The following research results were an action item I received at a previous IDS teleconference call. The original action item was to research vendors within the NEA/TNC community that might be willing to work with PWG participants with regards to server-side implementations, and evolving code that NEA participants might be working on that would eventually be NEA compliant. After thinking about the goals of vendor participation, I realized that there is really no need to wait to see what vendors are doing in the NEA technology space, nor is there necessarily a need to engage in discussions with vendors' internal development teams. Most, if not all, of the vendors interested in implementing an NEA solution are probably already in the NAC marketplace, and a number of them are TCG members.

Since the proposed NEA protocol suite is based on the TNC base specifications, there's really no need to try and figure out what vendors are doing with their evolving NEA efforts. Rather, we can just look and see which vendors are shipping TNC-compliant products. If you remember, the TNC specs have more or less been "implementation-ready" for 3 or 4 years, and as I expected, there are a number of TNC-compliant solutions shipping. After discussing my "alteration" of the action item a bit with Steve Hanna, he agreed that we should be working with publicly available TNC implementations that are currently shipping, because not only are they shipping (what will be) NEA-interoperable TNC implementations, they are also shipping offerings with much more functionality, including a number of TCG and/or TNC technologies that will not necessarily be addressed by the IETF, such as IF-MAP support.

NAP/NAC Vendor Landscape

In addition to the advantages of working with TNC implementations offering more functionality than just NEA interoperability, most, if not all, of these vendors considered in the following analysis support Microsoft NAP agents, as well as TCG-TNC agents. With NAP and TNC support, these server-side implementations can be used to test both MS-NAP and TNC/NEA hardcopy agents.

Additionally, many of the TNC server-side products included in this NAC/TNC landscape analysis will probably soon be supporting TPMs.

The following list of vendors available (shipping) implementations includes descriptions of the product features that reference specific TNC acronyms/definitions. The following text describes these TNC-specific feature definitions so that the remaining vendor product descriptions are completely understood.

TNC FUNCTIONS

PDP - (Policy Decision Point)
This is the fundamental server-side component of a TNC NAC product. The Policy Decision Point is the software component that receives assessments from Access Requestors (ARs) and makes the actual decision as to whether or not the AR assessment meets site security policy.

The PDP consists of the following functions:

- Network Access Authority (NAA): The NAA function decides whether an Access Requestor (AR) should be granted access. The NAA consults a TNC Server to determine whether the AR's integrity measurements comply with the PDP's security policy. In many cases, an NAA will be included within a AAA Server but this is not required.

- TNC Server (TNCS): The TNCS function manages the flow of messages between IMVs and IMCs, gathers IMV Action Recommendations from IMVs, and combines those recommendations (based on policy) into an overall TNCS Action-Recommendation to the NAA.

- Integrity Measurement Verifier (IMV): The IMV function verifies a particular aspect of the AR's integrity, based on measurements received from IMCs and/or other data.

PEP - (Policy Enforcement Point)
The PEP consists of the following function:

- Network Access Enforcer (NAE): The NAE function controls access to a protected network. The NAE consults an NAA to determine whether this access should be granted. One example of the NAE is the Authenticator in 802.1X, which is often implemented within the 802.11 Access Point.

AR - (Access Requestor)
The Access Requestor is basically the device under assessment. It's an implementation of the "agent-side" of NAC. It's called Access

Requestor because it is the device that is requesting access to the network by sending it's "statement of health" to the "network" for assessment and adherence to policy.

MAP - (Metadata Access Point)
The Metadata Access Point functionality is implemented within a Metadata Access Point Server (MAPS). The MAPS function is a component to which other TNC components may publish, subscribe, and search data which reflects the state of TNC elements and aids in decision making and policy enforcement. The MAPS allows components which are not involved with the initial network access process, like Flow Controllers, to enforce policies based on relationships to endpoints, users, capabilities, roles, device activities and postures as well as other run time data. The MAPS allows elements which are not directly connected to an AR, like Sensors, to publish information about network activities which may be of interest to PEPs, PDP, and other MAP Clients.

MAP Clients consist of the following functions:

- Flow Controller: The Flow Controller function makes and enforces decisions about network activities utilizing information from the MAP. Flow Controllers take action (e.g. block) on network flows (i.e. network traffic associated with a particular AR, device, user, etc.) based on data obtained via IF-MAP. Examples of Flow Controllers include internal firewalls, rate limiters, and proxies. Examples of network activities being controlled include accessing particular services in a network, accessing particular geographies in a network, and restricting the amount of bandwidth allowed.

- Sensor: The Sensor function monitors network activities and publishes information to the MAP via IF-MAP. Examples of Sensors include intrusion detection devices, network virus detection devices, layer 3 traffic monitors, and application traffic scanners. Examples of network activities being monitored include accessing particular services in a network, authentication activity, broadcast requests for various services (e.g. DHCP), and advertising of services.

