Secure Mobile VoIP

Alex Talevski, Elizabeth Chang and Tharam Dillon
DEBI Institute, Curtin University, GPO Box U1987, Perth, WA, 6845, Australia
e-mail : (alex.talevski, elizabeth.chang, tharam.dillon)@cbs.curtin.edu.au

Abstract

The rapid growth of computing, the Internet and telecommunications systems have resulted in a broad range of ways to communicate and access information.

Voice over Internet Protocol (VoIP) is a Computer Telephony Integration (CTI) solution that transports voice traffic over a data network as an alternative to the Plain Old Telephone Service (POTS). VoIP products promise converged telecommunications and data services that are cheaper, more versatile and provide higher voice quality as compared to traditional offerings.

Although VoIP products are rapidly gaining market share with home users, uptake in the enterprise market has remained slow as a result of security and mobility concerns. This paper addresses the issues surrounding VoIP security and mobility through the integration of robust security features into a lightweight VoIP protocol that is tailored for mobile devices. A theoretical approach is realized with the development of a software prototype whose security and mobility properties are analyzed.

1. Introduction

Telephone and computer systems are two technologies that impact many aspects of our daily lives. These technologies drive the world's economy and are central to the operation of virtually every enterprise. However, the functionality of the telephone system has not improved in the last 100 years. Although handsets have become more sophisticated, and operators are no longer required to connect calls in telephone exchanges, the basic operation remains the same. Conversely, computing has grown significantly throughout its lifespan.

Computer Telephony Integration (CTI) incorporates computers and telephony systems [1]. Computer features such as data handling, media processing and graphical user interface are combined with telephone features such as call handling and routing. Currently CTI is predominantly used to drive software-based Private Automatic Branch eXchanges (PABX). However, CTI is heading toward the convergence of voice and data services over a data network. Voice over Internet Protocol (VoIP) is a CTI solution that is commonly used as an alternative to the Plain Old Telephone Service (POTS). Generally, VoIP refers to the transport of voice traffic over a packet-switched data network where hardware and software act as an Internet transmission medium for telephone calls. Packet switched networks route data packets on a hop-by-hop basis. These networks have the following properties:

- Telephone calls can be transmitted with little or no loss in functionality, reliability, or voice quality.
- Reduced telephony and infrastructure costs.
- Useful when there is limited or financially prohibitive access to alternative telephony networks.
- Increased line efficiency due to single lines being dynamically shared by many packets over time. By contrast, circuit switched networks rely on synchronous time division multiplexing where links are often idle.
- Packet-switched networks can perform data-rate conversions. Two nodes utilizing different data rates can exchange data because each can connect at its optimal data rate.
- When traffic becomes heavy on a circuit switched network, additional calls are blocked. On a packet-switched network, response time slows down gradually without immediate service interruption.
- Priorities can be used on packet-switched networks to give precedence to more important traffic.
- New levels of integration are possible for voice and a variety of data services.

VoIP has rapidly emerged as a popular alternative to existing telephony networks. Many sources [2, 3, 4, 5] indicate that VoIP will grow from approximately

0-7695-3038-9/07 $25.00 © 2007 IEEE
DOI 10.1109/ICCIT.2007.425

100,000 US households in 2004 to more than 12 million by 2009. Although VoIP products are rapidly gaining market share with home users who have reaped the benefits, uptake in the enterprise market has remained slow as a result of security and mobility concerns.

1.1 VoIP security

Corporate customers are generally more security conscious. They require that potential new technologies are proven not to be a security risk. Most current VoIP offerings do not offer a practical security solution. However, an important aspect behind the corporate success of the VoIP technology is security. As VoIP technology becomes more heavily integrated into the workplace, so too do the opportunities for hackers. Voice information during a VoIP call is generally routed unsecured through data packets on a public network. There is software that can capture, reconstruct and/or modify these sensitive voice conversations. Standard VoIP implementations offer numerous undesirable opportunities for creative hackers [6]:

- Eavesdropping and recording phone calls
- Tracking calls
- Stealing confidential information
- Modifying phone calls
- Making free phone calls
- Pranks / Practical jokes
- Board room bugging
- Sending spam (voice or email)

There are currently several competing VoIP standards in the market (such as SIP [7], IAX [8] and H.323 [9]), and very few practical security standards available to secure them. Furthermore, many enterprises that have adopted VoIP technology have not been able to effectively secure these solutions as a result of multi-vendor incompatibilities [10]. A standard installation of VoIP using SIP, H.323 or IAX protocols does not provide any kind of security for voice traffic. To alleviate this, it is necessary to add some form of protection, such as encryption, at the transport or network layer. To facilitate secure mobile VoIP, security must be addressed at each layer of the network. We must secure the VoIP devices, segregate the network, encrypt the traffic and introduce intrusion detection systems [6]. By incorporating security at each level of the network, it makes successful attacks much more difficult. Simply breaking one type of security will not expose the entire network; it would require multiple levels of protection to be compromised.

