How Trustworthy Is Trusted Computing?

Steven J. Vaughan-Nichols

One of the biggest issues facing computer technology today is data security. And the problem has gotten worse because users are working with sensitive information more often, while the number of threats is growing and hackers are developing new types of attacks.

Because of this, many technology experts advocate development of trusted computing (TC) systems that integrate data security into their core operations, rather than implementing it via add-on applications. In essence, TC systems would cryptographically seal off the parts of the computer that deal with data and applications and give decryption keys only to programs and information that the technology judges to be trustworthy.

Online content providers could also use the systems' ability to prevent computers from accessing applications and data to keep people from listening to, copying, or otherwise using intellectual property in ways that providers don't want.

Companies have established three major trusted-computing initiatives: Microsoft's Next-Generation Secure Computing Base (NGSCB), formerly known as Palladium; Intel's LaGrande; and the Trusted Computing Platform Alliance (TCPA), an industry work group of more than 190 companies.

Wave Systems has released a cryptography chip for trusted computing and Microsoft is already developing its system.

Proponents say the initiatives will

increase users' trust in their ability to protect their systems from malicious code and guard their data from theft.

Opponents, on the other hand, contend the projects provide security by giving TC technology control that users should have over their own machines. They say this gives the vendors too much power over computing platforms, which they could abuse to help their own bottom line. Detractors also say that trusted computing's intellectual-property protection capabilities unfairly favor online content providers, often partners with TC vendors, over consumers.

Nonetheless, vendors are moving forward with trusted-computing technology, so the key issue is whether businesses will adopt it.

CRYPTOGRAPHIC TRUSTED COMPUTING

Cryptographic TC technology protects data and programs on users' computers by sealing them in an encrypted virtual vault. If outside data or programs want access to the vault, they must pass muster with the TC system and obtain decryption keys. Only trusted processes would gain access to disk storage; the CPU memory space, including the stack and on-chip cache; and main memory.

TC systems don't actually decide whether code is safe. Instead, they identify users, their computing systems (based on a unique identifying digital signature), and the applications or data they want to run. Trusted agents would provide much of the information. The agents identify the users and their computers to TC systems, which would then consult directory services to determine whether the users are authorized to run the applications or data on their systems, if the material is from a source deemed in advance to be trustworthy, and what level of access it should have to system resources.

Trusted computing uses technologies such as digital certificates and public key infrastructure to authenticate participants and provide cryptographic keys.

For maximum protection, TC systems would encrypt data not only as it moves from machine to machine but also as it moves between machine components such as the video card and monitor.

This would thus address two thorny PC-security problems: users getting encrypted data from the Web but storing it unencrypted locally, leaving the information vulnerable; and hackers installing applications—such as keystroke loggers or screen-capture software—on PCs to gain access to stored data.

Peter Biddle, product unit manager in Microsoft's Windows Trusted-Platform Technologies Group, said TC systems could block viruses, which wouldn't be authorized to enter the virtual data vault.

However, said Ross Anderson, a University of Cambridge computer scientist and noted security expert, "Most viruses nowadays exploit the scripting languages embedded in products like [Microsoft] Office." He said a document containing malicious scripting could be deemed trustworthy by a TC

system and then access a computer and cause damage.

TRUSTED-COMPUTING INITIATIVES

The major TC initiatives differ primarily in where the encryption/decryption functionality occurs. In NGSCB and La Grande, it is incorporated into the main CPU, thereby avoiding the problem of unencrypted data going over the data bus to the dedicated processor. However, this would require new CPUs that have the encryption/decryption functionality built in.

In contrast, TCPA and Wave Systems' Embedded Application Security System (Embassy) move the workload from the CPU to a special-purpose chip.

Microsoft's NGSCB

Of the three major TC projects, NGSCB is closest to deployment.

Microsoft has not set an official release date for the technology. There had been speculation that it would ship with the next major Windows release, code-named Longhorn, in 2004. However, Mary Jo Foley, editor of the *Microsoft Watch* newsletter, said NGSCB probably won't appear until the 2006 release of Windows. Details of the technology are in the sidebar "Microsoft's Next-Generation Secure Computing Base."

Intel's LaGrande

Intel has not issued any technical information on LaGrande and did not respond to requests for comments.

From available information, it appears that Intel will integrate LaGrande capabilities into future processors and chipsets. The technology would sandbox numerous risky processes by putting the CPU, chipset, I/O devices, and the graphics processor in an encryption-based security wrapper, as called for by NGSCB.

Rob Enderle, research fellow for the Giga Information Group, a market research firm, said LaGrande and NGSCB have a huge potential to stall the TC market because they would require a major, expensive, and time-consuming redesign of the OS and microprocessor.

TCPA

The TCPA—formed in 1999 by Compaq Computer (now part of Hewlett-Packard), HP, IBM, Intel, and Microsoft—calls for creation of a trusted platform module, a motherboard-mounted cryptographic processor with a unique digital signature.

Unlike the Intel and Microsoft plans, though, the TPM would be on a separate chip and handle only motherboard and network traffic. And unlike NGSCB, TCPA wouldn't extend security to each component of the system but instead only to communications between the CPU and network. Thus, a keyboard reader program on a PC could still pick up a user's keystrokes.

Some models of the IBM ThinkPad T30 high-end laptop use an Atmel processor based partly on TCPA. For

Microsoft's Next-Generation Secure Computing Base

Microsoft's NGSCB is further along in development than the other major trusted-computing projects and thus shows how TC might work in practice.

