Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

7th International Conference
on Electrical Engineering
ICEENG 2010

Secured Voice Over Internet Protocol Based On Blowfish

By

Amr Fouad Khalil* Dr. BAHAA ELDIN** Prof. Dr. GAMAL SELIM***

Abstract:

Voice over Internet Protocol, commonly known as VoIP, is the routing of voice conversations over the Internet Protocol (IP)-based network. As the technology is in need to extend the IP telephony deployments, securing the VoIP infrastructure will become increasingly important. This thesis outlines the VOIP technology, the current VoIP security threats and a brief look is taken at present methods of how to secure the emerging technology where Voice over the Internet Protocol is vulnerable to a number of attacks.Security is an essential consideration for VoIP providers since each component in the VoIP infrastructure can be used as a target, and VoIP has specific security challenges as well.Firstly this thesis discusses the VOIP as the new promising technology over the old deployed PSTN. Secondly, addresses the security issues and concerns of this new technology. Finally, will discuss my proposal of securing the voice over IP using the blowfish encryption technique at a layer between the SAPI. "Speech application programming interface" and the TAPI. "Telephony application programming interface"on the hardware level compared to other VOIP security proposals.

Keywords:

VOIP, BLOWFISH, TAPI, SAPI, H323

---

* Orange Business Services
** Arab Academy for Science & Technology
*** Arab Academy for Science & Technology

1. Introduction:

VoIP is one of the hottest trends in telecommunications.Before VoIP, telecommunications occurred over a public switched telephone network (PSTN), that is, voice data traversed circuit switched connections. The cost savings of Internet telephony systems by converging voice with other data applications, both in dollars and bandwidth, compared to that of circuit switched networks, is encouraging companies to move to VoIP. But many companies are unaware of the additional security baggage that voice brings along with it.Once voice is converged with data on the network, a company's voice systems are suddenly vulnerable to many of the same kinds of attacks that occur on the data side. Phones can suddenly become destinations for spam. Hackers can Target phone systems with denial of service attacks, or program a company's phones to call other businesses, shutting down the second company's phone systems. People can spoof a phone's IP address and make calls that are billed back to the company. And as with a traditional phone system, calls can be intercepted and listened to.VoIP security is complicated by the requirement of multiple components, in most cases, more components than traditional circuit switched networks, and the fact that it is normally deployed on the current data network. Often, normal deployment requires co-existence of the circuit switched network until VoIP functions have replaced those of the circuit switched network. The security approach taken should address circuit switched network and VoIP for as long as both exist. VoIP's next big step is toward wireless. Phones that can roam between Wi-Fi and cellular systems are on the way and will place further roaming and security challenges on VoIP systems.

2. Voice over IP:

Voice over Internet Protocol is the routing of voice conversations over the Internet (Voice on the net, VON) or any other IP-based network (Voice over IP, VoIP). The voice data flows over a general-purpose packet-switched network, instead of traditional dedicated, circuit-switched voice transmission lines. VoIP traffic might be deployed on any IP network, including ones lacking a connection to the rest of the Internet, for instance on a private buildingwide LAN. Protocols used to carry voice signals over the IP network are commonly referred to as VoIP protocols. There are currently three protocols widely used in VoIP implementations the H.323 family of protocols, the Session Initiation Protocol (SIP) and the Media Gateway Controller Protocol (MGCP). A basic difference between these three protocols is where intelligence is concentrated. SIP places most of the intelligence at the end points of the system. MGCP places the intelligence at the network components. H.323 places intelligence everywhere.

