

white paper - white paper - white paper - white paper - white paper - white paper - white paper

# IP voice security: red herring or real risk?

Albert Siu  
IP Advanced Services, Hong Kong



Business  
Services



# summary

- 3 executive summary
- 4 infrastructure and application-based attacks
- 6 denial-of-service (DoS) attacks
- 7 eavesdropping
- 8 toll fraud
- 9 protocol-specific threats
- 11 conclusion

# executive summary

Corporations are increasingly realizing the benefits of transforming their circuit-switched networks to IP packet switching networks in order to run their voice and data applications over a converged infrastructure. Typically, cost savings and productivity enhancements are both major drivers for this change.

While there are definitely benefits associated with convergence, businesses should be aware that there are also potential risks involved, so they can take the steps necessary to protect their company's interests. One of those risk areas is voice-over-IP (VoIP) security and the related security problems that emerge when converging voice and data networks.

When voice and data traffic are merged onto a single network, voice becomes an application on the network and is, therefore, exposed to the same threats as data applications. Some of the threats are denials of service (DoS), viruses and worms.

The good news is that security risks are well understood, and steps can be taken to mitigate them. With proper security planning and practices, Orange can address VoIP security risks and threats in a managed and controlled manner and thereby maximize the benefits of VoIP deployment with a minimum of exposure.

In this paper, we will identify and discuss five key issues related to VoIP security, their respective impacts and our suggested actions:

1. infrastructure and application-based attacks
2. denial-of-service (DoS) attacks
3. eavesdropping
4. toll fraud
5. protocol-specific threats

# infrastructure and application-based attacks

In VoIP, voice is essentially an application on the data network that is fine-tuned to ensure voice-quality performance. VoIP equipment and end-point devices (e.g., IP phones) are computing devices and are becoming standardized and commoditized just like other data components, such as PCs and notebooks. Therefore, these voice end points are vulnerable to attacks from viruses and worms. Opening up protocol standards encourages vendor participation by providing more choices to the market; however, it also inevitably eases exploitation by ill-intentioned attacks. Hackers will find it increasingly easy to compromise and exploit voice devices to disrupt the network from normal service and/or perform criminal actions, such as data theft.

Various measures can be taken to address this area of concern. The first, and perhaps the most basic, is for the IT manager to maintain current patch levels in all IT and network equipment and applications. This is straightforward and critical, but it's often overlooked because of its tedious nature. Procedures should be implemented to automatically update software in all VoIP devices as it becomes available.

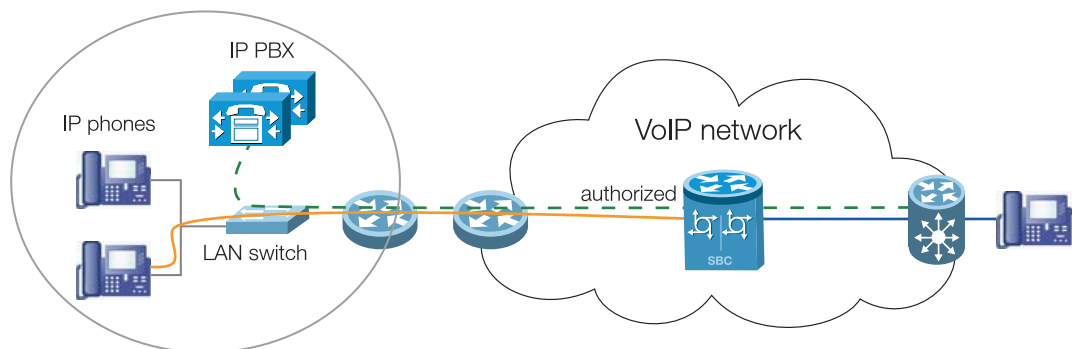
Another simple tip is to install and maintain an anti-virus system, including software tools and proper guidelines. Service providers, like Orange, use even more stringent measures to further safeguard equipment and software to give customers peace of mind regarding their IT operations.

