SearchFinancialSecurity.com
E-Guide

# Top Defense Strategies and Security Considerations for Unified Communications (UC)

Organizations turn to unified communications as a cost-effective alternative to traditional communication systems. This results in cost savings and the creation of an innovative set of digital resources.

However, security professionals often struggle to wrap their arms around the problem of securing voice over IP (VoIP) and unified communications. This problem spans servers, endpoints and network infrastructures, so the enterprise must deploy defenses at all levels.

Read this expert E-Guide and discover unified communications infrastructure threats and basic techniques and technologies for addressing them.

*Sponsored By:*


TRADE UP. TRADE ON.

SearchFinancialSecurity.com
E-Guide

# Top Defense Strategies and Security Considerations for Unified Communications (UC)

## Table of Contents:

# Unified communications infrastructure threats and defense strategies

by John Burke

IT operations and security staff often struggle to get their arms around the problem of securing voice over IP (VoIP) and unified communications. Whether CIO, systems administrator or security engineer, it helps enormously to know what the threats are and the basic techniques and technologies for addressing them. That's what we'll cover in this tip.

First, let's define the technology. Unified communications incorporates voice, video and text communications in a number of formats: telephony-type voice traffic (VoIP), including audio conferencing; instant messaging; email, which is often combined with voice messaging and fax to create unified messaging; desktop-to-desktop video conferencing; and Web conferencing. User interactions with all these tools can be managed via a collection of separate client interfaces (Web browsers, email clients, IM clients, etc.), or all the clients can be collected into a single interface, a real-time communications dashboard (RTCD). There may or may not be a separate, physical IP desk phone; many users are now getting only a softphone, which is a computer application that performs the function of a phone on a desktop, laptop or handheld device.

## Unified communications threats

Integration of all voice and video communications onto a common data network and the common desktop means that unified communications are no more secure than the enterprise desktop and data network. However, there are some threats and avenues of attack that are specific to unified communications or have new application to unified communications.

A top concern is eavesdropping, or the unauthorized interception of VoIP, IM or other traffic. UC endpoints, whether desktops, laptops, or IP phones -- not really phones but rather computers with specialized user interfaces -- all connect to the data network, and can be tapped by compromising the network anywhere along the data route. Moreover it has become possible with hard or softphones, once they are compromised, to have their conferencing or handset/headset microphones activated without being taken off hook. This enables remote eavesdropping on private conversations taking place in person, and often behind closed doors. Performing such compromises may not be easy, but the changing nature of security attacks -- from amateur to professional, from general to targeted -- means that these techniques will be developed and available to anyone for a price.

A related fear is toll fraud. IP telecommunications providers around the world lose hundreds of millions of dollars annually due to stolen services, especially long-distance services. Unified communications voice and video traffic typically now use the Session Initiation Protocol (SIP) to control calls, but the actual media stream for a call is separate from that control stream. It is possible, therefore, to use SIP to perpetrate a new kind of toll fraud. An attacker can use SIP to lie to the call manager about what kind of call it is controlling. For example, the perpetrator might tell the call manager that a call will be voice-only, but then stream high-definition video instead, essentially defrauding the system owner of the higher revenues for the video traffic.

Vishing, the VoIP-enabled form of phishing, is a third category of security concern around unified communications. Applying the basic techniques of phishing to a new toolset, vishers use spoofed Caller ID or other call information to suggest that they are calling in an official capacity from corporate or vendor IT support, or a government agency, etc., in order to get recipients to reveal confidential information over the phone.

Denial of service is an attack method that has new and specific applications in the unified communications world. While it was virtually unknown with traditional telephony, with armies of compromised zombie PCs at their disposal, today's attacker can aim to disrupt the communications infrastructure at the desktop level by swamping or crashing phones. or at the gateway level by taking out the network nodes that interface an enterprise VoIP installation with the outside world. They can also attack call managers directly by using SIP or other protocols to crash the manager with an endless flood of valid but dishonest session requests.

Another security threat that is now an increased problem for unified communications is platform compromise. No longer an issue restricted to email systems and IM, attackers can now subvert applications on servers, desktops and handhelds, or by taking over an IP phone via UC protocols like SIP or SIMPLE. From there, malicious hackers can launch all manner of attacks, including stealthy information-gathering campaigns and more brazen attempts at further compromises, denial of service or vandalism.

## Securing unified communications

The problem of securing unified communications spans servers, endpoints and network infrastructures, so the enterprise must deploy defenses at all levels -- something it should already be doing, and to which unified communications only adds more urgency.

Phones should be secured like other network devices: unused services (many IP phones have Web servers embedded, for example) should be shut down, unused ports disabled, and default management passwords changed. All management should be forced through authenticated and encrypted connections, if possible.

Firewalls, router access control lists, VLANs, port-level switch security and authenticated network access comprise some of the low-level strategies IT should deploy on the network to protect IP phones and/or desktops from each other.

Host- and network-based intrusion detection is also important, for traffic to and from clients and unified communications servers. Intrusion prevention systems (IPSes), where they can be made robust enough to manage unified communications traffic without adding insupportable latency, will be another key. Especially important will be IPS or proxy servers -- focused specifically on SIP and SIMPLE -- that can look deep inside unified communications network packets and examine the actual data being sent to see not only whether it is acceptable in format and length but also to spot ill-intended data using probabilistic analysis.

