VoIP Softphones

David Premeaux
U.S. Army Information Systems Engineering Command

Voice over Internet Protocol (VoIP) provides the user with an opportunity to combine the use of a telephone with a personal computer (PC) into what is known as a Softphone. A Softphone allows users to place and receive calls using a PC. This article covers what a Softphone is and its issues, such as quality of service and security, which affect Softphones. The Technical Integration Center (TIC) currently does not recommend significant use of Softphones in the Army due to security and certification issues.

In the past 10 years technology has advanced to the point whereby telephone calls can be placed over Internet Protocol (IP) packet networks, also know as VoIP. One of the developments in this transition to VoIP was to turn a computer into a VoIP telephone by loading and running a VoIP software application on the computer. This VoIP application has emerged to be called a Softphone. A key motivation for using the Softphone is lower cost. This is due to the fact that the Softphone is little more than software, as compared to a traditional telephone that is mostly or all hardware. Softphones are also able to take advantage of making calls over the Internet with little additional equipment. This can save on long distance charges, especially when talking to another Softphone. Other advantages of the Softphone include potential integration with other applications, no space needed on the desk for a telephone, and the ability to move one's phone number with a computer.

What Is a Softphone?

For this article, a Softphone is a VoIP client application running on a computer. The Softphone uses VoIP signaling to establish calls, tear down calls, and take advantage of call features such as call forwarding. The Softphone also uses VoIP protocols to transport audio traffic in IP packets to another VoIP device. The Softphone is a client device, as it is the user device for establishing and tearing down calls. Other applications, such as a call processor application running on a computer, would not be considered a Softphone. The Softphone is also a software application loaded onto a computer and not a hardware device running in a computer.

Softphones using the Microsoft operating system will generally use the Telephony Application Programming Interface (TAPI), which enables PCs to support telephone services. TAPI provides support for such features as the volume control, microphone level, speakerphone, call control, etc. The version in Extra Professional also provides support for telephones connected to a PC via a Universal Serial Bus port.

The most common motivation for using a Softphone is avoiding long distance telephone calls. People using them for business can connect up from a hotel room and place calls back to the office using a PC and avoid using the hotel telephone or cell phone minutes. Home users are able to call and talk to each other using PCs (sometimes with video added) and avoid toll charges.

For the Department of Defense (DoD), Softphones have potential applications with tactical users. A user could gain telephone service simply by connecting a PC to an IP network and be able to place calls without a local call processor set up. An added advantage is that the user's telephone number would move with the PC, making the user more reachable.

Operational Aspects of Softphones

Operation of a Softphone is significantly different from the operation of a traditional telephone. In order to place/receive calls at any time, the user's computer must be turned on and the Softphone application running all the time. Power must also be provided to the computer at all times, and in the event power is lost, the computer needs to be re-booted. This can be avoided by providing power backup to the computer in the form of an uninterruptible power supply. The Softphone will also only be as reliable as the computer. If the computer is not stable and has to be rebooted periodically, the reliability of the Softphone will be affected.

Most traditional telephones have a handset the user utilizes for talking and listening. Most Softphone applications either use the computer speakers and a microphone or use a headset that includes both an earpiece and microphone. Answering a call with a traditional telephone is done by picking up the handset; whereas a Softphone is answered by clicking on an *answer call* icon. Likewise, ending a call with a traditional telephone is typically done by putting the handset into the cradle; whereas a Softphone call is ended by clicking on an icon to end the call.

Call features also work differently, and this is one of the areas where Softphones have an advantage over traditional telephone sets. With a traditional telephone call features are activated by selecting different combinations of digits. For example, to have calls forwarded a user might have to dial the digits #75 and then the call transfer number. With a Softphone, the user would select the call transfer icon and then enter the call transfer number. This eliminates the need to remember or look up various digit combinations to enable call features. A number of vendor implementations of Softphones allow the graphical user interface (GUI) on the Softphone to be used with a traditional telephone. Each user has a computer with the GUI loaded and a separate telephone. The telephone is used as a traditional telephone, but when the user wants to utilize a call feature, such as forwarding a call, it is done on the GUI interface.

