

SENTINEL COMPUTER SECURITY SYSTEM



The Sentinel Computer Security System (Sentinel) is targeted to address important cyber security vulnerabilities and operational needs that were uncovered by Secured Processing Inc. (SPI) personnel, while assisting Delta Security Technologies (DST) during Vulnerability Assessments, Penetration Tests, Security Audits, and Certification and Accreditations (C&As) performed for various Federal Government and commercial organizations. These needs that are addressed by the Sentinel include the following:

- The need to counter and detect potential Insider Attacks at the computer terminal and counter External Threats from Hackers and Malware;
- The need to provide the computer user with a level of Information Assurance that would allow secure access to classified data at the desktop without a special facility;
- The need to provide the computer user with secure access to multiple levels of sensitive and classified data and networks in a single desktop computer;
- The need to reduce computer costs, space, and power requirements (Sentinel is a Green Technology) by replacing the current use of separate computers for each security domain;

In the current DoD and commercial environment the Insider Attack accounts for most of the successful security intrusions within an organization's Information Technology Infrastructure. The publication of data-loss statistics from reputable organizations such as Ernst & Young show that at least 66% of all successful security intrusions originate within the organization. The National Security Telecommunications and Information Systems Security Committee (NSTISSC) published "*The Insider Threat to U.S. Government Information Systems, NSTISSAM INFOSEC /I-99*" in which the Insider Threat was designated as one of the most difficult to detect and counter. This same document also described the threat as being comprised of disgruntled employees, terrorists, foreign agents, and criminals with goals that include obtaining access to restricted data or the destruction of critical data and/or assets. The countermeasures for Insider Attacks recommended by the NSTISSC include the implementation of strong Access Control, User Identification and Authentication, and Audit Capability for Information Technology used to access sensitive data and resources. SPI used this as the basis for the conceptual design of its Sentinel Computer Security System by implementing these security functions within a hardware-based system that is independent of the computer processing hardware and software.

The Sentinel consists of a kit as depicted in FIGURE 1 that can be installed in minutes within or external to any desktop PC and is independent of the software and operating system. The core of the system is the Security Module shown in FIGURE 2 that consists of a Smart Card Reader, Secure Microcontroller, and Asset Status Sensor Board. A user's encrypted Personal Identification Number (PIN) and data and resource access rights are stored on any standard Smart Card along with the card's Machine Authorization Code (MAC). The user's Password is stored as an encrypted value in the memory of the Secure Microcontroller. This encryption and physical separation of PIN and Password decreases their susceptibility to discovery. To access restricted data which is usually stored on Removable Drives as seen in Figure 1, the user must insert their Smart Card into the Smart Card Reader otherwise the Sentinel will allow access to only the unclassified data on the unrestricted internal hard drive and all unrestricted resources such as the unrestricted Network port, USB ports, and portable media drives (CD/DVD). These resources are unrestricted since they are only connected to unclassified data sources. The inserted Smart Card is validated by the Sentinel Security Module by comparing the MAC on the card with the MAC in the Secure Microcontroller. If there is a match, the Security Module initiates the Sentinel User Identification and Authentication (I&A) process via a request displayed on the host computer display for the entry of the user's PIN and password. The user enters their PIN via the keyboard interface and if the entered value meets preset length and format requirements it will be compared with the encrypted value stored in the Smart Card. If there is a match, the user is identified and then must enter a password via the keyboard that is read by the Security Module Secure Microcontroller and compared with the encrypted value stored in the microcontroller memory. A match will authenticate the user as being authorized,

