Trusted Network Connect to Ensure Endpoint Integrity
May 2004

The Trusted Computing Group (TCG) is extending its efforts in trusted computing to the development and promotion of an open solution architecture to enhance the integrity of networks by establishing and enforcing security policies for endpoint connections to multi-vendor networks.

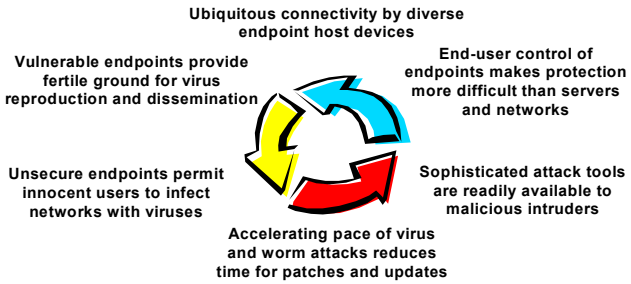
Since it was announced in 2003, the Trusted Computing Group has created work groups to address the PC client, mobile devices and PDAs, servers, infrastructure, best practices, and a number of other platforms and issues. The Infrastructure Work Group was created to focus on integrity services, authentication, and migration issues. The Trusted Network Connect Sub Group (TNC-SG) is part of the Infrastructure Work Group and extends TCG's standardization efforts to enhance 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

The networks, systems, software applications, and data of many enterprises and organizations form a critical foundation and essential structure for their daily operations. "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 are enormous, and growing. The lost revenue and large recovery efforts required when those systems and information are shutdown or corrupted due to inadequate security can devastate a company's bottom line and jeopardize its future prospects.

Inappropriate and unauthorized access takes many forms and has many consequences. Network resources are vulnerable to attack from viruses and email worms, Trojan horses, denial of service attacks, and other threats that utilize the endpoint connections as a means of entry into the network. While it is difficult to estimate the business disruption and total impact of viruses and similar attacks, those costs include the cost of help desk calls, desktop and network rebuilding and restoration, loss or corruption of data, lost productivity, and the 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 and having caused $525 million worth of damages. According to some surveys, more than 7,000 new viruses were discovered in 2003. The threat of even more sophisticated and more frequent attacks motivates TCG members to build a standards-based framework for better protection.

The Way to a Better Solution

Network administrators face the difficult task of developing and enforcing unified security policies for network access by an increasingly diverse array of communication and computing devices and software from a plethora of vendors. The pressure on network managers to support access by these new products and services must be balanced with the requirement to maintain the integrity of their networks and services.

To reduce the risks and costs of recovery from attack, operators of enterprises and public networks seek to establish and enforce security policies requiring a level of trust or integrity for the devices that connect into their networks and implement mechanisms to enforce these policies or at least identify compliance of devices before allowing them to connect. For example, a network administrator might establish a policy requiring that only systems using anti-virus software with the most recent signature definition file would be allowed to connect into the network. Furthermore, endpoint devices might be required to use the most recent patches for operating system and application vulnerability and the most recent version of firewall or intrusion detection and protection software.

As the diversity of communications and computing devices seeking network access has increased, so has the diversity of the interfaces and protocols. Smart cell phones and PDAs that synch up to desktops, wireless devices and networks, and the increasing use of outside contractors and consultants who need access to corporate networks are only three examples of the new connectivity demands. This increased diversity magnifies the need for a cooperative effort to address the vulnerabilities and reduce the risks.

Security Needs and Interoperability Efforts

Security Requirements	Interoperability Standards
▪ Permit only authenticated users and devices to connect to the network	IEEE 802.1x, IETF RADIUS, IETF EAP
▪ Enable administrator to establish security policies for anti-virus, patch levels, software versions, etc.	Focus of TCG Efforts
▪ Measure device configuration against security policies before connection to the network is allowed	
▪ Identify devices that are not compliant	
▪ Quarantine non-compliant devices	
▪ Remediate non-compliant devices to ensure compliance to security policies	

The Trusted Network Connect Mission

The TNC will develop specifications for interoperable security solutions that will assist network administrators in protecting networks from viruses, worms, and denial of service attacks by allowing them to enforce security policies to prevent untrusted systems or devices from connecting to their networks. The TNC specifications will build on existing industry standards, and will define and submit new standards as necessary, with the objective of enabling truly interoperable solutions within multi-vendor environments and significantly reducing the risks of doing business electronically. The standardization efforts will encompass the definition of software interfaces and protocols for communication among endpoint security components and between endpoint hosts and networking elements. TCG anticipates that the initial TNC specification will be available later this year.

