Miercom

The leading edge in networking information

Independent Lab Test Report:

Security of Cisco CallManager-based IP Telephony against malicious hacker attacks

Synopsis: Cisco Systems becomes the first, and to date still the only, IP-Telephony vendor to earn Miercom's highest rating of "**Secure**" for its proven ability to defend an IP phone service against malicious attack. An expert team of hackers, assembled and supervised by Miercom, could not disrupt, or even disturb, phone service or features after three round-the-clock days of sophisticated attacks.

Report Issued: **24 May 2004**

379 Princeton-Hightstown Rd., Bldg. 1, Cranbury, NJ 08512 ● 609-490-0200

Summary of Testing, Results

In independent testing conducted by Miercom, Cisco Systems® proved that it could build and deploy a Cisco® CallManager-based, IP-telephony network that a sophisticated hacker assault team could not break, or even noticeably disturb – even after days of round-the-clock assaults, including dozens of the most insidious Denial-of-Service (DoS) attacks.

The attack team struck at all layers, systematically attacking the Layer 2 infrastructure (MAC-level, switches, forwarding), the Layer-3 infrastructure (IP routing level), and then Layer 4 and above, targeting the VoIP and IP-telephony infrastructure.

The security testing of the Cisco IP-telephony environment resulted from a joint undertaking between Miercom and ***Network World***, the industry's leading trade magazine. ***Network World*** in late 2003 engaged Miercom to realistically assess the state of VoIP security by evaluating the vulnerability of leading IP-telephony systems to malicious disruption. The results of the first round of testing, in which Cisco emerged with the highest rating of the vendors tested, were published in the May 24, 2004 issue of ***Network World.***

Cisco earned an impressive overall rating of **Secure** (see the *Rating Scale* below). As the only **Secure** rating awarded to date by Miercom for an IP-telephony package, Cisco has set the bar that other IP-telephony vendors will now try to reach.

Overall rating: **Secure**

Miercom's VoIP-Security Rating Scale

Overall Rating	**Maximum impact that Miercom's assault team could achieve** *
Secure	No perceptible disruption to voice service
Resistant	Only minor and/or temporary disturbance(s)
Vulnerable	Phone service affecting many phone users could be disrupted for a protracted period, via a sophisticated or coordinated attack
Open	Phone service affecting most phone users could be significantly disrupted, indefinitely, via a fairly straightforward assault
Insecure	Phone system, or service, affecting all users could be readily and indefinitely disabled

* In compliance with the hacker-assault ground rules adopted for this testing.

Plan of Attack

In order to assure a fair and impartial evaluation of the vendors' capabilities, Miercom developed a set of testing ground rules for both vendors and the hackers. These "rules of engagement" helped assure that all vendors and IP-telephony systems were tested consistently. The Cisco submission was tested in March 2004 in accordance with these rules.

The ground rules required the vendors to build a system simulating a single-site, 1,000-user IP telephony system that was secured based on off-the-shelf products that a customer could currently deploy. Vendors were not required to include a remote site (WAN connected), VPN telecommuter solution, or IP softphone in their configurations. These features may be evaluated in a future test.

The vendors were required to provide three avenues of attack: 1) a connection from the outside, simulating Internet access, 2) data ports on the access-layer Ethernet switch, and 3) IP phones, including access to the built-in switch ports on the back of the IP phones. These "attacks points" are shown in the diagram on page 5.

Once testing began, no configuration changes were allowed unless explicitly agreed to by Miercom. In this test Cisco was allowed to add one access list, or ACL, to fix an internal IP routing issue, which had been overlooked. Finally, the vendors were required to disconnect administrative keyboards to prevent any configuration modifications during testing.

The ground rules also imposed certain operational restrictions on the hacker assault team. For example, only hacker tools and attacks that are available on the Internet could be used. "Insider" attacks were launched via an end-user data port or IP-phone connection – simulating the access that a hacker might have via a standard "office cubicle." Outside attacks were launched through the simulated Internet connection. Also, attackers were not permitted to disassemble or dissect the vendor's IP phone.

The objective of all the attacks was to disrupt phone communications. Via the data and IP-phone connections the hackers used scanning tools and other techniques to see and learn what they could of the topology: They were told nothing of the vendor's configuration beforehand.

After discerning and identifying "targets," the hackers systematically launched dozens of attacks, at times in combinations concurrently. The attacks, aimed at disabling devices and functions at all layers, continued for at least three full days.

Given the scope, duration, ground rules, tools and techniques of our assault plan, experts we have interviewed characterize the Miercom attack severity, overall, as **"moderate intensity."**

It should be noted that in the real world, the Cisco access-switch ports could be set to turn off permanently on detection of violations. For the purposes of this evaluation the ports were set to temporarily shut down in the event of a detected violation, and then re-enable after five minutes. Also, Cisco, or its customers, would normally be actively monitoring hacking attempts, and hackers would not be allowed to continue their attacks, once detected. In the test bed Cisco was not allowed to actively monitor or act on alerts generated by the system.

After three full days of effort, the hackers could achieve no perceptible disruption to the IP telephony infrastructure or Cisco CallManager, earning Cisco Systems the first ***Network World*** and Miercom **Secure** rating.

Phone calls could not be disrupted, but the hackers were able to insert a passive probe into an IP-phone station connection, and observe and collect traffic details. With this information, the hackers could insert their own computer and gain access to the voice VLAN. But in no case could the hackers exploit the system. And neither could they impersonate an IP phone or spoof an IP phone call. Both of these intrusions required physical access and could not have been accomplished remotely.