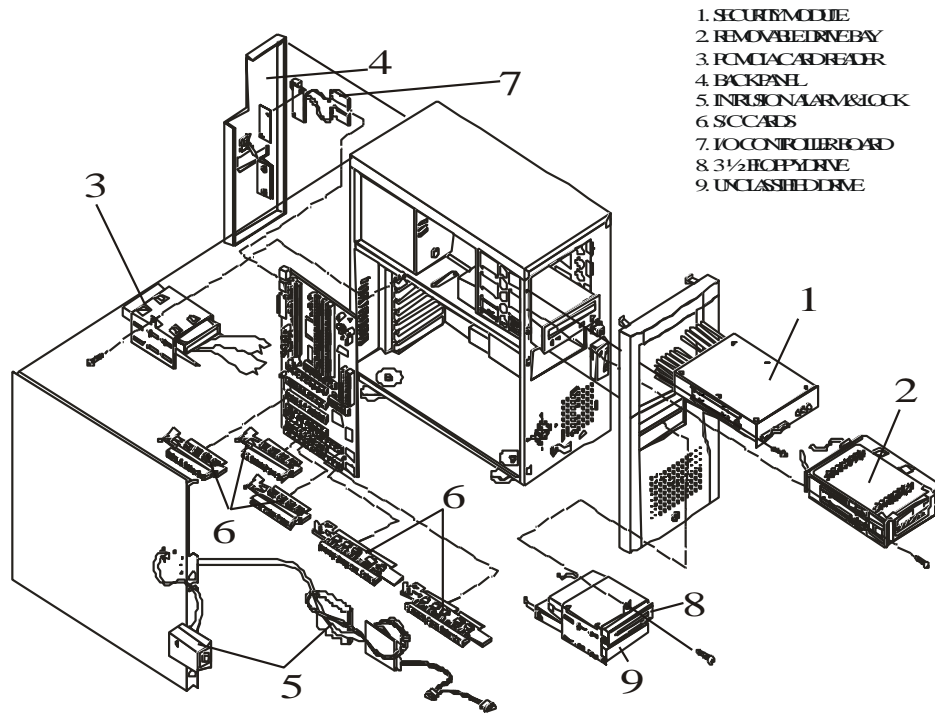
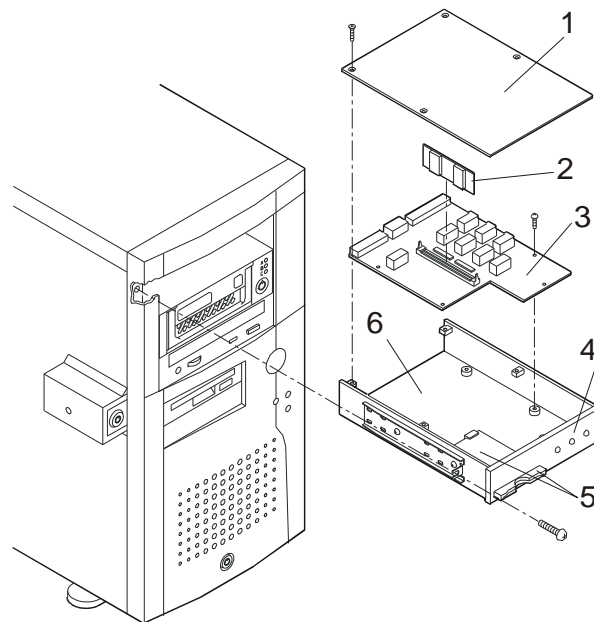


FIGURE 1. TYPICAL SENTINEL INSTALLATION WITHIN A HOST PC



1. COVER
2. MICRO CONTROLLER
3. ASSET STATUS SENSOR
4. LEDs
5. SMART CARD READER
6. CHASSIS AND FRONT PANEL

FIGURE 2. SECURITY MODULE

while a failure after 3 PIN and/or Password entry attempts will cause the Security Module to bar user access to any restricted security domain until the I&A process is successfully completed. This I&A process essentially binds the authenticated user to both their Smart Card and the host computer.

Upon successful completion of the I&A process, the Access Control process is initiated by the Security Module. Under this process, access to any restricted domain used to process restricted (classified or sensitive) data requires access to a specific Removable Drive (as shown in FIGURE 1) that has a preset security level and MAC. The Security Module will first determine if the user has access to the level of data stored on the selected Removable Drive by comparing the data access level on the user's Smart Card with the level designated on the Removable Drive and the level programmed in the Secure Microcontroller. If there is a match the Secure Microcontroller will then compare the MAC on the Removable Drive with the MAC on the user's Smart Card and the MAC stored in the microcontroller memory. If either the data access level or MAC comparison fails, the Security Module will default to the unrestricted domain in which the host internal hard is powered on along with all computer resources.

If the comparison of the security level and MAC is successful, the Security Module will deactivate the host computer internal hard drive and will read the resource rights on the user's Smart Card and on the Secure Microcontroller. Allowed resources can include any combination of Network or USB ports in which any resource is either activated or deactivated. The identification of the allowed Removable Drive and resource access rights is read by the Security Module Secure Microcontroller, which outputs control signals to the logic on the Security Module Asset Status Sensor Board. This logic ensures that only the selected resources at the correct security level can be activated by the output signals from the Secure Microcontroller and that all disallowed assets are simultaneously deactivated. Control over resources that plug into any motherboard slots is controlled via the Sensor/Controller (S/C) Cards shown in FIGURE 1. These S/C cards are inserted between the slot and the resource to enable or disable motherboard power and signals based on control signals from the Security Module. The I/O Controller Board, Shown in FIGURE 1 can perform this same signal and power isolation function for USB and Network Ports at the port output using the same control signals from the Security Module.