Industry Leadership

A number of companies—including Foundry Networks, Extreme Networks, Funk Software, InfoExpress, iPass, Juniper Networks, Meetinghouse Data Communications, Trend Micro, Network Associates, Sygate, Symantec, and Zone Labs—have joined TCG in 2004 to support the standards work of TCG and to participate with HP, Intel, Verisign and other TCG members in the development of the TNC specification. Participation is open to all promoter and contributor TCG members. The participating switch and network equipment manufacturers, security vendors, managed service providers, chip manufacturers, and other companies with a stake in enterprise networks will work together to enhance the integrity of network environments. These members bring together the necessary knowledge and perspective to be able to address the complex multi-disciplinary issues and develop interoperable standards.

Some members have already been working on the general concept and have developed solutions that demonstrate some of the benefits of the anticipated Trusted Network Connect specification. These solutions of currently available capabilities have been demonstrated at Networld+InterOp May 2004. These demonstrations illustrate the degree of vendor cooperation that is already underway and signify that the goals of a standards-based open architecture solution are achievable within a reasonable timeframe. Information about these demonstration solutions is available on the member companies' web sites. Additional products will be available later this year as TCG finalizes the initial specification.

TCG Standards Efforts

TCG will develop specifications for the interaction of various parts of the network 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, to decide if the client has met the minimum security policy requirements for "trust", and then to determine how the network reacts to the request for access.

The standardization effort will define software interfaces and protocols for communication among endpoint security components and between endpoint hosts and networking elements. The work of the Trusted Network Connect Sub-Group will provide a common architecture for vendor solutions that 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 upgrade level of mandated applications, revisions of signature libraries for anti-virus and intrusion detection and prevention system applications, and the patch level of the endpoint's operating system and applications.
- Maintain access policy by helping to ensure endpoint device and/or user authentication and establishing a level of trust before allowing connection to the network.
- Provide quarantine and remediation measures 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 specification are expected to 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 helps limit 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. For example, the organization currently is considering using the IEEE 802.1x protocol and the IETF EAP RFC 3748 protocol for host access negotiation with network devices. It is expected that the specification also will incorporate RADIUS [RFC 2865] for making access verification decisions and defining network access privileges. IEEE's 802.1x and IETF's EAP standards were created to address secure network connectivity. Both provide a natural vehicle for

enhancing the network connect process and are widely supported by networking equipment across the industry. Their availability and wide distribution enables customers to leverage existing investments without sacrificing interoperability and choice.

The work of the Trusted Network Connect Sub Group will extend these existing standards to provide a comprehensive network security structure that incorporates fundamental aspects of trusted computing. This framework will provide customers with interoperable solutions from multiple vendors—giving them greater choice in selecting components best suited to their requirements. This framework will be an open industry standard that will enable development and deployment of products for secure heterogeneous environments.

Trusted Network Connect and the Trusted Platform Module

The Trusted Network Connect Specification is being developed for implementation on a wide variety of platforms and devices, including those that incorporate the Trusted Platform Module (TPM) microchip and those that do not. The TPM is a special purpose microcontroller that stores encryption keys, passwords, and digital certificates in platforms. TPM has been the subject of a number of existing TCG specifications. While solutions based on the Trusted Connect specification can be used to protect any network, those networks and systems incorporating TPM chips will exhibit higher levels of security and trust by leveraging the hardware-based assurance of the TPM. TCG's mission is to develop standards specifications for products that will let users protect critical systems, data, and information for trusted computing across multiple platform types. The work of the Trusted Network Connect Sub Group is highly complementary to TCG's mission and will augment other TCG efforts to secure the platform.

Learn More about TCG and TNC

TCG is an industry standards body formed to develop, define, and promote open standards for trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. TCG specifications are designed to enable more secure computing environments without compromising functional integrity with the primary goal of helping users to protect their information assets from compromise due to external software attack and physical theft.

More information on TCG membership and the organization's specifications is available at www.trustedcomputinggroup.org.