4 in a Series

What is TCG's Trusted Network Connect?

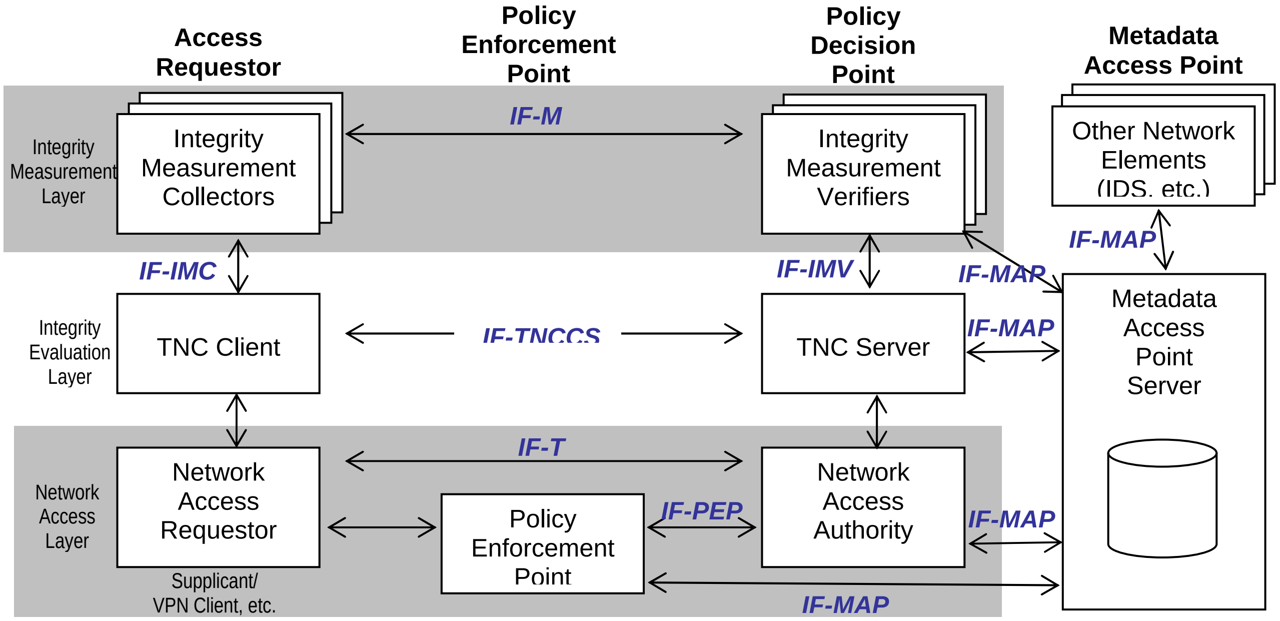
The Trusted Computing Group (TCG) is an industry standards body formed to develop, define, and promote open standards for trusted computing and security technologies. TCG has developed an open architecture and standards for Network Access Control called Trusted Network Connect (TNC). In early 2007, TCG and Microsoft announced interoperability between TNC and NAP thus opening the door for a single unified Network Access Control client

The most important aspects of the TNC architecture are vendor-independence through open standards and support for hardware-based endpoint security to address the "lying endpoint" problem.

The TNC Architecture

As an open architecture, TNC is designed to encompass a wide variety of products and technologies. Therefore, it starts by dividing the NAC problem into three basic entities: the Access Requestor, the Policy Decision Point, and the Policy Enforcement Point. The Access Requestor is the entity attempting to access the network. The Policy Decision Point is the entity that decides whether access should be granted, based on the network's policies. And the Policy Enforcement Point is the entity that implements the Policy Decision Point's decision, granting full network access, limited access, or no access at all.

