



CONTACT: Anne Price
602-840-6495
Mobile 602-330-6495
press@trustedcomputinggroup.org

**TRUSTED NETWORK CONNECT PROVIDES PERVASIVE SECURITY
WITH NEW SUPPORT FOR REMOTE ACCESS, CLIENTLESS ENDPOINTS
AND FEDERATED ID**

**New Specifications Link Network and Physical Security for First
Time; TCG Members Show Enterprise-Wide Security in Interop Booth #869**

LAS VEGAS, May 18, 2009 – [Trusted Computing Group](http://www.trustedcomputinggroup.org) (TCG) today announced it has extended its [Trusted Network Connect](http://www.trustedcomputinggroup.org) (TNC) security architecture and multi-vendor standards to allow all devices on any IP network to be protected against threats and unauthorized access.

This extends the architecture beyond PCs on an enterprise network, adding security for remote users, printers, scanners, and process control or SCADA (Supervisory Control and Data Acquisition) systems. Integration with physical access control systems is also supported, allowing network and physical security to be tied together for greater security.

In TCG's booth at Interop Las Vegas (booth #869), TCG members will show how customers are using TNC specifications in a typical enterprise setting to secure employee cubicles, conference rooms, data centers, remote users and the factory floor.

New Specifications Extend TNC Security To All Devices on Any IP Network

To support and enable this new broader scope for the TNC architecture, TCG is releasing three new specifications today. These new TNC specifications provide standards that ensure multi-vendor interoperability for the following technologies:

- Running TNC protocols across any IP network using the widely deployed security protocol TLS. This means that any IP network can benefit from TNC's security measures without changes to that network. This specification (known as "IF-T for TLS") also permits ongoing monitoring of device health so that infections or vulnerabilities can be immediately detected and repaired.
- Securing "clientless endpoints" (devices without native TNC support), such as printers, VoIP phones, and guest PCs. This "Clientless Endpoint Support Profile" means that any IP device can benefit from TNC's security measures without changes to that device. This will help protect against attacks from devices on the network and assist in monitoring them.

-- more --

- Conveying TNC security information across security domains when necessary. This “Federated TNC” is based on the widely supported federated identity standard SAML (Security Assertion Markup Language). This capability enables users to be authenticated and assessed not just in their home organizations, but in other locations.

“As network threats and attack vectors continue to increase, protecting not just typical endpoints but any device on any network significantly increases the value of TNC in both the traditional enterprise as well as newer more dynamic deployments,” noted David O’Berry, Director of Information Technology Systems and Services, South Carolina Department of Probation, Parole and Pardon Services. “Static health checks are now of limited value due to the rapid evolution of the digital environment. However, if you take that next step and can combine persistent real-time monitoring of users who have the capability to roam between security domains with authentication vetted by their own organization, you have the potential to offer much higher security assurances to organizations concerned with defending their networks, systems and data while actually increasing the computing services available to users. TNC has taken significant steps forward with these specifications and set the stage for a flexible open framework which can enable advanced correlation and mitigation of threats in a potentially much more effective and usable model.”

FAQs and more information on these new specifications can be found at http://www.trustedcomputinggroup.org/resources/interop_las_vegas_2009_press_kit.
From Cubicle to Remote Locations, Network Security Demonstrated at Interop

Here at Interop Las Vegas in TCG’s Booth #869, Hirsch Electronics, Infoblox, Juniper Networks, Lumeta Corporation, nSolutions, Trapeze Networks, and eight other TCG member companies are showing how these pervasive security applications will secure the entire enterprise.

- In the **employee cubicle**, TNC interfaces enable location, identity, endpoint health and behavior-based access control decisions, including for unmanaged devices. Integration with physical security access control using contact and contactless smart card readers also is shown.
- TNC-based technology interoperates to provide appropriate access for **conference room users**, including visitors, partners, contractors, employees, and privileged employees, based on their identity, physical presence, endpoint compliance, role, and behavior.
- TNC interfaces enable a consistent user experience and thorough compliance checking for **remote users**, who connect via a number of untrusted or semi-trusted intermediate networks. Optional integration with a TPM provides additional hardware-based assessment to thwart rootkits.

- In the **data center**, the TNC metadata access protocol (IF-MAP) enables detection and remediation of illicit activity, such as data leakage to an endpoint or unauthorized changes to network device configurations, as well as integration with physical security devices that access the network.
- Protection for a **process control network** such as a factory floor is demonstrated, allowing provisioning, defense against attacks and enforcement against unauthorized access.

About TCG

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 and the organization's specifications are available at www.trustedcomputinggroup.org.