3. H.323:

H.323 is a protocol suite that lays a foundation for IP based real-time communications including audio,video and data.The architecture schematic is depicted in figure (1).There are audio codecs (G.711,G.723.1, G.728,etc.) and video codecs (H.261,H.263) that encode and decode the audio and video data.The H.323 proposes an architecture that is composed of four logical components Terminals, Gateways,Gatekeepers and Multi-point Control Units (MCUs).Terminals are LAN client endpoints that are normally bound to a specific address and gateway, and provide real-time, two-way communication with either another H.323 terminal, an H.323 gateway or an MCU. Gateway is an endpoint on the network that provides for real-time, two-way communications between H.323 terminals on the IP network with other ITU terminals on a switchbased network like traditional public switched telephone network (PSTN), SIP network or to another H.323 gateway .The gateway handle different transmission formats. Gatekeeper is the central point for all the calls within its zone and provides services to the registered endpoints such as address translation, admissions control, call signaling, call authorization and authentication, call management, call routing, accounting,and bandwidth management. MCU acts as an endpoint on the network for providing capability for three or more terminals and gateways to participate in a multi-point conference. The MCU consists of a mandatory Multipoint Controller(MC) and an optional Multi-point Processor(MP).The MC's functions are to determine the common capabilities of conferencing terminals, using the H.245protocol. The multiplexing of audio, video and data streams is handled by the MP under control of the MC.A schematic description of the H.323 protocol stack is shown in figure (2). The unreliable but low latency UDP is used to transport audio, video and registration packets.Whereas the reliable but slow TCP is used for data and control packets in call signaling. The T.120 protocol is used for data transfer. H.323 provides three control protocols H.225/Q.931 call signaling, H.225/RAS call signaling and H.245Media control. The H.225/Q.931is used for call signaling control. The H.225/RAS channel is used for establishing a call from the source to the receiving host. After thecallisestablished,H.245 is finally used to negotiate the Session Initiation Protocol

4. Session Initiation Protocol:

SIP is used for initiating, modifying, and terminating a two-way interactive user session that involves multimedia elements such as video, voice, instant messaging, online games, and virtual reality. SIP is used in association with its other IETF sister protocols

like the SAP, SDP and MGCP(MEGACO) to provide a broader range of VoIP services. The SIP architecture is similar to HTTP (clientserver protocol) architecture. It comprises requests that are sent from the SIP user client to the SIP Server. The Server processes the request and responds to the client. A request message, together with the associated response messages makes a SIP transaction. SIP is an application-level protocol, i.e., it is decoupled from the protocol layer that it's transported across. Using TCP allows use of secure socket slayer(SSL)/transport layer security(TLS) providing more security where as, UDP allows for faster, lower latency, connections. SIP depends on Session Description Protocol (SDP) for negotiation of session parameters such as codec identification and media. It supports user mobility through proxy servers and redirecting requests to the user's currently registered location.The SIP architectureas shown in figure(3) specifies two components: user agents and servers. A SIP User Agent is an end system acting on behalf of the user. The UA software contains client and server components. User Agent Client(UAC) is the user client portion, which is used to initiate a SIP request to the SIP servers or the UAS, whereas User Agent Server(UAS) is the user server portion that listens and responds to SIP requests. SIP Servers provide SIP call setup and services. Registration Server receives and authenticates registration requests from SIP users and updates their current location with itself. Proxy Server receives SIP requests and forwards them to the next-hop server, which has more information of the called party. Redirect Server resolves information for the UA client. On receipt of the SIP request, it determines the next-hop server and returns the address of the next-hop server to the client instead of forwarding the request to the next-hop server itself (as in the case of SIP proxy). The endpoints begin by connecting with a proxy and/or redirect server which resolves the destination number into an IP address. It then returns that information to the originating endpoint which is responsible for transmitting the message directly to the destination. A security advantage of SIP is that it uses one port.

5. Media Gateway Control Protocol (MGCP):

MGCP exploded H.323's gatekeeper model and removed the signaling control from the gateway, putting it in a media gateway controller or soft-switch. This device would control multiple media gateways. A Media Gateway executes commands sent by the centralized Media Gateway Controller (MGC) and is designed to convert data between PSTN to IP, PSTN to ATM, ATM to IP, and also IP to IP, thus providing mechanisms to interconnect with other VoIP networks. MGCP defines the communication between "Call Agents" (call control elements or MGCs) and gateways as shown in figure(4). It is a control protocol that monitors the events on IP phones and gateways and instructs them to send media to specified addresses. These Call agents are assumed to have

synchronized with each other and they issue coherent commands to the gateways under their control. The issued commands are executed by the gateways in a master/slave manner. MGCP defines the concepts of "Endpoints" and "Connections" to describe and establish voice paths between two participants. Similarly, it has defined "Events" and "Signals" to describe set-up or teardown of sessions.

