

white paper

Java Platform Security on ClearPath  
OS 2200 Mainframes

Dr. Glen Newton

security

In a little more than a decade since the inception of the Java language, the Java ecosystem has evolved into one that businesses around the world look to for secure, robust, and manageable web-based applications that serve the enterprise. At the same time, OS 2200, the operating system for the Unisys ClearPath Dorado Series mainframes — an operating system designed from the ground up with security in mind — continued its evolution to provide even greater security. This paper explores the integrated Java platform security that results from the synergy of these two world-class environments.

## Table of Contents

Executive Summary	4
ClearPath OS 2200 Java EE Environment	4
ClearPath OS 2200 Data Security	6
ClearPath OS 2200 Java EE Technology	7
Authentication	9
Authorization	9
Auditing	9
Data Protection	9
Data Integrity	9
Summary	10
About the Author	11

## Executive Summary

Have you made a strategic decision to use the Java platform (Java Standard Edition or Java Enterprise Edition [Java EE]) for your new application development? Are you running Java applications on Microsoft Windows, UNIX, Linux, or another operating system whose mission-critical nature requires that these applications run in a more secure and reliable environment?

Do you have business requirements that can be satisfied only by a new web-based application using ClearPath resident data or business rules? Do you want to integrate off-the-shelf business solutions from independent software vendors into your enterprise, without incurring the security risks associated with non-secure platforms? Do you want to extend or modernize your existing mainframe applications with mainstream technology?

Unisys ClearPath Dorado mainframes offer a highly secure Java environment that satisfies all of these concerns, combining the flexible Java EE environment with the enterprise-class security and reliability of the OS 2200 environment. ClearPath Dorado mainframes provide excellent platforms for solutions in which multiple applications can cooperate to execute the steps in a business process. You can update your existing applications with confidence, using mainstream Java EE on ClearPath Dorado mainframes.

“Why run the Java platform on ClearPath OS 2200?” The short answer is that the Java platform and ClearPath OS 2200 not only complement one another very well, but the OS 2200 environment also provides higher levels of security, scalability, real-time application server configurability, and many other value-added capabilities to a Java application architecture. This white paper focuses on the security aspects of this combination.

## ClearPath OS 2200 Java EE Environment

The ClearPath OS 2200 Java EE environment is a state-of-the-art ClearPath Dorado Series system running the Java platform. The OS 2200 Java EE environment provides a highly secure environment for Java applications that must be available 24 hours a day, 7 days a week. This foundation technology features the rock-solid security inherent to the ClearPath OS 2200 system architecture that is resistant to

hackers, malware, and malicious users while holding all users accountable for their actions.

Dorado Series Servers are available in fully redundant configurations that ensure 24/7 availability. Furthermore, they are designed to host all the tiers of your application in a single environment, which significantly reduces your operational complexity and system administration costs. With database connectors, you can share data with applications running in the OS 2200 environment, and you can count on proven OS 2200 stability and recoverability.

What's more, Unisys offers and supports the JBoss Application Server, the industry's leading Open Source Java EE application server.

Java applications benefit from a Dorado Server's high levels of reliability, availability, and security. Your data assets held in OS 2200 files and databases are guarded by a robust, integrated transaction and recovery system.

ClearPath OS 2200 mainframe attributes give you a unique competitive advantage for your mission-critical applications:

- OS 2200 offers enterprise-class security. Unisys provides Java login modules for integration of the Java security model with OS 2200 security. (See Figure 2.)
- OS 2200 can handle the most intensive transaction processing with full data integrity, such as banking and stock trades where a transaction cannot be lost.
- Availability is more than hardware availability. There is a difference between unplanned and planned downtime. Many system vendors can claim low unplanned downtime but require lots of planned downtime. In contrast, it is not unusual for an OS 2200 system to go a year or more between planned or unplanned downtime events.
- OS 2200 has application-independent, transparent, integrated recovery, which no one else offers. With competing systems, the programmer must make changes to the application in order to take advantage of the recovery system. In contrast, OS 2200 recovery is transparent to the application programmer, end user, and operator.
- Placing Java EE applications as close to their data assets and application assets as possible affords maximum efficiency and unified administration and manageability.
- The fully redundant Dorado series hardware and multiprocessing environment are a cost-effective, robust alternative to the clustering technology used by other servers.

