

Merging NAC Strategies of Microsoft and TCG/TNC

The Merger of NAC Strategies

The most significant event in the evolution of NAC occurred in May, 2007, when the Trusted Computing Group's Trusted Network Connect (TCG/TNC) working group and Microsoft's Network Access Protection (NAP) team effectively merged their work into a single set of compatible standards. This is important for the NAC world because it brings the Microsoft NAP client into an open, standards-based framework that will allow other network and security vendors to build on the infrastructure within the Windows Operating system. Microsoft's NAP client was included in Microsoft Vista and Windows Server 2008, and will be added to Windows XP when Service Pack 3 is released (estimated to be 29/April/2008).

Why Microsoft NAP Client?

Although a number of companies have add-on NAC clients for both Windows and non-Windows operating systems, the clear preference of desktop managers is to use, to the extent possible, Microsoft-included software as part of their desktop and laptop deployments rather than third-party tools.

When the Microsoft NAP client was locked into a Microsoft-only architecture, this made Microsoft's NAC approach unattractive to many security professionals for a variety of reasons, including the requirement to use the Microsoft NPS policy server and a broad reluctance to lock in to a single vendor with relative inexperience in network security.

Several critical benefits came by opening the Microsoft NAP client to integration with other security products. First, network and security professionals now have the choice of integrating with vendors more familiar to their industry, including both commercial and open source products. Second, the use of the Microsoft NAP client acted to reassure those same professionals by letting the one vendor most familiar with Windows – Microsoft – continue to provide the tools that require the greatest operating system integration.

Enterprise-sized NAC projects, by their nature, require an integration of desktop, security, and network team expertise. The use of the Microsoft NAP client keeps the desktop team on familiar territory with a familiar vendor that they trust (or at least understand how to deal with). It also reduces the requirement for the network and security teams to work in areas where they have significantly less experience or responsibility, by providing a well-documented and standardized "line in the sand" which separates out the client side of the NAC deployment from the enforcement and policy sides.

Who Standardized What?

Microsoft NAP is a family of protocols and tools that can be used to provide Network Access Control. With several different "styles" of enforcement and authentication, Microsoft NAP is larger in scope than the TCG/TNC architecture. For example, one way of using Microsoft NAP is to enforce access controls using DHCP. This isn't included in the TCG/TNC architecture. However, one particular mode of operation of Microsoft NAP using 802.1X-style authentication on wired and wireless LANs is especially similar to and compatible with the TCG/TNC architecture. Although the terms for each of the pieces are slightly (or very) different, when the two are compared, they are functionally almost identical.

Bringing these two sets of protocols and standards into alignment calls for the discarding of duplicate protocols and the selection of a preferred strategy. At this time, the TCG/TNC has not explicitly said that they will stop development on the protocols that overlap with Microsoft's NAP architecture. However, it is likely that given roughly equivalent functionality, vendors will elect to implement the Microsoft-supported protocol (if they implement only one).

The TCG/TNC has specifically announced that Microsoft's Statement of Health (SOH) protocol, which has a functional similarity to TCG/TNC's IF-TNCCS protocol, is now considered to be a peer protocol and part of the TCG/TNC architecture. There are some differences in the capabilities of the two protocols. The most important one is that the Microsoft SOH protocol only allows for a single 'statement of health' from the client towards the policy server, while the TCG/TNC protocols allows for a back-and-forth dialog of queries and responses between the client and the policy server.

Simply adopting the Microsoft SOH protocol is not sufficient to guarantee interoperability and compatibility between Microsoft NAP and TCG/TNC. The underlying transport mechanism chosen by Microsoft, a particular EAP method, must also be specifically selected for the 802.1X dialog to work. This method was already in the TCG/TNC specifications as one of the options at the Network Access Layer.

A second, and more important, difference is in the interface between the Integrity Measurement/ Collection layer and the Integrity Evaluation layer. In the TCG/TNC architecture, this is done with protocols called IF-IMC and IF-IMV. In Microsoft's NAP, this is handled by Microsoft's own SHA and SHV APIs. What this means is that if someone wants to write a Policy Decision Point for NAC that is compatible with the Microsoft NAP framework, they will have to implement the Microsoft "SHV" API to talk to the Integrity Measurement Verifier (or SHV in Microsoft NAP terms).

The diagram below (courtesy of the TCG/TNC) shows how Microsoft's NAP protocols, APIs, and specifications can be mapped into the TCG/TNC architecture. The protocol elements above the TNC Client and TNC Server (MS-SHA, MS-SHV, and MS SoH Report APIs) are not part of the TNC protocol specifications. However, because Microsoft has made these APIs available to third parties, it will be possible for network managers to select from policy servers beyond the Microsoft NPS policy server. This wouldn't, strictly speaking, be a completely TNC-compliant NAC deployment, but it would take advantage of the built-in NAC client in Vista and Windows XP.