In addition, to controlling access to Network and I/O ports and any resources within motherboard slots, the Security Module can be set (as a manufacturing option) to also disable access to any computer portable media devices such as CDs, or DVDs in any or all restricted modes of operation. In addition, the control over USB ports can also control access to any USB memory systems such as Jump Drives that have been shown to be primary sources of cyber vulnerability and attacks as was seen in the recent malware attack on DoD via corrupted Jump Drives that was reported by CBS 60 Minutes on November 8, 2009. This capability allows control over potentially dangerous portable storage media that could be used to improperly transport restricted data or transmit malware. The Sentinel also prevents data from one restricted level from being also used at a different level thus ensuring total separation of security levels. The Sentinel is the only security system that has been specifically tested and validated to prevent this method of data transfer between separate security levels in a PC or workstation. Upon successful completion of the access control process the user is bound to a restricted domain defined by a specific Removable Drive with an operating system, programs, and data plus a set of data resources all at the approved security level as defined on the user's Smart Card.

The programming of user access privileges on all user Smart Cards is under the control of a Security Administrator who uses a Smart Card Reader/Writer and programming software called Audit-X to setup and change the user security level and resource allocations. User Smart Card settings can also be set and reset remotely by Audit-X via a network interface. Access privileges to host computer domains and domain assets can also be restricted at the host computer through the setup of security module privileges at the factory or by the Administrator when they logon to the Security Module setup menu via an Administrator Smart Card. These privileges can also be restricted based on Time of Day capability in

which a user's access rights to a security domain or any domain assets including Network or USB Ports can be controlled in intervals is small as a minute over a 24 hour period. This allows a lower level of access or no access after normal working hours for certain users or allows potentially vulnerable assets such as Jump Drives to be available for a very limited time period. Overall user access is based on the accepted security concept of "Least Privilege" in which a user can only get access to those domains and assets based on the lowest common denominator of User Smart Card and Security Module access privileges. This allows the Security Administrator to minimize "Insider" risks based on host computer location, assigned user base, or threat environment.

To prevent the Security Administrator from becoming a Super User the Sentinel uses its validated role separation function which prevents a user from being an administrator and vice versa. Although the administrator can program the user's PIN they cannot access the password in the Secure Microcontroller. In addition, the user's password must be selected by the user during initial login to prevent any other user or an administrator from gaining unauthorized access. Thereafter, the user is required to periodically change their password to a new value. Conversely a user's Smart Card will not allow access to stored audit data thus preventing the data from being erased or modified. Stored audit data can only be downloaded by the Administrator to an Administrator Smart Card or via a Network Interface with a designated computer such as an Administrator Workstation or a designated server. The Network Interface for uploading stored audit data is implemented between the Sentinel's Secure Microcontroller and an independent Network Appliance via a direct interface and a dedicated port that does not interface with the Host Computer.

Other Security Features of the Sentinel include a capability for the user to enter a command during computer use that can quickly shut down Network and/or USB ports if the connected network or host computer is under attack. A fast shutdown feature is implemented so that the removal of the user's Smart Card will cause automatic shutdown of the system. The Sentinel also has certain built-in self-protection mechanisms such as fail-safe that ensures that the failure or destruction of any component of the system or the rewiring of the system will at worst disable the system in a secure mode. Self-protection is also inherent in the Secure Microcontroller that is tamper resistant to electrical and physical attack. Such attacks cause the microcontroller memory to be erased. In addition, the Secure Microcontroller creates dummy instructions as it operates so attempts to monitor its operation in order to decipher its program will not work. Finally, the Secure Microcontroller memory is encrypted with a secret algorithm and key at the end of each session preventing access to all data including the program and stored audit data. Sentinel options include the use of a Biometric Fingerprint Reader to enhance the user I&A Process. It can be setup to either replace the use of a password or supplement the password.

The Sentinel can be implemented in various configurations and security levels depending on the needs of the user and the organization. Multiple users can access the same host without having the same access privileges to resources and/or data. The Sentinel provides secure I&A, Access Control, and Audit capability that is strong enough to allow access to classified data and resources such as the SIPRNet at the desktop. Current architectures in which access to classified data via a computer is only permissible in a secure vault could be replaced or supplemented with an architecture that is more secure and resistant to Insider Attacks. The Sentinel technology has been validated by the National Information Assurance Partnership (NIAP) at EAL 4 allowing it to process classified data as referenced on the NIAP webpage under "Sentinel Model III Computer Security System" at <http://www.niap-ccevs.org/st/vid1000>. Since all NIAP validations are performed in accordance with the ISO 15408 International Common Criteria, it is also recognized by over 15 countries including the UK, Australia, Canada, France, Germany, Greece, Italy, Japan, New Zealand, Spain, and South Korea. There are also three existing U.S. patents on the Sentinel security apparatus and processes including: U.S. Patent No. 6,351,817; U.S. Patent No. 6,389,542; and U.S. Patent No. 6,643,783 and one pending patent application. These patents cover the Sentinel technology for any processing environment.