Running new Java code in parallel with legacy code lets you:

- Maximize OS 2200 utilization by running mixed workloads with existing OS 2200 batch, demand, and transactions
- Deploy composite applications on a single platform, combining OS 2200 native and Java EE open components
- Take advantage of the large pool of Java applications and software developers with Java programming skills
- Stage or phase a modernization effort using economical Open Source-enabling technologies backed by mainframe-class support

- Take advantage of enterprise-class support and services from Unisys — a support provider you can trust — for the Open Source JBoss Application Server

As you develop, extend, and deploy mission-critical applications in the Java EE environment on OS 2200, you can depend on Unisys' trusted and time-proven:

- Understanding of enterprise-class computing
- High-availability platform
- Commitment to upward compatibility
- Responsive customer service

## ClearPath OS 2200 Data Security

One of the most compelling reasons to run Java applications on ClearPath OS 2200 is the added security that OS 2200 customers have come to expect and even take for granted.

A corporation's databases are one of its most precious assets. The ClearPath OS 2200 environment provides a nearly impenetrable fortress to protect these assets, as illustrated in Figure 1 below.

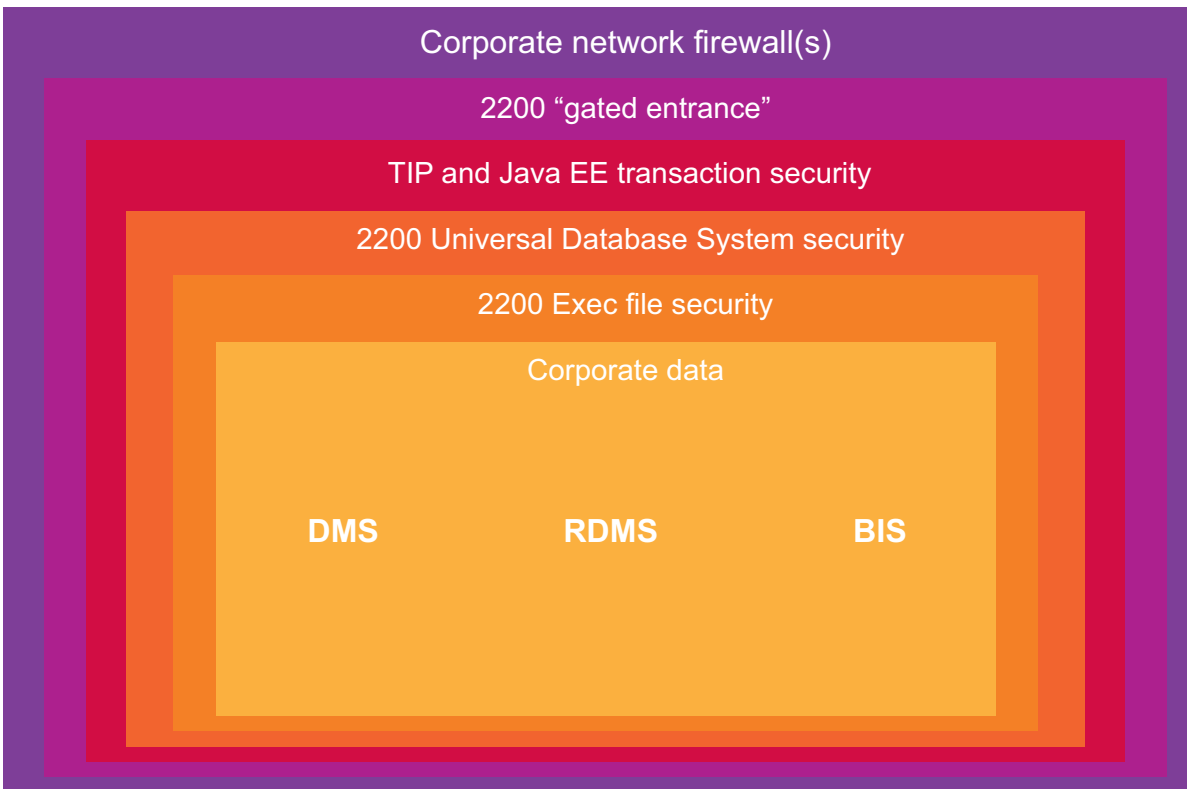


Figure 1. OS 2200 protects corporate databases

Immediately surrounding the database files is a layer of OS 2200 Exec file security, which can use powerful access control records for data access authorization. Wrapped around that is a security layer provided by Universal Database System (UDS). Around that lies the transactional security traditionally provided by the transaction interface package (TIP). When Java EE transactions are added to the mix, they have not only the security defined by the Java platform, but also the underlying OS 2200 platform security. Above the transactional layer are the controls providing a "gated entrance" to the OS 2200 server; and above that lie other firewalls and security measures in the corporate network.

Furthermore, the Java EE Connector Architecture-compliant resource adapters provided by Unisys supply access to the highly secure mainframe databases using the OS 2200 network/communications security protocols.

Taken together, this is a security system second to none for mission-critical Java applications.

## ClearPath OS 2200 and Java EE Technology

OS 2200 is an excellent choice for running mission-critical applications and managing and securing data. Security is designed into the OS 2200 hardware and software architectures, the operating system, the database infrastructures, and the communications structures. Since security inspections have been a cornerstone of the OS 2200 development process for over two decades, OS 2200 has evolved with security at its very core rather than as an add-on attribute.

