



www.trustedcomputing.org

Trusted Computing Platform Alliance

Building Levels of TRUST Into Every Transaction

Governments, businesses, and even our personal lives depend so much on computers, it's alarming how susceptible they are to security breaches and computer viruses. While total security may be an unattainable goal, significant improvements can be made through a new approach called Trusted Computing.

Trusted Computing focuses on building levels of trust into the computing platform, whether it's a PC, PDA or other device. Instead of the current strategy of continually adding and updating outside barriers to viruses and intrusions, Trusted Computing starts with a first level of trust integrated into both the hardware and pre-operating system environments. Once these environments are better protected, other portions of the computing platform can be addressed to provide additional levels of trust.

In 1999, five companies – **Compaq, HP, IBM, Intel** and **Microsoft** – formed the Trusted Computing Platform Alliance as the first step in defining a standard for advancing and implementing the concepts of Trusted Computing. Today TCPA has over 170 members, including leading companies in hardware, software, communications, and other technologies. These companies are joined in an open alliance to help develop the necessary technology and cooperation to make Trusted Computing a reality. The first level of trust will be achieved through adaptation of a TCPA specification for silicon technology.

Why Security Is Becoming a Greater Issue

Computer use is so ubiquitous, it's easy to become complacent about data security. But the truth is, the nature of computing today has created an even greater need for security – a need that must be addressed for more secure computing and applications like e-business to truly flourish.

Where once PCs were totally isolated or connected to only an organization's network, today's PCs are connected to the Internet and feed data back and forth to devices such as PDAs and cellular phones. Newly popular peer-to-peer networks even put PCs in direct communication with one another through the Internet. The result? PCs are becoming more like personal servers and the opportunities for unauthorized break-ins, criminal mischief and virus attacks are greater than ever.

This increasing vulnerability is costly. With an estimated effect on business losses and computer management expenses, this vulnerability accounted for 5.57% of gross revenues in 2000 (Omni Report 2001). Unless something is done, these costs are going to continue unabated.

A New Approach to Computer Security

For years, computer security has consisted of adding layers (passwords, encryption and anti-virus software) between the outside world and the PC. With each new virus threat or attack, a layer has to be strengthened or a new one added. This band-aid approach only mends the tear. It doesn't address the core problem.

Through Trusted Computing, TCPA promotes a more integral solution. This solution incorporates progressively greater levels of trust by first adding a layer of protection to the platform and applications running on that platform, then adding a layer of protection to the input and outputs of that platform and its communications and networking channels.

Trusted Computing Requires Transactions and Computing Devices to be:

Trusted – acting in a recognized and attestable manner

Reliable – readily available for transactions and communications, as well as prepared to act against viruses and other intrusions

Safe – able to stop unwanted intervention or observation

Protected – sharing information with only those who are authorized

Private – providing users a way to manage their privacy



Trusted Clients communicate their platform configuration. Prior to a transaction, other Trusted Clients and Servers use this information to verify the clients are operating in an uncompromised state.

Trusted Computing Will:

- Provide protected storage of cryptographic and sensitive data by a TCPA device
- Authenticate a host computing device, verifying its identity to other computing devices
- Supply metrics providing reliable, trusted network environments
- Provide protected public key cryptographic and authentication processes

The Value of Trusted Computing

For computer owners: Trusted Computing hardens computing devices to software-based attacks, integrating capabilities to better protect transactions through the addition of trusted hardware and operating systems. This will help make PCs more manageable, lowering the total cost of ownership by reducing risks of information theft.

For business: Trusted Computing reduces one of the greatest barriers to e-business – the fear that everything from credit card numbers to confidential corporate data could be stolen. It defines a platform security framework that will help allay fears of sharing sensitive information and spur a new burst of growth in e-business.

For OEMs: Trusted Computing gives original equipment manufacturers a new way of adding value to their products and building trust in their brands. They can ensure interoperability with this new standard in computer security while differentiating their products with their own innovations.

Find Out More

Through Trusted Computing, the TCPA is engineering a new world of trust. You can be a part of it. To learn more, visit:

www.trustedcomputing.org



TCPA Program Office
Carol Burke, M/S JF1-229
Intel Corporation
2111 NE 25th Ave.
Hillsboro, OR 97124
Phone: 503.264.9660
Fax: 503.264.0281