VOIP - VULNERABILITY OVER INTERNET PROTOCOL?

Consultant Wil Allsopp highlights some of the risks inherent in Voice over Internet Protocol.

During the past few years the two most significant focuses for remaining IT budget have been security and cost saving systems capable of demonstrating rapid ROI. But in almost all areas of business there is a trade off between risk and cost. As companies have double-locked the doors by spending on security for the data network, they may have left the windows open by pursuing saving in areas such as VoIP (Voice over Internet Protocol).

The VoIP 'revolution' has been talked of since the 1990's as the 'next big thing' in the enterprise telecoms sector; saving companies vast amounts of money on both call charges and internal network infrastructure and support costs. But just as the VoIP market is finally taking a cautious step towards delivering some of its long-overdue promise, the increasing priority of IT security may force it two steps back.

Recent research, by Secure Test, on the Cisco 7900 series VoIP phones have revealed serious security concerns (Note: Secure Test have independently tested the Cisco 7900 as this is the most widely used enterprise VoIP solution. Similar problems may well exist in other vendors products). With susceptibility to both DoS (denial of service) attacks and interception issues, it is clear that transferring phone systems to an IP network opens them up to many of the same security concerns as Ethernet data networks. More worryingly, phone systems may be harder or even impossible to patch.

Like many IP devices Cisco's VoIP phones are vulnerable to ARP (Address Resolution Protocol) spoofing, allowing 'man-in-the-middle' attacks and including data interception and packet injection. This means that any VoIP phone can be tapped by anyone else with a phone on the same network, any individual VoIP phone can be crashed easily and any VoIP network infrastructure is heavily vulnerable to DoS attacks.

Looking first at the vulnerabilities of VoIP phones to DoS attacks, Secure Test's initial research has shown that Cisco 7900 series phones, specifically where running the default Skinny (SCCP) protocol for messaging, can be crashed relatively easily using one of several methods. By attaching a PC to the VoIP network it is possible to send malformed messages to a target phone or to cause a buffer overflow on one of several fields resulting in a crash. By performing any of these attacks on the switchboard phone, research demonstrated that it would be relatively trivial for an attacker to disable an entire phone system in minutes.

Further research then went on to show that using a similar DoS attack, a Cisco 1760 VoIP enabled router was also vulnerable. Sending a message of 50,000 characters plus to port 2000 (the TCP port used by the router to communicate with the phones) causes every VoIP phone on the network to reboot or crash, completely disrupting communications.

Given the number of Cisco VoIP implementations in companies where the telephone constitutes a business critical system this vulnerability quite rightly send chills down the spine of many a communications manager, especially as avoiding the problem is difficult. Ideally, Cisco would release a patch to better handle malformed or malicious traffic and recover from network errors. However, whilst Secure Test responsibly informed the vendor of the problems several months ago, as yet, there have been no visible signs of progress. Understandably there may be greater problems in patching 'dumber' devices such as telephone hardware, relative to providing security updates for PC's and servers. But, if the window of exposure cannot be effectively shortened by a company with the development capacity of Cisco, this could be seen as a good argument not to run phones on open IP networks until these problems have been overcome.

Having discovered the vulnerabilities with regard to DoS attacks, tests then moved on to see whether the ARP spoofing attacks, specifically data interception, were possible. Any fan of spy films will know that telephone tapping is perfectly possible on traditional PSTN based phones. Since this usually requires a hardwire tap to be set into the PBX, however, this becomes a question of the physical security of the core infrastructure. Initial tests on VoIP phones, however, have shown that where data is not encrypted, it is relatively easy to intercept, listen-in on or record conversations on any phone, from any other phone point on the network. Worryingly, most of the commonly used VoIP phones do not encrypt traffic by default and currently, many do not even support the necessary protocols to make this possible.

Initial tests on the Cisco 7900 have proved that it is possible to carry out an ARP attack on a target phone which draws the data stream through the attacker's computer. As any conversation is transmitted in the clear using standard RTP (Real time Transfer Protocol), this can easily be decoded, listened in-on and recombined in real time, leaving the victim(s) none the wiser.

As researchers found it relatively simple to develop a tool to automate this process, it can safely be assumed that such tools are freely available on the Internet. This means that where VoIP handsets do not support the secure RTP protocol necessary to protect traffic (as with all current Cisco phones) it should be assumed that all communications could be intercepted.

All of the attacks outlined above are difficult to guard against as they work using the very essence of convergence; that you do not physically segregate the data network and the phone system. Even where separate IP networks are used, you can simply plug a PC in to the telephone network via the phone port. As one of the major advantages of VoIP is

computer telephony integration (ie. screen pop-up with call information and multi-channel CRM systems) most hardware phones contain a built in switch to allow a PC and a phone to occupy the same port.

Looking beyond this, the increased sophistication of an IP based telephone network even makes it easier to create Trojans to carry out these and other attacks remotely. Secure Test most recent studies suggest that once a network has been infected, this makes is perfectly feasible to tap VoIP calls and carry out DoS attacks remotely from outside the company network.

Wil Allsopp is a consultant with Secure Test. Secure Test will be demonstrating VoIP vulnerabilities over Internet Protocols on their stand at Infosecurity Europe 2004, Europe's number one IT Security Exhibition. Now in its 9th year, the show features Europe's most comprehensive FREE education programme, and over 300 exhibitors at the Grand Hall at Olympia from 27th to the 29th April 2004.

www.infosec.co.uk