PC Chip Will Protect Users From Hackers and Viruses

September 16 2004

IBM ***First PC Manufacturer to Equip Its Desktop PCs with New Security Technology From National Semiconductor***

National Semiconductor today introduced two SafeKeeper™ Trusted Input/Output (I/O) devices, new hardware products designed to embed security into desktop and notebook computer motherboards. **These devices allow PC manufacturers to protect their customers' computer systems from hackers and viruses.**

IBM is the first manufacturer to equip selected models of its desktop computers with National Semiconductor’s SafeKeeper Trusted I/O devices. “IBM has led the industry in developing secure, manageable systems since pioneering embedded PC security in 1999,” said Clain

Anderson, program director of wireless and security solutions, IBM Personal Computing Division. “Security, encryption and password management are key components of IBM ThinkVantage Technologies, which simplify the PC user experience and reduce management costs for organizations of all sizes. Using National Semiconductor’s Trusted I/O chip for our newly launched desktop models helps make IBM ThinkCentre models featuring the IBM Embedded Security Subsystem the most secure industry-standard desktop PCs you can buy.”

Unlike other security hardware, National’s Trusted I/O devices integrate a Trusted Platform Module (TPM), Super I/O and embedded firmware to implement industry-standard Trusted Computing Group security functions. TPMs are microcontrollers that securely store passwords, digital certificates and encryption keys for PCs and other systems. These devices, which comply with Trusted Computing Group (TCG) specifications, protect computer software, such as BIOS, operating systems and applications, from unauthorized or malicious attacks. IBM has used TPMs since 1999.

Why Offer Computer Security in Hardware?
In an era of increased national security concerns and weekly reports of malicious attacks on PC systems, companies and consumers rely primarily on software programs to protect corporate and personal information. Unfortunately, these software-based security solutions are still vulnerable to attacks. In contrast, National’s Trusted I/O devices integrate the TPM into the existing PC architecture (Super I/O), storing the computer’s identity in silicon and making it virtually impossible for outsiders to locate key information.

Hardware solutions provide a stronger foundation for a secure computing infrastructure than stand-alone software systems. This infrastructure provides protected storage of cryptographic or sensitive data, authenticates a host computing device by verifying its identity to other computing devices, and supplies metrics that provide a reliable and trusted network environment.

Key Technology Features and Benefits

National's SafeKeeper family includes two parts, the PC8374T Desktop and PC8392T Notebook Trusted I/O devices, which are based on National's embedded 16-bit CompactRISC® core technology. Both reside on the low-pin-count (LPC) bus, an ideal place for integration because it sits at the intersection of input devices to the PC.

Since these new Trusted I/O devices are pin- and software-compatible with National's current Super I/O products, system engineers easily can create a dual-system design that can accept either part. This gives manufacturers flexibility to design "TPM-ready" systems without designing in an additional empty socket.

Industry Standards and Partnerships

National developed its Trusted I/O devices to meet the Trusted Computing Group's TPM 1.1b specification. TCG developed these specifications with industry-leading system, silicon and software providers to create standard interfaces and interoperability between hardware and software layers. These industry standard interfaces allow National to partner with security software developers such as IBM and Wave Systems Corp. to offer customers multiple software solutions that work in conjunction with National's integrated hardware.

Pricing and Availability

National's Desktop PC8374T Trusted I/O device is available now in a PQFP-128 package and is priced at $5 each in 1,000-unit volumes. The Notebook PC8392T Trusted I/O device will be available in the fourth quarter of 2004 and will be priced at $7 each in 1,000-unit volumes. All packages are available lead-free.

Citation: PC Chip Will Protect Users From Hackers and Viruses (2004, September 16) retrieved 18 April 2024 from https://phys.org/news/2004-09-pc-chip-users-hackers-viruses.html