ClearPath OS 2200 systems not only offer powerful protection against outside attacks, but they also provide some of the industry's most robust safeguards against inside security breaches that can cause even more damage. Unisys has designed and implemented all the critical hardware and software components to work together reliably and securely. In addition, Unisys provides complete worldwide support for the JBoss Application Server as though it were a product developed by Unisys. This allows our clients to have the best of both worlds: the economic value of an Open Source product and the enterprise-class support that Unisys is famous for delivering.

Protection on the OS 2200 system from outside attacks is demonstrated by the fact that no virus damage on the OS 2200 has been reported to independent agencies. It is resistant to viruses and worms because of its protection against the exploitation of buffer overflows and any resulting execution of malicious code — problems to which Windows and UNIX operating systems have been vulnerable.

Even though the Java platform has its own security mechanisms (Java Authentication and Authorization Service, JAAS) based on the development and deployment of secure applications, it does not substitute for the intrinsic layers of OS 2200 security. JAAS adds security capabilities without diminishing or replacing any of the security mechanisms on the OS 2200 system.

The result is the combination of both security models that gives you unsurpassed security—the best of both worlds.

Beyond the protection provided by these two security models, the optional product Unisys Application Defender provides run-time protection for Java/JBoss applications. It detects and prevents common web-application vulnerabilities

such as cross-site scripting, field tampering, and SQL injection.

The Java security model defines how to specify security constraints, but not how authentication and authorization are configured or implemented on the server. It is up to the server operating system to provide the integration with underlying user-id security mechanisms for authentication and authorization, enforcing security on system resources, ensuring the data integrity of server data sources and logging security events in the system event log. In other words, a truly secure Java application requires that it be run on a truly secure platform — ClearPath OS 2200.

In a 2007 security assessment of the OS 2200 Java environment, Symantec Corporation concluded that the OS 2200 Java and JBoss web-application development and run-time environment provide “a security architecture that maps to industry best practice standards.”