6. VoIP Security Threat Scenarios:

A VoIP deployment faces a variety of threats from different networking layers and areas of trust from within the network. For instance, an attacker can try to compromise a VoIP gateway, cause a denial of service attack to the Call Manager, exploit a vulnerability in a vendor's SIP protocol implementation or try to hijack VoIP calls through traditional TCP hijacking, UDP spoofing, or application manipulation. The attacks against a VoIP network can be categorized as follows:

•**VoIP Application Level Attacks**: At the application level, there are a variety of VoIP specific attacks that can be performed to disrupt or manipulate service. Some of them include:

Call Hijacking: An attacker can also spoof a SIP response, indicating to the caller that the called party has moved to a rogue SIP address, and hijack the call.Resource Exhaustion: A potential DoS attack could starvethe network of IP addresses by exhausting the IP addresses of a DHCP server in a VoIP network.

Eaves dropping: An attacker with local access to the VoIP LAN may sniff the network traffic and deciphers the voice conversations. A tool named VOMIT (voice over misconfigured Internet telephones) can be downloaded to easily perform this attack.

Message Integrity : The attacker may be able to conduct a man-in-the-middle attack and alter the original communication between two parties.

Toll Fraud : An attacker can impersonate a valid user/IP phone and use the VoIP network for making free long distance calls.

Denial of Service (DoS) : DoS is caused by anything that prevents the service from being delivered. A DoS can be the result of unavailable bandwidth or VoIP components being unavailable. Many things can cause a DoS including: a network getting congested to a level that it cannot provide the bandwidth needed to support the application; servers not capable of handling the traffic; extraneous services may be running that reduce the available resources to the server; malicious programs such as viruses and Trojan horses; other malicious programs with the purpose of causing DoS; or hacking activity. By spoofing end-point identity, an attacker may cause a DoS in SIP based VoIP networks by sending a "CANCEL" or "BYE" message to either of the communicating parties and end the call. Since SIP is UDP based , sending a spoofed ICMP "port unreachable" message to the calling party could also result in a DoS. If DoS is caused by bandwidth

constraints, potential solutions are increasing the bandwidth and/or isolating the VoIP traffic so that it gets service first. Various methods of ensuring servers don't stop working, such as fail-over methods like clustering, can help reduce DoS from failing components. Each component of the VoIP system offered by the vendor, should be evaluated, removing those that are unnecessary. Server size should be planned such that all desired vendor services and expected traffic can be supported,adding some percentage for expected growth. Defense against DoS attacks of public server scan best be done by locating the device with the public available IP addresses behind a firewall or other device that only allows communication from trusted sources. Also, harden the operating systems in use, removing all unnecessary services and applications from the servers and workstations, patching, etc.

• **Availability :** VoIP networks face a serious risk of availability. The availability risk result from availability-based attacks against protocols, endpoints, network servers, and the kind of attacks designed to reduce the quality of speech or that target simple equipment malfunction(s). The main risk and one that is even more basic is the lack of electricity to power endpoints and other elements making up a VoIP network or infrastructure.

