Secure Audio Conferencing with JITC Certified USN

An XOP Networks White Paper

What's Inside

EXECUTIVE SUMMARY

Certain professions have responsibility to manage and control classified information. For example, people involved with battlefield command and control, public safety, financial regulation etc. need means for secure communications on a daily basis. This communication typically occurs using secure telephony equipment. In the United States, National Security Agency (NSA) provides guidelines for the encryption standards that are used to encrypt voice traffic to facilitate secure voice calls.

Several equipment vendors including General Dynamics and L3 Communications provide a variety of secure telephone instruments. These include a range of secure wire-line phones, secure wireless phones, secure PDAs and secure wireline terminals.

A secure wireline terminal supports a FXS port that allows an ordinary analog desktop telephone to be used for making a secure phone call. By placing two such analog terminals at two end points, one can create a secure voice connection over the Public Switched Telephone Network (PSTN) or Defense Switched Network (DSN).

Besides point to point secure calls, frequently there is need to have secure audio conference calls. That requires use of a secure audio conference bridge placed in a trusted environment.

Besides providing audio conferencing a secure conference bridge needs to be compliant with Information Assurance (IA) aspects and meet interoperability criterion such as support for Meet Me conferencing, Preset conferencing, Progressive conferencing and Multi-level Precedence and Preemption (MLPP).

In United States, the Department of Defense (DoD) requires that a piece of equipment be Joint Interoperability Test Command (JITC) certified before it is considered 'secure' enough to be connected to the Defense Switched Network.

This paper describes XOP Networks' JITC certified audio conference bridge's use in conducting secure conference calls in military and secure commercial environments.

WHAT IS ENCRYPTION?

U.S. Government National Security Agency (NSA) sets the standards for cryptographic systems that are used in various US government entities. Encryption protects voice and data by encoding it at the transmitting point and decoding it at the receiving point. An encrypted voice path is immune from any risk of eavesdropping.

The NSA has categorized encryption items into four product types, generally referred to as Type 1 through Type 4. Type 1 encryption is used for classified or sensitive U.S. government information and is used with cryptographic equipment on the Public Switched Telephone Network (PSTN) and Defense Switched Network (DSN). Other encryption types are used for securing communications of lesser sensitivity.

SECURE VOICE COMMUNICATIONS

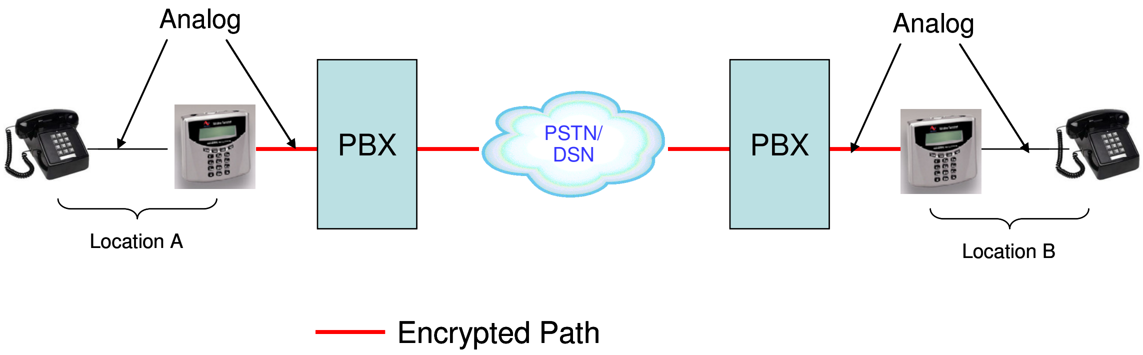

Figure 1: End to end secure voice call on PSTN/DSN

Figure 1 shows an end to end secure voice call between two locations. At each location a General Dynamic's Sectera[2] Wireline Terminal is used. Such terminals provide a FXS interface towards the subscriber's analog phone and a FXO interface towards the PBX. The wireline terminal on location A encrypts the voice path based on NSA provided Type 1 security key. The wireline terminal at location B is set up with a corresponding Type 1 security key. It is therefore correctly able to de-crypt the audio and generate a normal audio signal towards the telephone set. The voice path between the two PBXs may traverse the PSTN or DSN or both.

