Compro Computer Services, Inc.
105 East Drive
Melbourne, FL 32904
Telephone: (321) 727-2211
Fax: (321) 727-7009
www.compro.net

S-LCRS Option
Technical White Paper

Meeting Worldwide Security Requirements for Legacy Computer Programs

August 2010

Notices

Trademarks

Compro Computer Services, Inc.
105 East Drive
Melbourne, Florida 32904

Pub. No. 204-364-00-A4-CEF

Table of Contents

Table of Figures

OVERVIEW

Legacy host computers abound in the U.S. Department of Defense (DoD) and international military installations worldwide. Many of these hosts will eventually need replacement for improved maintainability, reliability and performance. While host replacements alone pose a technical challenge, recent Information Assurance (IA) security requirements further complicate any potential solution.

This paper provides a brief background of IA, and explains how Compro's Secure Linux Gateway (SLG) can address IA requirements for 3rd-party legacy host replacements (such as DEC, SGI and IBM), and how Compro's Secure LCRS (S-LCRS) option meets the IA challenge for LCRS.

INFORMATION ASSURANCE

Definition of Information Assurance

Generally speaking, Information Assurance (IA) is the practice of managing information-related risks. More specifically, IA seeks to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-repudiation (that is, one party of a transaction can not deny having received a transaction nor can the other party deny having sent a transaction). These goals are relevant whether the information are in storage, processing, or transit, and whether threatened by malice or accident.

In other words, *IA is the process of ensuring that authorized users have access to authorized information at the authorized time*.

IA History

IA has existed since the 1960s, where it simply meant locking a door and posting a guard. Since then, things have become more complicated.

In the 1970s, IA was refined to address confidentiality, integrity and availability (known as the 'CIA triad'):

- *Confidentiality* means that only authorized personnel, who have a genuine need to know, should access sensitive information.
- *Integrity* means that data cannot be created, changed or deleted without proper authorization.
- *Availability* means that the information, the computing systems used to process the information, and the security controls used to protect the information are all available and functioning correctly when the information is needed.

IA now requires classifying all the information assets requiring protection, a detailed risk assessment and a risk management plan. The plans are complex, and include countermeasures, contingency procedures, security hardening, and more. IA is an ongoing process; regular audits result in updates to the management plan and security procedures.

The Department of Defense (DoD) IA Mandate

Today, the DoD Information Assurance Certification and Accreditation Process (DIACAP) mandates and enforces security risk management on information systems. DIACAP defines a DoD-wide set of activities, general tasks and a management structure process for any information system to ensure it will comply with IA requirements throughout the system's life cycle. The final version of this mandate is entitled *Department of Defense Instruction 8510.01* and was signed on November 28, 2007. Worldwide, similar defense-related mandates are either in existence or arising.

Note: Since this mandate, most new DoD computer installations must meet IA requirements. It is possible this mandate may apply retroactively to past DoD installations, and even sensitive commercial applications may require IA-like compliance.

Compro meets the IA challenge with the Secure Linux Gateway and Secure LCRS products.

SECURE LINUX GATEWAY (SLG)

Compro's Secure Linux Gateway (SLG) Block Diagram

Figure 1 above illustrates a typical 3rd-party manufacturer configuration using Compro's Secure Linux Gateway (SLG).

