

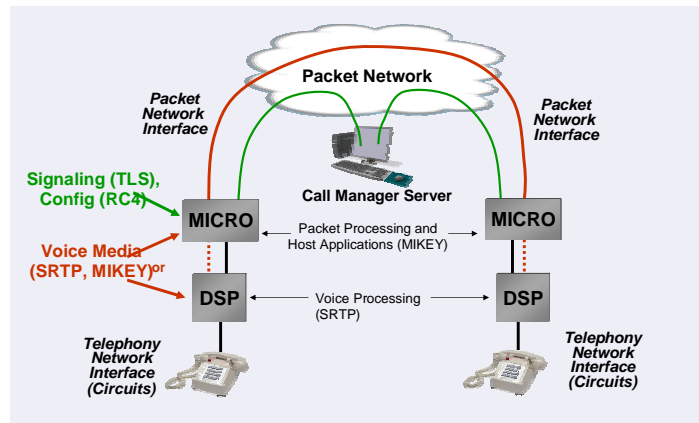
**Building Residential VoIP Gateways: A Tutorial**  
**Part Four: VoIP Security Implementation**  
*by Debbie Greenstreet and Sophia Scoggins PhD*  
*VoIP Business Unit*  
*Texas Instruments Incorporated*

## Demand For VoIP Security

Customer Premises Equipment (CPE) -- IP phones and media gateways with VoIP capability -- is vulnerable to many Internet attacks, such as malformed frames or packet floods, both of which lead to Denial of Service attacks (DoS). Since DoS consumes significant equipment CPU processing cycles, this results in impaired voice quality in a real-time call processing scenario. VoIP CPE is also open for intrusion, monitoring, and alteration of the packet contents and destination addresses, and identity fraud in a non-managed environment. Therefore, VoIP security is a mission-critical element for the deployment of VoIP products. This article, the fourth in a series on CPE voice gateways addresses the implementation of security in such residential voice gateways.

## Areas For VoIP Security

Fig. 1 shows a VoIP CPE gateway architecture consisting of two major components: Micro (voice application) and DSP. These can be inside an IP phone or in a separate box, such as a media gateway.

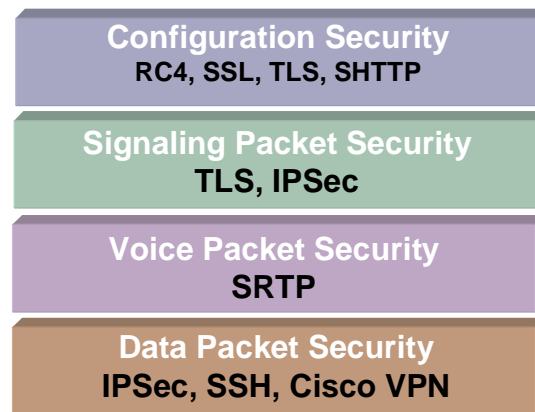


**Fig. 1: CPE Packet Telephony Security**

The voice stream is packetized using IETF RFC1889 Real-Time Protocol (RTP), and as shown (using red dashes) is processed by the DSP using a voice encryption protocol and key exchange method. The encryption can be done by either the DSP or Micro. The key exchange method for voice encryption is between two Micros, relayed through the Call Manager/Server using IETF RFC 2327 Session Description Protocol (SDP).

The call processing signals (shown in green) are communicated between a Micro and a Call Manager/Server. In some situations, after a few messages between Micro and Call Manager/Server, the call processing messages may not go through the Call Manager/Server any more, but directly between two Micros. The common call processing protocols are Session Initiation Protocol (SIP), H.323, and Media Gateway Control Protocol (MGCP).

In the architecture above, VoIP security can be divided into four areas: configuration, call control, voice streams, and data streams (see Fig. 2). Configuration is performed at the equipment startup stage with a configuration server. After configuration, the equipment may start data stream traffic. The data stream is independent to the call control or voice stream. When the equipment detects an off-hook signal, or incoming message, it starts the call control process with a Call Manager/Server. Once a call is established, the voice streams can be transmitted between two CPE gateways.



**Each Area Needs:**

- Configuration
- Authentication
- key exchange
- Encryption

**Fig. 2: VoIP Security Area**

### **VoIP Security Components**

Although the four areas have different security mechanisms, the basic security components are the same. The major security goals are authorization, authentication, integrity, privacy, and non-repudiation. In order to achieve these goals, the security mechanism often consists of configuration, authentication, key exchange, and encryption. Configuration is the initial stage to authorize the device in the network. Authentication may take place during configuration or at a later stage. Encryption is the mechanism for achieving integrity and privacy and requires a security key that can be statically assigned, or dynamically obtained, through key exchange. Non-repudiation can be achieved by a signature from the sender and/or sender and receiver reports, such as using the sender and receiver reports with the IETF RFC 1889 Real-Time Control Protocol (RTCP).