OS 2200 provides many security features that directly benefit the Java EE environment:

- All Java Virtual Machine access to files goes through the highly secure OS 2200 Common Internet File System (CIFS) implementation.
- Web Transaction Server for ClearPath OS 2200 provides a highly secure web server that can function as the front-end to Java applications. At the conclusion of their independent security assessment, Symantec concluded that, like the OS 2200 Java EE environment, Web Transaction exemplifies the security industry's best practices.
- Security events such as authentications, violations, file accesses, and database accesses are logged in detail.
- Both the Java environment and the OS 2200 native environment are protected by the comprehensive, architecturally based set of low-level OS 2200 operating system and hardware security mechanisms that prevent unauthorized or accidental misuse of computer memory and processing instructions. These mechanisms include execution-only code banks, compartments, gates, domains, and memory access controls.

Figure 2 shows the relationship between Java EE security and the additional security provided by the ClearPath OS2200 environment.

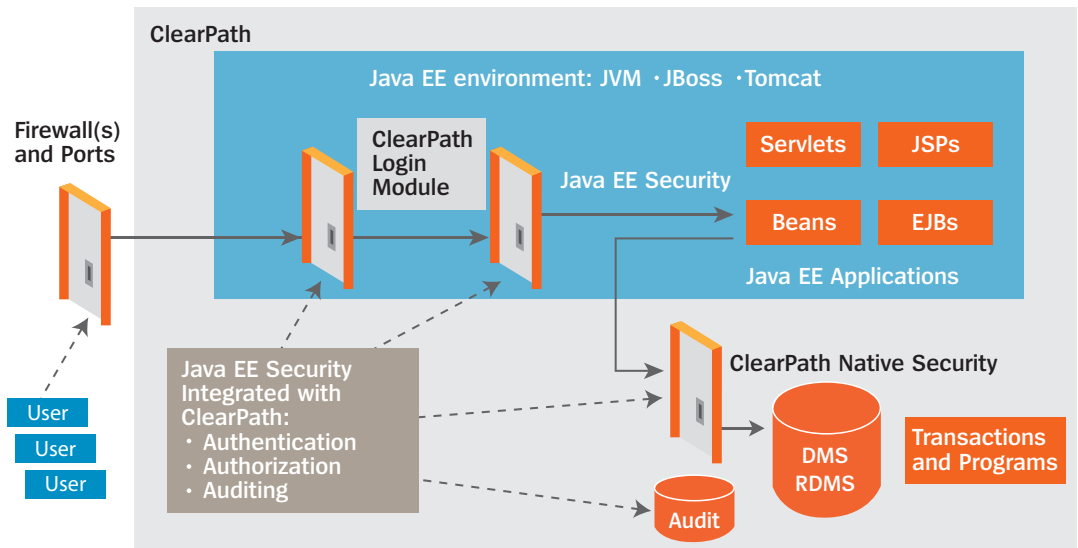


Figure 2. Java security is integrated with OS 2200 security

## Authentication

Java platform and OS 2200 security integration includes login modules that comply with Java Authentication and Authorization Services and provide user-id/password authentication:

- The OS 2200 ClearTextLoginModule uses an OS 2200 user-id/password for authentication. (Note that although the module name includes “ClearText,” the user interface may use encryption when obtaining the user-id and password.) The authentication process compares the user-id/password that is input by the user to the user-id/password contained in the OS 2200 user record.
- The OS2200Krb5LoginModule uses a network user-id/password for authentication via Kerberos. The OS2200Krb5LoginModule “wraps” the Sun Krb5LoginModule. The authentication process is performed in two steps. First, the network user-id/password that is input by the user is authenticated by accessing the Kerberos Key Distribution Center through the Sun Krb5LoginModule. Then the Krb5LoginModule compares the principal name obtained from the Kerberos ticket to the principal name (network user-id) contained in the OS 2200 user record to determine the user’s authenticated OS 2200 user-id.
- The OS 2200 JBoss Application Server login module provides authentication for users of secure web and Enterprise JavaBeans (EJB) applications. The OS 2200 JBoss Application Server login module provides a wrapper around the OS 2200 ClearTextLoginModule or OS2200Krb5LoginModule. Therefore, its authentication mechanism is either OS 2200 user-id/passwords or network user-id/passwords.
- The JBoss security model is role-based. You grant permissions (e.g., for file or code access) to JBoss defined roles. To accomplish this task, the OS 2200 login modules map OS 2200 group names to JBoss role names. The ClearTextLoginModule and OS2200Krb5LoginModule obtain OS 2200 group names from the OS 2200 user record and store them with the principal object (authenticated user-id) that is associated with the user.

