TECHNICAL WHITE PAPER

PSTN to IP Attack Scenario

Version: **1.0** Date: **November 25, 2002**

CID: **95509** Author: **CSD Security Architecture Team**

Background

With the introduction of the converged IP telephony solution, customers are concerned that a perpetrator might be able to gain access to their IP network through the PSTN. The concern is that a perpetrator could use a modem to call into the IP telephony system and immediately gain IP connectivity. This paper describes an attack scenario and explains how the Avaya voice-over-IP (VoIP) solutions are protected against this type of attack.

Attack Scenario

The perpetrator is presumed to have access to the public-switched-telephone network (PSTN) and has computer equipment, skills, and architectural knowledge of the internal voice-over-IP solution at their disposal. Additionally, the targeted customer has a voice-over-IP solution with a mixture of analog, digital, and IP telephones deployed throughout their enterprise. Finally, presume there is connectivity between the IP telephony network and the regular data network of the enterprise.

Given these conditions, the attack scenario suggests that the perpetrator could call a phone number of any of the extensions within the enterprise and use a modem to establish connectivity. An IP data link could then be established between the perpetrator and the internal IP telephony network, unrestricted by firewalls, resulting in the perpetrator having the same network connectivity as if they were inside the enterprise.

Inherent Resilience and Defense in Avaya VoIP solutions

Although this attack may appear possible, the components to successfully execute the attack are not available within Avaya voice-over-IP solutions.

When the perpetrator attempts to make a call into the enterprise and connect to a media module inside one of the gateways or port networks (PNs) of the IP telephony system, the media modules would convert analog or digital traffic (as appropriate to their interface) into TDM traffic (encoded as standard mu-law or A-law PCM). The TDM traffic then traverses the TDM buss of the gateway or PN to another media module, which in turn, converts the TDM data to the appropriate signal type for the receiving extension. Media modules do no other type of coding or decoding. Specifically they do not emulate modems or support tandem modem traffic, nor do they possess native PPP capabilities.

When needed, the conversion of the TDM traffic to IP is done in the VoIP processors (not media modules). That IP traffic is directed to some other VoIP processor, or to an endpoint, under the complete control of Avaya MultiVantage™ Software**.** There is no opportunity for the caller to cause the IP traffic to be diverted to or establish a PPP connection with another IP address of the caller's choosing.

Unlike competitive systems, Avaya does not produce media modules with built-in capabilities to demodulate and establish PPP connections for modem communications. Additionally, all data traffic direction is under the control of the Avaya MultiVantage Software.

Summary

The threat of implementing a PSTN-to-IP attack, as in the above scenario, is thwarted by three basic elements of the Avaya voice-over-IP solution. First, the media modules do not terminate IP traffic or establish PPP connections. Second, the media modules designs allow for only voice traffic to the TDM bus. Third, all traffic between media modules and VoIP processors are under the complete control of the MultiVantage media. Thus, the only access to a network an outside party would have to the system via the PSTN is the ability to ring a station whose number was assigned by the customer. The system cannot be perverted to inherently convert an inbound call to a PPP/modem session on the customers network. As a result of these inherent restrictions, this attack scenario should not be considered possible.