To allow multi-vendor solutions to interoperate it is essential that such solutions are integrated into the VoIP standard. Since VoIP protocols already use negotiation options to determine call parameters (such as codec), it is reasonable to suggest that security parameters could be agreed on in a similar fashion.

1.2 Mobility

People are no longer desk-bound. Enterprises have to consider the growing population of mobile users that would benefit from the next generation of Information Technology and Telecommunication (IT&T) services. As more sophisticated wireless devices emerge, the demand for mobile two-way communication will rise dramatically. Flexible, rich access to telecommunications services is crucial in order to achieve optimum performance. New technologies offer innovative features that result in better ways of doing business. It is essential to be

To offer these VoIP services on mobile devices, it is necessary to consider the restrictions imposed by this platform. Mobile devices typically have limited processing power, memory, storage, network connectivity and performance and poor battery life. While this may not compete with desktop machines, the amount of processing power and other PDA features have improved rapidly and could reasonably be expected to continue to advance.

1.3 Existing solutions

There are various existing options to secure VoIP traffic. Unfortunately, no solutions are offered that provide suitable security characteristics while running on a mobile device. The following gives a brief summary of the existing solutions in the areas surrounding secure VoIP communication.

1.3.1 Secure real-time transport protocol. The Secure Real-time Transport Protocol (SRTP) was developed for securing the media stream of VoIP protocols (such as H323 and SIP) that rely on the Real-time Transport Protocol (RTP). However, the protocol is not designed for mobile use. Solutions surrounding the RTP protocol suffer NAT traversal problems which create serious issues for mobile users.

1.3.2 IP security / Virtual private networks. Another option to secure media streams is to pass all traffic through an existing VPN. This approach has several problems. The most obvious is that a Security

Association must exist between the originating and destination networks.

This paper details the research and development of a secure VoIP client that is geared toward mobile devices. In particular, the key outcomes are the utilisation of a lightweight VoIP protocol and proven encryption techniques to implement a fully functioning, lightweight VoIP peer client. Special considerations are given to the characteristics and operation environment of mobile devices.

Section 2 outlines the solution background. Section 3 describes the design and implementation of the prototype solution. Section 4 provides performance analysis and evaluation discussion. Section 5 concludes the paper.

2. Solution background

There have been many attempts to provide secure services for the major VoIP protocols [6, 11, 12, 13]. Unfortunately, these systems typically suffer from the following problems:

- Complicated to deploy and maintain
- Rely on proprietary and/or incompatible solutions
- Require an existing Public Key Infrastructure (PKI) and/or other resources
- Experience Significant routing problems when passing through NAT

2.1 Inter-asterisk eXchange (IAX)

The Inter-Asterisk Exchange protocol (IAX) is a new protocol that has recently been developed in conjunction with the open-source Private Automatic Branch eXchange (PABX) known as Asterisk [8][14]. This protocol was created as an alternative signalling protocol to SIP and H.323 [8]. It is currently rapidly gaining market-share in the VoIP market and shows considerable promise in the near future. The primary features of IAX are [15]:

- Highly optimised for the existing requirements of VoIP.
- Superior efficiency to H.323 and SIP when passing VoIP traffic [16]
- Minimised efficient bandwidth utilisation for both signalling and media transfers [16].
- Native support for Network Address Translation (NAT) technology. Able to share a single port number, and transfer all data over a well known UDP port.
- Single protocol without the requirement of a separate media transfer protocol. All call signalling information, sequencing, and timing information is included in the transferred IAX frames.
- Written in a lightweight fashion.
- Designed to be easily implemented [15]
- Can be used with any type of streaming media data (including video).

2.1.1 IAX security. IAX has been demonstrated to provide significantly greater efficiencies than SIP or H.323 when running unsecured [16], its performance in a secure environment is investigated here. If IAX can provide the same comparative levels of efficiency it is an ideal protocol for deployments with NAT environments and mobile users.

2.2 VoIP quality considerations

The parameters that a user would normally associate with their determination of call quality are known as Quality of Service characteristics. When voice data is traversing a packet-switched network, the handling of the traffic will achieve certain operational performance levels under various demand levels. Inter-arrival delay, jitter and packet loss are used as intrinsic QoS measures [17].