Maximum Security

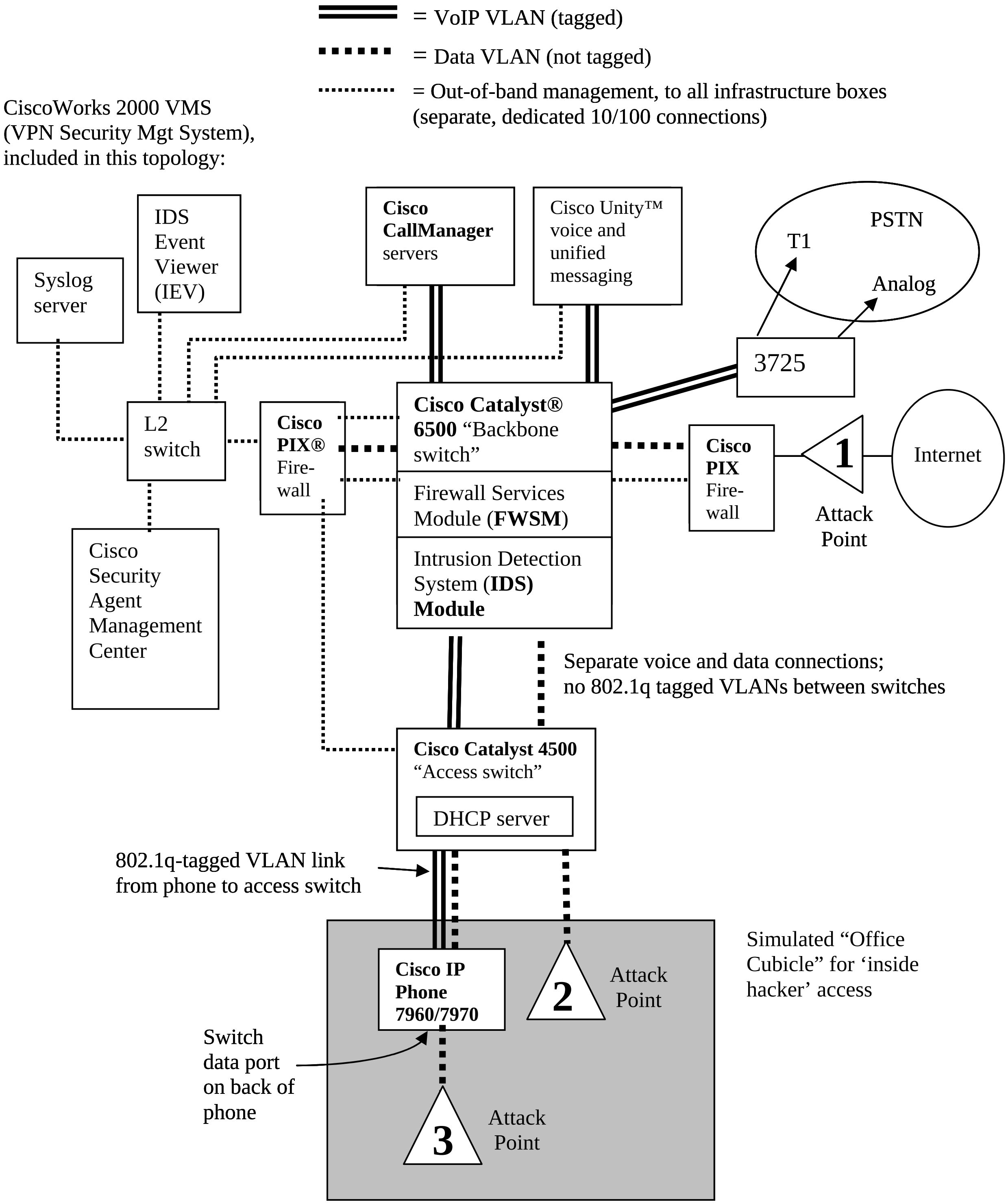
For this review Cisco was challenged to provide a highly secure system that could be deployed today by a customer requiring maximum security. The elaborate IP-telephony package that Cisco provided – with underlying Layer-2 and Layer-3 infrastructure and assorted security add-ons (see Figure: "Cisco VoIP-Security Topology Tested," next page) – was the most secure that the collective network-security experts at Cisco Systems could muster and employed virtually every defense in the company's broad network-security arsenal.

The topology we tested represents more security options and stricter security settings than most users currently employ. But that should not detract from Cisco's fine showing here: All of the capabilities and features Cisco used are available today to anyone.

Summary

Along with the other vendors, Cisco conformed to both the letter and the intent of the ground rules for this evaluation. Based on the results of this first of its kind independent assessment, Miercom recognizes the Cisco solution as the most capable of those tested to date, and looks forward to tracking the development of the market through future evaluations.

Cisco VoIP-Security Topology Tested

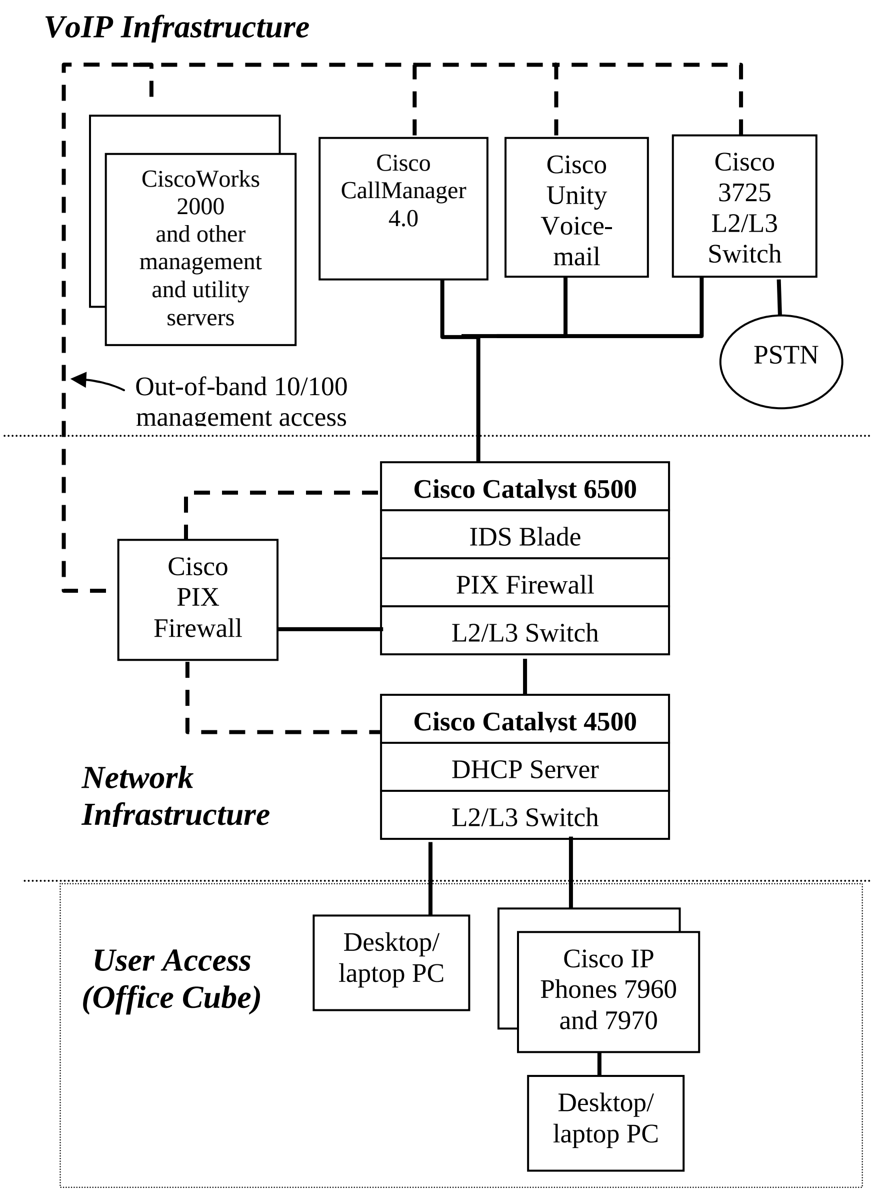

= VoIP VLAN (tagged)
= Data VLAN (not tagged)
= Out-of-band management, to all infrastructure boxes (separate, dedicated 10/100 connections)
CiscoWorks 2000 VMS (VPN Security Mgt System), included in this topology:
Syslog server
IDS Event Viewer (IEV)
Cisco CallManager servers
Cisco Unity™ voice and unified messaging
PSTN
T1
Analog
3725
L2 switch
Cisco PIX® Fire-wall
Cisco Catalyst® 6500 "Backbone switch"
Firewall Services Module (FWSM)
Intrusion Detection System (IDS) Module
Cisco PIX Fire-wall
1
Attack Point
Internet
Cisco Security Agent Management Center
Separate voice and data connections; no 802.1q tagged VLANs between switches
Cisco Catalyst 4500 "Access switch"
DHCP server
802.1q-tagged VLAN link from phone to access switch
Cisco IP Phone 7960/7970
2
Attack Point
Simulated "Office Cubicle" for 'inside hacker' access
Switch data port on back of phone
3
Attack Point

