Golden Code Development Corporation
1455 Old Alabama Road, Suite 135
Roswell, Georgia 30076 USA
+1 678-352-2301 (Tel)
+1 678-352-2305 (Fax)
www.goldencode.com

Briefing

Golden Code™ SESAME™ - Local Security for OS/2

Contents

Executive Summary

This document serves as an introduction to Golden Code Development's security software product for OS/2, code named SESAME. The intended audience is the corporate IT professional who is responsible for ensuring that an organization's OS/2-based computing environment is secured against abuse or misuse. This document will describe the purpose, features and functions of SESAME.

Without modifications, the OS/2 operating system is essentially insecure. Any user with local access to a computer's input devices can easily disable or disrupt the system's operation, intentionally or otherwise. A comprehensive security policy, enabled and enforced by security software, properly administered, can greatly enhance the security of an enterprise's OS/2 computing environment.

Product Description

SESAME is a general purpose, software-based, local security solution which provides numerous features and powerful security capabilities for the OS/2 platform. SESAME is designed to protect the system from unauthorized access to protected system resources with a flexible and robust local security framework.

The product leverages the Security Enabling Subsystem built into OS/2. SES enables an installable security subsystem (ISS), such as SESAME, to intercept function calls into the OS/2 kernel and to apply a security policy to enable or deny the services provided by these calls. Security policies are defined for the users of the system by an administrator, based on access permissions to carefully selected system resources. SESAME provides both the tools to define a security policy and the framework which enforces it.

SESAME's features include:

- Granular, discretionary resource definition/access control
- Multi-user authentication
- Session management
    - Client logon authority framework
    - Remote logon authority framework
    - Background logon
- Trusted application support
- STARTUP.CMD protection

- Graphical user shell
- Integrated screen saver

Resource Definition and Access Control

SESAME defines local security in terms of resources available to users and to applications. Resources include hard drives, directories, files, programs, devices, drivers, and application programming interfaces (APIs).

Each resource can be restricted for multiple levels of access by users or by applications on the users' behalf. Access control is managed by a security administrator using a permissions system. The system should be familiar to users of IBM' s LAN Server product; permissions are defined in terms of access rights: CDRWAXN (create, delete, read, write, attributes, execute, none).

Thus, resource access is as granular as necessitated by an organization' s security policy. Access control over any drive, directory, or file in the system can be individually controlled in this manner. The launching of individual applications may be denied or permitted as necessary. Dynamic link library loading can be controlled. Dangerous kernel APIs can be disabled (e.g., shutdown, kill process, etc.). Even access to device drivers and to certain devices can be controlled.

Accounts may be made valid for certain times of day or within certain date ranges. By creating account validity time windows, better control can be exercised over the availability of logons and trusted applications.

Multi-User Authentication

SESAME provides for user and group level security accounts. Users may be members of one or more groups. User and group accounts are each associated with an access control list (ACL) which defines the permissions available to that account for a specific set of system resources. Multiple accounts may be assigned to the same user or group.

Authentication is necessary for the user to access the system. Multiple users may share the same system (though not simultaneously), using a different set of access rights, or the same user may fulfill multiple security roles by authenticating using different accounts.

The accounts database is stored locally on the target machine. User configurable authentication exits, or hooks, provide the capability to substitute the default accounts database with a customer' s own authentication mechanism.

Session Management

SESAME provides logon, logoff, lockup, unlock, shutdown, reboot, and poweroff capability. Session management options are customizable by user/group account, and are invoked via "trusted path control" (CTRL-ALT-DEL). Automatic session control processing features are available, allowing for example, an automatic logon then lock-up at IPL time.

Multiple, user configurable exits allow a high degree of session management customization. User exits are provided for the following states of session control:

- INIT (IPL time)
- pre/post logon
- pre/post lockup
- pre/post unlock
- pre/post logoff
- pre/post shutdown

Client Logon Authority Framework

Client logon authorities (CLAs) allow a single signon with multiple back-end systems, such as LAN Server. SESAME includes a plug-in architecture, which allows customers to install their own CLAs. A UPM CLA that will allow LAN Server, Peer, and DB2 integrated logons currently is in plan for shipment with SESAME version 1.1.

Remote Logon Authority Framework

Remote logon authorities (RLAs) allow server processes running on a locally secured system to share a common authentication and access control database. Thus, individual accounts can be enabled for local access and/or specific remote access (servers), on a granular basis. SESAME provides support for the IBM versions of FTPD, TELNETD, and REXECD which are part of TCP/IP 4.x. Additional RLAs will be shipped with later releases. A framework is provided to build and install additional RLAs, so customers can provide their own as necessary.

Background Logon

This capability allows a specific process to be started with a different account than the locally authenticated user. This is necessary when executing a child process that has more restricted or different access than that of the parent user/process.