2.3 Audio codec

All VoIP technologies rely on a codec to transform analogue signals into digital voice packets. The choice of codec is a trade-off between voice quality, processing power and bandwidth requirements. A selection of commonly used VoIP codecs is given in the table below [18]:

Codec Name	Sample Rate (kHz)	Bit-rate (kbps)	Multi-rate	VBR	PLC	License
Speex	8, 16, 32	2.15-24.6	Yes	Yes	Yes	Free / open-source
iLBC	8	15.2 or 13.3	No	No	Yes	Free / closed source
AMR	8	4.75-12.2	Yes	No	Yes	Proprietary
G.729	8	8	No	No	Yes	Proprietary
GSM	8	13	No	No	No	Patented
G.723.1	8	5.3 6.3	No	No	Yes	Proprietary
G.728	8	16	No	No	No	Proprietary

Table 1. Codec feature comparison chart

2.4 Encryption algorithms

In order to provide secure transmission of data, it is necessary to offer confidentiality and authentication. In

other words, data must be valid and should not be available nor disclosed to unauthorized parties.

In order to support different codecs, the encryption algorithm must be able to support variable length data payloads where the amount of data per frame is likely to be short but send at a high frequency (approximately 30-100 bytes 50 times per second).

As the data payload is relatively small, it would be advantageous to use an encryption method that will not increase the size of the data to be sent. Any small increases in size will add significant overhead to the transmission.

2.5 Mobile clients

A goal of this paper is to produce a secure VoIP client that can be run in a mobile device such as a PDA or smart phone. As there are currently no mobile open-source IAX clients suitable for testing, evaluations of our solution can be performed on a laptop. The table below compares a low end laptop with a high end PDA [11].

Device Name:	IBM X30 Laptop	Dell Axim X51 PDA [14]
CPU Manufacturer:	Intel	Intel
CPU Speed:	800 MHz	624 MHz
Available RAM:	512 MB	64 MB
MIPS Rating:	2142	800
Comparative MIPS:	1.0	0.37

Table 2. CPU comparison of laptop and PDA

Although using MIPS (Million Instructions per Second) does not take into account the different instruction sets between CPUs, it is often used to give an approximate performance rating. Based on a simple MIPS comparison, a Dell Axim X51 PDA is able to perform 37% of the integer operations capacity of an IBM X30 laptop.

3. Design and implementation

To demonstrate the proposed modifications to the IAX protocol, it was necessary to add these features to a VoIP client. An open source client was selected, the code examined, and an injection point to add the security code was identified. The tools and methodology to accomplish this are described below.

3.1 Kiax VoIP client

Kiax [19] is an open source soft-phone designed to exclusively utilise IAX. Like many other open source IAX clients, Kiax relies on the freely available "libiax" library to take care of the low level network functions. This library was constructed by the makers of Asterisk, and is commonly used by open source IAX clients. The code modifications necessary to support encryption were mostly required within libiax.

3.2 Cryptlib

Cryptlib is an powerful, general purpose open-source cryptography package designed to provide security services to applications. Its main purpose is to provide cryptography functions that can be integrated into applications. The design of Cryptlib is based on a layered structure that can provide different levels of control to the user. Using Cryptlib, it was possible to experiment with a variety of different encryption methods to assess their impact on performance. A complete architecture diagram is given in Figure 1, below [20]:

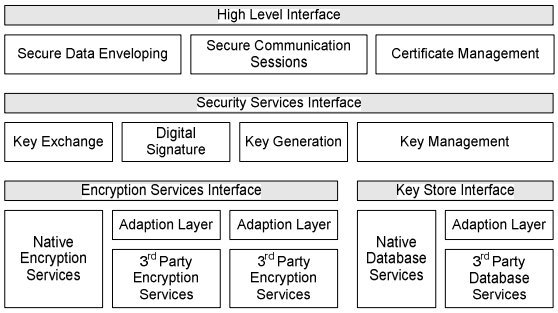

Figure 1. Cryptlib Architecture Diagram

3.3 Solution architecture

The block diagrams below give a basic description of the structure of the kiax software layers.