Physical Access : Physical access to the network or to some network component(s) is usually regarded as an end-of-game scenario, a potential for total compromise in VoIP .For example ,if a malicious party is able to gain unauthorized physical access to the wire connecting a subscriber's IP Phone to its network switch, the attacker will be able to place calls at the expense of the legitimate subscriber while continuing to let the subscriber place calls at the same time. With the PSTN, a similar scenario would unveil the malicious party when the legitimate subscriber took the handset off hook

Attacks against the underlying VoIP devices' Operating System: VoIP devices such as IP phones, Call Manager, Gateways, and Proxy servers inherit the same vulnerabilities of the operating system or firmware they run on top of. For instance, the Cisco Call Manager is typically installed on Windows 2000 and the Avaya CallManager onLinux. There are hundreds of remotely exploitable vulnerabilities in flavors of Windows and Linux operating systems for which there are numerous "pointand-shoot" exploits freely available for download on the Internet. No matter how secure an actual VoIP application happens to be, this becomes irrelevant if the underlying operating system is compromised

7. Insecure VoIP:

The Voice over Internet Protocol (VoIP) is an application that meets the challenges of combining legacy voice networks and packet networks by allowing both voice and signaling information to be transported over the packet network. VoIP is the technique

for transporting voice over the Internet.Analog signal from speakers is digitized. Packets with digitized signals as payload are generated according to the TCP-UDP/IP protocols. Packets are transmitted across the IP packet network from originator to terminate and vice versa.The receiver performs packet reception and analog original signal reconstruction as shown in Figure(5).VoIP transmission addresses some challenging processing in order to raise the quality up to regular wired phone lines. Indeed, as the Internet was originally designed for data transfer, it has inherent Impairments such as packet loss and delay variation which can directly impact the quality of voice calls. As VoIP is a typical real-time application, the Real Time Protocol (RTP) was introduced by IETF in 1989 in an attempt to overcome the IP constraint. RTP came up with its dual protocol for control such as RTCP. Over years,RTP has proven its ability to support VoIP calls.However, as RTP was not designed to address any secure request, it is completely vulnerable to Eaves dropping and attacks as shown in Figure(6). Hence, any VoIP communication can be vulnerable to spying or voice data corrupting attack Encryption is the key feature for VoIP to empower its security to achieve confidential and authenticated calls.

8. Encryption basis:

Encryption is based on mathematical theorems related to the Number Theory and the Combinatorial Analysis. They are the common root foundations of all encryption algorithms. This pool of techniques Determine both voice and data information security. Encryption algorithms have been developed for Many years and their efficiency keep improving over time. This paper will describe later the main algorithms deployed to date and used for secured voice.Cryptography is usually referred to as "the study of secret", while nowadays is most attached to the definition of encryption. Encryption is the process of converting plain text "unhidden" to a cryptic text "hidden" to secure it against data thieves. This process has another part where cryptic text needs to be decrypted on the other end to be understood.Figure(7) shows the simple flow of commonly used encryption algorithms. As defined cryptographic system is "a set of cryptographic algorithms together with the key management processes that support use of the Algorithms in some application context." This definition defines the whole mechanism that provides the necessary level of security comprised of network protocols and data Encryption algorithms.

The Data Encryption Standard (DES)
was created by the IBM Corp. it is a 64-bit block cipher Algorithm. However, DES is considered today to have some security weaknesses. Today, DES is mentioned more for backward compatibility than for regular usage.

The Triple Data Encryption Standard (TDES) was created to reinforce DES against attack. It is in fact The DES algorithm applied three times on the data. It was developed by Diffie and Hellman in 1978. It is a 64-bit block cipher algorithm. Its difference with the DES is a key size between 128 bits and 192 bits. There are several ways of implementing triple DES to encrypt a clear text

The Advanced Encryption Standard (AES) was approved as the symmetric private key algorithm to be used by US government organizations and recommended for information security. AES will be used also for secure 3G wireless networks. It is a 128-bit block cipher algorithm with core processing divided into two parts: key expansion, and data permutation and substitution. Those two parts can be configured differently depending on the required security level.AES is, so far, the most robust encryption algorithm against the modern cryptanalysis attack.Apart from this, the Ron Rivest version 4 (RC4) was developed in 1987 for RSA Data Security Inc. It is a stream cipher with variable key length. It has been deployed in commercial activities. However, it tends to be used less today because of several weaknesses compared to block cipher.

