A Safer System for Home PC's Feels Like Jail to Some Critics

By JOHN MARKOFF

SAN FRANCISCO, June 29 — Your next personal computer may well come with its own digital chaperon.

As PC makers prepare a new generation of desktop computers with built-in hardware controls to protect data and digital entertainment from illegal copying, the industry is also promising to keep information safe from tampering and help users avoid troublemakers in cyberspace.

Silicon Valley — led by Microsoft and Intel — calls the concept "trusted computing." The companies, joined by I.B.M., Hewlett-Packard, Advanced Micro Devices and others, argue that the new systems are necessary to protect entertainment content as well as safeguard corporate data and personal privacy against identity theft. Without such built-in controls, they say, Hollywood and the music business will refuse to make their products available online.

But by entwining PC software and data in an impenetrable layer of encryption, critics argue, the companies may be destroying the very openness that has been at the heart of computing in the three decades since the PC was introduced. There are simpler, less intrusive ways to prevent illicit file swapping over the Internet, they say, than girding software in so much armor that new types of programs from upstart companies may have trouble working with it.

"This will kill innovation," said Ross Anderson, a computer security expert at Cambridge University, who is organizing opposition to the industry plans. "They're doing this to increase customer lock-in. It will mean that fewer software businesses succeed and those who do succeed will be large companies."

Critics complain that the mainstream computer hardware and software designers, under pressure from Hollywood, are turning the PC into something that would resemble video game players, cable TV and cellphones, with manufacturers or service providers in control of which applications run on their systems.

In the new encrypted computing world, even the most mundane word-processing document or e-mail message would be accompanied by a software security guard controlling who can view it, where it can be sent and even when it will be erased. Also, the secure PC is
specifically intended to protect digital movies and music from online piracy.

But while beneficial to the entertainment industry and corporate operations, the new systems will not necessarily be immune to computer viruses or unwanted spam e-mail messages, the two most severe irritants to PC users.

"Microsoft's use of the term `trusted computing' is a great piece of doublespeak," said Dan Sokol, a computer engineer based in San Jose, Calif., who was one of the original members of the Homebrew Computing Club, the pioneering PC group. "What they're really saying is, `We don't trust you, the user of this computer.'"

The advocates of trusted computing argue that the new technology is absolutely necessary to protect the privacy of users and to prevent the theft of valuable intellectual property, a reaction to the fact that making a perfect digital copy is almost as easy as clicking a mouse button.

"It's like having a little safe inside your computer," said Bob Meinschein, an Intel security architect. "On the corporate side the value is much clearer," he added, "but over time the consumer value of this technology will become clear as well" as more people shop and do other business transactions online.

Industry leaders also contend that none of this will stifle innovation. Instead, they say, it will help preserve and expand general-purpose computing in the Internet age.

"We think this is a huge innovation story," said Mario Juarez, Microsoft's group product manager for the company's security business unit. "This is just an extension of the way the current version of Windows has provided innovation for players up and down the broad landscape of computing."

The initiative is based on a new specification for personal computer hardware, first introduced in 2000 and backed by a group of companies called the Trusted Computing Group. It also revolves around a separate Microsoft plan, now called the Next Generation Secure Computing Base, that specifies a tamper-proof portion of the Windows operating system.

The hardware system is contained in a set of separate electronics that are linked to the personal computer's microprocessor chip, known as the Trusted Platform Module, or T.P.M. The device includes secret digital keys — large binary numbers — that cannot easily be altered. The Trusted Computing Group is attempting to persuade other industries, like the mobile phone industry and the makers of personal digital assistants, to standardize on the technology as well.

The plans reflect a shift by key elements of the personal computer industry, which in the past had resisted going along with the entertainment industry and what some said they feared would be draconian controls that would greatly curtail the power of digital consumer products.

Industry executives now argue that by embedding the digital keys directly in the hardware of the PC, tampering will be much more difficult. But they acknowledge that no security system is perfect.
The hardware standard is actually the second effort by Intel to build security directly into the circuitry of the PC. The first effort ended in a public relations disaster for Intel in 1999 when consumers and civil liberties groups revolted against the idea. The groups coined the slogan "Big Brother Inside," and charged that the technology could be used to violate user privacy.