Within these three entities, TNC defines certain components. The Access Requestor contains a Network Access Requestor, the software that is used by the client to connect to the network – an 802.1X supplicant, a VPN client, or similar. The Access Requestor also contains a TNC Client (software that manages the overall NAC process) and Integrity Measurement Collectors (IMCs, plugin software modules specialized for reporting the status of AV software, patches, or other things). The Policy Decision Point contains a Network Access Authority, software that makes the final decision on whether network access should be granted. The Policy Decision Point also contains a TNC Server (software that manages the NAC process on the server) and Integrity Measurement Verifiers (IMVs, plugin software modules that compare reports from IMCs against policy, supply access recommendations to the TNC Server, and send remediation instructions to the IMCs). The Policy Enforcement Point doesn't have any internal components. The following diagram illustrates the TNC architecture.



Standard Interfaces and Protocols in TCG-TNC

Probably the most important part of the TNC architecture is the interfaces between the components. The TCG has issued standards that define these interfaces, allowing a component from one vendor to interoperate with another component from another vendor. For example, an open source Linux TNC Client can have its health checked by a TNC Server on a network appliance as long as they both support the TNC's standard IF-TNCCS interface. Some of the TNC interfaces are protocols and some are Application Programming Interfaces (APIs).

IF-IMC – API that allows a TNC Client to load IMCs and allows IMCs to exchange messages with IMVs
IF-IMV – API that allows a TNC Server to load IMVs and allows IMVs to supply recommendations to the TNC Server and exchange messages with IMCs
IF-M – protocol for messages sent between IMCs and IMVs. This protocol is transported by IF-TNCCS.
IF-TNCCS – protocol for messages sent from TNC Client to TNC Server and vice versa, containing IF-M messages, session management messages, etc. This protocol is transported by IF-T so that it remains transport-independent. With the recent interoperability agreement with Microsoft's NAP, the content of these messages can be carried either with the original XML encoding, or the Microsoft Statement of Health enconding.
IF-T – the transport protocol. TNC plans to provide several standard options for IF-T. So far, the only method standardized is an EAP method that can be carried over 802.1X or IPsec's IKEv2 protocol.
IF-PEP – protocol for the Policy Decision Point to communicate decisions to the Policy Enforcement Point. TNC plans to provide several standard options for IF-PEP. So far, the only method standardized is RADIUS.
IF-MAP - protocol creates a structured way to store, correlate, and retrieve identity, access control, and security posture information about users and devices on a network. See the accompanying whitepaper on IF-MAP for a detailed discussion on this new development.

Vendor Independence

These standard interfaces provide TNC with its most valuable feature: vendor-independence. Every component in the TNC architecture has been implemented by multiple vendors and these products have been tested to ensure they actually work together. Customers retain full choice and are not tied down to any one vendor.

Trusted Platform Module – Solving The "Lying Endpoint" Problem

Another special aspect of the TNC architecture is that it provides a strong solution to the "lying endpoint" problem, a serious problem that affects all software-based NAC systems. The problem is that if an endpoint becomes infected or otherwise compromised, that machine may well lie about its health. This can result in infected machines gaining access to the network and infecting other systems. Endpoint security software can reduce the likelihood of infection but not eliminate it. The lying endpoint problem can be mitigated by monitoring endpoints after they connect to the network to detect misbehavior but this approach has several disadvantages. First, it detects infected systems only after they start to spread their infection. Second, it will miss stealthy infections like keystroke loggers and rootkits.

TNC's solution to the lying endpoint problem is based on the Trusted Platform Module (TPM), a hardware security component now included in all corporate-grade laptop and desktop computers. The TPM is based on standards from TCG. It can be used for many purposes such as disk encryption and strong authentication but in the TNC architecture it is primarily used for integrity measurement and remote attestation. During the endpoint's boot sequence, the TPM measures (hashes) all the critical software and firmware components before they are loaded: BIOS, boot loader, operating system kernel, etc. During the TNC handshake, these measurements are sent to the TNC server, where they are compared against the values for proper configurations. If they don't match, the endpoint is infected and can be quarantined. Because this technology is based on security hardware, it cannot be evaded by even the most stealthy infection. TPM-based verification is optional with TNC. Machines without a TPM can be checked with the normal software-only techniques.

For More Information

The TNC standards and architecture, lists of products that implement the TNC standards, and lots more information is available at the TCG's web site: https://www.trustedcomputinggroup.org