SPLY008—April 2004
White Paper

Security Challenges for CALEA in Voice over Packet Networks

Sophia Scoggins, Ph.D.

Voice over Packet Business Unit, Texas Instruments

Introduction

While many broadband VPNs run in tunnel modes, the PacketCable™ security specification defines security for transport modes. This presents new challenges in security for electronic surveillance (also known as Communications Assistance for Law Enforcement Act, or CALEA). Furthermore, the PacketCable Electronic Surveillance Specification defines the security model starting from the Cable Modem Terminal System (CMTS), but many VPNs start with PCs or IP phones that are attached to the Multimedia Terminal Adaptor/Cable Modem (MTA/CM) and tunnel through the CMTS and/or Media Gateway (MG). Only those specific end devices know the security keys and associated parameters. Another concern is secured RTP (SRTP), which provides end-to-end encryption for voice. Not only does encryption/decryption pose a challenge, but in some cases, it is difficult to intercept the message. One example in particular is trying to encrypt/decrypt in the presence of NAT.

In this discussion, Texas Instruments will survey the stated security challenges, present the technical background and expertise to help participants understand the ramifications of these issues, and discuss how the industry might address and resolve these concerns.

CALEA Security Challenges

The goal for security services is to provide privacy, packet integrity, authentication and non-repudiation. A brief definition of each is provided below:

- Privacy: Packets cannot be intercepted.
- Packet Integrity: Packets have not been modified.
- Authentication: The person involved in the communication is who he/she claims to be.
- Non-repudiation: The message sent and received cannot be denied.

In this paper, packets can be data, voice, signals, video, images or any other formats.

CALEA is another term for electronic surveillance. It means that the legal enforcement agent taps into a communication channel to intercept, but not alter, the information. However, the goal of CALEA seems to conflict with the goals of security, and yet there is a need for law enforcement to intercept the VoP packets. Supporting CALEA over

VoP is of particular concern with regard to fighting terrorism. Many terrorist activities took place over the Internet. The U.S. Telecom Industry Association (TIA) promotes CALEA over the Internet and is currently setting standards for CALEA over PSTN and packet networks. Additionally, the U.S. Federal Communications Commission (FCC) intends to regulate support of CALEA over packet networks. All U.S. PSTNs have been supporting CALEA, but support for CALEA in a VoP network has not been fully implemented. The deadline for packet networks to support it was extended to January 30, 2004.

From the logistic point of view, there are still debates about whether packet networks (especially Internet) should be under FCC telecommunications regulation. From the technical perspective, there are still many unresolved issues.

Security Mechanism

The security mechanism starts with establishing a Security Association (SA) between two end-points. Establishment of an SA requires two steps. The first step is to authenticate both end-points. The second step is to exchange security keys for encryption and decryption. After an SA is established, both end-points encrypt and decrypt the packets using the security keys.

Between the two end-points, there are many other devices in the data path that need to be accounted for. If there is at least one device in the path involving SA establishment, then the SA is in a transport mode. The intermediate device is called a Security Gateway (SG). An SG has the security keys to encrypt and decrypt packets from both end-points. The end-points do not encrypt or decrypt the packets. Thus in a transport mode, the SG can support CALEA by providing the security keys needed to the intercept box.

If no other device in the path takes part in SA establishment, then the SA is running in a tunnel mode. In this case, only the two end-points have the keys for encryption and decryption. In such a scenario, law enforcement can still intercept the packets, but they won’t be able to decrypt the packets without the security keys. Therefore, the tunnel mode network cannot support CALEA without new methods.

Call Signaling and CALEA

In a VoP network, the signal packets take different paths from the media paths. The signal packets are transmitted between an end-point and a call server (CS) or proxy server (PS) while the media packets are transmitted between the two end-points. There is typically one SA between an end-point and a CS or PS, and one SA between the two end-points. Each SA is independent of each other. The SA between an end-point and a CS can be established once for all calls or on a per-call basis. However, the SA between an end-point and CS must be established before the SA between two end-points for each call. In order for the SA to prevent an intruder, it must have a limited life-time, which often is a few seconds to a few minutes. When the life-time is expired, an

SA is disconnected. Therefore, the SA must be re-established or renewed before the life-time expires.

Inside the signal packets, the media path is specified in a different protocol, such as Session Description Protocol (SDP). The media path is determined by more than one parameter, such as an application port, RTP/RTCP port and IP port. If the signaling path and the media description protocol cannot be decrypted and interpreted by a law enforcement agent, then law enforcement will not know what path the two end-points took and therefore, they will be unable to intercept and interpret the media packets.