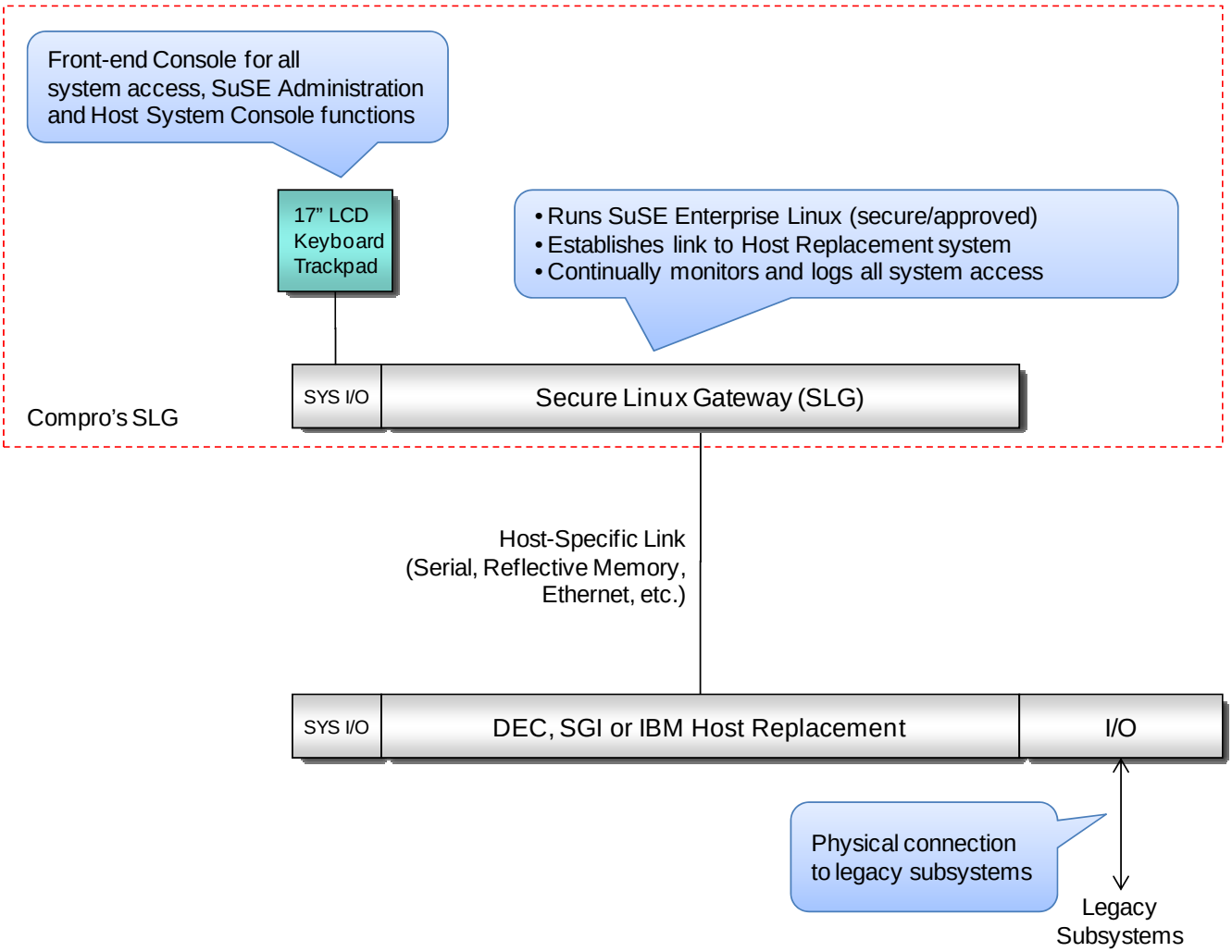

Figure 1. Compro's Secure Linux Gateway (SLG) Block Diagram

Major components include:

1. **Secure Linux Gateway (SLG)**: This is a simple rack-mounted, commercial-off-the-shelf (COTS) computer system, preferably the same used as in the host replacement nodes to simplify logistics. It includes the following major components:
   a. SuSE Enterprise Linux, an IA-approved operating system (OS). If necessary, any IA-approved Linux OS may be used.
   b. Standard LCD display, keyboard and mouse.
   c. A host-dependent connection to the 3rd-party host replacement system.

2. **DEC, SGI or IBM Host Replacement**: This is one or more 3rd-party computer systems as determined by configuration requirements. Other manufacturer hosts are potentially supportable.

Secure Linux Gateway (SLG) Function

The SLG provides a single entry point for system control, while capturing, logging and storing all human I/O activity to meet IA requirements. SuSE Enterprise Linux natively captures this activity and meets security certification requirements established in the *Common Criteria for Information Security Evaluation*, a broad agreement that encompasses practically every security standard worldwide.