## **VoIP Security Performance Measurement**

The major VoIP security performance measurement consists of the level of security, encryption delay, message delay, and processing power. Usually, the smaller the key size is, the less security, encryption delay, and processing power it has. A security key size less than 56 bit can be broken in three hours with sophisticated computers. 128 bit is the desirable security key size. A security key of size 192 bit consumes too much computation power. Although it does provide a high level of security, is not desirable for real-time call processing. The complexity of the security algorithm also impacts the level of security, encryption delay, and processing power. The message delay occurs during the authentication, key exchange, and call control process. In a real-time call processing application, delay can cause significant voice degradation and interfere with call establishment. Therefore, delays should be minimized. Any security mechanism introducing more than one second of delay is not suitable for real-time VoIP applications.

## **Encryption Protocols**

The following summarizes common encryption protocols used in CPE applications, and their tradeoffs:

### **(Triple) Data Encryption Standard (DES/3DES)**

The pioneers of voice encryption used IPsec with Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES). DES, 3DES, and AES are all endorsed by the US National Institute of Science and Technologies (NIST). DES uses a 56-bit key to encrypt blocks of 64-bit plain text. The key length is not long enough to provide security. 3DES uses 192-bit key. 3DES provides more security, but the computation time is too long so that it is not suitable for real-time voice processing.

### **Advanced Encryption Standard (AES)**

AES uses a 128-bit key. AES provides much higher security level than DES, while the computational power is 3 to 10 times less than 3DES. AES is an ideal encryption protocol for voice and signaling systems.

### **Rivest Cipher (RC4)**

RC4 was invented by Ronald Rivest at Rivest, Shamir, and Adelman (RSA). RC4 is a shared key stream cipher algorithm. The algorithm is used identically for encryption and decryption as the data stream is merged with the generated key sequence. The algorithm is serial as it requires successive exchanges of state entries based on the key sequence. Hence implementations can be very computationally intensive. RC4 is still the most common encryption method for encrypting configuration files.

### **Voice Encryption Protocol -- Secure RTP (SRTP)**

SRTP is IETF RFC3711 [4]. SRTP provides a framework for encryption and message authentication of RTP and RTCP streams. SRTP adds two parts to the RTP header: authentication and encryption. Authentication is optional for SRTP, while required for SRTCP. Encryption is required for SRTP. Only AES encryption scheme is supported in SRTP.

## **Key Exchange Methods**

The common key exchange methods are symmetric, public, hybrid, and Diffie-Hellman (DH).

### **Symmetric Key**

This scheme uses only one key for encryption and decryption. Both ends of a phone call use the same key. The key can be generated by one end and distributed to the other end, or it can be assigned by a server to all parties in a domain. This method is not scalable, but it is the simplest method.

### **Public Key**

This method uses two keys. The remote end's public key is used to encrypt the outgoing message. The private key is used to decrypt receiving message. This method is scalable, but needs 100 to 1000 times more computational power.

### **Hybrid Key**

This method uses public key to encrypt the symmetric key. Once the symmetric key is received, it is used to decrypt the messages. This is the most efficient method and is used in many applications such as MS Outlook, Netscape Communicator, and secured data storage.

### **Diffie-Hellman Keys (DH)**

Two interacting endpoints must agree on a password in order for the call to go through. This is called the Diffie-Hellman Scheme. One of the two CPE devices will pick a random number of base 2 and the other device has to match that number. There are five DH algorithms, or groups. The higher the group is, the more complex the algorithms are: which leads to a higher security level and more intensive computations. Due to the computation power required, the DH method is less used in voice applications.

IETF RFC 2401 Internet Security (IPSec) provides the security framework for key exchange, but refers to International Security Association (ISA) IETF RFC 2409 Internet Key Exchange (IKE) protocol for key exchange. IKE uses the DH key exchange method. IPSec has been very used in the pioneer voice applications.

An alternative to IPSec is to use the Multimedia Internet Keying (MIKEY) for key exchange for SRTP. MIKEY is currently an IETF draft, but is in the process of becoming a RFC. MIKEY requires the supporting of both public key and symmetric key methods, while Diffie-Hellman (DH) is optional. Key exchange method will be carried in a SIP SDP attribute field. This field can be used for any key exchange method for media stream. MIKEY has limited implementations, but it is gaining industry attention.