Cipher Operation Modes

Cipher operation modes handle how the cipher algorithm is used to encrypt/decrypt data. They define a cipher context attached to the original cipher algorithm. Many modes have been proposed in order to reinforce the cipher strength against new attacks.

Operation modes:

- **The Electronic Codebook Mode (ECB)** is the natural way of encrypting one block after another with no block connection. Its main drawback is to raise some detectable correlation.
- **The Cipher Block Chaining Mode (CBC)** introduces some recursive chaining to overcome the ECB issue. It requires an Initial Vector of the same size as the block. It is the most robust mode against Attack. However, its chaining profile aggravates the losses in case of packet loss
- **The Output Feedback Mode (OFB)** ciphers data by only xoring them with an encrypted vector.Hence, the clear data does not pass through the cipher.
- **The Cipher Feedback Mode (CFB)** is based on OFB, but with variable clear data size granularity.
- **The Counter Mode (CTR)** is a block independent mode. The process to encrypt the counter is the Challenge of this mode, since a weak one may impact the whole encryption chain.The two main characteristics that identify and differentiate one encryption algorithm From another are its ability to secure the protected data against attacks and its speed and Efficiency in doing so. This paper also provides a performance comparison between four of The most common encryption algorithms: DES, 3DES, Blowfish and AES (Rijndael).The comparison has been conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithm's

encryption/decryption speed.As the importance and the value of exchanged data over the Internet or other media types are increasing,the search for the best solution to offer the necessary protection against the data thieves' attacks along with providing these services under timely manner is one of the most active subjects in the security related communities.This paper tries to present a fair comparison between the most common and used algorithms in the data encryption field. Since our main concern here is the performance of these algorithms under different settings, the presented comparison takes into Consideration the behavior and the performance of the algorithm when different data loads are used

Cryptography Goals This section explains the five main goals behind using Cryptography.Every security system must provide a bundle of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories:

Authentication: This means that before sending and receiving data using the system, the receiver and sender identity should be verified.

Secrecy or Confidentiality: Usually this function (feature) is how most people identify a secure system. It means that only the authenticated people are able to interpret the message (date) content and no one else.

Integrity: Integrity means that the content of the communicated data is assured to be free from any type of modification between the end points (sender and receiver). The basic form of integrity is packet check sum in IPv4 packets.

Non-Repudiation: This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.

Service Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems should provide a way to grant their users the quality of service they expect.

Block Ciphers and Stream Ciphers

One of the main categorization methods for encryption techniques commonly used is based on the form of the input data they operate on. The two types are Block Cipher and Stream Cipher. This section discusses the main features in the two types, operation mode, and compares between them in terms of security and performance.

Block Cipher

Before starting to describe the key characteristics of block cipher, the definition of cipher word must be presented. "A cipher is an algorithm for performing encryption (reverse is decryption) . In this method data is encrypted and decrypted if data is in from of blocks. In its simplest mode, you divide the plain text into blocks which are then fed into the cipher system to produce blocks of cipher text.ECB (Electronic Codebook Mode) is the basic form of clock cipher where data blocks are encrypted directly to

generate its correspondent ciphered blocks as shown in Figure(8).
Stream Ciphers :As shown in Figure(9) Stream cipher functions on a stream of data by operating on it bit by bit. Stream cipher consists of two major components: a key stream generator, and a mixing function.Mixing function is usually just an XOR function,while key stream generator is the main unit in stream cipher encryption technique. For example, if the key stream generator produces a series of zeros,the outputted ciphered stream will be identical to the original plain text.Symmetric and Asymmetric encryptions Data encryption procedures are mainly categorized into two categories depending on the type of security keys used to encrypt/decrypt the secured data. These two categories are:

Asymmetric and Symmetric encryption techniques

Symmetric Encryption: As shown in Figure(10)In this type of encryption, the sender and the receiver agree on a secret (shared) key.Then they use this secret key to encrypt and decrypt their sent messages.Node A and B first agree on the encryption Technique to be used in encryption and decryption of communicated data. Then they agree on the secret key that both of them will use in this connection.After the encryption setup finishes, node A starts sending its data encrypted with the shared key, on the other side node B uses the same key to decrypt the encrypted The main concern behind symmetric encryption is how to share the secret key securely between the two peers. If the key gets known for any reason, the whole system collapses.The key management for this type of encryption is troublesome, especially if a unique secret key is used for each peer-to-peer connection, then the total number of secret keys to be saved and managed for nnodes will be n(n-1)/2.