Components

NGSCB's nexus component would function like an OS microkernel to manage trusted code throughout the system and enforce user choices.

The technology requires a new basic machine instruction set and CPU operating mode, as well as hardware designed specifically to support it. AMD and Intel are developing NGSCB-aware microprocessors.

In addition, Microsoft's NGSCB would require several types of hardware to add the ability to handle encrypted I/O: the CPU, the chipset, I/O devices, and the graphics processor. Each PC also needs an 8-bit, tamper-resistant cryptographic chip with unique encryption keys.

Identity service authorities

TC systems would accept only applications and code approved by a company or organization serving as an identity service authority. According to Peter Biddle, product unit manager in Microsoft's Windows Trusted-Platform Technologies Group, identity service authorities would authenticate trusted applications and data sources. This is designed to keep out unapproved code such as viruses.

Users would thus trust code based on whether they have confidence in the signing authority. The trustworthiness of these authorities is key to TC systems' effectiveness and appeal.

There will be multiple identity service authorities, although Microsoft hasn't determined who they will be and what the company's relationship with them will be. Vendors of TC-compatible applications, including Microsoft, could be considered authorities for their own software.

Intellectual-property protection

Either a CPU or a cryptographic processor would encrypt files with coding for use by a specific PC. This makes the files useless if moved or copied from one PC to another. Such a capability would help content providers enforce their intellectual-property usage policies.

In addition, Biddle said, TC systems would control a user's ability to work with content providers' intellectual-property protection capabilities—specifically, the keys embedded in content files that lock and unlock protected material. Only users with the appropriate rights for a particular file could obtain the keys and use the content.

example, the processor generates and stores digital certificates and private keys, and provides hardware support for multiple authentication schemes, as well as the encryption and decryption of files on demand.

Wave Systems' Embassy

Wave Systems' Embassy doesn't get the attention that the other initiatives do, but it's the only TC technology already in a desktop computer: NEC's Packard Bell Secure PC.

Embassy is an open-system hardware and software approach that uses HP's VerSecure Framework, a network-encryption system for secure transaction processing. Embassy's primary emphasis is enabling secure e-commerce transactions rather than providing a complete TC environment for PCs. It encrypts financial transactions over the network, rather than securing processes within the PC.

In Embassy's model, Integrated Technology Express makes a motherboard chip that handles the RSA encryption duties, Standard Microsystems supplies TC-capable I/O, and VeriSign contributes digital certification services.

CONTROVERSY AND CONCERNS

Trusted computing faces numerous challenges. For example, vendors must generate demand for security features that may add cost to systems. In addition, technology companies must balance the additional security created by closing off parts of a system with users' desire to have open network access.

Andrew Huang, cofounder of Xenatera Partners, a technology development and consulting company, contended that TC doesn't provide enough trust. He said that cryptographic systems don't offer adequate security for computer memory and thus leave machines vulnerable to buffer overflow and other memory-based attacks.

One major concern is that TC software and hardware would take away freedom by making decisions about data and applications that typically have been left to users. In essence, some critics say, TC systems would control a user's access to data and applications. If the system malfunctions, the user could be denied access for no reason.

Some critics say that TC companies are pushing the technology because it helps online-content owners enforce intellectual-property policies at the expense of the end user.

While trusted-computing proponents say the technology will secure users' programs and data, opponents say it will take control of too many computer functions away from users.

In fact, *Microsoft Watch's* Foley predicted that intellectual-property protection will be NGSCB's primary application.

However, Microsoft's Biddle said, intellectual-property protection is not a necessary part of NGSCB, although the technology could enhance its implementation.

This could be a problem for the technology, according to Giga's Enderle. He explained, "It is viewed as a tool to control and monitor the user, not as a lock that keeps the bad guys out."

Martin Reynolds, vice president in market-research-firm Gartner Inc.'s Dataquest organization, said, "Consumer backlash and the risk of hardware hacks [could] compromise the business value of the system."

TC proponents argue that users have the choice of not running the technology if they don't like what it does. However, opponents say not running TC systems might cause them to lose the ability in the future to use applications or download content that will work only with trusted technologies.

Despite his concerns about today's proposed TC implementations, Xenatera's Huang said that eventually, "trusted computing has to become successful in order for the Internet to become a cornerstone business medium."

Well-known open source software advocate Richard Stallman said one reason he opposes TC is that it may threaten open source operating systems and applications by viewing them as nonstandard and untrustworthy and thus not letting them run.

Biddle acknowledged that TC has image problems. He said, "We believe our biggest challenge is educating people about the facts of what we are doing. There are many misconceptions about NGSCB, so we are engaging many stakeholders in a collaborative dialogue."

However, some critics won't be won over. "I hope that trusted computing will die in the marketplace, or be blocked by legislators," said Cambridge's Anderson. "Trusted computing doesn't necessarily provide adequate security," he argued. "[It] benefits big companies at the expense of consumers and lets technology take too much control of systems away from users."

In the end, perhaps the real issue is how TC will be deployed. As Reynolds said, "Trusted computing could be used for content protection. However, such applications will lead to both consumer backlash and hardware hacks that destroy the ability of third parties to trust computers. So there is a balance to be achieved. If it's not found, consumers will refuse to buy trusted software and machines." ■

Steven J. Vaughan-Nichols is a freelance writer based in Arden, North Carolina. Contact him at sjvn@vna1.com.

Editor: Lee Garber, *Computer*, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; l.garber@computer.org