Introduction
The Department of Defense (DoD) invests billions of dollars every year in weapons research and development to obtain and maintain full spectrum dominance in military operations. An increasing percentage of the critical technology in our state-of-the-art weaponry is comprised of software algorithms and data. Adversaries and competitors use open source literature research, computer network attacks, theft by well placed insiders, and reverse engineering to access and exploit our software technology. Stolen technology and data are used to compete with us not only on the battlefield, but also within the global economy.

To counter these efforts and protect critical software, the DoD established the Software Protection Initiative (SPI). SPI researches, develops, tests, and deploys protections to prevent the unauthorized modification, reverse engineering, and distribution of critical DoD software. SPI established the Software Protection Center (SPC) to serve as the focal point for protecting critical software. The SPC has deployed software protection solutions to more than 187 DoD, contractor, and other government facilities, safeguarding nearly $150M of critical DoD intellectual property.

Secure Viewer
Requirements to share critical Intellectual Property (IP) outside of their immediate control has forced computer code owners to face a challenging question: “How can I satisfy the requirement to share my source code or data and still maintain control over its distribution?”

To satisfy this requirement, the SPC has developed a unique protection tool: Secure Viewer. At the heart of Secure Viewer is a locked-down operating system, coupled with hardware anti-tamper techniques. The code owner specifies what input and output devices can be accessed by the user, and which activities are allowed—Secure Viewer enforces the code owner’s policies.

Out-of-Band Protection
Secure Viewer uses the SPI endorsed concept of out-of-band protection—meaning software protections are implemented outside the code’s normal data path. One example of an out-of-band protection mechanism is to store decryption keys, which are required for program execution, on a separate processing module.

Proven Utility
Based on one code owner’s requirement to allow potential contractors to review critical source code and data to assemble a proposal without risking loss of the IP, the SPC developed the Secure Viewer. Simply plug a keyboard, mouse, and monitor into the viewer and you’re ready to go.

The code can only be used as directed by the code owner. In this case, no additional I/O ports were enabled, meaning there was no way to exfiltrate the code from the system. Attempts by the end user to use the data in an unauthorized manner will result in an irrevocable loss of the data stored on the Secure Viewer system.

Unlimited Possibilities
Secure Viewer can address many different scenarios. It can be tailored to:
- Allow output of data but not program code. This will enable users to execute a code and make use of the output as intended, but not allow theft of the actual code.
- Allow editing and compilation of code for test and evaluation purposes.
- Allow data input from files, but prevent any output from being removed.
- Run a virtual machine with nearly any operating system and applications.
- Expire after a number of uses or days.
- Execute any incarnation of a data viewer for easy browsing of source code and data.

The flexibility of this protection tool provides the code owner with multiple options for sharing critical source code and data without the risk of loosing control of critical DoD intellectual property.

Approved for release: 88 ABW 08-1185
**Secure Viewer**

**What's Required**

The customer needs to provide the SPC with the following information:

- The IP needing protection.
- Detailed policy on what user actions are allowed or prohibited when interacting with the Secure Viewer.

**IP Protection Process**

Protecting IP with Secure Viewer depends, in large part, on the requirements of the customer. The customer needs to coordinate closely with the SPC in defining a set of rules for protecting the IP. The SPC configures the Secure Viewer to meet the specific requirements of the code owner.

**Distribution Details**

Each distribution requires a Secure Viewer unit.

**Cost**

The SPI program currently covers the cost of protecting critical application software and data with the Secure Viewer. (Subject to change based on program funding) Code owners may be required to provide funding to cover hardware and distribution costs.

**Hardware Specifications**

Secure Viewer ships as a normal ATX form factor PC. Customer is expected to supply any peripherals (monitor, keyboard, etc).

**Performance Impact**

The performance of the Secure Viewer mirrors the performance of a standard PC. The system can be configured to meet application specific requirements as identified by the code owner. The protected version of the application/data performs just as it would on an unprotected system.

SPI is executed under the cognizance of DUSD(S&T) and is funded through the High Performance Computing and Modernization Program (HPCMP).

**Autonomic Trusted Sensors for Persistent Intelligence (ATSPI) Technology Office**
Software Protection Center (SPC)
AFRL/RYT
WPAFB, OH 45433-7320
(937) 320-9068 x150

Approved for release: 88 ABW 08-1185