"We don't like to make the connection," said Mr. Meinschein. "But we did learn from it."

He said the new T.P.M. design requires the computer owner to switch on the new technology voluntarily and that it contains elaborate safeguards for protecting individual identity.

The first computers based on the hardware design have just begun to appear from I.B.M. and Hewlett-Packard for corporate customers. Consumer-oriented computer makers like Dell Computer and Gateway are being urged to go along but have not yet endorsed the new approach.

How consumers will react to the new technology is a thorny question for PC makers because the new industry design stands in striking contrast to the approach being taken by Apple Computer.

Apple has developed the popular iTunes digital music store relying exclusively on software to restrict the sharing of digital songs over the Internet. Apple's system, which has drawn the support of the recording industry, permits consumers to share songs freely among up to three Macintoshes and an iPod portable music player.

Apple only has a tiny share of the personal computer market. But it continues to tweak the industry leaders with its innovations; last week, Apple's chief executive, Steven P. Jobs, demonstrated a feature of the company's newest version of its OS X operating system called FileVault, designed to protect a user's documents without the need for modifying computer hardware.

Mr. Jobs argued that elaborate hardware-software schemes like the one being pursued by the Trusted Computing Group will not achieve their purpose.

"It's a falsehood," he said. "You can prove to yourself that that hardware doesn't make it more secure."

That is not Microsoft's view. The company has begun showing a test copy of a variation of its Windows operating system that was originally named Palladium. The name was changed last year after a trademark dispute.

In an effort to retain the original open PC environment, the Microsoft plan offers the computer user two separate computing partitions in a future version of Windows. Beyond changing the appearance and control of Windows, the system will also require a new generation of computer hardware, not only replacing the computer logic board but also peripherals like mice, keyboards and video cards.

Executives at Microsoft say they tentatively plan to include the technology in the next version of Windows — code-named Longhorn — now due in 2005.
The company is dealing with both technical and marketing challenges presented by the new software security system. For example, Mr. Juarez, the Microsoft executive, said that if the company created a more secure side to its operating system software, customers might draw the conclusion that its current software is not as safe to use.

Software developers and computer security experts, however, said they were not confident that Microsoft would retain its commitment to the open half of what is planned to be a two-sided operating system.

"My hackles went up when I read Microsoft describing the trusted part of the operating system as an option," said Mitchell D. Kapor, the founder of Lotus Development Corporation, and a longtime Microsoft competitor. "I don't think that's a trustworthy statement."

One possibility, Mr. Kapor argued, is that Microsoft could release versions of applications like its Office suite of programs that would only run on the secure part of the operating system, forcing users to do their work in the more restricted environment.

Microsoft denies that it is hatching an elaborate scheme to deploy an ultra-secret hardware system simply to protect its software and Hollywood's digital content. The company also says the new system can help counter global cybercrime without creating the repressive society imagined by George Orwell in

Microsoft is committed to "working with the government and the entire industry to build a more secure computing infrastructure here and around the world," Bill Gates, Microsoft's chairman, told a technology conference in Washington on Wednesday. "This technology can make our country more secure and prevent the nightmare vision of George Orwell at the same time."

The critics are worried, however, that the rush to create more secure PC's may have unintended consequences. Paradoxically, they say, the efforts to lock up data safely against piracy could serve to make it easier for pirates to operate covertly.

Indeed, the effectiveness of the effort to protect intellectual property like music and movies has been challenged in two independent research papers. One was distributed last year by a group of Microsoft computer security researchers; a second paper was released last month by Harvard researchers.

The research papers state that computer users who share files might use the new hardware-based security systems to create a "Darknet," a secure, but illegal network for sharing digital movies and music or other illicit information that could be exceptionally hard for security experts to crack.

"This is a Pandora's box and I don't think there has been much thought about what can go wrong," said Stuart Schechter, a Harvard researcher who is an author of one of the papers. "This is one of those rare times we can prevent something that will do more harm than good."