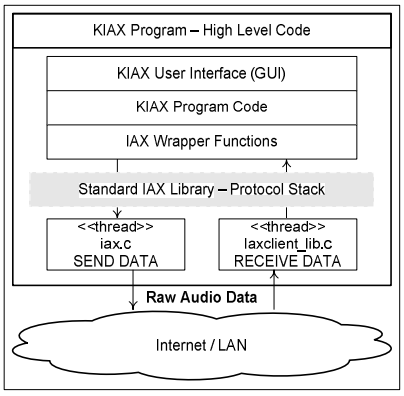

Figure 2. Standard Kiax architecture

Figure 2, above, demonstrates the architecture of the original version of Kiax. Kiax provides a GUI interface to the user, which communicates the settings and preferences to the Kiax program code. The low level IAX protocol program code is provided in the form of a standard library known as libiax.c. This library package is also responsible for encoding and transporting the audio data captured from users.

The modified version of Kiax adds another layer of processing to the audio stream. After the voice data has been encoded via the audio codec, it is intercepted and encrypted before being sent across the network. At the receiver's side, the audio is decrypted, and passed back through the normal Kiax processing stack.

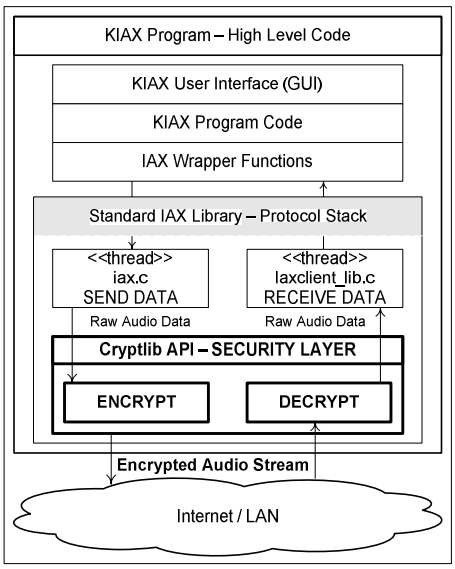

Figure 3. Modified Kiax Architecture Diagram

4. Results and evaluation

Testing was carried out to assess the impact of security modifications to the Kiax program. After configuring the Local Area Network and the client machines, calls were placed and the data was collected. All tests were repeatable and provided very consistent data. A summary of the results is given below:

VoIP Client:	Kiax	Kiax	Kiax	Kiax
Encryption:	None	IDEA/CBC	IDEA/CFB	RC4
Min. CPU Use:	5.812%	17.818 %	16.132 %	17.635 %
Max. CPU Use:	10.020%	28.629 %	26.226 %	27.756 %
Avg. CPU Use:	7.935%	24.158 %	22.756 %	23.090 %
Max. Bandwidth:	1.75 kB/s	2.08 kB/s	1.75 kB/s	1.75 kB/s
Delay Range:	16-58 ms	16-58 ms	16-58 ms	16-58 ms
Jitter Range:	26-28 ms	26-28 ms	26-28 ms	26-28 ms

Table 3. LAN test results 1

VoIP Client:	Kiax	Kiax	Firefly
Encryption:	AES/CBC	AES/CFB	None
Min. CPU Use:	17.818 %	14.629 %	8.719 %
Max. CPU Use:	27.427 %	27.227 %	13.123 %
Avg. CPU Use:	23.447 %	22.592 %	11.364 %
Max. Bandwidth:	2.48 kB/s	1.75 kB/s	1.69 kB/s
Delay Range:	16-58 ms	16-58 ms	2-3 ms
Jitter Range:	26-28 ms	26-28 ms	2-4 ms

Table 4. LAN test results 2

Using Kiax with no encryption, the average processor utilisation is 7.9%, and the bandwidth used approximately 1.75 kilobytes per second. This provides a baseline for Kiax's performance.

Idea - In CBC mode, the quality of the call remained similar to using no encryption, however the bandwidth use increased. This is to be expected, as the data size increased from 33 to 40 bytes. When using IDEA in CFB mode, although the bandwidth was identical to the baseline, the call quality was more frequently interrupted by audio drop outs.

AES - In CBC mode, AES had slightly lower CPU usage as compared to IDEA/CBC, and can be attributed to the AES algorithm being more efficient. This method used the highest amount of bandwidth, adding approximately 0.7kB p/s. The bandwidth increase is larger for AES than IDEA, since the AES algorithm has a block size of 128 bits compared to IDEA using only 64. AES using CFB produced the lowest average CPU utilisation of the encryption methods tested, and did not require additional bandwidth.

RC4 - The RC4 algorithm performed slightly worse than AES/CFB. This is surprising, considering that it is natively a stream cipher.