The Cisco Approach: Layered Security

Security threats come in a wide variety of forms and from many directions (see the section: "Threats to IP Telephony" in this report for descriptions of various attack scenarios). Cisco has taken a systems approach to mitigating as many of these attacks as possible by providing defense in depth through a layered approach.

This maximum-security environment employs defensive mechanisms at many layers across the topology. Some of the security mechanisms are now a built-in part of certain Cisco components; others are extra-priced packages. These are detailed in the following sections.

Network Architecture



Key Security Components

- Cisco Security Agent running on all servers
- Firewall-protected, out-of-band (OOB) management access to all servers and infrastructure boxes
- Aggressive monitoring of security related events
- Built-in Denial-of-Service protections in Cisco Catalyst IOS Software, including rate-limiting
- Dynamic ARP Inspection; other attacks addressed, suppressed in Cisco Catalyst IOS Software
- Multiple firewalls at strategic locations
- Separate voice and data
- Certificate-authenticated, encrypted VoIP call control and signaling
- Media (VoIP RTP stream) encryption on 7970 IP phone
- Local IP-phone administrative access disabled

Cisco Integral Security Measures

Many of the security features that helped Cisco achieve the impressive results in this testing are "built-in," integral parts of the Cisco IP-telephony solution and network components. Among the ones that most contributed to the solid defense in the Miercom security testing:

1. An impressive and effective array of security defenses is now an integral part of the Cisco IOS® Software in Cisco Catalyst switches and Cisco routers.
2. Cisco Security Agents: These are 'host-based' intrusion-prevention-system (HIPS) software modules that protect the server from various high-level assaults, and which now are integral on Cisco CallManager Windows 2000-based servers.
3. Cisco CallManager, Cisco IP Phones and Cisco "Secure" Skinny (S-SCCP)-based security mechanisms, including RTP stream encryption (now supported on Cisco 7970 IP phones), and certificate-based phone authentication.

1. Built into Cisco IOS Software in Cisco Catalyst Switches

In the Cisco network tested, our phone and data connections went directly to a Cisco Catalyst 4500 similar to that pictured below, running Cisco IOS Software version 12.1(20)ew. This served as the "access" switch, which also powered our Cisco 7960 and 7970 IP phones (using Power-Over-Ethernet, per the IEEE 802.3af standard).

Cisco Catalyst 4500 and Cisco 7960G IP Phone

Serving as a "backbone" switch was a Cisco Catalyst 6500, running Cisco IOS Software version 12.2(17b)sxa.

A Cisco Catalyst 4500 was the first line of defense against our "inside" hacker attacks, and proved extremely effective. A key to this is a "binding table" that is built, which maintains MAC addresses with their correct IP addresses, ports, VLAN affiliations and DHCP lease times.

A considerable number of the attack team's assaults were deflected by one or more of these defensive mechanisms, built into the Cisco Catalyst 4500 IOS Software:

-**DHCP Snooping**: Combats against rogue DHCP servers, while protecting the network from Denial-of-Service (DoS) attacks by rate-limiting incoming DHCP requests and responses, preventing DHCP exhaustion attacks. DHCP Snooping also forms the basis for other security features, such as IP Source Guard and dynamic ARP inspection (DAI), because it builds a table (the DHCP Snooping binding table) of authorized IP and MAC addresses. Besides IP and MAC addresses, this table also contains port number and VLAN information. Violations can turn off an offending port temporarily or permanently.

-**Dynamic ARP Inspection (DAI)**: Prevents ARP spoofing and man-in-the-middle attacks, for both static and dynamic IP addresses, without requiring any changes on the end hosts. ARP requests are rate-limited and ARPs are checked to ensure legitimacy. Violations can cause ports to shut down temporarily or permanently.

-**IP Source Guard**: Ensures packets' IP and MACs addresses are legitimate using the DHCP snooping binding table. This feature dynamically prevents impersonation attacks (IP spoofing).

-**Port Security**: Prevents MAC flooding attacks by limiting the number of MAC addresses that can appear on a port. MACs are flushed after 5 minutes when a device is disconnected and re-learned when a device is plugged in. Violations can shut down an offending port, and its phone, for a pre-defined lock-down period, or permanently.

-**VLAN Access Control Lists, or VACLs**: Applies Layer-3 type ACLs to a Layer-2 VLAN. Traffic not allowed, per VLAN and ACL rules, is filtered out. Allows only necessary traffic to reach IP phones. For instance, only RTP traffic was allowed between IP phones mitigating TCP DoS attacks against the IP phone.

-**Traffic Policing**: Limits the amount of traffic allowed. Traffic can be policed at an aggregate level per port, per VLAN, or per flow - a new feature called MicroFlow Policing can police traffic per source and destination IP address. Extremely effective in throttling Denial-Of-Service attacks, where high volumes of traffic are flooded to a target node.

2. System hardening via Cisco Security Agent

The Cisco Security Agent is software that runs on servers, and can also be put on client PCs and laptops, and protects against a spectrum of hacker assaults. It is a "host-based" intrusion-prevention system, or HIPS.

According to Cisco Systems, a Cisco Security Agent solution is now available at no charge for all voice application servers, application including Cisco CallManager, Cisco Unity voice and unified messaging, Cisco IP Contact Center, etc. Cisco Security Agent constantly examines traffic, looking for 1,000 or so predefined events. If it recognizes one, Cisco Security Agent automatically intervenes and takes corrective action.

Among the most effective security measures that Cisco Security Agent incorporates are:

-**Buffer overflow protection and prevention.** Many attacks seek to overrun a server's buffers, and then install malicious code that operates with system privilege. Cisco Security

Agent prevents any unauthorized access to system functions from code executing in data or stack space.

-Preventing malformed-packet attacks. Attacks such as Ping-of-Death attacks, where too-large packets are sent in high volumes, are common. Cisco Security Agent is able to drop these, and other malformed packets, before they enter and can affect the operating system.

-**Monitors and enforces which applications can run on the server.** Cisco Security Agent can be set to strictly monitor and enforce the programs that can access system functions.