SECURE AUDIO CONFERENCING

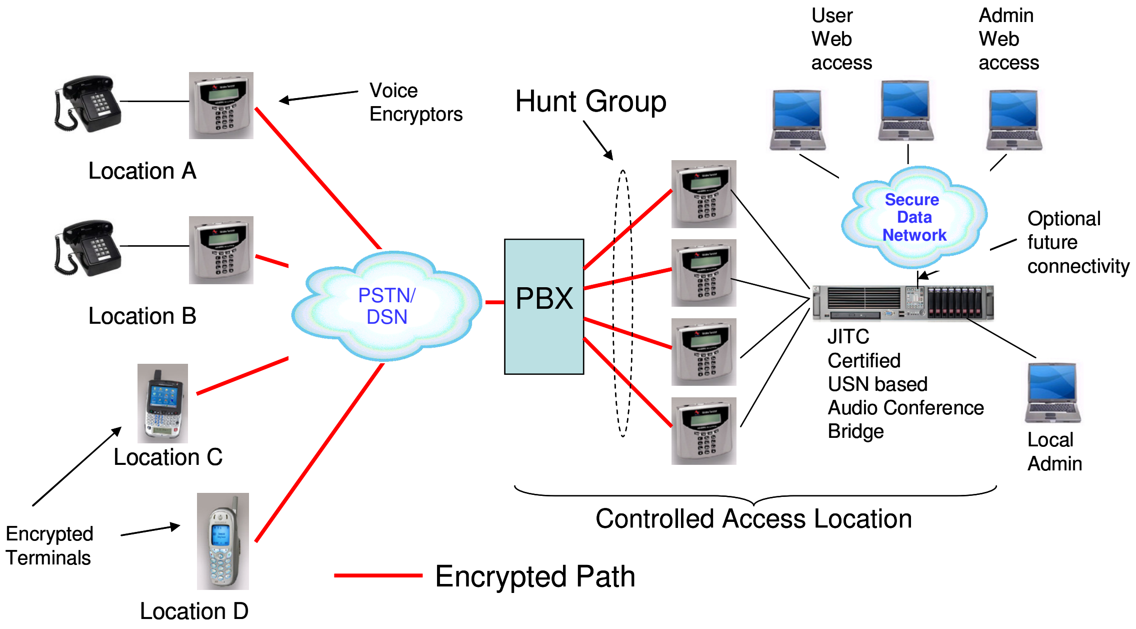

Figure 2: Secure Audio Conferencing on PSTN/DSN

Figure 2 shows a secure audio conferencing network. Multiple people from different locations can dial into a conference bridge over the secure voice network and conduct an audio conference.

Similar to Figure 1, Location A, B, C and D use the wireline terminals or secure wireless phones and secure PDAs to encrypt the voice traffic per the NSA provided Type 1 key. At the other end, multiple wireline terminals are deployed – one for each voice path. Each wireline terminal is equipped with its corresponding Type1 key. The PBX at the far end is set up to support a hunt group. Consequently, all participants need to only dial a common lead phone number. The PBX automatically distributes the incoming calls to different wireline terminals that in turn de-crypt the signal and then present the normal audio signal to the audio conference bridge. The conference bridge in turn places the callers into a conference.

To ensure the security of the conference call, the conference bridge in use is required to be JITC[1] certified. JITC certification implies that a product has gone through rigorous Information Assurance (IA) and interoperability testing at one of DISA sponsored JITC test centers.

INFORMATION ASSURANCE (IA)

For a conference bridge to be considered 'secure' it needs to meet a number of IA[2] requirements. Collectively these requirements make sure that the product a) only does what it is certified for, b)

[1] JITC – Joint Interoperability Test Command

cannot be hacked into, c) its data base cannot be compromised inadvertently or under duress, d) no unnecessary logical or physical ports are open and cannot be opened, e) there are no security vulnerabilities in the operating system, and f) is immune from denial of service attacks.

In addition to the platform security, IA aspects for the system must be configured, audited, and maintained on a continual basis. It is critical to properly configure the secure conference system to prevent un-encrypted or lower classification voice mixed with the desired secure voice. The configuration of the USN along with the wireline encryptors must only allow one classification to be conferenced. In addition a real-time administrator is essential to enforce Operational Security (OPSEC) for not only the local but also for remote sites. All sites must be in secure facilities with measures taken to not have lower classification phones be off-hook within range of the secure phone. Participants must adhere to the OPSEC rules briefed by the administrator.

Before implementing the secure conference system, the organization must also ensure that the system is Certified and Accredited by a process in accordance with FISMA[3] law. This ensures that a local Designated Approving Authority (DAA) has accepted the implementation and usage of the system for the organization.