Overall, the results of both call quality and processor usage are similar for the different encryption algorithms. However, AES in CFB mode should be considered as the preferred method, as it gives the lowest average CPU load, does not add any additional bandwidth requirements and introduces a minimum number of problems in the audio stream.

5. Conclusion

VoIP products promise converged telecommunications and data services that are cheaper, more versatile and provide higher voice quality as compared to traditional offerings. Although VoIP products are rapidly gaining market share with home users, uptake in the enterprise market has remained slow as a result of security and mobility concerns. This paper addresses these security and mobility issues through the integration of robust security features into a

lightweight VoIP protocol that is tailored for mobile devices. A theoretical approach is realised with the development of a software prototype whose security and mobility properties are analysed. The prototype that was created to assess this approach had the following properties:

- Provided a choice of 5 different encryption methods
- Successfully traverses NAT
- Simulated key exchange by the use of pre-shared session key
- Strong security
- No change to bandwidth requirements
- Relatively low processor requirements

Kiax was selected as the basis for the proposed system as it was freely available under an open-source license. Although it provides a valid base for evaluating different encryption methods, the IAX library it provides does not give optimal performance or call quality. Despite the limitations of the client, the results of the performance testing clearly demonstrate the feasibility of this approach.

In the future we intend to extend this research with the use of optimised clients and encryption libraries and test these solutions on mobile devices and mobile device emulators.

6. References

[1] C. R. Strathmeyer, "An Introduction to Computer Telephony", IEEE Commun. Mag., 35(5), May 1996, pp. 106–11.

[2] S. Phil, F. Cary, *You Don't Know Jack About VoIP*, Queue, 2004, 2(6), p. 30-38.

[3] W. Stallings, *Data and Computer Communications* (Seventh Ed.), Pearson Educational International, 2004

[4] Deloitte, "Getting off the Ground: Why the move to VoIP is a decision for all CXOs", On-line at: http://www.deloitte.com/dtt/research/0,1015,sid%3D2245&cid%3D64027,00.html (2004)

[5] M. Grant, "Voice Quality Monitoring for VoIP Networks", Melbourne, 2005.

[6] D. Bilby, "Voice over IP: What You Don't Know Can Hurt You" 2005 [cited 11-04-06]; Available from: http://www.security-assessment.com/Presentations/VOIP_What_You_Don't_Know_Can_Hurt_You.ppt.

[7] J. Rosenberg, RFC3261 - SIP: session initiation protocol. Internet Engineering Task Force, 2002.

[8] M. Spencer, "IAX: Inter-Asterisk eXchange" Version 2. 2006 30/03/06 [cited 24-04-06]; Available from: http://www.rfc-editor.org/internet-drafts/draft-guy-iax-01.txt.

[9] P.E. Jones, H.323 Protocol Overview. [Presentation] 2003 [cited 10-04-06]; Available from: http://www.packetizer.com/voip/h323/papers/.

[10] N. Gohring, "Sysadmins express concerns on VoIP security" 2006 [cited 10-10-06]; Available from: http://www.techworld.com/security/news/index.cfm?newsID=6030&pagtype=samechan.

[11] I. Abad, "Secure Mobile VoIP", in Microelectronics and Information Technology, Royal Institute of Technology: Stockholm, 2003, p. 137.

[12] J. Arkko, E. Carrara, RFC3830 - MIKEY: Multimedia Internet KEYing. Internet Engineering

[13] B. Fuhrmannek, IAX Encryption. 2006 [cited 24-04-06]; Available from: http://voip-info.org/wiki/view/IAX+encryption.

[14] B. Schwarz, "Asterisk open-source PBX system", Linux Journal, 2004. 2004(118): p. 6.

[15] M. Spencer, F. Miller, IAX Protocol Description. 2005.

[16] T. P. Abbasi, S. Seddigh, N. Lambadaris, "A comparative study of the SIP and IAX VoIP protocols", Canadian Conference on Electrical and Computer Engineering, 2005.

[17] W.C. Hardy, *VoIP Service Quality: Measuring and Evaluating Packet-Switched Voice*. New York: McGraw Hill, 2003.

[18] Xiph.Org. Speex Homepage. 2006 [cited 2006 01-10-06]; Available from: http://www.speex.org.

[19] Kiax Team. Kiax Homepage. [Website] 2006 [cited 2006 24/08/06]; Kiax Homepage]. Available from: http://www.kiax.org/.

[20] P. Gutmann, Cryptlib Security Toolkit Manual. 2005 [cited 04-10-2006]; Available from: http://www.cs.auckland.ac.nz/~pgut001/cryptlib/.