-Detects port scans. The scan tools used by hackers follow certain patterns, like trying ports in certain sequences. Cisco Security Agent logs such events and then correlates them to determine when a scan is occurring, even if undetected by other security equipment (firewalls, IDS, and so on)

-Detects and prevents Trojan assaults. Trojan attacks can take many forms, but in most cases executables are implanted on target servers, which may seek, for example, to download malicious executables, or steal local passwords. Cisco Security Agent detects and prevents such actions.

-Protects against SYN floods. These are popular DoS (Denial-of-Service) assaults, which overload the TCP processing resources of the target computer by causing many half-open connections. Cisco Security Agent prevents the proliferation of such half-open states.

In all, we had seven Cisco Security Agent agents running in the Cisco topology we tested. That included on two Cisco CallManager servers, on the Cisco Unity voice-mail server, and on other Windows 2000 servers, including CiscoWorks 2000 management server.

3. Built into Cisco CallManager and the Cisco VoIP Infrastructure

IP telephony in the Cisco world is delivered by Cisco CallManager software running on one or more servers, plus an assortment of other servers that collaborate in providing voice and related services, such as Cisco Unity voice messaging. We tested with the latest version 4.0 of Cisco CallManager.

A number of impressive security processes are now integral in the latest Cisco CallManager, and in the latest IP-phone firmware. These contributed significantly to the hackers' inability to impersonate a legitimate IP phone. These measures include:

-Encrypted call control – Secure SCCP. The Cisco network topology we tested employed Secure Skinny, or S-SCCP. This is where all call-control is carried within 128-

bit AES-encrypted TCP-based SSL v3.0 tunnels – with RSA signature and SHA-1 authentication. Collectively, that's a tough nut to crack.

-**Controls on Cisco IP phones.** The phones can be centrally "locked down" by the administrator, allowing no local configuration options. The ability of the local user to show network information can be disabled. Even the headphone and speakerphone capabilities can be disabled, as well as the switch port on the back of the IP phone.

-**Media encryption.** This release of Cisco CallManager supports media encryption, that is, encryption of the IP VoIP stream, currently between Cisco 7970 IP phones.

-**Certificate authentication of IP phones.** Each phone has a certificate, which establishes the phone's trusted identity, and a certificate trust list, which tells the phone which Cisco CallManager servers and TFTP servers it can trust. A bi-directional exchange of certificates is used for mutual authentication, and also in the signature process.

-**Signed IP phone loads and configuration files.** This all but prevents someone from downloading a bogus firmware image or configuration file to a Cisco IP phone. Authorized downloads are verified by authentication and certificate-based signatures.

Cisco Optional Security Components

The many security features discussed so far in the multilayered security architecture offered by Cisco Systems are *integral* capabilities of the main components of a typical Cisco IP telephony deployment - Cisco CallManager servers, IP phones, and Cisco Catalyst access and backbone switches. These safeguards are now built into this gear and are included at no charge.

Cisco's success in the Miercom security testing also entailed some additional, extra-priced, specialized security components, which are described below. These included:

1. Firewalls. Two standalone Cisco PIX 525 firewalls – one for the Internet data connection and another for the out-of-band network-management segment – were deployed in the Cisco topology tested, along with a Cisco Firewall Services Module (FWSM), which also runs Cisco PIX software. The FWSM was deployed in the "backbone" Cisco Catalyst 6500, which controlled traffic between the voice, data and server VLANs.

2. Intrusion Detection System (IDS). An IDS Switch Module (model IDSM-2) was also deployed in the Cisco Catalyst 6500. This passive device analyzes a copy of all traffic through the Cisco Catalyst backbone switch and issues alerts and notifications.

Cisco brought some of its highest performance (and thus most expensive) options in for the testing, profiling what a large enterprise customer would deploy. Miercom is aware that Cisco offers many models of firewalls and IDS solutions, which fit customers – and budgets – of all sizes.

Cisco PIX firewalls, for example, can be ordered in several forms (see picture below):

- Cisco PIX Security Appliance Series
- Cisco IOS Firewall Feature Set for Cisco routers and Cisco Catalyst switches, and
- Cisco Firewall Services Module (FWSM) for Cisco Catalyst 6500 switches and Cisco 7600 Series routers.

Similar options in the form of standalone appliances, Cisco IOS Software router modules and Cisco Catalyst 6500 switch modules are available for Intrusion Detection Systems.

How much does adequate security cost? As a rule of thumb, Cisco estimates that security adds between $50 and $370 per end user, depending on the level of security required (from minimal to maximum). (Source: "Managing Cisco Network Security", Cisco Press, 2001).

All shapes and sizes. Shown from left to right are: Cisco Routers, Cisco PIX Firewall Series Appliances, and the Cisco Firewall Service Module.

1. Controlling traffic flows via Firewalls

Cisco used the Cisco PIX appliances and FWSM to protect its network from various types of attacks, and to control what type of traffic was allowed between any two devices.

Here are some of the key firewall-deployment considerations, which helped secure the Cisco IP-telephony deployment:

- The Cisco Firewall Services Module (FWSM) was placed between the voice, data and server VLANs to block traffic from the data VLAN to the voice and server VLANs, while permitting hosts on the data VLAN to access the Internet and permitting the phones in the voice VLAN to communicate with the servers and gateways in the server VLAN.

- Access Control Lists in the FWSM were used to specify what IP-address ranges were permitted or denied access to the other IP-address ranges, and what protocols were allowed between them.

- Stateful packet inspection of voice signaling protocols, such as the Cisco SCCP, H.323 and MGCP, was also configured in the FWSM, as well as other protocols necessary to the operation of the system, including TFTP. For instance, when an IP phone in the voice VLAN placed a call to the Cisco IOS Software gateway to the PSTN, a temporary UDP port was opened between the voice and server VLANs to allow the RTP media packets to flow between the gateway and the phone. Likewise, when an IP phone requested its configuration file from the TFTP server, a temporary UDP connection was permitted through the firewall, for the duration of that session.

- One Cisco PIX 525 was placed between the Cisco Catalyst 6500 and the Internet, protecting the network from external attacks, while permitting data-VLAN access out to the Internet.

- A second Cisco PIX 525 was placed between the management subnet and the out-of-band interfaces of all the infrastructure equipment, and set to restrict traffic to management-related protocols only. These included: TFTP, FTP, HTTP/HTTPs and SSH.

- Telnet services were disabled throughout: Cisco personnel used SSH (Secure Shell) v2 to access and manage all of the routers and switches.

- In addition, all three firewalls performed a myriad of *standard* firewall functions. One such example is TCP intercept, which ensures there is a bi-directional TCP connection established before permitting traffic to flow. This mitigates many forms of TCP-based Denial-of-Service attacks.

The firewalls were first configured according to Cisco "best practices," and then additional voice-specific modifications were applied. Cisco "best practices" are a part of the vendor's SAFE blueprint for network-security planning. Details can be found at this location on the Cisco web site:

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_package.html

2. Staying Alert, with Intrusion Detection

An intrusion-detection-system (IDS) blade in the Cisco Catalyst 6500 passively observed all traffic passing through the backbone Cisco Catalyst switch in the test bed. Its job: to analyze and track patterns, in real-time, and identify potential attacks and assaults.

