



Trusted Network Connect to Ensure Endpoint Integrity May 2005

The Trusted Computing Group (TCG) is extending its efforts in trusted computing to the development and promotion of open solution architecture to enhance network trustworthiness, focused on establishing and enforcing security policies before endpoints connect to multi-vendor environments.

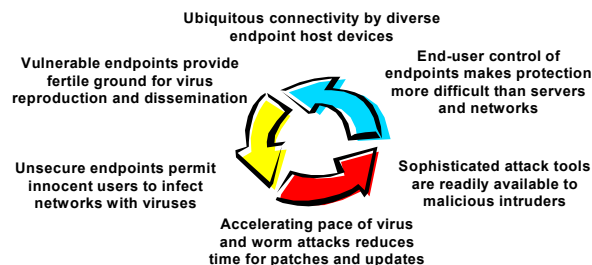
Since its announcement in 2003, the Trusted Computing Group has created work groups to address the desktop host, mobile devices and PDAs, servers, storage, peripherals, infrastructure and other issues. The Trusted Network Connect Sub Group extends TCG's standardization efforts to include the security and integrity of networks, by creating mechanisms to prevent untrusted devices from connecting to or disrupting a network.

The Nature of the Problem

Networks, systems, software applications and data form the critical foundation and essential structure for the day-to-day operations of most organizations. *"The computer is the network"* has given way to *"the network is the business."* Without a reliable and functional network, the business is not safe. The difficulty and expense of keeping the network secure and stable are enormous *and* growing. The lost revenue and large recovery efforts required when those systems are shut down, or corrupted, devastate a company's bottom line and jeopardize its future prospects.

Inappropriate and unauthorized access takes many forms and has many consequences. Viruses and email worms, Trojan horses, denial of service attacks, and other malicious activities frequently utilize end-user machines to penetrate enterprise environments, even when perimeter security mechanisms like firewalls are in place. While it is difficult to quantify the impact of the business disruption and havoc wreaked by these compromises, business losses include help desk calls, desktop restoration or rebuilding, network benchmarking and repairs, loss or corruption of data, lost productivity, and potential loss of new business.

Endpoint Security Issues



Secure endpoint connections reduce the risk of financial loss and compromised data

Some consulting groups, such as London-based Mi2g, estimate damages caused by viruses like Sobig or Klez to be in the billions of dollars. The Blaster virus alone is reported by Mi2g as having infected more than 300,000 computers in 24 hours, causing \$525 million in damages. Thousands of new viruses and exploits are discovered every year. The escalating threat from sophisticated and subtle compromises motivates TCG members to build a standards-based framework for more effective endpoint protection and malware detection.

The Way to a Better Solution

Network administrators face the difficult task of enforcing unified security policies for network access in an increasingly diverse network environment that supports heterogeneous devices and software from many vendors. The requirement for secure, appropriate access for these devices must be balanced with the requirement to maintain the integrity of their networks and services.

Since traditional access control security, based on user and machine identities, fails to protect organizations against these aggressive new attacks, operators must extend traditional definitions of authentication, authorization and access control to include more detailed endpoint inspection.

For example, a network administrator could require that only systems using anti-virus software with the most recent signature definition file for access to the production environment. Or, endpoint devices might be required to install critical operating system and application patches, as well as personal firewalls or other corporate security software. Theoretically, any property of the endpoint system could be used to define requirements for access to the enterprise network.

The explosion in network-based communications and computing platforms translates directly to an explosion in system interfaces and network protocols. Smart cell phones and PDAs that exchange data with desktops, wireless devices and networks – not to mention increasing use of outside contractors and consultants who need access to corporate networks - illustrate new demands for seamless and security connectivity.