Managed by a special application running in the SLG, a host-dependent link, such as serial, Reflective Memory, or Ethernet is established with the 3rd-party host replacement system. This link carries command information between the SLG and host for overall system control.

COMPRO'S HOST COMPUTER HISTORY

In the 1960s, Systems Engineering Laboratories (SEL) began manufacturing the first SelBUS-based 32-bit computer systems, including the 32/5*x* and 32/77 series. Later successors including Gould and Encore continued the product line with the 32/27, 32/87, 32/97 and finally the RSX. Many of these systems are still in use today around the world, especially in military and commercial simulators.

Compro's Legacy Computer Replacement System (LCRS) is an integrated collection of commercial-off-the-shelf (COTS) hardware, PCI-based interfaces, and legacy host computer simulation software. LCRS' function is simulating physical legacy computing hardware with a primary objective – preserve customer application software and connected I/O subsystems while dramatically improving host computer performance, reliability, maintainability, and supportability. LCRS can replace all the aforementioned systems, and has been on the market since the late 1990s, with over 100 nodes operational worldwide.

SECURE LCRS

Compro's S-LCRS Block Diagram

Figure 2 illustrates Compro's LCRS configuration with the Secure LCRS (S-LCRS) option.

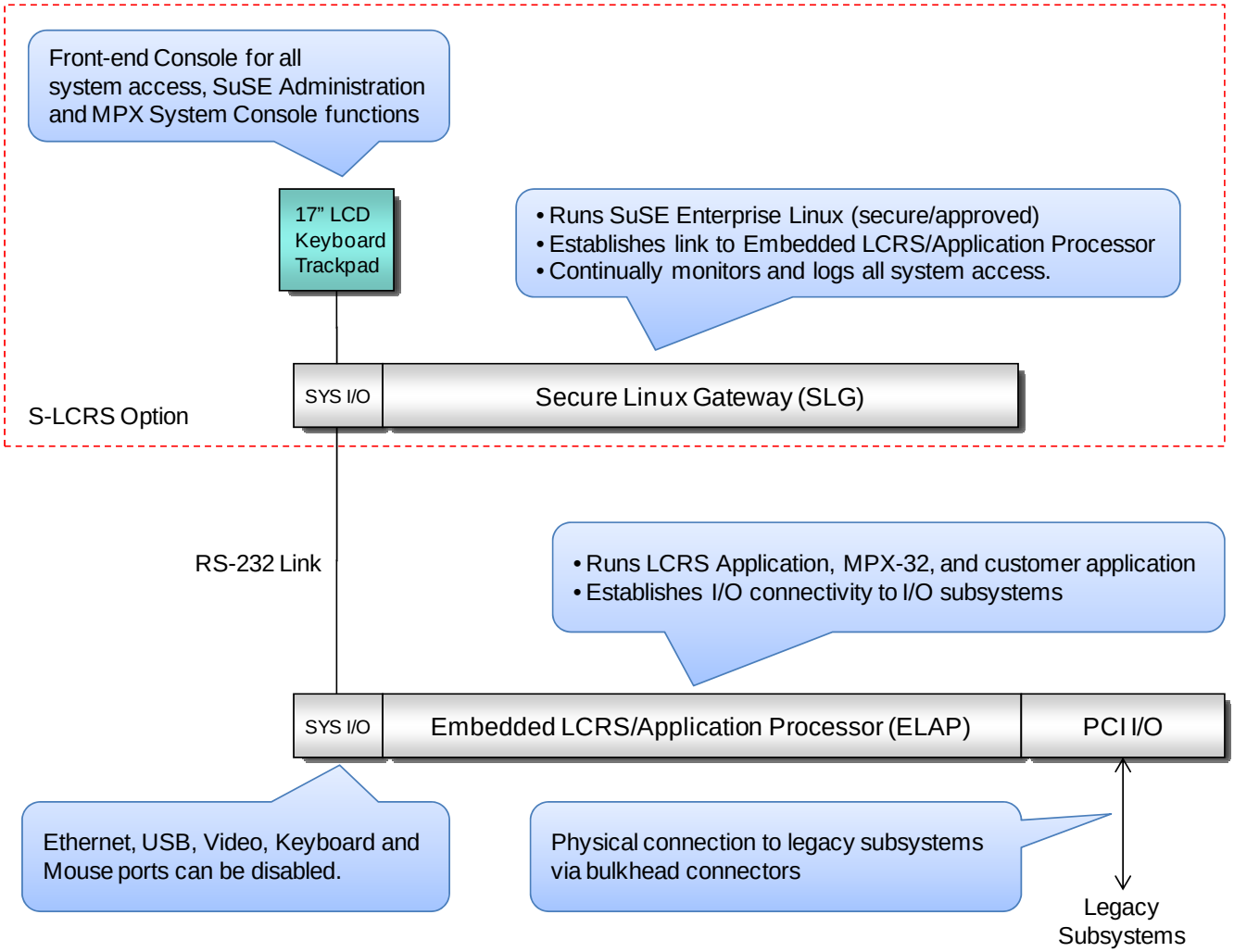

Figure 2. Secure LCRS Block Diagram

Major components include:

1. **Secure Linux Gateway (SLG)**: This is a simple rack-mounted COTS computer system, preferably the same used as in the ELAP nodes to simplify logistics. It includes the following major components:
   a. SuSE Enterprise Linux, an IA-approved operating system. If necessary, any IA-approved Linux OS may be used.
   b. Standard LCD display, keyboard and mouse.
   c. A single RS-232 connection to the Embedded LCRS/Application Processor (ELAP). – See item 2 below.

2. **Embedded LCRS/Application Processor (ELAP)**: This is one or more rack-mounted COTS computer systems, with the following major components:
   a. A UNIX operating system with a "Custom Compro kernel" required for LCRS function.
   b. PCI I/O boards that connect with legacy subsystems.
   c. The LCRS software application, which simulates the legacy SEL/Gould/Encore computer hardware architecture.
   d. A copy of the legacy operating system (RTM, MPX-32, XPM, etc.).
   e. A copy of the customer's legacy executable binary application code.