A Cisco IDS lets administrators quickly respond to suspected security breaches. Upon identifying a hacker-attack pattern, or "signature," the IDS will typically respond by sending alarms, which show up at the Cisco IDS security-management system. A screen shot of the IDS Event Viewer (IEV) application that Cisco employed during the testing is shown on the following page.

Cisco says it chose signatures for this testing from a broad cross section of intrusion-detection signatures included in the latest release of its IDS package. These represent the most common network attacks and scans, and are designed to detect attacks in all of the following categories:

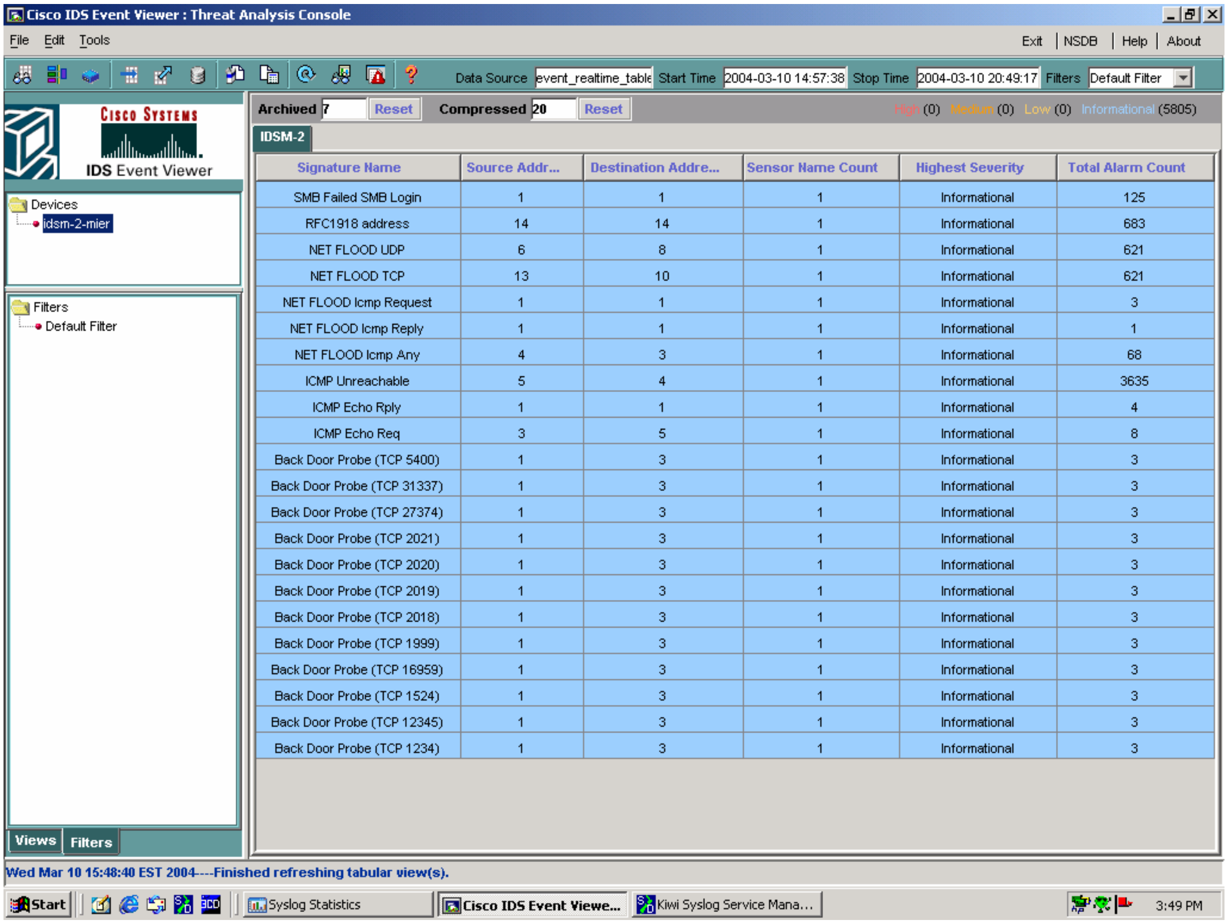
- *Exploits*: indications that someone is attempting to gain access or compromise systems on the network (such as: Back Orifice, failed login attempts, and TCP hijacking).

- *Denial of Service (DoS)*: activity indicating someone is attempting to consume bandwidth or computing resources to disrupt normal operations (including such DoS attacks as: Trinoo, TFN, and SYN floods).

- *Reconnaissance*: activity indicating someone is probing or mapping the network, such as with ping sweeps and port sweeps, to identify "targets of opportunity," usually as a precursor to an actual attack.

- *Misuse*: Activity indicating someone is violating corporate policy, which can be detected by configuring the audit rules to look for custom text strings in the network traffic. For example, XYZ Corporation could configure the Cisco IDS Sensor to send an alarm on the phrase "XYZ Confidential" in e-mail or File Transfer Protocol (FTP), and subsequently eliminate any such connection that transmits that phrase.

Besides sending alarms, the Cisco IDS solution can be configured to respond to attacks by dropping all traffic from the attack source or sending out TCP reset packets to break any established connections from the attack source.



Data Source event_realtime_table Start Time 2004-03-10 14:57:38 Stop Time 2004-03-10 20:49:17 Filters Default Filter

Archived 7 Reset Compressed 20 Reset High (0) Medium (0) Low (0) Informational (5805)

Signature Name	Source Addr...	Destination Addre...	Sensor Name Count	Highest Severity	Total Alarm Count
SMB Failed SMB Login	1	1	1	Informational	125
RFC1918 address	14	14	1	Informational	683
NET FLOOD UDP	6	8	1	Informational	621
NET FLOOD TCP	13	10	1	Informational	621
NET FLOOD Icmp Request	1	1	1	Informational	3
NET FLOOD Icmp Reply	1	1	1	Informational	1
NET FLOOD Icmp Any	4	3	1	Informational	68
ICMP Unreachable	5	4	1	Informational	3635
ICMP Echo Rply	1	1	1	Informational	4
ICMP Echo Req	3	5	1	Informational	8
Back Door Probe (TCP 5400)	1	3	1	Informational	3
Back Door Probe (TCP 31337)	1	3	1	Informational	3
Back Door Probe (TCP 27374)	1	3	1	Informational	3
Back Door Probe (TCP 2021)	1	3	1	Informational	3
Back Door Probe (TCP 2020)	1	3	1	Informational	3
Back Door Probe (TCP 2019)	1	3	1	Informational	3
Back Door Probe (TCP 2018)	1	3	1	Informational	3
Back Door Probe (TCP 1999)	1	3	1	Informational	3
Back Door Probe (TCP 16959)	1	3	1	Informational	3
Back Door Probe (TCP 1524)	1	3	1	Informational	3
Back Door Probe (TCP 12345)	1	3	1	Informational	3
Back Door Probe (TCP 1234)	1	3	1	Informational	3

Wed Mar 10 15:48:40 EST 2004----Finished refreshing tabular view(s).