## Authorization

Java EE role-based and OS 2200 security models are also integrated for authorization. The Java EE container controls access to container objects, methods, etc. OS 2200 controls Java platform access to applications, transactions, database components, and other system resources.

## Auditing

The login modules supplied by Unisys support an optional configuration parameter for audit control. The user application can choose to log successful logins, failures, or logouts. Furthermore, OS 2200 database software audits all accesses to the database and can determine when the changes were made and by whom.

## Data protection

Access controls at the database level (such as database procedures, grant/revoke privileges, and access control lists) protect data objects. A misbehaving or incorrect EJB can change the database only in the ways in which it is allowed to do so. In addition, the Java database connector for the Relational Database Server (RDMS) provides a simple, yet effective, way to protect data from unauthorized reading or updating by Java clients. It evaluates the OS 2200 user-id of the Java user against an Access Control Record for the database application group to grant or deny access to RDMS.

## Data integrity

Even if something is changed incorrectly, the OS 2200 audit and recovery systems provide easy ways to restore the data to any point in time.

## Summary

ClearPath OS 2200 systems have evolved with security at their very core. Applications running in the ClearPath OS 2200 Java EE environment enjoy enterprise-class security due to

Java EE integration with the ClearPath OS 2200 platform:

- Integration with underlying OS 2200 user-id security mechanisms for authentication, authorization, and auditing
- Integration with OS 2200 backup, availability, and recovery capabilities
- Integration with Kerberos
- Auditing, detection, and reporting of security violations
- A hardware and software architecture that ensures the protection and integrity of server data resources

The ClearPath OS 2200 and Java EE environment provides 24/7 availability, enterprise-class reliability and security, and heavy-duty transaction processing support for your Java applications, backed by dependable Unisys support.

## About the Author

Dr. Glen Newton is a member of the Unisys technical staff in Roseville, Minnesota. After earning his Ph.D. in computer science from the University of Iowa in 1973, Dr. Newton served on the Washington State University Computer Science Department faculty before joining the Unisys predecessor company, Sperry-Univac, in 1976. In his technical and managerial positions at Unisys, Dr. Newton has contributed to several Unisys products for enterprise-level operations management. He has two patents in this area.

Dr. Newton would like to acknowledge the authors of the white paper “Java-J2EE and ClearPath OS 2200,” which served as a basis for much of the information contained in this document.

For more information, contact your Unisys representative.

Or call:

1-800-874-8647, ext. 405 (U.S. and Canada)

00-1-585-742-6780, ext. 405 (Other countries)

In a hurry to learn more? Visit:

<http://unisys.com/cp/dorado>

For even more details, visit:

<http://unisys.com/cp/ecommunity>

© 2007 Unisys Corporation.

All rights reserved.

Unisys and ClearPath are registered trademarks of Unisys Corporation. Java, J2EE, J2SE and all other Java-based identifiers and logos are trademarks or registered trademarks of Sun Microsystems, Inc. JBoss and JBoss Application Server are trademarks or registered trademarks of JBoss, Inc. All other brands and products referenced in this document are acknowledged to be the trademarks or registered trademarks of their respective holders.

Printed in U S America 05/07



BL100035-100