Secure Linux Gateway (SLG) Function

The SLG provides a single entry point for system control, while capturing, logging and storing all human I/O activity to meet IA requirements. SuSE Enterprise Linux natively captures this activity and meets security certification requirements established in the *Common Criteria for Information Security Evaluation*, a broad agreement that encompasses practically every security standard worldwide.

Managed by a special application running in the SLG, the RS-232 link establishes a physical connection to the ELAP RS-232 port. This link carries command information between the SLG and ELAP for overall system control.

Embedded LCRS/Application Processor (ELAP) Function

Essentially a pre-configured Legacy Computer Replacement System (LCRS) running UNIX with a custom kernel, the ELAP emulates legacy hardware, and executes legacy applications while communicating with legacy subsystems. (Compro's *LCRS Technical White Paper*, publication no. 204-361-04, provides extensive functional detail.) One or more ELAPs may exist in a single configuration.

The ELAP USB port is disabled by default to assure deterministic performance. Ethernet, video, keyboard and mouse ports may also be disabled during normal operation. In multiple-node ELAP configurations, these ports may be temporarily enabled to facilitate system reconfiguration and/or troubleshooting.

"Embedded" and IA

The term "embedded" is valid in the sense that the ELAP is not simply COTS software running an emulator application. The ELAP hardware and UNIX operating system (with custom kernel) are carefully selected and tuned to provide a true, real-time, deterministic computing environment that delivers a faithful simulation of legacy hardware. Thus the ELAP itself must be delivered as a "whole" for successful performance.

This "embedded" moniker is important in the IA world since it exempts the ELAP itself from security auditing requirements. Instead of forcing performance-robbing logging and auditing functions into the ELAP, Compro's SLG "front end" satisfies IA requirements while leaving the ELAP to do its job.

SUMMARY

Compro's Secure LCRS (S-LCRS) and Secure Linux Gateway (SLG) solutions offer a convenient, effective and affordable method for meeting Information Assurance (IA) and other security requirements when host replacement computer is considered. S-LCRS is ideal for any existing or future Compro LCRS installation, and SLG is a flexible solution for other legacy host replacements.