Cisco IDS Event Viewer. Shown above is the main display of the Cisco IDS Event Viewer (IEV), which updates in real-time. Administrators can choose to display the volume and extent of events they wish, from all events, including ‘informational’ notes, to just critical alarms.

Threats to IP Telephony

How will they come at me? That's one of the first questions users investigating their VoIP security options ask. The answer: There are many ways, but most assaults do follow certain steps and patterns. A subset of typical approaches and threats is summarized in this section, but this is by no means an exhaustive listing of potential attacks.

In order for these threats to happen to you, two things must occur: First, the assailant needs to be able to observe your voice-network traffic. That is not as difficult as it sounds: In all the different vendors' IP-telephony networks we have tested so far, our hackers have been able to insert a passive probe into an IP-phone station connection, and then observe and collect full VoIP-network traffic details – such as protocols and addresses.

Secondly, the assailant needs to be able to deliver traffic onto the VoIP network. That is usually done by configuring a computer – a Linux-based laptop is a favorite – to spoof a legitimate IP phone, using the network information collected. Then, with spoofed access to the voice VLAN, the perpetrator can issue traffic to virtually every other component in the VoIP infrastructure.

Our hackers readily accomplished both of these tasks because they had physical access to an IP-phone connection, for insertion of the passive probe and for subsequent delivery of spoofed traffic. Neither could have been accomplished in this manner without physical access.

Reconnaissance

Tools readily available on the Internet can be employed to scour networks and report active IP and MAC addresses, protocols, services, operating systems, and potential vulnerabilities. These tools can provide a large amount of information that a hacker can use to develop a plan of attack, and reduce the time necessary to launch an effective assault.

Cisco locked down the "settings" button on its IP phones in the test bed, restricting casual users from viewing their phones' configurations – and completely blocking their ability to change the settings. While the Miercom assault team was still able to ascertain some of these settings by inserting a passive probe between the switch and the phone, the phone lock-down feature still went a long way towards making their reconnaissance task more difficult and ensured that they could not tamper with the phones configuration

Man-in-the-Middle

There are several ways to perform a "man-in-the-middle" attack. The most common involves ARP, which can cause an IP phone to redirect its traffic to the attack computer. The attack computer then gains complete control over that IP phone's sessions, which can be altered, dropped, or recorded. Or the phone can readily be rendered inoperable.

The Cisco DHCP Snooping, Dynamic ARP Inspection, Port Security, IP Source Guard and VLAN Access Control Lists in the "access" Cisco Catalyst 4500 thwarted all such attacks that the Miercom assault team attempted. The hackers could only capture packets being sent to, or from, the IP phone on the particular switch port they were attached to.

Legitimate traffic replay

Captured traffic from a passive probe can also be re-transmitted onto the network. Since this traffic is allowed through the network, it can prompt a destination computer to respond to this replayed traffic, and issue a response or otherwise consume that host computer's resources. Depending on how the destination computer responds, this can potentially cause a denial-of-service for other IP nodes trying to send traffic to the same destination.

The combination of Layer-2/Layer-3 security features configured in the Cisco Catalyst 4500 listed earlier, along with the Microflow policing applied by the Cisco Catalyst 6500, and the Access Control Lists in the FWSM, provided enough protection to block the hackers' ability to launch this type of an attack, or neutralize it by shedding the packets. For instance, the TCP Intercept feature would block a TCP replay attack since there would not be a bi-directional connection established.

DHCP starvation

A malicious computer on the network can issue excessive requests to a DHCP server and force the server to issue all of its allocated IP addresses. The server could then not service the next legitimate request that comes in, thus stopping new stations from entering the network.

The Cisco DHCP Snooping and Port Security features in the Cisco Catalyst 4500 completely mitigated this threat by rate-limiting DHCP requests on each client port and ensuring that no more than three MAC addresses existed on each client port.

DHCP server spoofing

As an IP phone boots up it requests a DHCP lease, which is sent across the entire broadcast domain. A malicious computer can reply to the request and provide incorrect information. This can cause a denial-of-service, or enable a man-in-the-middle attack.

Again, the Cisco DHCP Snooping feature in the Cisco Catalyst 4500 mitigated this threat by denying DHCP responses on all but trusted ports. Each switch port on the Cisco Catalyst system can be configured as trusted or untrusted. Untrusted ports are rate-limited, and are only permitted to send DHCP Discovers and Requests; trusted ports are not rate-limited and are permitted to send DHCP Offers and Responses.

Forwarding-table corruption

A Layer-2 switch will typically learn what MAC addresses are connected on which ports and build a forwarding table. Some switches can readily be tricked into building a forwarding table containing non-existent stations or stations on incorrect ports. If applied at an intense enough level, the switch could fill its forwarding table, allowing no more new entries. At this point the switch would stop accepting MACs, or else broadcast all frames to every port, or experience a serious system failure.

Again, the Cisco Catalyst 4500's DHCP Snooping, IP Source Guard and Port Security features mitigated this type of attack, by limiting the number of MAC addresses permitted on each client port and validating that the source MAC address and source IP address of each frame matched the DHCP binding table.

Endpoint-configuration substitution

IP phones can often be set-up to request a configuration file or firmware download from a TFTP server. It is possible for a malicious intruder to redirect the IP phone to instead obtain a configuration file or firmware download from a host other than the intended server. An incorrect configuration or an invalid firmware image could thus be loaded on the IP phone – to disrupt its call capability, selectively disable features, or redirect its traffic.

Cisco thwarted this type of attack in three ways. First, the IP phones were administratively locked down, so their configurations could not be changed locally. Secondly, the DHCP Snooping, Dynamic ARP Inspection, IP Source Guard and Port Security features of the Cisco Catalyst 4500 blocked the hackers' attempt to impersonate the TFTP server. Finally, all Cisco IP-phone configuration files and firmware files are digitally signed, and the Certificate Trust List (CTL) in each phone ensures that the TFTP server is a trusted host. So even if an attacker could access the local configuration of the phone, or masquerade as the TFTP server, the phones would not have trusted the phony TFTP server or downloaded any files that did not match the digital signature engrained in them.

Rate limit abuse

Rate limiting can be used *against* a network if it is applied, for example, to a group of hosts. An assailant can issue excessive amounts of seemingly legitimate traffic, and, when rate limited, the effect could be to deprive other computers or stations of needed bandwidth.

Cisco prevented this type of attack, too, in several ways. The Cisco Catalyst 4500 restricted the number of MAC addresses allowed on a port (Port Security), and then validated the source IP and MAC addresses of each packet (IP Source Guard). Firewalls and access lists stopped all but necessary TCP and UDP port traffic. In addition, unused ports on the switch were shut off, so that the assault team could not generate enough traffic to cause any damage.