Virtual local area networks (VLANs) can be used to protect voice traffic from data network attacks. By implementing application gateways between trusted and untrusted zones of the network, a VLAN will complement the protection provided by corporate firewalls. These gateways, also known as session border controllers (SBCs), are highly specialized components that provide multiple functions, such as call set-up and control, VoIP signaling payload inspection, malformed packet and DoS attack prevention and network address translation (NAT). Using these functionalities, SBCs enable interoperability between network segments and dynamically manage pinholes for media and signaling of VoIP traffic. The SBC provides the NAT function in a centralized and scalable manner and provides a number of security features, including:

- customer topology (IP address range) suppression to prevent DoS attacks

- private vs. public IP address conflict resolution
- full termination and re-origination of sessions on both sides of the application-level gateway (trusted and untrusted) in layers 3-4 for a strong defense
- access control
- policy-based filtering of VoIP traffic that allows only explicitly permitted traffic
- signaling validation that permits only legitimate call set-up scenarios to flow through the firewall and opens pinholes for media on a call-by-call basis
- dynamic port allocation as media firewall that allows only pre-negotiated ports in the application layer that are allocated temporarily and then torn down upon session completion
- multi-vendor equipment compatibility (built for standards compliance independent of the router provider, e.g., Cisco, Huawei, etc.)

figure 1 – session border controller (SBC)



Orange Business Services has long provided SBC functionality for network separation and transparency and to protect the network, and hence customers' operations, from external attacks.

Another critical consideration is the implementation of an intrusion detection and prevention (IDP) system that employs strong detection and prevention techniques to protect against current and emerging threats at both the application and network layers.

# denial-of-service (DoS) attacks

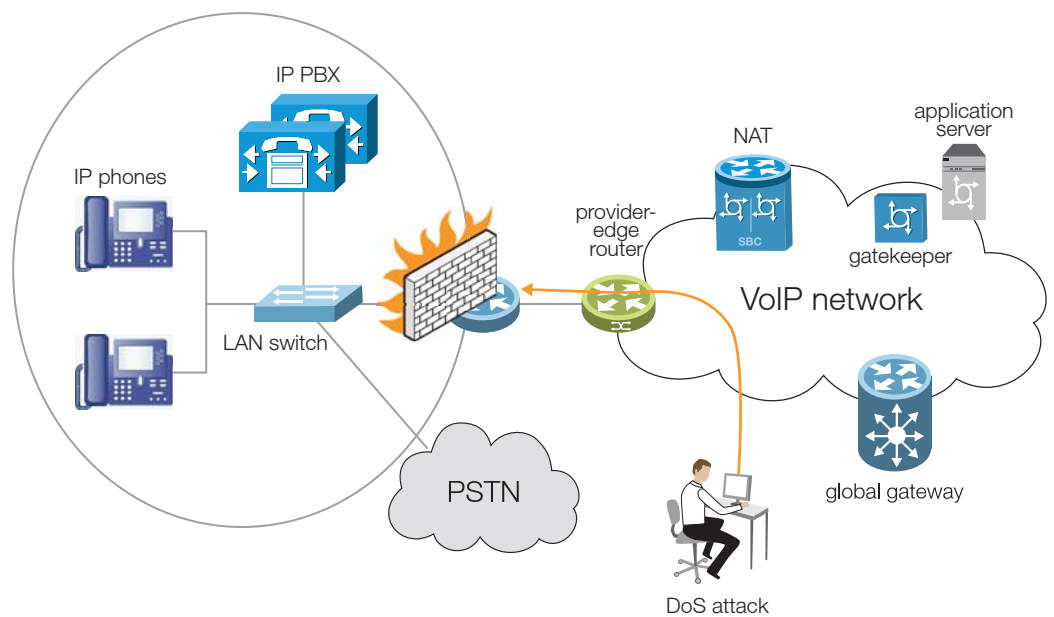
A denial-of-service (DoS) attack occurs when someone deliberately floods a particular network with so much illegitimate network traffic that it affects the support of legitimate traffic. Obviously this can impact voice traffic once voice and data traffic are converged on the data network.