NAT and CALEA

Network Address Translation (NAT) is used in a device to map a set of private IP addresses into one or more public IP addresses. For different applications, such as SIP, SNTP, FTP, etc., there must be an application specific algorithm (ALG) implemented into each application to support NAT.

When the end-point encrypts its packets (which have a private IP address in the header and media description field, such as SDP), the NAT device must have the security key to decrypt the packets and modify the address fields in the header and media description field. Otherwise, it has to turn off the NAT function and assign each device a public IP address. If the end-point does not willingly supply the security key to the NAT device, the NAT device can implement the same security and CALEA mechanism that the CALEA intercept box did to obtain the key. However, the NAT device is, unlike the law enforcement agent, not legally permitted to intercept and interpret the packets.

Law enforcement must have the security key and support of NAT with the ALG in order for the application to intercept the packets from the targeting devices. The challenge is to know what private IP address to map to a given public IP address. Additionally, the interception box must obtain this information from the NAT device.

Different Security and Encryption Protocols

There are many different security protocols (IPSec, SSH, SRTP, etc.). In each security protocol, different encryption/decryption protocols might be used. IPSec can be used with any one of the encryption protocols, be it the Data Encryption Standard (DES), Triple Data Encryption Standard (3DES) and the Advanced Encryption Standard (AES). In each encryption protocol, different key sizes can be used as well. The encryption protocol, key size and other parameters are negotiated during SA establishment. A CALEA interception box must be able to support a variety of security protocols, encryption methods and their associated parameters (such as key sizes).

Hardware vs. Software Encryption

Encryption takes a significant amount of processing time. Some devices use hardware to perform encryption/decryption for efficiency. Since hardware encryption is specific to an encryption protocol, it is difficult for a CALEA interception box to provide hardware encryption for a variety of security and encryption protocols. A CALEA interception box must be equipped with a fast processor to perform encryption when the targeting device might be using hardware for encryption/decryption.

Security Mechanism and CALEA in PacketCable

The “PacketCable Security Specification” PKT-SP-SEC-I109-030728 and “PacketCable Electronic Surveillance Specification” PKT-SP-ESP-I102-030815 specify the security model only in a transport mode. These two specifications do not mention how to handle the tunnel mode.

The “PacketCable Electronic Surveillance Specification” shows the security transport mode is performed by the CMTS rather than the end-points, such as PCs or IP Phone (IPP). However, most of security is implemented on the end-points in the current VoP market, and the majority of them are in the tunnel mode. PacketCable must address this security architecture.

Other security challenges for CALEA listed in the earlier sections are applicable for PacketCable as well.

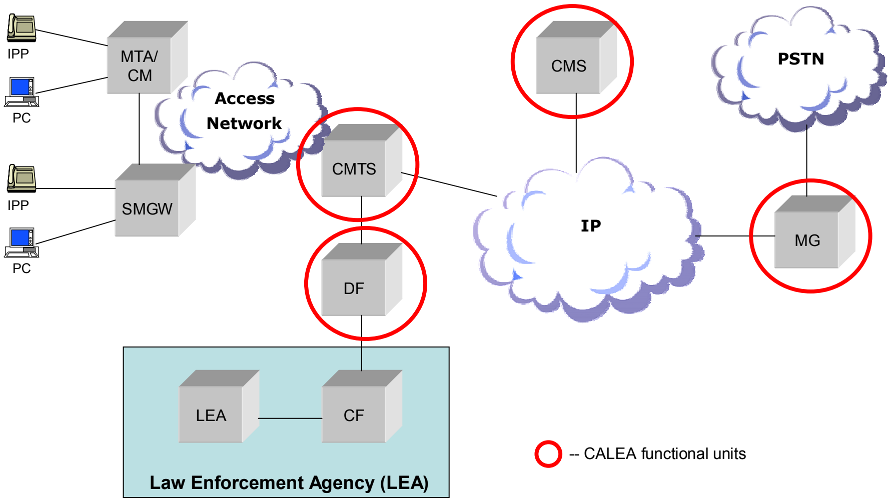

Figure 1: PacketCable™ CALEA Model

Possible Solutions for Security Challenges in CALEA

In order to solve the security issues for CALEA, a CALEA interception box must intercept packets from the targeting devices during an early stage of the SA establishment in order to obtain the security keys and other security parameters needed. Where interception occurs should be dependent on many factors: NAT, Dynamic Host Configuration Protocol (DHCP), VPN/security end-point, etc.