Even more impressive is the new MicroFlow Policing feature of the Cisco Catalyst 6500, which can police traffic on a per-flow basis (for example, per source/destination IP address). While traditional policers rate-limit traffic in an aggregate fashion, Microflow policing allows the administrator to police traffic per source IP address. For instance, SCCP signaling traffic between the voice VLAN and the call-control servers was policed to allow only a few kilobits per second, per host.

The uplink between the Cisco Catalyst 4500 and the Cisco Catalyst 6500 in the test bed was a 1-Gbps fiber-optic connection, and the servers were 100-Mbps attached to the Cisco Catalyst 6500. Therefore, no one station could ever send enough SCCP packets to overflow the policers and cause a DoS of SCCP service to the other phones. Likewise, RTP media traffic was policed to allow no more than 80-kbps per endpoint.

Toll Fraud

In other IP-telephony environments, an unauthorized computer, posing as an IP phone, can be placed on the network and attempt a brute-force password assault on the call-control or authentication server. If a weak authentication method is used, the unauthorized station can often guess the password in short order, and then be permitted to make calls.

There are many other forms of toll fraud, such as transferring calls off-net to a long-distance number, enticing users to dial certain area codes which apply a toll charge for the call, and many more variations of manipulating the system or manipulating the users of the system to allow unauthorized calls to be placed.

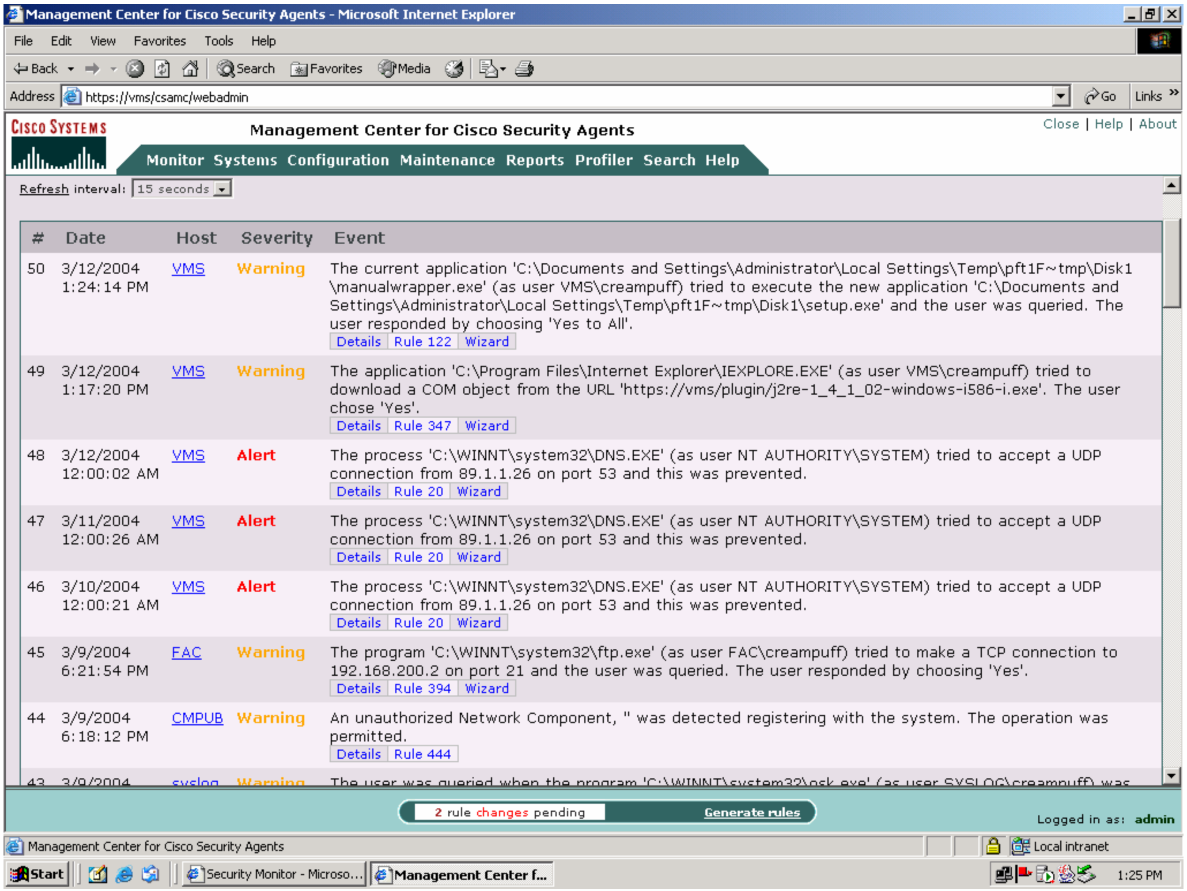
Cisco CallManager supports a broad set of toll-fraud-mitigation capabilities. An administrator may, for example, define what numbers each user is allowed to call, and what numbers each user can forward or transfer their calls to. The same rules also apply to applications, such a voicemail and IVR servers, so those applications cannot be used to make unauthorized calls (by transferring out of voicemail to a long-distance number, for instance). In addition, through the use of digital certificates in the IP phones and Cisco CallManager servers, only authenticated phones can register with the system, thus blocking the hackers' ability to insert a phone in the network, or impersonate a phone, and place unauthorized calls.

Misdirected administrative attention

In a typical secure environment there are logging, alerting, and monitoring services going on continually. These normally useful tools can be used against the administrator, too, by obscuring malicious assaults. An assailant may intentionally cause a flood of traps or alerts by sending traffic that is likely to prompt violations, resulting in log entries, traps or alerts. Meanwhile, the assailant may undertake other, more dastardly attacks, presuming that the high influx of event alerts would inundate and distract the administrator. Also, some alert and log services, and sometimes their servers, can be made to fail if log sizes exceed a size limitation.

While Cisco did not fully demonstrate its abilities to filter and intelligently track logs and alerts, the CiscoWorks 2000, Syslog and IDS Monitor packages could all have been brought to bear, and highly tuned for this purpose, according to the vendor. Whether this could have been exercised in our test environment is questionable, however: It seems the security features in the Cisco Catalyst switches and firewalls largely prevented our hackers from generating enough types of alarms – via various forms of threatening attacks – to cause any significant confusion.

Event logs. A security event log, this from the CiscoWorks 2000 Management Center for Cisco Security Agents, is shown below.