DoS attacks are difficult to stop and prevent. However, like with proper intrusion prevention practices, special network devices and proper patch updates can minimize the risk of exposure.

To prevent data network problems from affecting voice traffic, voice and data traffic, as well as customer traffic (voice and/or data), should be logically separated from administrative traffic. This is one of the customer VLAN design strategies adopted by Orange Business Services. Segregation also provides the benefit of confining problems to within one logical network for easier operations.

Traffic shaping, due to classification, queue disciplines, scheduling, congestion management, quality of service (QoS) and class of service (CoS), as well as NAT and private IP addressing, will provide another layer of control and protection for the network.

figure 2 – preventing DoS attacks



# eavesdropping

In a data network, intercepting data traffic is a trivial endeavor; with convergence, the same is now true for voice traffic. Many tools, even freeware, are available to collect packets associated with VoIP conversations and reassemble them for nefarious purposes. Two measures can be taken to prevent eavesdropping:

- isolate VoIP traffic using virtual private networks (VPNs)
- apply encryption on voice packets

Running VoIP traffic on VPNs can prevent eavesdropping; however, since encryption processing can increase latency, encryption of voice should be applied selectively based on business requirements. For example, encryption and decryption could be used for only those conversations over untrusted networks. In this way, you maintain a balance between privacy and cost.

IT managers should evaluate the use of encryption of VoIP signaling, media streams or both. That evaluation should include using end points with encryption capabilities and ensuring that the network supports end-to-end transport of encrypted voice packets. When implementing encryption, VLANs can be used to prioritize voice traffic and minimize latency by segmenting voice and data traffic.

To address critical security requirements, voice and data traffic can be segregated completely through VLANs. Depending on the connection of the IP end points to the network (whether via a shared cable with PC or a separate connection), full isolation can be achieved by end-point support of the IEEE 802.1Q standard for trunking between VLANs or by using a voice-aware firewall, respectively.

When selecting a managed service provider for VoIP, companies should ensure that all of the above measures are being used by the potential provider to ensure secure conversations within the network.

# toll fraud

Just as with traditional time-division-multiplexing (TDM) systems, we cannot ignore the presence of toll fraud when considering VoIP systems. Using toll fraud, attackers gain unauthorized access to a private branch exchange (PBX) call-control system to make long-distance or international calls, which could mean significant financial impact to the business. In some scenarios, poor implementation of authentication could allow calls from unauthorized IP phones and/or allow unauthorized use of the VoIP network.

Most importantly, companies should impose proper control in access to the VoIP systems, including gateways and switches. In order to avoid the occurrence of toll fraud, attention needs to be placed on system configuration, including numbering and dialing plans, administrator password control and permission to perform direct inward system access (DISA, or remote access). Centralization of management and configuration control is also recommended, as are periodic configuration and usage audits.

# protocol-specific threats

VoIP was developed on an open standard, which means the protocols that support the communications are well known and, therefore, vulnerable to probing for their weakness and security flaws.

As session initiation protocol (SIP) gains popularity, attacks based on exploiting SIP and its vulnerabilities advance up the IT manager's alert list. SIP is a session and call-control protocol, components of which are used by standards-based IP PBX and IP telephony systems. In addition to the standard IP vulnerabilities, SIP brings other risks.

