



**Trusted Network Connect (TNC) Pervasive Security
FAQ
May 2009**

Q. Trusted Network Connect has been considered a NAC architecture. What is new?

A. The initial focus of the TNC architecture was on identifying the devices on a network and checking their integrity when they joined the network. From the beginning, we have recognized that doing so is only a small part of defending and protecting corporate networks and assets. Based on the feedback of our customers and users, our overall vision has evolved to encompass pervasive security.

Q. What exactly is pervasive security?

A. We are using this term to indicate that all aspects of security can and should be linked together through open standards. Traditionally, organizations deploy separate systems for client security, server security, network security, data security, physical security, incident handling, and other forms of security. These systems are largely isolated, connected only through ad hoc mechanisms. By linking security systems together with open standards, threats can be identified more rapidly, correlation and response performed more accurately, and countermeasures enforced more broadly.

Q. How are you enabling these new capabilities?

A. The existing TNC architecture already includes many of the capabilities needed to enable pervasive security, such as the IF-MAP protocol for information sharing. However, we have continued to extend the existing TNC architecture to support additional capabilities and devices. Recent additions to the TNC architecture include:

- IF-T Binding to TLS specification: TNC has added a method of performing assessment of endpoints over a TLS session. This allows endpoints already on a TCP/IP network to be assessed. This is in addition to existing support for assessment over tunnelled EAP methods. The new TLS assessment method also allows for continuous monitoring of client health and reassessment whenever the client or server detects suspicious behavior.
- Federated TNC specification: TNC has defined a standard way to convey endpoint posture information between security domains. The widely implemented Security Assertion Mark-up Language (SAML), designed to support federated identity, is extended by this specification to convey information about device identity and health. Organizations that previously employed SAML for single sign-on and roaming can now consider device identity and health as well.
- Clientless Endpoint Support Profile: This specification provides a standard methodology for authorizing devices (like printers and VoIP handsets) that attach to the network but do not support security protocols. These devices have traditionally been difficult to secure, but now they can be identified and monitored in a standard, interoperable manner.

Q. Why are you providing support for clientless endpoints?

A. Security experts have been concerned for some time about the ability to monitor and health check devices such as printers, cameras, etc. that get an IP address and live on the network. There currently is no standard way to authenticate and monitor them. The new TNC specification enables this.

Q. Why is TNC extending its architecture to include physical security? Isn't that typically a different network and a totally different ecosystem of vendors and users?

A. It used to be. However, physical security systems are moving to IP networking. On the positive side, this presents opportunities for better integration with other systems and for cost savings. On the negative side, network security measures must be implemented in physical

security systems now. The bottom line is that network security and physical security worlds are converging. Several TCG members, including Hirsch Electronics and HID Global, are providing their physical security expertise to this convergence.

Q. What are the benefits of integrating physical security and network security?

A. There are two aspects to this integration and therefore two sets of benefits. First, physical security systems that have moved to IP networking require appropriate network security measures. Otherwise, conventional IP network attacks can be brought to bear without detection. Second, sharing information between physical security and network security systems provides valuable benefits on both sides. Network security systems can detect odd occurrences such as a user logging into the network from one location when the physical security system reports they're elsewhere. Thus, social engineering attacks and stolen credentials can be more easily detected.

One interesting and beneficial side effect of integrating physical and network security is that if users are required to swipe into a building before they log into the network, normal users will no longer want to "tailgate" into the building (following someone else in without swiping their badge). Tailgating will become an abnormal and suspicious behavior, thus making it more difficult for thieves to enter the building.

Q. How realistic is this vision? When will we see this put into place?

A. Here at Interop Las Vegas 2009, we are showing all of these capabilities. Some of the products are shipping, others soon will be available. For example, we demonstrated:

- 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 devices such as badge readers is also 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, 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.

Q. What kinds of changes or upgrades to equipment or software are necessary to begin using some of these new capabilities?

A. Federated TNC was designed to avoid any software changes to the client. The Roaming Assessment Profile will work with any standard 802.1X supplicant. The Web Assessment Profile will work with any HTTP/1.1 browser.

The IF-T Binding to TLS protocol is a protocol that operates on top of a standard TLS session. This means that existing TLS implementations can be used to carry the new IF-T protocol. No changes or extensions to the TLS library are required for this binding of IF-T to operate. However, changes to application code or to a TNC client may be required.

Software updates may be required to the TNC server to enable support for the Clientless Endpoint Support Profile.

Q. The IF-MAP (Metadata Access Protocol) you announced a year ago seems very interesting. Are there any updates there?

A. Yes, the idea of synchronizing data from a variety of different security devices and applications really caught a lot of attention. If you recall, IF-MAP defines a shared, real-time network information service with a powerful, real-time publish/subscribe/search mechanism

for data regarding network devices, their state, and their activities. IF-MAP automatically aggregates and associates real-time information from many different sources. IF-MAP is key to integrating security systems such as physical security and network security. This month, several companies, such as Insightix, have announced products to support IF-MAP, adding to products already available from companies such as Juniper Networks.

A few updates to the IF-MAP specification have been published this month, reflecting implementation experience and easing implementation with popular software development libraries.

Q. Who is using any products based on TNC specifications?

A. There are a number of organizations using products that incorporate various TNC specifications. Several of these are featured on TCG's website, http://www.trustedcomputinggroup.org/?e=category.solutionDetail&urlpath=network_security&resource_category_id=6, including Bankchak Petroleum, Portland Community Colleges and St. Mary's County Public Schools. The U.S. National Security Agency, working with TCG members including GDC4 Systems, is using TNC as part of its High Assurance Program (HAP) to secure and protect PCs used by military personnel; more information on that program is available at http://www.gdc4s.com/documents/D-HAPWS-6-0207_p1.pdf.

Q. For several years, there has been a battle of sorts among NAC standards. What is the status of that?

A. Initially, there were three primary NAC approaches: TNC, Microsoft's Network Access Protection and Cisco's C-NAC. Several years ago, Microsoft contributed its Statement of Health protocol to TNC, ensuring that any client with Windows Vista or Windows XP Service Pack 3 can participate in a TNC or NAP network and have its health checked.

TCG has been active in the IETF Network Endpoint Assessment working group, alongside Cisco, and that group has adopted several TNC protocols with final publication expected later this year. This should result in convergence of all three NAC approaches.

Q. There has been a lot of coverage of the potential cost and complexity of NAC implementations. What is your opinion on this?

A. Certainly there are a lot of moving parts to securing the network. We believe that by providing an open, non-proprietary framework that has been widely adopted by dozens of vendors, we can give users options as to which capabilities they can use and cost-effective ways to get them. For example, they will find support for TNC embedded in a number of switches and other hardware.

We recommend that those interested in NAC implementation:

- Work with what you have and look for non-proprietary approaches
- Tackle low-hanging fruit first to reduce complexity, scope; phase the implementation
- Maintain transparency, communication, auto-remediation to keep support costs low and increase user acceptance
- Evaluate future needs as well as present ones

Case studies that might help you are online at

http://www.trustedcomputinggroup.org/?e=category.solutionDetail&urlpath=network_security&resource_category_id=6 and a presentation from TCG on this topic is available at http://www.trustedcomputinggroup.org/files/resource_files/C4F1F0AF-1D09-3519-AD9242AB9BEABABC/2009-RSA-TNC-seminar-afternoon-final.pdf.

Contact: Anne Price, TCG market communications
anne@prworksonline.com
1-602-840-6495