Management Center for Cisco Security Agents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://vms/csamc/webadmin
Go Links
Cisco Systems
Management Center for Cisco Security Agents
Close | Help | About
Monitor Systems Configuration Maintenance Reports Profiler Search Help
Refresh interval: 15 seconds
2 rule changes pending
Generate rules
Logged in as: admin
Management Center for Cisco Security Agents
Local intranet
Start
Security Monitor - Microso...
Management Center f...
1:25 PM

#	Date	Host	Severity	Event
50	3/12/2004 1:24:14 PM	VMS	Warning	The current application 'C:\Documents and Settings\Administrator\Local Settings\Temp\pft1F~tmp\Disk1\manualwrapper.exe' (as user VMS\creampuff) tried to execute the new application 'C:\Documents and Settings\Administrator\Local Settings\Temp\pft1F~tmp\Disk1\setup.exe' and the user was queried. The user responded by choosing 'Yes to All'. Details | Rule 122 | Wizard
49	3/12/2004 1:17:20 PM	VMS	Warning	The application 'C:\Program Files\Internet Explorer\IEXPLORE.EXE' (as user VMS\creampuff) tried to download a COM object from the URL 'https://vms/plugin/j2re-1_4_1_02-windows-i586-i.exe'. The user chose 'Yes'. Details | Rule 347 | Wizard
48	3/12/2004 12:00:02 AM	VMS	Alert	The process 'C:\WINNT\system32\DNS.EXE' (as user NT AUTHORITY\SYSTEM) tried to accept a UDP connection from 89.1.1.26 on port 53 and this was prevented. Details | Rule 20 | Wizard
47	3/11/2004 12:00:26 AM	VMS	Alert	The process 'C:\WINNT\system32\DNS.EXE' (as user NT AUTHORITY\SYSTEM) tried to accept a UDP connection from 89.1.1.26 on port 53 and this was prevented. Details | Rule 20 | Wizard
46	3/10/2004 12:00:21 AM	VMS	Alert	The process 'C:\WINNT\system32\DNS.EXE' (as user NT AUTHORITY\SYSTEM) tried to accept a UDP connection from 89.1.1.26 on port 53 and this was prevented. Details | Rule 20 | Wizard
45	3/9/2004 6:21:54 PM	FAC	Warning	The program 'C:\WINNT\system32\ftp.exe' (as user FAC\creampuff) tried to make a TCP connection to 192.168.200.2 on port 21 and the user was queried. The user responded by choosing 'Yes'. Details | Rule 394 | Wizard
44	3/9/2004 6:18:12 PM	CMPUB	Warning	An unauthorized Network Component, " was detected registering with the system. The operation was permitted. Details | Rule 444
43	3/9/2004	syslog	Warning	The user was queried when the program 'C:\WINNT\system32\osk.exe' (as user SYSLOG\creampuff) was

Tips, Tricks for Securing VoIP

As it tests the security soundness of more and different IP-telephony packages, Miercom is amassing a growing collection of "Rules of Thumb" for enhancing the security of VoIP and IP-telephony networks and services. Here is a condensed list of recommendations that we hope VoIP network managers will read and consider applying to their IP-telephony environments. These are listed in no particular order.

How much is not enough: Perform a risk and benefit analysis

Before deploying an IP telephony package, conduct a close review of the associated risks that every component of your network poses. Think: What if this component were attacked and rendered useless? Then consider what security options are available to protect the component or resource. The costs associated with adequate security can be considerable, so you need to weigh that cost against the alternative – telephony disruption or downtime.

Adopt and Enforce physical security

Often overlooked as a vital security consideration, physical security can considerably reduce your risks. You may want to know who is entering and leaving your facilities, and why they are there. Consider especially any wireless networks: A poor security infrastructure on a wireless network can potentially negate any physical security measures.

Keep Hackers in the Dark: Reduce available information

Information is a hacker's best friend, so the less you provide the less accurate and effective a hacker's attack will be. It's impossible to cover all your tracks, but disabling the ability of an IP phone user to locally view or modify the IP phone's configuration is a step in the right direction. Discovery protocols and management protocols like SNMP, if they can be viewed from a user's office cube, can yield model numbers and software versions of the network infrastructure, giving a hacker a head-start in building and fine tuning his attacks.

Consider Physically Separating Management & User Traffic

Management traffic does not have to traverse the same physical links as user data and voice. Routers, switches, firewalls, and the like, can in almost all cases be configured with physically separate management links, which if properly implemented can be invisible and inaccessible to hackers.

Restrict VoIP Components to only the Resources they need

Creating a tiered architecture, which prevents VoIP components from interacting with data components – and vice versa – is also often a worthwhile consideration and undertaking. VLAN tagging can separate traffic types logically. Where possible, though, physically separate the data and voice traffic. Within the VoIP network a firewall can effectively restrict access, so only known endpoints communicate on known protocols and ports.

Too much of anything is bad: Rate limit all traffic

When an IP phone registers or places a call, that traffic should pass through the scrutiny of your security components. A phone shouldn't be making 1,000 calls per second. Understand the expected VoIP bandwidth utilization of your network, and rate-limit traffic accordingly, as close to the access point as possible, before it reaches your VoIP components.

Batten down the hatches: Harden your systems

Take the time to see what is running on your servers and who can access and manage them. If there are services and/or protocols running that are unnecessary for your operation, disable them. Likewise, user passwords need to periodically be changed, and unused accounts closed down. Admin and manager accounts should also be role-based, where these people only have access to what they need to perform their duties. Logs should be used to track all activity.

Where possible, encrypt signaling, media streams, and management

Encryption can provide a cloak to mask signaling and management, and prevent wiretapping of VoIP voice streams. Encryption that's available today can prevent hackers from gathering information they can use to identify targets and possible vulnerabilities. Eavesdropping no longer requires being on the same physical wire as the call. Many tools permit VoIP streams to be captured and replayed, but not when the traffic is encrypted.

The secret handshake: Authenticate endpoints

Unauthorized phone use can be effectively addressed by requiring that IP phones use some form of authentication, like certificates, which is a much stronger control than passwords.

Stop the attack before it happens: Consider IDS and HIPS

Many intrusion detection (IDS) and host-based intrusion prevention systems (HIPS) can detect and possibly deter application layer exploits, hacker scanning, and denial-of-service attacks before they reach their target. Proper tuning is often required to provide useful alerts.

Detailed logging, effective alerting, and attentive monitoring

Even with automated security measures in place, a human somewhere still needs to regularly monitor the logs, alerts, traps and reports that network devices generate. Logs and reports often allow knowledgeable administrators to trace the events that reveal a security breach, so holes can be patched. Effective alerting can reveal that a violation has occurred and give users a fighting chance to stop an attack in progress. But alerts need to be fine tuned, so an administrator doesn't get swamped, and then miss the really important problems.

About Miercom’s Product Testing Services…

With hundreds of its product-comparison analyses published over the years in such leading network trade periodicals as *Business Communications Review* and *Network World*, Miercom’s reputation as the leading, independent product test center is unquestioned.

Founded in 1988, the company has pioneered the comparative assessment of networking hardware and software, having developed methodologies for testing products from SAN switches to VoIP gateways and IP PBX’s. Miercom’s private test services include competitive product analyses, as well as individual product evaluations.

Products submitted for review are typically evaluated under the “Net**WORKS** As Advertised™” program, in which networking-related products must endure a comprehensive, independent assessment of the products’ usability and performance. Products that meet the appropriate criteria and performance levels receive the “Net**WORKS** As Advertised” award Miercom Labs’ testimonial endorsement.

Miercom

379 Princeton-Hightstown Road, Cranbury, NJ 08512
609-490-0200 ● fax 609-490-0610 ● www.miercom.com