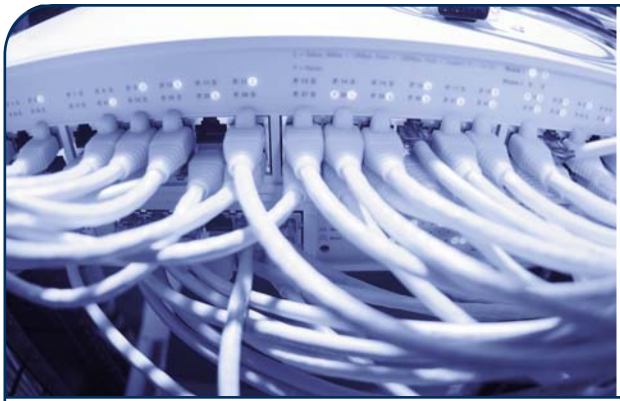

Executive Summary

Defend Your Network Against “Lying Endpoints”

Standards-based Hardware Makes Network Access Control Solutions More Secure

The emerging network access control (NAC) market was taken aback when researchers at the German security firm ERNW published a means of breaking a NAC solution by attacking the software agents that report endpoint integrity information. The hacked trust agent was modified to lie about its status and the integrity of endpoint applications it monitored. This hack results in what is known as a “lying endpoint” attack.

This demonstration highlighted the fact that corporate networks are increasingly at risk of being compromised. Computing devices, or endpoints, expose the entire network when they access network resources such as email, CRM databases, time sheets, purchase orders, and other data stored on the central network. Given the continued growth of the mobile workforce coupled with escalating compliance regulations, IT administrators are compelled to address this very real risk to the corporate network. In fact, protecting corporate assets and resources from malware-infested endpoints has emerged as one of the primary security challenges facing IT administrators, many of whom are taking a proactive stance by using NAC solutions to evaluate the endpoint’s configuration and health prior to granting access to network resources.

NAC solutions involve four main components: (1) authenticating the user, (2) authenticating the machine, (3) evaluating the integrity of the platform, and (4) enforcing security policies based on the platform’s health. In the many NAC solutions available today, some utilize proprietary interfaces, while others support open standards. User and machine authentication is supported in various combinations and with various options. For evaluating the platform’s health, however, almost all NAC solutions rely upon software agents to collect information from the endpoint and report it to a server.

The Trusted Computing Group (TCG) has been publishing vendor-neutral standards that not only detail open interfaces that allow vendors to support network access control solutions, but that also define an architecture for utilizing a Trusted Platform Module (TPM) to collect and report application integrity measurements. This hardware-based security protects the software agents and mitigates the threat from “lying endpoints.”

Wave Systems provides TCG-compliant software solutions for the network access control market. Wave’s EMBASSY software provides machine and user authentication as well as protected data access prior to the verification of a NAC solution’s security policy. Wave’s EMBASSY Endpoint Enforcer (EEE) hardens platform integrity by securing the measurements of the endpoint software components via the TPM and delivering verifiable integrity reports on demand. EEE is not a stand-alone product, but is designed to extend the security of third-party network access control solutions. Wave has demonstrated the integration of EMBASSY Software including EEE with Juniper’s Unified Access Control solution and with Microsoft’s Network Access Protection solution.

Utilizing Wave’s software and the TPM in conjunction with a NAC solution, IT administrators can have greater confidence in knowing what PCs are accessing their network as well as the true state of their health. The end result is that IT administrators have significantly increased assurance that network assets will not succumb to the threats of malware.

For more information, contact Wave Systems at (877) 228-WAVE or visit us at www.wave.com.