CALEA Compliant Secure Voice over IP System

C. Goodrich, N. Thanthry, and R. Pendse

Department of Electrical and Computer Engineering, College of Engineering

1. Introduction

Voice over IP is one of the fastest growing internet based application in today’s networking world. As more and more enterprises are moving towards IP based voice network, the security has become an important issue. The voice traffic is exposed to the similar kind of threats as the normal data traffic. However with voice traffic, the issues are more complicated than the normal data traffic. While it is important to protect the voice packets from spoofing and eaves dropping, it is equally important that the law enforcement agencies have access to these voice packets. With the recent terrorist attacks and increased threat to national security, the law enforcement agencies are requesting permission to tap every voice call and screen them for information pertaining to national security. With the deployment of security mechanisms like encryption, it will become harder for the law enforcement agencies to decipher the information hidden in these IP packets related to voice calls. Hence it is important that, the security mechanism used in these voice calls need to be standardized. This would provide the law enforcement agencies an easier access to the information during crisis situations. In this paper, the authors propose a new security mechanism that will help the law enforcement agencies in gathering information pertaining to national safety.

2. CALEA Complaint Voice over IP Security System:

The proposed CALEA compliant Voice over IP security system is a modified version of the current security system being used for voice communication over the internet. In its current form, before establishing a voice session, the voice gateways exchange encryption keys being used for the session. The source gateway (gateway at the caller’s side) sends a message to the destination voice gateway requesting an encryption key. The message will also contain the key being used by the source gateway. In response, the destination gateway will generate its own key for the session and includes it in the reply message to the source gateway. The key exchange mechanism is explained in Figure 1. All future communication initiated by the sender gateway to the destination gateway will be encrypted using the sender’s key while all the communication originated at the destination gateway to the source gateway will be encrypted using the destination gateway’s encryption key.

While the above system works well as far as protecting the integrity and confidentiality of the voice conversation is concerned, it is not a good solution as far as law enforcement/national safety is concerned. With the encryption enabled, it is extremely difficult to gather information from the encrypted datagrams in real-time. This issue becomes even more important in the case of voice communication, as, most of the times delayed information might not help in preventing the possible security/safety threats.

The proposed security system considers involving the service provider gateways in the key exchange process. This requires the introduction of two new message formats and an additional field in the IP datagram. The proposed protocol operation is as follows:

1. The source and destination gateway exchange the encryption key’s for the voice session.
2. Once the key exchange process is complete, both voice gateways send a message (key_update) to their corresponding service provider gateway. The key_update message contains information related to the encryption keys being used by both the source and destination voice gateways.
3. The service provider gateway accepts the key_update message, and updates its session_key table with the new information. Then it forms a session_ID for the communication between the two voice gateways. This session_ID will be included in the reply (key_update_reply) from the service provider gateway to the source/destination gateway.
4. All future communication between the source and destination gateway will be encrypted using the respective keys. At the same time, all the IP datagrams originated
from either gateway will contain the session_ID information in the optional IP header part of the IP datagram.

Figure 2 describes the working of the proposed security mechanism.

![Figure 2: Working of the proposed security mechanism](image)

One of the major challenges for the proposed security system is the identification of the voice packets. Once encrypted, every IP datagram look similar for the intermediate nodes (including the service provider gateways). Hence, the authors propose either of the two approaches described below to address the packet identification issue.

1. **Source based approach:** In this approach, the authors propose that every service provider gateway build a database with information about the voice gateways in their domain. This will help them in identifying the voice communication. All the IP datagrams originated from the voice gateways can be considered as datagrams pertaining to voice communication. If any IP datagram originated from the voice gateway is encrypted and does not contain a valid session_ID, the service provider gateway can drop the packet forcing the voice gateway to reestablish the communication and including the service provider gateway in the loop.

2. **Global encryption approach:** In this approach, the authors suggest that every node using encryption needs to inform the service provider gateway about the key being used for communication and obtain a session ID for the communication. This would help the law enforcement agencies in gathering all kinds of information in a timely manner. However, one of the major concerns with this approach is its scalability. This approach requires the service provider gateway to keep track of all the communication sessions that are going through it and are encrypted. This requires higher memory and CPU power at the service provider gateways. However, looking at the advantages in terms of national safety, the cost could be overlooked.

As compared to the traditional security mechanism, the proposed mechanism has higher overhead in terms of additional message formats and additional information in every IP datagram. However, the proposed system reduces the time involved in decrypting the information hidden in the communication during unusual circumstances.

### 3. References

1. D E Denning, And W E Baugh, Jr, “Hiding Crime In Cyberspace,” Cybercrime, B. D. Loader And D. Thomas (Eds.), Routledge, 1999
3. “Communications Assistance For Law Enforcement Act and Broadband Access And Services,” Fcc 04-187, Notice Of Proposed Rulemaking And Declaratory Ruling, August 9, 2004
5. Communications Assistance For Law Enforcement Act, H.R.4922, One Hundred Third Congress Of The United States Of America