Trusted Application Support

Trusted application support allows certain applications to be assigned access rights which the currently authenticated user may not have, in order to perform privileged operations (e.g., password change, system configuration changes, database access, etc.). Thus, a trusted application will be able to perform its privileged work on the user' s behalf, even if the user would not normally be able to access the resources used by the application.

Furthermore, the behavior of individual applications can be controlled. For example, a SINGLE_COPY attribute allows an administrator to prohibit multiple copies of the same application to run simultaneously; a LOCAL_LOGON attribute limits application availability to locally logged on users only.

STARTUP.CMD Protection

Processing of STARTUP.CMD can be protected to prevent user intervention at IPL time, or may be disabled completely. An IPL time user configurable exit enables customer-specific processing as a replacement for STARTUP.CMD

Graphical User Shell

A lightweight user shell, which enables program launching and task switching, is integrated into SESAME. Session management is controlled from this user interface as well. Optionally, the user shell can display multiple, graphical, system monitors (clock, memory, virtual memory, disk space, CPU utilization, TCP/IP utilization, process and thread activity, etc.). This shell can be used with or without the Workplace Shell.

Integrated Screen Saver

A user-configurable screen saver, with multiple modes, is integrated into SESAME. The screen saver is activated when the system is in the lockup state.

Known Limitations

The first implementation of SESAME has some known limitations which are the result of choices made by IBM in the design of OS/2 and its security enabling subsystem (SES). Most of these issues involve APIs which perform much or all of their work outside of the OS/2 kernel, in privilege level 3 (ring 3). Since SES was designed only to intercept service requests at privilege level 0 (ring 0), SESAME cannot intercept requests for system services without additional technology.

Known limitations at this time are:

- it is possible to switch to processes which one would not normally have the right to execute;
- interpreted programs (e.g., REXX, Java) cannot be directly controlled via the execute (X) access permission;
- there are many security relevant API interfaces implemented in ring 3, which cannot be secured via SES (e.g., PM, print spooler, etc.);
- limitations within SES cause improper behavior during the lockup state.

Since all of these limitations represent potential security threats, Golden Code Development is working to address each of them for version 1.1 of the product. By augmenting the base capability of SES with technology which will allow SESAME to intercept requests for system services in ring 3, these issues will be eliminated. Version 1.1 currently is under development in parallel with the final phase of version 1.0 development.

Development Plans

In addition to the resolution of the current known limitations in version 1.1, Golden Code Development has the following plans for ongoing development of the SESAME product. These plans are subject to change without notice.

Version 2.0

- Lock down OS/2 Recovery Choices with a CMD.EXE replacement for command line authentication and access control.
- Add audit capability.
- Event generation and integration with a generic event processing framework.
- Security administration GUI.

Beyond Version 2.0

- Boot/partition protection via a Boot Manager replacement with authentication and ACL processing.
- Boot message logging with optional elimination of device driver screen output.
- Application-specific authentication and custom ACLs via a standard API.
- Partition/directory/file level encryption.
- Workplace Shell security and integration with session management.
- Central, network directory for the security database with data caching and aging for offline use.
- Installation program.
- Granular network resource ACL (e.g., port access by account).
- Interception of MVDM worker routines.
- Porting to other platforms (customer-driven).

Pricing

Pricing for the SESAME product has not yet been determined. Aggressive volume discounts are planned. Version 1.1 of SESAME is the first version which will be offered for sale (see Availability section below).

Availability

A SESAME version 1.0 release candidate currently is undergoing testing, code review and bug fixes as necessary. Documentation is currently in progress. This version of the product will be made available to selected clients for test, evaluation, and feedback, but SESAME version 1.0 will not be made available to the general public.

In the coming weeks, Golden Code Development will be working on solutions that eliminate the known limitations referenced above and which will enable SESAME to be a complete, local security solution. The resulting version 1.1 product will be made generally available.

About Golden Code Development

As a consulting firm and independent software developer, Golden Code Development Corporation helps its clients design, build, and manage mission critical, networked computing environments. The company specializes in technologies and techniques which enable the creation of enterprise-class systems with exceptionally low cost of ownership. Golden Code' s core competencies include OS/2, Java, and Server-Managed Client solutions, such as IBM' s WorkSpace On-Demand. Its expertise in these areas, combined with a disciplined design and implementation methodology, make Golden Code an ideal technology partner for the enterprise customer.

Trademarks

Golden Code and SESAME are trademarks of Golden Code Development Corporation.
IBM and OS/2 are registered trademarks of International Business Machines Corporation.
LAN Server, WorkSpace On-Demand, and DB2 are trademarks of International Business Machines Corporation.
Java is a trademark of Sun Microsystems, Inc.
Other product names referenced herein are the property of their respective owners.