ERUCES architecture significantly mitigates risk against Cold Boot RAM encryption vulnerability

Lenexa, KS. – February 26, 2008 – ERUCES Inc., a leading provider of encryption technologies, today announced its Tricryption software is significantly less vulnerable to Princeton University's Cold Boot Attacks on Encryption after examination of the research findings and the Tricryption system architecture. In particular, ERUCES would not be vulnerable to the researchers' examination of whole disk encryption, the system's key granularity limits the extent of damage at any one time, and the elimination of key material with the data on the end workstation (also referred to as co-location) mitigates most compromise risks.

The Cold Boot Attack was presented last Thursday by researchers from Princeton University, and the Electronic Frontier Foundation as well as others. The vulnerability surrounds the fact that a computer's memory, or RAM as it is more commonly called, does not immediately erase its contents upon turning off the power. In fact, the researchers cited data that techniques could be used to extend the amount of time before the memory erases itself to a week.

"A combination of Tricryption's features mitigate most of the risks associated with reading data through the Cold Boot Attack," said Jon-Michael Brook, ERUCES' Vice President of Security Solutions & Sales. "Our patented Hidden Link feature eliminates co-location of cryptographic key material with the end user's data. The trusted insider threat protections built into the architecture also minimize most of the attack vectors delineated in the Cold Boot Attack paper. Several other defense in depth techniques protect our customers from key disclosure and thereby data corruption or compromise."

The breakthrough resides in ERUCES's patented "Hidden Link". Only a pointer to the decryption key exists on the end host with the data. The technology virtually eliminates trusted insider threats, such as those associated with IT Administrators pilfering company secrets. This same protection extends to the ERUCES' Key Server, where the decryption keys are themselves encrypted, with no direct or unencrypted connection between the data and the keys.

The Princeton research also presents ways to decipher key material found on memory, and detect and correct errors within. They also included several new and novel methods for reducing the overall decryption time considerably versus a brute force attack, or the equivalent of trying every key on a huge key ring against a lock. They specifically designated Microsoft's BitLocker, and Apple's File Vault.

"We find that a moderately skilled attacker can circumvent many widely used disk encryption products if a laptop is stolen while it is powered on or suspended," said the research team in the paper. "Actually imaging memory and locating keys took only a few minutes and were almost fully automated by our tools. We expect that most disk encryption systems are vulnerable to such attacks."

"That's not to say we are completely immune to everything within the (Cold Boot) report", says Oggy Vasic, ERUCES' Vice President of Software Development. "If you access cryptographic material on a computer system, a key must be stored somewhere on the machine. However, with ERUCES, only a handful of files may be in use, and therefore only a handful of keys stored locally. The rest of the keys reside elsewhere on an encrypted Key Server. This is in stark contrast to analyzed full disk encryption products, where a single key protects the entirety of a computer's hard disk."

About ERUCES:
ERUCES is redefining cryptographic security, providing encryption key server management and key distribution products that protect Databases, Workstations, Servers, Web Services/Application Servers and third-party applications. ERUCES Tricryption software utilizes standard encryption algorithms implemented in validated cryptographic modules. ERUCES is a privately held software company headquartered in Kansas City with offices in Tampa, Orlando, and Columbia, MD. For further information on ERUCES, visit www.eruces.com.