Softphones also have the advantage of integrating well with other applications. For example, the Microsoft Netmeeting application can place calls, but it can also share out an application between users. This would enable two users to hold a conversation and share a Word document they would both be able to see and change. Other applications that can be integrated with the Softphone are Video Teleconferencing and whiteboards, which allow both sides to write on a virtual *chalkboard* and each can see what the other is drawing. A new feature forthcoming to the Web is a Softphone built into a Web site. A user could read a Web page, have a question, and click on a link that would provide audio communication with someone at customer service. This ability to integrate with applications also makes Softphones ideal for call centers. A worker in a call center could have a conversation with a customer while other applications integrated with the Softphone could bring up information on the customer.

Softphones have the ability to call other Softphones on the Internet or place calls to the Public Switched Telephone Network (PSTN). Softphones can contact each other directly over the Internet a couple of ways. One way is to have the calling party *dial* the IP address of the called party and establish a connection. Another way is to register with a service. The service provides either a telephone number or name that is put into a registration server along with the user's IP address when the user registers. The calling

party receives the called party's IP address using the registration service and establishes the call. It should be pointed out that Network Address Translation (NAT) can cause problems for Softphones connecting directly, and this will be covered later in more detail.

Softphones can also be set up to make calls to the PSTN. This is done as part of a VoIP solution that includes a VoIP gateway with connectivity to the PSTN. A popular option in the commercial world is to pay for a service that includes a gateway to the PSTN. When the Softphone connects to the PSTN, it will need to have either a real telephone number or an extension number. The service provides the means of registering the telephone number with the user's IP address.

When a Softphones is loaded onto a laptop computer it has the added advantage of being mobile. It still has the ability to connect peer-to-peer or to its PSTN service provider when its location has changed. One interesting feature of a mobile Softphone is that its telephone number moves with it. For example, if a user is connected with a Softphone to the Internet in Dallas and has a Dallas telephone number, and that user disconnects, goes to Denver and connects to the Internet there, then the user's telephone number will appear to be the number from Dallas. If someone calls the user's Dallas telephone number, the Softphone in Denver will ring. This adds an element of convenience to the Softphone, but also has an effect on 911 service.

911 service is designed to map the user's telephone number to a location. When a user dials 911, the operator is able to query a database and determine location from the user's phone number. When a Softphone has a telephone number assigned and stays in one location, there is no issue with mapping this number in the database to the location. When the Softphone has a phone number and changes location, this can pose a problem. If the user in the previous example were to dial 911 while in Denver, the call would be answered by an operator in Dallas, who would assume that the user was in Dallas. This could have a serious impact on emergency services. A law was passed recently that requires commercial providers of VoIP service (including Softphones) to offer users with a means of providing their location information. This only applies to the PSTN connection services and not to the peer-to-peer services. The U.S. Army system has not provided such a number-to-location Softphone service, and it is recommended that 911 calls be placed using Softphones only as a last resort.

Technical Aspects of a Softphone

This section will discuss how a Softphone works and the protocols it uses for communication. Figure 1 shows a typical VoIP configuration that includes a Softphone and a PSTN gateway. For the peer-to-peer case, the configuration consists only of two or more Softphones connected to an IP network.

The Softphone uses the registration server to register its user name (typically a telephone number or Universal Resource Identifier to IP address mapping). Registering will require some form of authentication, such as a personal identification number or Common Access Card. The IP connection between the Softphone and the registration server should be encrypted to protect authentication information.

The call processor is used for establishing calls, tearing down calls, routing calls, and supporting call features. The Softphone sends and receives call signaling messages from the call processor. The Softphone uses the call signaling messages to establish calls to the other devices, including gateways, IP telephones, and other Softphones.

