unplanned downtime is sabotage. The final category is disasters. Although infrequent, these causes of downtime can have extreme impacts on enterprises because of their prolonged effect on operations. Possible causes of disasters include fires, floods, earthquakes, power failures, and bombings. A well-designed, high-availability solution will account for all these factors in preventing unplanned downtime. Planned downtime can be just as disruptive to operations, especially in the DoD, which must support users in multiple time zones up to 24 hours per day. In these cases, it is important to design a system to minimize planned interruptions.

Databases systems are designed to address the causes of unplanned and planned downtime. In the event of a failure, a database can quickly and automatically recover. No committed data are lost. In addition, database systems support features that obviate the need for planned downtime, allowing administrators to perform many management and maintenance tasks while the system is online and data are fully accessible. Management tools are available that identify potential problems and rectify them before they affect data availability.

Assurance

It is important not only to support security features but also to have validation that the features have been implemented in a correct and secure manner. This is provided by formal and independent security evaluations. A commitment to past and continuing product evaluation of new releases against the Common Criteria (ISO-15048) and encryption technology against FIPS 140-1 is a proven measure of a product vendor's commitment to security. This level of commitment should be a requirement for use by the most security-conscious customers in the world: governments, defense, and intelligence agencies. The database, however, is only part of an enterprise-wide, end-to-end security model. A comprehensive approach to security, i.e., a multitiered distributed enterprise, is important to satisfying the mission of large government customers like the U.S. armed forces.

Conclusion

The DoD has a requirement for secure, interoperable, and available systems. While additional technical research and advancement will improve available security technology, much of the security technology needed to meet the DoD security requirements exists today. What is required is a commitment to use the security technology that exists, to demand secure and independently evaluated solutions, and to incorporate security into the entire computing infrastructure.◆

About the Author

Kevin J. Fitzgerald is senior vice president, Oracle Corporation Government, Education and Healthcare. He has been a leader in information technology sales and sales management for more than 25 years. Fitzgerald previously worked for Oracle from 1987-97 as vice president and general manager of the public sector sales group. During his initial tenure, he served in a number of sales roles and also helped initiate new product development areas and product enhancements, enabling Oracle to meet specialized government requirements. Fitzgerald served in the U.S. Air Force and has a bachelor's degree from Boston College.

Point of Contact: Tracy Strelser
1910 Oracle Way
Reston, VA 20190
Phone: (703) 364-6118
Fax: (703) 364-3026
E-mail: tracy.strelser@oracle.com