## **Security Association (SA)**

A Security Association (SA) is a virtual connection between two or more devices for the purpose of security. During the SA establishment stage, the devices perform authentication and exchange tokens or certificates, which are used to create encryption keys. Once the SA is established, some security mechanism will perform key exchange. In Fig. 1, there is at least one SA between each CPE and a Call Manager/Server. If there is a separate Configuration Server, then there will be a SA between each CPE and the Configuration Server. There is also a SA between each pair of CPEs.

SA establishment is often time consuming, mainly due to exchanging messages. Therefore, SA establishment is recommended at the configuration stage between CPE and server. If the SA is expired, and requires renewal, it should be done when the devices are not in the call processing stage.

In addition to the SA between a CPE and a server, it is required to have the SA established between two or more CPEs. Pre-establishing a SA among all CPEs is not only unlikely, but also creates a meshed connection that will be difficult to manage in terms of memory and CPU processing power. Therefore, it is recommended to establish the SA among the CPEs on an as-needed basis. Since voice connections are often short, the SA can be terminated before it expires. It may be possible to reuse a previously established SA between two CPEs, if there is one. This can reduce some steps in the SA establishment stage.

## **VoIP Configuration Security**

At start up, the customer premise equipment provides a pre-installed secure ID to the network configuration server. The configuration server responds with an authentication key. The CPE uses the authentication key to start the authentication process. Once the CPE gateway is authenticated, the configuration server provides an encryption key. From that point on the encryption key is used to encrypt all the messages between the CPE and the configuration server. The most common protocols used in this process are Rivest Cipher (RC4), Session Security Layer (SSL), Transport Layer Security (TLS), and Secure Hyper Text Transfer Protocol (SHTTP).

SA establishment is part of the configuration process. Configuration is not unique to voice applications. However, while a data network may not require configuration at all, configuration for voice application is a must.

RC4 is a shared/symmetric key stream cipher algorithm. The key size is from 54 to 128 bit. The algorithm is serial as it requires successive exchanges of state entries based on the key sequence. Hence implementations can be very computationally intensive.

## **Security In VoIP Call Control Process**

The VoIP call control or signaling system may use the authentication/encryption key generated at the configuration stage or use key exchange methods to obtain the encryption key.

## **Internet Security (IPSec)**

The cable industry has been using IPSec using Kerberos key exchange method for the call control message in Media Gateway Control Protocol (MGCP). IPSec can be implemented under the IP stack and above the network driver, called bump-in-the-stack (BITS). An alternative is to implement IPSec away from the host, in the gateway, or router, or firewall. This method is called bump-in-the-wire (BITW). If IPSec is implemented in the IP stack, it can be used for all the applications in that device and the applications may not even notice it is in place. This is often implemented on a PC to set up a VPN to a Corporate Local Area Network (COLAN). If IPSec is implemented in a gateway, router or firewall, then many devices have to share the IPSec security association. This is often implemented between two office branches.

## **Transport Layer Security (TLS)**

TLS 1.0 is derived from Session Security Layer (SSL) v3.0, but it is not backwards compatible with SSL. The SIP community first recommended using IPSec, but then changed to TLS. The old SIP spec was based on UDP, which required IPSec to provide more reliability, while the latest SIP specification is based on TCP. TCP provides sufficient reliability and therefore TLS over TCP does not cause reliability concerns. The TLS equips with key exchange function. Since TLS is above TCP, it often provides security association between two applications on two devices.

IPsec is used for long and reliable connection, while TLS is more for web-based applications with short and bursty traffic. With TLS, even after the SA is terminated, the application may reuse the previous SA information and re-establish a connection, which shortens the SA establishment time. IPSec does not allow reuse of the previous SA information to establish a new SA connection.

## **Security In Voice Processing**

As stated earlier, the pioneers of voice encryption used IPSec with DES, 3DES, and AES. The latest standard voice encryption standard is the IETF RFC3711 Secure Real-Time Transport Protocol (SRTP) with AES. SRTP does not define what key exchange protocol to use. The industry trend is to use MIKEY for key exchange for SRTP.

## Denial of Services (DoS)

DoS attacks are common in the Internet, and approaches to handling these attacks are not unique to VoIP. Highlighted below are some examples of DoS attacks and actions. There are public websites, such as CERT advisory board (<http://www.cert.org/advisories/CA-1996-21.html> or <http://www.cert.org/advisories/CA-1997-28.html>) which offer solutions to DoS attacks, as well as commercial products, which address this problem.