IT needs to attend to standard host-level security measures too, such as firewalls, antispyware and antivirus agents. Malicious hackers always seek out the path of least resistance, so compromising unified communications systems via servers or clients instead of direct assault on network traffic makes no difference.

In the end, although specific technologies like SIP proxies and firewalls are useful in securing unified communications, it is more important to take the deployment of unified communications as yet another impetus to a well-rounded, multi-level and multi-layer defense strategy for security across the enterprise infrastructure.

**About the author**

*John Burke is principal research analyst with Nemertes Research. With nearly two decades of technology experience, he has worked at all levels of IT, including end-user support specialist, programmer, system administrator, database specialist, network administrator, network architect and systems architect. He has worked at The Johns Hopkins University, The College of St. Catherine, and the University of St. Thomas.*

# VoIP security considerations

by Sandra Kay Miller

When it comes to leading-edge technologies, financial institutions have always been at the forefront, and Voice over Internet Protocol (VoIP) is no exception. Leveraging existing network infrastructures to deploy a cost-effective alternative to traditional Public Switched Telephone Network systems has resulted in significant savings while delivering an innovative set of digital resources.

Stamford, Conn.-based research firm Gartner Inc. estimates that more than 80% of companies are currently engaged in IP telephony trials and that within three years, VoIP deployments will be ubiquitous.

But the reality of packetizing voice calls and routing them over the same network used for Internet traffic exposes organizations to the same cyber security challenges facing data transmissions.

There are a number of considerations financial services organizations should explore prior to integrating VoIP technology into their business.

## Solid architecture

New protocols and resources are ripe targets for exploits. "From an architectural perspective care must be taken to prevent access to network resources from the VoIP network," says Paul Henry, vice president of technology evangelism at Secure Computing in San Jose, Calif.

For example, isolating SIP servers and assigning granular access controls to define what users can establish connection to specific resources. Additionally, Henry suggests the use of a SIP proxy. "As an integral part of the overall architecture, this can offer significant risk mitigation by validating the protocol and applying policy to SIP."

## Degrees of separation

Although convergence is the buzzword often associated with VoIP, many organizations are considering isolated networks -- either physical or virtual -- for voice and data. Cisco advocates logical separation of VoIP traffic from the data network.

By putting voice and data on a single network, organizations are subject to losing both in a network outage.

However, separate networks require additional resources, regardless of whether they are virtual local area networks or completely separate physical networks.

"In reality, few will take it to that level," predicts Henry, who points out the key to VoIP security is access control and policy enforcement.

Similarly, due to the types of information traversing financial services networks and residing on servers, IT shops, especially those tasked with regulatory compliance in addition to security, are questioning how to best protect their VoIP infrastructure.

"Treat VoIP applications the same as any other application: Lock down servers and protect against unwanted access using intrusion detection and firewalls," suggests Irwin Lazar, senior analyst at Burton Group, based in Midvale, Utah.

"The current generation of firewalls can easily handle VoIP and all other gateway protocols," Henry added.

## Security equals quality of service

In the data world, users have often equated increased security with decreased performance. In the world of VoIP for financial services companies, dropped calls, latency or a jittery connection -- all common issues associated with VoIP -- pose serious risks to business continuity in addition to IP-centric threats including viruses, hackers and exploits.

"No matter what you do with the fanciest phone in the world, if an end user hears jitter, gets latency or just has a bad overall VoIP experience, all the investment that you made and the utility you get from VoIP goes out the window because the user thinks it stinks. The end game is that you are able to deliver service the way people expect it to be," explained Neil Darling, of EtherSpeak, a Virginia-based company focusing on VoIP in vertical markets.

At the 2006 CeBit roundtable on VoIP security, industry leaders and experts estimated it could be two more years until the right balance of security and quality of service in enterprise deployments could be achieved. One of the primary concerns was the latency created by firewalls unable to handle VoIP traffic, but in the last year, firewall vendors have responded by adding features specific to VoIP to existing products.

Even with VoIP-capable firewalls, Henry pointed out that a firewall must be properly sized to handle the amount of traffic present on the network or quality of service will suffer.

**About the author:**
*Sandra Kay Miller is a technical editor for* Information Security *magazine with 15 years of experience in developing and deploying leading-edge technologies throughout the petroleum, manufacturing, luxury resort and software industries, and has been an analyst covering enterprise-class products for 10 years.*

# Resources from IPC Systems, Inc.


TRADE UP. TRADE ON.

IPC Whitepaper: Rising Above Risk: Sinsible Continuity Solutions for Voice Trading Communications…

IPC Whitepaper: The Turret vs. PBX Trade-off: Optimizing Productivity. Managing Volatility.

**About IPC Systems, Inc.**
IPC Systems, Inc. is a leading provider of indispensable communications solutions to financial services firms worldwide. IPC offers customers a suite of products and enhanced services that includes advanced Voice over Internet Protocol (VoIP) technology, and integrated network and management services to more than 40 countries.