A laptop version of the Sentinel, as shown below in FIGURE 3, has actually been developed and tested as a prototype. The desktop Sentinel System and the laptop use the same basic Sentinel architecture that includes the same hardware including the Smart Card Reader, Asset Status Sensor Board, and Secure Microcontroller with the exact same program. A laptop version could also access the same Removable Drives as are used with the Desktop system. The Sentinel technology could also be built directly into a Desktop or Laptop motherboard to provide Sentinel security with no impact on existing motherboard operations, software, or operating system requirements.

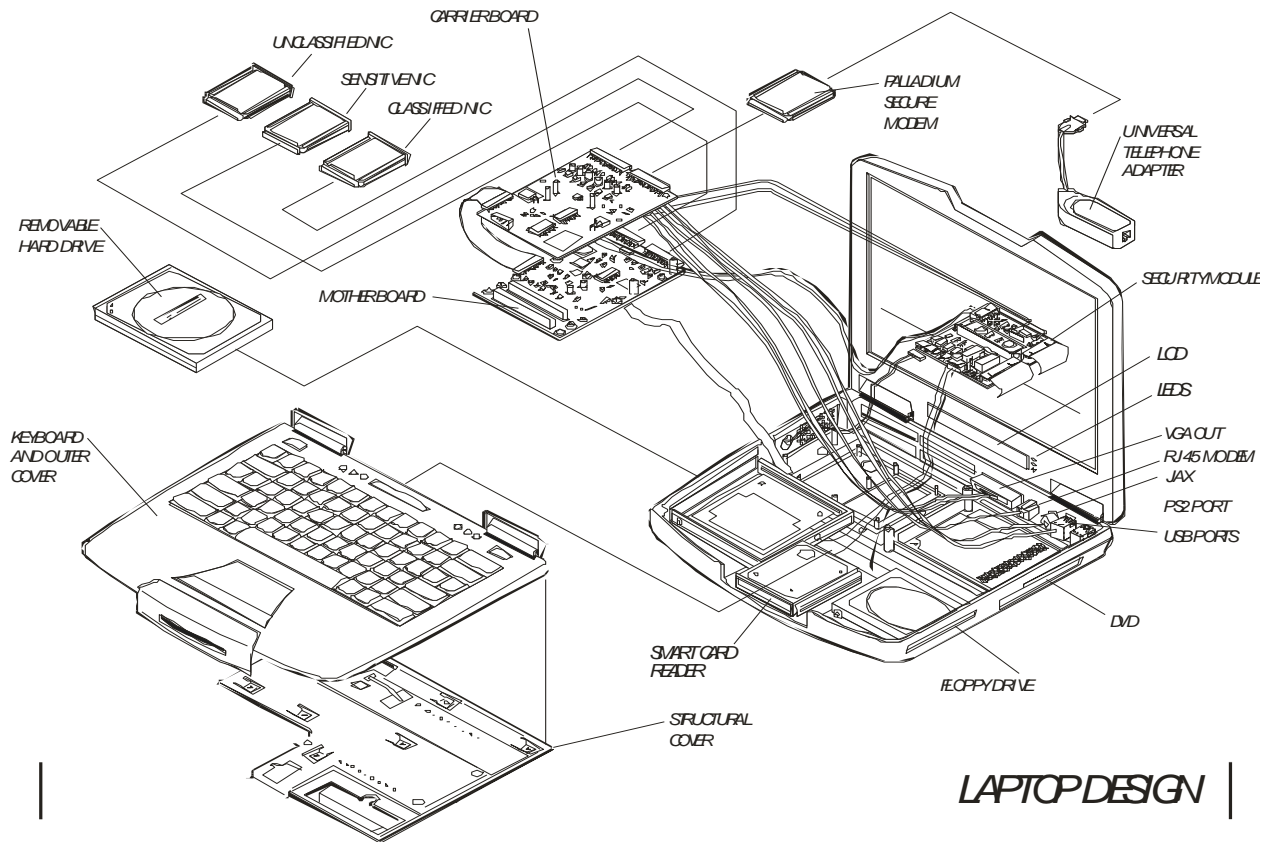


FIGURE 3. SENTINEL LAPTOP PROTOTYPE