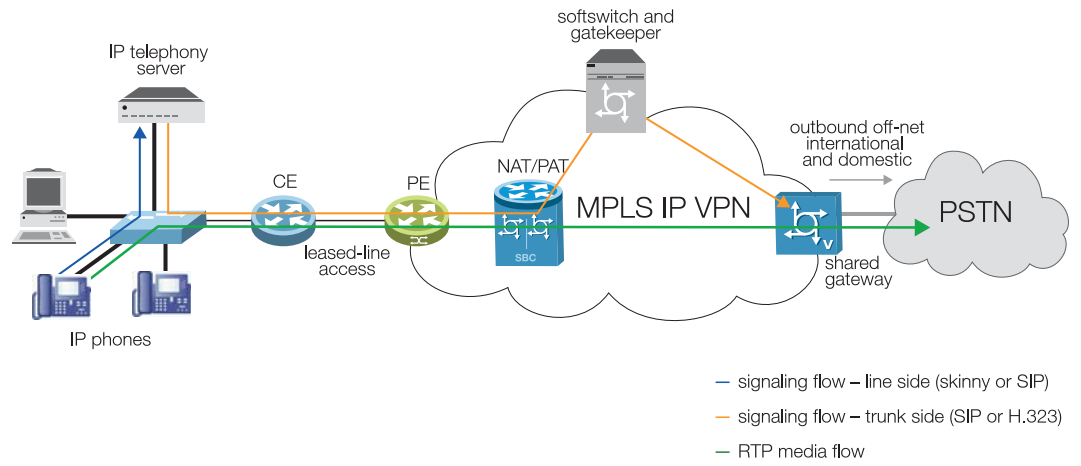
SIP is a text-based protocol, like the common HTTP and SMTP. Hence, attackers can easily monitor and analyze traffic, and spoof into various application-level attacks. They can perform impersonation registration for system access and unauthorized access to corporate directory information, as well as place unsolicited calls and voice messages and take control of calls to disconnect them, perform transfers or initiate multi-party conferences. Also, in order to complement the limited standard set of call features, SIP is now generally implemented by different system vendors with their own proprietary protocol extensions. This non-standard nature further induces complications in maintaining a foolproof platform for communications.

IT managers also need to be aware of the potential security risks of the VoIP H.323 protocol. H.323 was originally a series of recommendations developed to support multimedia transport over LANs. Later it was used in VoIP networking to support fundamental voice functions, like call signaling, control-message formatting and packet streaming. H.323 is always a challenge to network management for its flexibility in random port usage, which makes it difficult to enforce strict firewall policies.

The key to secure SIP and H.323 transactions is strong authentication, authorization and IPSec. A proxy server for authentication, which is a function provided by the SBC as described above, can help to ensure validation of the signaling payload and provide necessary suppression of customer topology information from outsiders. Similar consideration should also be applied to the media gateway control protocol (MGCP), which moves intelligence from the center of the network to the edge, much like SIP.

In the managed services model, operators will separate voice (media) and signaling streams and provide protocol gateways and authentication engines to encapsulate the network from protocol threats.

figure 3 – media and signaling flows



# conclusion

Convergence and VoIP implementations are fast becoming mainstream among multinational corporations and, at the same time, are posing certain serious security challenges. However, with proper diligence, businesses can address and tackle those challenges.

Convergence can simply mean the merging of both "traditions" of data and voice technologies. It can also mean the consolidation of traditional voice risk considerations with the risk considerations for data.

Whether you are planning to build your own converged network or utilize the services of a managed services provider, a primary goal should be the implementation of VoIP security that is properly built and validated, with on-going management support.

Generally, security policy standards should include:

1. implementation of application gateways (e.g., SBCs) to provide network separation and transparency
2. strong authentication
3. patch/upgrade management and ongoing system fortification
4. anti-virus and device-level protection
5. end-to-end encryption over the call path

Security has to be managed through proactive monitoring, event management, remediation and follow-up.

Business hinges on a stable and reliable communications infrastructure. The result of not implementing and managing proper security measures can be degradation of VoIP quality or, simply, the total disruption of the VoIP network. That makes it critical to adopt the right security standards to ensure that your VoIP infrastructure is stable, secure and reliable.

Ask your local account team how Orange Business Services can help secure your VoIP infrastructure, or visit us at [www.orange-business.com](http://www.orange-business.com) to find out more.

For more information about Orange Business Services, visit our website:

[www.orange-business.com](http://www.orange-business.com)

© Copyright Equant 2007. All rights reserved. All trademarks are the property of their respective owners. This publication is issued to provide outline information only. Specifications subject to change without prior notice. Orange Business Services is a name used by companies within the France Telecom Group, including Equant, France Telecom and Orange.

1007/MNC-WPR-IPT-002(1)



**Business  
Services**