S.No	Attack Name	Scenario	Counter action
1	ICMP flood	High incoming rate of ICMP packets	Software restricts the number of packets to be received in time slot, if packet exceeds in defined time slot, log and drop the packets.
2	Teardrop	Not properly handling overlapping IP fragments.	Check IP fragments. Drop packets if they are not properly formatted.
3	Land	Source and destination IP address of packet is the same	RFC2267 -- Software input filter (for external traffic) does not allow packets through if the address is from internal. Software output filter does not allow packets through, if the source address is not from internal. Compare Source with destination IP address of packet, if same, log and drop the packet.
4	Ping to Death	High incoming rate of Ping packets	Restricts the number of ping packets to be received in time slot, if packet exceeds in defined time slot, log and drop the packets.
5	IP spoof, SYN flood	High rate of TCP SYN packets	RFC2267 -- Software input filter (for external traffic) does not allow packets through if the address is from internal. Software output filter does not allow packets through, if the source address is not from internal.

## Open Issues

Although the industry has provided many solutions for VoIP security, there are still issues to be resolved. Most of the challenges come from managing the security keys. There is still no consensus on how to distribute the keys, update the keys, store the keys, and prevent them from being stolen. Meanwhile, the FCC has issued requirements for VoIP to comply with the Communications Assistance for Law Enforcement Act (CALEA). That means that VoIP service providers must provide a way for law enforcement agents to tap into the VoIP lines, or risk facing big fines.

## Conclusion

Despite some of the challenges outlined, VoIP security is achievable now. With security in place, VoIP applications are expected to proliferate in the years to come.

## About The Authors

Debbie Greenstreet is the Director of Product Management for CPE VoIP Gateways at Texas Instruments. She is responsible for product direction of CPE voice products, including VoCable, VoDSL and SME solutions. She has been working in the VoIP industry since its infancy, and has authored many articles and presented at numerous conferences on the subject. Ms. Greenstreet has over 20 years experience in the networking and telecommunications field in hardware and software design, as well as product management, at companies such as Hyundai and Raytheon. She holds a BSEE from the University of Virginia and has done graduate work in Computer Engineering at George Mason University. She can be reached at [dgreenstreet@ti.com](mailto:dgreenstreet@ti.com)

Sophia Scoggins joined Texas Instruments in 2003 as a software system engineer. Earlier she had held many different positions (Director of Software Architecture, Sr. Product Manager, Architect, Sr. Software Engineer, and Research Assistant Professor) at companies, such as Nortel Networks, Siemens Efficient Networks, Coppercom, UMKC, etc. She holds a PhD in IE from TTU, is a PhD candidate and holds a MS degree in Telecommunications, Networking, and CS from UMKC, an MBA degree from ENMU, and a B Law from Taiwan. She holds two international patents and has published one textbook *Open Internetworking with OSI* and 45 conference, seminar, and journal papers. She can be reached at [sscoggins@ti.com](mailto:sscoggins@ti.com)

## References

- For more information on Texas Instruments, and its VoIP solutions, visit [www.ti.com/voip](http://www.ti.com/voip)
- Steve Burett & Stephen Paine, "RSA Security's Official Guide to Cryptography", McGraw-Hill, 2001.
- Peter Thorsteinso, G. Ganesh, ".NET Security and Cryptography", Prentice-Hall, 2004.
- "PacketCable Security Specificatio", PKT-SP-SEC-II11-040730, July 30, 2004.
- J. Rosenberg & H. Schulzrinne, IETF RFC 3581- "An Extension to the Session Initiation Protocol (SIP) for symmetric Response Routing", Aug. 2003.
- Mark Baugher, Ran Canetti, Lakshminath Dondeti, and Frederik Lindholm, IETF-DRAFT draft-ietf-msec-gkmarch-07.txt, "Group Key Management Architecture", Jan. 2003.
- Kavita Jain & John Albert, IETF draft-jain-sipping-srtp-00.txt, "Using SRTP with SIP", Feb. 2004.
- C. Jennings, IETF draft-jennings-sip-sec-flows-01.txt, "Example Call Flows Using SIP Security Mechanisms", Feb. 14, 2004.
- J. Arkko, et. al, IETF draft-ietf-msec-mikey-08.txt, "MIKEY: Multimedia Internet KEYing", December, 2003.
- T. Dierks & C. Allen, IETF RFC 2246, "The TLS Protocol version 1.0", Jan. 1999.

McGrew Baugher, et. al, IETF RFC 3711, "The Secure Real-Time Transport Protocol (SRTP)", March, 2004.

D. Maughan, et. al, IETF RFC 2408, "Internet Security Association and Key Management Protocol (ISAKMP)", Nov. 1998.

D. Harkins & D. Darrel, IETF RFC 2409, "Internet Key Exchange (IKE)", Nov. 1998.

<http://www.webtorials.com/main/eduweb/security/tutorial/index.shtml>

<http://www.cert.org/advisories/CA-1996-21.html>

<http://www.cert.org/advisories/CA-1997-28.html>