Following is a list of IA features that the JITC certified USN complies with:

1. Password management:
   - Complex passwords enforced
   - Prevent password reuse for 'n' generations
   - Force password change upon first account access
   - Passwords & PINs encrypted in database
   - Enforce periodic password changes
   - Prevent frequent password changes
   - Conference PINs encrypted in database

2. Intrusion Prevention
   - Lock account after multiple login failures
   - Temporary freeze access from IP address upon multiple login failures
   - Lock unused accounts
   - Prevent multiple logins from the same accounts or bump upon second login
   - Restrict administrator account logins by IP address
   - Disconnect idle sessions
   - Disconnect sessions that are unable to communicate with server for 15 seconds
   - Detect and lock against automated PIN attacks on dial-in lines

3. Alerting and logging
   - Log login attempts, both success & failure
   - Email alerts for important security events

4. Authorization restrictions
   - Administrator accounts optionally allowed access to user accounts
   - Administrator may lock/unlock accounts

[2] IA – Information Assurance - the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. (excerpted from Wikipedia)

[3] FISMA – Federal Information Security Management Act

- Auditor accounts to review system alerts, but not allowed user rights

5. SSL
    - Only modern TLSv1 (SSLv3) connections allowed (No lesser secure SSL version connections allowed)
    - Client certificates required for access
    - Certificate Revocation Lists supported

6. Programming quality control
    - Internal code reviews performed for XSS (Cross site scripting) attacks
    - External third party security review performed

All JITC certified DoD secure bridge deployments will require support for all the items listed above. However, lesser secure and some of the commercial deployments may not require each and every item on the list above. The XOP Networks USN allows majority of the items on the list above to be 'configured'. This allows organizations to be able to configure different levels of 'security' based on their needs.

MULTI-LEVEL PRECEDENCE AND PRE-EMPTION (MLPP)

Besides supporting location and platform security, a secure bridge needs to be able to operate in the DSN. One of the important facets of the DSN is its ability to support Multi-Level Precedence and Pre-emption (MLPP). Precedence involves assigning a priority level to a call. Preemption involves the seizing of resources, which are in use by a call of a lower precedence, by a higher level precedence call in the absence of idle resources. For DSN, five precedence levels have been defined. From lowest to highest, these are ROUTINE, PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE. DISA's 'Unified Capabilities Requirements 2008' has specified special digit sequences that are to be used to invoke calls at different precedence levels.

Now imagine a conference call where on a 16 port conference bridge 16 callers have dialed in with priority level 'FLASH'. Next a person in higher authority calls in. That call will not make it to the conference bridge as all the ports are already in use. If however, the person calls in by pre-pending digit sequence for 'FLASH OVERRIDE' the PBX will recognize the incoming call as having higher priority. It will then insert a special tone in the call leg of the last caller who joined with precedence level FLASH. The bridge will recognize the tone and drop the attendee with priority level FLASH thereby making room for higher priority call to be received. The PBX will then be able to route the call with priority level FLASH OVERRIDE towards the bridge to place the person into the conference.

SUMMARY

In order for a conference bridge to be able to take part in secure conferences, it needs to support all necessary Information Assurance (IA) capabilities as well as meet the interoperability requirements for different types of audio conferences and provide support for MLPP.

This paper describes the features of XOP Networks highly secure USN-16 Audio Conferencing System and how it is used to support secure conference calls in conjunction with third party cryptographic equipment. It also describes how multi-level precedence and pre-emption capability is used in DSN in the context of secure audio conferencing.

Usually IA and interoperability capabilities described in this paper are only available on conference bridges with one or more T1 carriers. Such bridges are expensive, physically large, and difficult to use with secure telephony Customer Premises Equipment that operate with analog interfaces. XOP Networks JITC certified analog 16 port Universal Service Node is a much better alternative as it provides native termination for analog audio signals. Further, it is cost effective, and resilient (industrial grade 2U server with RAID1 mirrored hard disks, redundant power supplies & NICs).

Want to Learn More?

For more information, please visit our Web site http://www.xopnetworks.com or send an email to marketing@xopnetworks.com

XOP Networks, Inc.
5508 West Plano Parkway, Suite B
Plano, TX 75093
Tel: 972-590-0200

About XOP Networks

Headquartered in Plano, Texas at 5508 West Plano Parkway XOP Networks was founded in 2002 and is backed by a seasoned management team. Deployed at multiple Fortune 100 companies, US defense organizations, Mobile operators and CLEC/IOC customers, XOP Networks' products allow customers to improve employee productivity, promote business continuity and generate new revenue streams. Having both legacy and VoIP interfaces, XOP products allow customers to seamlessly transition their value added services from legacy circuit switched networks to VoIP based packet switched networks.

Information in this document is provided in connection with products of XOP Networks, Inc. No license, express or implied, to any intellectual property rights is granted by this document. Except as provided in a signed agreement between you and XOP Networks, Inc. XOP Networks, Inc. assumes no liability whatsoever, and XOP Networks, Inc. disclaims any express or implied warranty, relating to sale and/or use of XOP Networks, Inc. products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any intellectual property right of a third party.

XOP Networks, Inc. may make changes to specifications, product descriptions, and plans at any time, without notice.