If the VPN/security end-point is a PC or IPP, it will matter how the end-point obtains the IP address. If the end-point IP address is obtained through Dynamic Host Configuration

Protocol (DHCP), then there is no NAT and interception can be performed in any device. However, the packets from the same device can take different routes, therefore, it is better to intercept the packets before a different path can be taken, usually from CMTS to the Internet.

When NAT is present, the best place to intercept is where the NAT function resides. Often that is the MTA, instead of the CMTS, as defined in the “PacketCable Electronic Surveillance specification.” However, it is possible for NAT to be on a CMTS. The NAT unit maps the private IP address to a public IP address and vice versa, so the packets should be intercepted on the LAN site before NAT is performed. Otherwise, the interception box needs to do packet filtering in a stream of mixed messages with the same public IP address. Also the NAT unit has the application algorithm (ALG) to handle the application specific translation function. For example, an initial incoming SIP call only has a public IP address. How does the NAT unit know which private IP address to map to? It has to run SIP ALG, which uses the user ID in the SIP message, such as alice@wonderlane.com or the CallerID in the header, to find Alice’s private IP address. Note that Alice must already register with the NAT device with her private IP address and her name and/or CallerID.

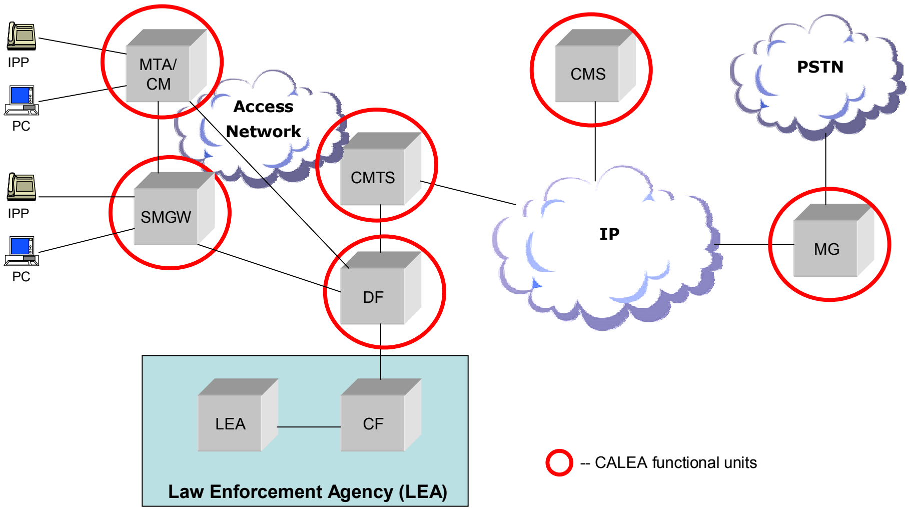

Figure 2: Proposed CALEA Model

Once the CALEA interception box is able to intercept the targeting device’s packets, it should try to obtain the SA establishment messages. If the security mechanism is not based on the standard protocols, then the law enforcement agent will have a difficult time interpreting the security messages and subsequently decrypting the SA messages and media packets. If the security messages are based on the standard protocols, then from the SA establishment messages, the CALEA interception box should be able to figure out the key, key size and encryption method.

The U.S. TIA has published a set of message formats for CALEA in PSTN. Since the Internet has a completely different architecture, set of protocols, message formats and call flows, TIA must publish a new set of specifications for CALEA over Internet. The PacketCable specifications can be a subset, and in fact, they are mentioned by TIA. However, modifications to the PacketCable Security Specification and PacketCable Electronic Surveillance have to be made in order to support many VoP security requirements. Also, a VoP security solution that is not Cable based should be specified outside the PacketCable specifications, although the principle may be the same.

Conclusions

Security has many new challenges for CALEA in the VoP networks. The major challenges are how to intercept the packets from/to the targeting devices and how to interpret and encrypt/decrypt them. This paper provides some solutions to the security issues in the VoP networks. There are still unresolved issues that are challenging the VoP vendors, service providers and law enforcement. That resolution will be the next step needed to move the industry forward.

To learn more about how Texas Instruments has addressed these challenges, go to: www.ti.com/voip

Important Notice: The products and services of Texas Instruments Incorporated and its subsidiaries described herein are sold subject to TI's standard terms and conditions of sale. Customers are advised to obtain the most current and complete information about TI products and services before placing orders. TI assumes no liability for applications assistance, customer's applications or product designs, software performance, or infringement of patents. The publication of information regarding any other company's products or services does not constitute TI's approval, warranty or endorsement thereof.