TNC INTERFACES

IF-IMC (Integrity Measurement Collector Interface)
IF-IMC is the interface between Integrity Measurement Collectors (IMCs) and a TNC Client (TNCC). IF-IMC is primarily used to gather integrity measurements from IMCs so they can be communicated to Integrity Measurement Verifiers (IMVs) and to enable message exchanges between the IMCs and the IMVs. It also allows IMCs to coordinate with the TNC Client as needed. Software, firmware and hardware components are expected to report status information to the TNC Client on the AR platform. The TNC Client supports an API to allow these components to communicate with it locally to report component-specific status information. The TNC Client acts as a conduit for the IMC that collects information from possibly multiple software, firmware and hardware components, and delivers the integrity measurements to the peer IMV through the TNC Server. In the case where the AR is a Trusted Platform with a TPM, the integrity-measurements are also deposited in the AR's Stored Measurement Log. How the measurements were collected on the platform (e.g. whether a TPM was used or not) must also be conveyed to the TNC Server.

IF-IMV (Integrity Measurement Validator Interface)
IF-IMV is the interface between IMVs and a TNC Server (TNCS). IF-IMV is primarily used to deliver integrity measurements sent from client-side IMCs to corresponding IMVs, to enable message exchanges between the IMCs and the IMVs, and to allow IMVs to supply their recommendations to the TNCS.

IF-PEP
IF-PEP allows the PDP to communicate with the PEP, especially allowing the PDP to instruct the PEP to isolate the AR during remediation and later grant it full network access once remediation is complete.

IF-TNCCS-SOH
The SoH binding for IF-TNCCS (herein referred to as IF-TNCCS-SOH) plays the same role in the TNC architecture as the XML binding of IF-TNCCS. It describes a standard way for the TNC Client and the TNC Server to exchange messages. However, IF-TNCCS-SOH does this in a manner that is compatible with the Microsoft Network Access Protection (NAP) system. More specifically, this interface defines a protocol and format for carrying:

(a) Messages from IMCs to IMVs (such as integrity measurements)

(b) Messages from IMVs to IMCs (such as requests for additional integrity measurements, or remediation instructions)

(c) Messages from TNCClients to TNCServers (such as control messages)

(d) Messages from TNC Servers to TNC Clients (such as the TNCCS-Recommendation message)

Note that the contents of the messages being passed between the IMCs and IMVs ((a) and (b) above) are opaque to the IF-TNCCS-SOH layer. IF-TNCCS-SOH relies on the underlying transport protocol (IF-T) to provide a secure authenticated channel to protect the messages in transit between the TNC Client and the TNC Server and ensure they are delivered to the correct TNCC or TNCS.

IF-MAP

IF-MAP allows elements in the TNC architecture to share and correlate stateful runtime metadata such as relationships of TNC components to endpoints, users, capabilities, roles, and attributes. IF-MAP provides publish, subscribe, and search interfaces between MAP Clients and the MAP. The data published and available via IF-MAP augments other sources of data for security related decision making. Searches and subscriptions using IF-MAP return data which approximately reflects recent metadata values and relationships as reported by MAP Clients.

LIST OF VENDOR SHIPPING IMPLEMENTATIONS + FEATURES

Juniper UAC (IC 4500, 6500)
TNC Components: PDP, AR, MAP, Sensor, Flow Controller
TNC Interfaces: IF-IMC, IF-IMV, IF-PEP, IF-TNCCS-SOH, IF-MAP

Juniper SSL-VPN (SRX, SA)
TNC Components: PDP, AR, Sensor, Flow Controller
TNC Interfaces: IF-IMC, IF-IMV, IF-PEP, IF-MAP

Microsoft Windows (XP SP 3, Vista, 7, Server 2008)
TNC Components: PDP, AR
TNC Interfaces: IF-PEP, IF-TNCCS-SOH

Any switch or AP that supports 802.1X
TNC Components: PEP

Wave Embassy Endpoint Enforcer
TNC Components: IMC, IMV
TNC Interfaces: IF-IMC, IF-IMV

Great Bay Software Beacon
TNC Components: Sensor
TNC Interfaces: IF-MAP

Lumeta IPsonar
TNC Components: Sensor
TNC Interfaces: IF-MAP

Insightix BSA Visibility
TNC Components: Sensor
TNC Interfaces: IF-MAP

Avenda Systems Health Agents
TNC Components: AR
TNC Interfaces: IF-TNCCS-SOH

Napera Insight
TNC Components: PDP
TNC Interfaces: IF-TNCCS-SOH

Nortel SNA
TNC Components: PDP, AR
TNC Interfaces: IF-PEP, IF-TNCCS-SOH

UNET SHA
TNC Components: AR
TNC Interfaces: IF-TNCCS-SOH

Of course, many of these products integrate with other products through proprietary interfaces. For example, the Juniper products integrate with Juniper firewalls and IDS and Microsoft's NAP server integrates with Microsoft's DHCP server.

From my research at this point, none of the products described above supports the inclusion of a TPM to secure the integrity of device assessments. However, it is expected that one or more of these products (Symantec, Juniper, etc.) will support TPM hardware some time in 2010.