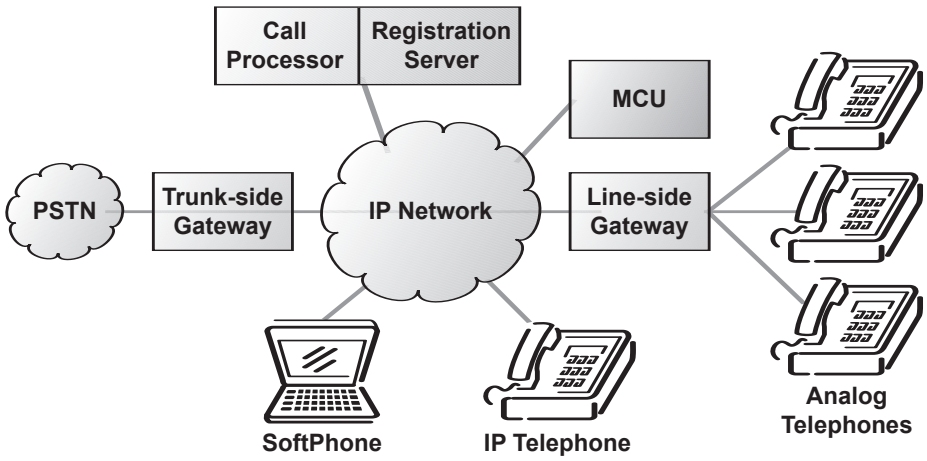
Call signaling messages currently used today include H.323 and Session Initiation Protocol (SIP). The H.323 and SIP protocols are designed to have the intelligence of the VoIP system pushed to the edge, enabling them to call each other without requiring a call processor. The H.323 protocol was developed by the International Telecommunications Union and is the oldest of the protocols and currently the most heavily implemented [1]. The SIP protocol was developed by the Internet Engineering Task Force (IETF) and is considered *lighter* from a code implementation and processor perspective [2]. The SIP protocol is becoming more popular and is expected by many to replace H.323 in the future.

The actual audio traffic flows between the Softphone and other devices in packets that use the Real-time Transfer Protocol (RTP). These packets contain the audio, as well as timing information, sequence numbering, an identifier of the information (compressed voice, video, etc.), and other information. There is also a secure version of RTP available, called Secure RTP, which provides encryption and authentication of the voice traffic. The Real Time Control Protocol supports RTP by conveying information about the quality of the communication, such as jitter and packet loss.

Quality of Service (QoS) is one of the major issues for Softphones. When data traffic experiences packet loss or significant delay, the packets are present and the user observes that the data is taking longer to send or receive. For VoIP traffic, significant packet loss, delay, or jitter (variations in delay) is noticeable to the user. Resending lost packets is not an option, as the conversation will have moved on by the time they are retransmitted. QoS solves these problems by enabling voice packets to get queuing priority over data packets in the IP network.

The Softphone sets QoS and tells the IP network it needs priority in a couple of ways. The first way is by setting the Diffserv bits in the IP header to a higher priority. Layer 3 Ethernet switches will look at these bits and put these packets into a higher priority queue. Another way is to set the Institute for Electrical and Electronics Engineers (IEEE) 802.1P priority bits, which are sent in the IEEE 802.1Q virtual local area network (VLAN) tag. Layer 2 Ethernet switches look at these bits and use them to prioritize the packets. The VLAN tag also has a significant role in logically separating the voice and data traffic, with voice traffic receiving one tag value and data traffic another. Both of these methods of providing QoS work fine in DoD local area networks (LANs), but they are currently not supported in the Non-secure Internet Protocol Router Network or in the commercial Internet. This means Softphones used in a remote fashion will not have any

Figure 1: *Softphone in a Typical VoIP Configuration*



QoS and its traffic will receive no priority.

A problem with QoS and Softphone is the need for QoS within the computer. Computers are generally not set up to provide priority on the internal buses and interfaces to certain applications. There is a means to provide priority to an application within Windows, but this tends to make the system unstable. As a result of the lack of QoS, the latency in the Softphone can be on the order of hundreds of milliseconds, which are at a level where the human ear can begin to detect it and is outside the 60 milliseconds DoD end-to-end VoIP limit.

Another technical issue for Softphones is circumventing the NAT point. When all of the VoIP devices are connected in the same LAN this is not an issue. However, when the calling party is on one side of a NAT point and the called party is on the other, there is a problem. The signaling message the calling party sends to the called party contains the IP address of the calling party. When packets pass through the NAT point this IP address is changed. When the called party attempts to send packets to the IP address in the signaling message, they are dropped (especially if private addressing was used). One current solution is to use the Simple Transversal of User Datagram Protocol through NAT protocol. This protocol works by having the Softphone communicate with a server outside the NAT point. The server is able to see its real IP address and port number and communicate this back to the Softphone. The Softphone then uses this IP address and port number in its signaling messages.

The VoIP devices, including Softphones, have a few tricks for reducing the amount of bandwidth that they utilize. One of them is to use voice compression algorithms. Uncompressed voice (G.711) uses 64 Kilobits per second (Kbps) plus IP network overhead. Other algorithms, such as G.729 (which uses eight Kbps), use less bandwidth. The drawback is that voice quality may be affected. Current DoD policy only allows G.711, but this is expected to change in the future, especially when VoIP goes to tactical units. Another trick is to use Voice Activity Detection (VAD). When a Softphone uses VAD it only sends voice packets when the user is talking. No packets are sent that contain silence. In a typical conversation, only one person is talking at a time so there is audio in one direction and silence in the other. When the silence packets are removed, the amount of bandwidth utilized can be reduced by 50 percent or more. One feature to look for in a Softphone that uses VAD is background noise insertion. Without this, the telephone connection sound is so quiet during periods of silence removal it appears the connection is dead.