Security Needs and Interoperability Efforts

<i>Security Requirements</i>	<i>Interoperability Standards</i>
<ul style="list-style-type: none"> ▪ Permit only authenticated users and devices to connect to the network 	<ul style="list-style-type: none"> ▪ IEEE 802.1x, IETF RADIUS, IETF EAP <p>Focus of TCG Efforts</p>
<ul style="list-style-type: none"> ▪ Enable administrator to establish security policies for anti-virus, patch levels, software versions, etc. 	
<ul style="list-style-type: none"> ▪ Measure device configuration against security policies before its connection to the network is allowed 	
<ul style="list-style-type: none"> ▪ Identify devices that are not compliant 	
<ul style="list-style-type: none"> ▪ Quarantine non-compliant devices 	
<ul style="list-style-type: none"> ▪ Remediate non-compliant devices to ensure compliance to security policies 	

Industry Leadership

More than 60 of TCG's 100+ member companies are working on the TNC architecture. TNC participants include switch and network equipment manufacturers, security vendors, managed service providers, chip manufacturers, and other companies with a stake in enterprise networks, representing the broad range of organizations involved in building network infrastructures. These members provide the knowledge and perspective required to incorporate complex multidisciplinary issues into a functional, interoperable standard.

The Trusted Network Connect Mission

The TNC architecture has been designed to assist network administrators in protecting networks from viruses, worms, and denial of service attacks by allowing them to audit endpoint configurations and impose enterprise security policies before network connectivity is established. The TNC architecture builds on existing industry standards and defines new standards as necessary, with the objective of enabling non-proprietary and interoperable solutions within multi-vendor environments.

The TNC architecture will significantly reduce the risks of doing business electronically. The open specification efforts will encompass the definition of software interfaces and protocols for communication among endpoint security components and between endpoint hosts and networking elements.

Developing the TNC Architecture

The TNC architecture describes the interaction of various network entities to measure the state of a client system or device attempting to connect to a network; to communicate that state to other systems on the network for assessment of the client's compliance to minimum security policy requirements; and to determine the network's reaction to the request for access. The architecture incorporates software interfaces and protocols for communication among endpoint security components, and between endpoint hosts and networking elements.

The Trusted Network Connect architecture will:

- Enable endpoint integrity by establishing a "level of trust" in the state of an endpoint. Specifically, solutions based on the specification will ensure the presence, status, and patch level of mandated applications as well as revisions of signature libraries for anti-virus and intrusion detection and prevention system applications
- Maintain the organization's access policy, by validating the endpoint device and/or user authentication and establishing a level of trust before allowing connection to the network.
- Provide quarantine and remediation for endpoint devices by first isolating devices that do not meet the security policy requirements for "trust" and then, if possible, applying appropriate remediation, such as upgrading software or virus signature libraries, to satisfy the security policy and provide eligibility for connection.

Products based on the Trusted Network Connect architecture will help managers of enterprise and public networks protect their networks from compromises within the network or at its endpoints. Compromise and damage to endpoint configuration, including applications and data, will be detectable and remedied at the time of connection establishment. This approach limits the spread of malicious code (e.g., viruses, worms, Trojan horses) throughout networks, and will reduce the costs associated with containment and remediation.

Leveraging Existing Standards

The Trusted Network Connect efforts will build on existing industry standards when appropriate, such as the IEEE 802.1x and the IETF EAP RFC 3748 protocol for host access negotiation with network devices.

IEEE's 802.1x and IETF's EAP standards were created to address secure network connectivity. Both provide an obvious vehicle for extending the network connect process to include host-related security configuration information and are widely supported by networking equipment across the industry. Their wide distribution enables customers to incorporate TNC technology by leveraging existing investments, without sacrificing interoperability or freedom of choice.

The Trusted Network Connect framework gives customers interoperable solutions from multiple vendors—giving them greater choice in selecting the components best suited to their requirements.

Trusted Network Connect and the Trusted Platform Module

The Trusted Network Connect Specification has been developed for implementation on a wide variety of platforms and devices, including those that incorporate the Trusted Platform Module (TPM) microchip. The TPM, based on TCG specifications, is a special purpose microcontroller that stores encryption keys, passwords, and digital certificates in platforms. The TNC specification does not mandate the use of TPM, but those networks and systems incorporating TPM chips will have higher levels of security and trust by leveraging its hardware-based assurance.

Learn More about TCG and TNC

More information on the Trusted Computing Group and the TNC, including membership details and the organization's specifications, is available at <http://www.trustedcomputinggroup.org>.