An issue for VoIP and Softphones in the future will be Internet Protocol Version 6 (IPV6). Currently, all DoD IP networks are expected to be capable of transitioning to IPV6 by 2008. The computer, the Softphone application, and the operating system will need to support IPV6 for the Softphones to use IPV6. For the Softphone to work with the other VoIP devices, the call processor/registration server, gateways, IP telephones, etc. within its enclave will all need to be running IPV6. The IPV6 protocol may also have an impact on the NAT problem. Due to the large address space of IPV6, it is anticipated that IPV6 will make NAT unnecessary.

Security Issues With Softphones

Security is currently the most difficult issue to overcome with Softphones. The current Defense Information Systems Agency *Security Technical Implementation Guide* (STIG) states, "The use of Softphones is highly discouraged." This is due to a number of items related to the nature of Softphones [3]. This section will go into these, along with the STIG requirements, in more detail.

For VoIP implementations, the security requirements require that the voice and data traffic be separated into networks, either physically or logically. Separate physical networks require separate networking devices, such as switches and routers, for both data and voice networks. Logical separation means that the traffic is separated into logical networks, typically using VLANs. Data devices are connected to data network devices or ports in the data network VLAN and likewise for the voice devices. The major issue with Softphones is they tend to reside on computers having applications requiring access to both data and voice networks. For example, the Softphone computer would have the Softphone application, and then it might have other applications, such as e-mail, Web browsing, etc., that require access to the data network. The following requirement in the STIG addresses this issue:

> (VoIP0150: CAT I) The Information Assurance Officer (IAO) requirement will ensure that if/when approved Softphones are used in the LAN, the following conditions are met:
> - The host computer contains a Network Interface Card (NIC), (commonly called a network adapter) that is 802.1Q (VLAN tagging) and 802.1P (priority tagging) capable.
> - The host computer, NIC, and IP Softphone agent software is configured to use separate 802.1Q VLAN tags for voice and data.
> - Alternatively, dual NICs may be used where voice traffic is routed to one NIC and data traffic is routed to the other. Each NIC is connected to an access switch port residing in the appropriate VLAN.
> - The host computer will be connected to separate voice and data VLANs that have been created expressly for the Softphone host(s). That is to say that the LAN should have a voice VLAN and a data VLAN dedicated to hosts with IP Softphone agents installed. [3]

A couple of issues occur with implementing these requirements. The first is that most computer NIC cards are not able to support VLAN tagging. This would make two NICs in the computer necessary. The second is that some means need to be in place to ensure that the voice traffic only goes to the voice VLAN and the data traffic only goes to the data VLAN. The major security concern here is a hacker coming into a computer on the data network and routing over to the voice network.

The STIG also addresses the case where the Softphone is used in a computer that is accessing the network remotely. The STIG states the following:

> (VoIP0160: CAT I) The IAO will ensure that if/when approved Softphones are used in remote connectivity situations, the following conditions are met:
> - The host computer connects to the "home LAN" through a Virtual Private Network (VPN) connection.
> - The VPN is terminated at the enclave boundary in accordance with the Enclave STIG.
> - The voice and data traffic is routed appropriately to separate voice and data VLANs in the "home LAN."
> - The IP Softphone agent connects to the Call Manager (call processor) on the "home LAN" through the VPN using "home LAN" IP addressing. [3]

Implementing this has the same issues as connecting locally, namely keeping the voice and data traffic separate. This is harder to do remotely, as the remote computer would need to tag the traffic appropriately and put it into a VPN. There would also be QoS and Joint Interoperability Test Center (JITC) cer-

tification issues with using Softphones remotely (this is discussed in the next section).

The STIG also provides the following guidance when Softphones are used in a call center:

> (VoIP0165: CAT I) The IAO will ensure that, if/when approved Softphones are used in a call center situation; the call center network is configured as a separate enclave and secured in accordance with all applicable STIGs.

This means that the call center VoIP traffic must be separated, either physically or logically, from the rest of the IP traffic, in addition to complying with all of the other STIGs.

Due to the security issues with Softphones, the STIG also provides the following guidance to Designated Approving Authorities (DAAs):

> (VoIP0130: CAT I) The IAO will ensure that written DAA approval is obtained prior to the use of any IP Softphone agent software. The IAO will maintain documentation pertaining to such approval for inspection by auditors.
>
> (VoIP0135: CAT I) The IAO will ensure a local IP Softphone policy exists and is being enforced that addresses the following:
> - Prohibits the installation and use of IP Softphone agent software on workstations (fixed or portable) intended for day-to-day use in the user's normal workspace.
> - Prohibits the use of IP Softphone agent software in the user's normal workspace, which has been approved and installed on a portable workstation for the purpose of VoIP communications while traveling.
> - Prohibits the installation and use of IP Softphone agent software clients that are independently configured by end users for personal use or that is provided by commercial Internet Telephony Provider service providers.
> - Requires prior justification and DAA approval for the use of any IP Softphone agent software.
> - Requires that the justification and DAA approval of IP Softphone agent software use is reviewed annually and approval renewed if justified.

JITC Certification Issues

Public law and DoD policy requires that all voice solutions attached to the Defense Switched Network or PSTN obtain interoperability and become Information Assurance certified. For VoIP, the voice solution includes the call processors, registration servers, IP telephones, gateways, and Softphones. While a number of VoIP solutions currently are certified, none of them include a Softphone. This is partly due to difficulty in meeting the security and QoS requirements and partly due to the question of configuration change. The DISA/JITC policy requires a VoIP solution to be recertified if its configuration changes from what was certified. How this would affect Softphones is not yet known. For example, if a computer with a certified Softphone were to change its audio card to a different brand, would it need to be recertified? There is currently no experience with this issue.

There is currently a disconnect in DoD policy regarding the use of Softphones from a remote location, such as a hotel room. The STIG allows it under certain circumstances; whereas, the DISA General Switching Center Requirement (GSCR) (which contains the requirements for interoperability certification) requires end-to-end QoS and a certification of the entire network the VoIP traffic will be traversing [4].

One of the features that a Softphone would need to support to obtain JITC certification for command and control (C2) users is MultiLevel Precedence and Preemption (MLPP). The MLPP allows a caller with a higher precedence to preempt a call of lower precedence. This is typically used when high priority calls need to get through and lines are tied up.

Currently, all JITC certified solutions consist of a LAN for the IP network. The use of VoIP across the wide area network and between services has not been worked out. Currently, if there were a certified configuration that included a Softphone, the Softphone would need to go to a PSTN gateway in order to place a call off of an installation.

Conclusion

While IP Softphones offer several advantages, including mobility and a GUI for call features, it may be a number of years before they are common in DoD telephone systems, with the possible exception of call centers. This is due to a number of reasons. Softphones are still awkward to use due to the lack of a handset. Security and QoS issues will make them difficult to implement and secure. The lack of location awareness when used as a mobile device makes them risky for 911 use. Until JITC certifies a VoIP solution that includes a Softphone, it will be a violation of DoD policy to use one.

Recommendations

The U.S. Army Information Systems Engineering Command (USAISEC) Technology Integration Center (TIC) recommends a continuing effort to examine Softphones, especially in applications such as call centers. Due to the technical complexities of complying with security and performance requirements, we do not recommend any significant move to replace traditional telephones or IP telephones with Softphones at this time.◆

References

1. International Telecommunications Union. "H.323 Visual telephone systems and equipment for local area networks which provide a non-guaranteed quality of service." Nov. 1996.
2. IETF. Request for Comment 3261, Session Initiation Protocol, June 2002.
3. DoD. Voice over IP STIG, V2R1, 29 Aug. 2005.
4. U.S. Department of Defense, Voice Networks Generic Switching Center Requirements (GSCR), Sept. 2004.

Disclaimers

1. Approved for public release; distribution is unlimited.
2. Disclaimer: The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for advertisement.

About the Author

David Premeaux is the USAISEC Critical Skills Expert for Networking Technology for the TIC at Fort Huachuca, Arizona.

U.S. Army Information Systems Engineering Command
Technology Integration Center
ATTN: AMSEL-IE-TI
Fort Huachuca, AZ 85613
Phone: (520) 533-2867
DSN: 821-2867
Fax: (520) 533-5676
E-mail: david.premeaux@us.army.mil