Asymmetric Encryption
As shown in Figure(11) Asymmetric encryption is the other type of encryption where two keys are used. To explain more, what Key1 can encrypt only Key2 can decrypt, and vice versa. It is also known as Public Key Cryptography (PKC), because users tend to use two keys: public key, which is known to the public,and private key which is known only to the user. Figure illustrates the use of the two keys between node A and node B. After agreeing on
the type of encryption to be used in the connection,node B sends its public key to node A. Node A uses the received public key to encrypt its messages.Then when the encrypted messages arrive, node B uses its private key to decrypt them.problem of managing secret keys.But on the other hand, this unique feature of public key encryption makes it mathematically more prone to attacks. Moreover, asymmetric encryption techniques are almost 1000 times slower than symmetric techniques, because

they require more Computational processing power.To get the benefits of both methods, a hybrid technique is usually used. In this technique,Asymmetric encryption is used to exchange the secret key, symmetric encryption is then used to transfer data between sender and receiver.

Compared Algorithms

This section intends to give the readers the necessary background to understand the key Differences between the compared algorithms.

DES: (Data Encryption Standard),was the first encryption standard to be recommended DES became a standard in 1974. Since that time, many attacks and methods recorded that exploit the weaknesses of DES, which made it an insecure block cipher.

3DES: As an enhancement of DES, the3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is Slower than other block cipher methods.

AES: (Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. Rijndael (pronounced Rain Doll) algorithm was selected in 1997 after a competition to select the best encryption standard. Brute force attack is the only Effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers.

Blowfish: It is one of the most common public domain encryption algorithms provided by Bruce Schneier - one of the world's leading cryptologists,and the president of Counterpane Systems, a consulting firm specializing in cryptography and computer security.Blowfish is a variable length key, 64-bit block cipher.

The Blowfish algorithm was first introduced in 1993.This algorithm can be optimized in hardware applications though it's mostly used in software applications. Though it suffers from weak keys problem, no attack is known to be successful against it .In this section a brief description of the compared encryption algorithms have been introduced. This introductions to each algorithm are to provided the minimum information to distinguish the main differences between them.To give more prospective about the performance of the compared algorithms, this section discusses the results obtained from other resources.One of the known cryptography libraries is Crypto++ . Crypto++ Library is a free C++ class library of cryptographic schemes. Currently the library consists of the following, some of which are other people's code, repackaged into classes.Table 1 contains the speed benchmarks for some of the most commonly used cryptographic algorithms.All were coded in C++, compiled with Microsoft Visual C++ .NET 2003 (whole program optimization, optimize for speed, P4 code generation), and

ran on a Pentium 4 2.1 GHz processor under Windows XP SP 1. 386 assembly routines were used for multiple-precision addition and subtraction. SSE2 intrinsic were used for Multiple-precision multiplication.It can be noticed from the table that not all the modes have been tried for all the algorithms.Nonetheless, these results are good to have an indication about what the presented comparison results should look like.Also it is shown that Blowfish and AES have the best performance among others. And both of them are known to have better encryption (i.e. stronger against data attacks) than the other two.
Table 1 Comparison results using Crypto++ The popular secret key algorithms including DES,3DES, AES (Rijndael), Blowfish, were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were implemented in a uniform language (Java), using their standard specifications, and were tested on two different hardware platforms, to compare their performance.Tables 2 and 3 show the results of their experiments,where they have conducted it on two different machines: P-II 266 MHz and P-4 2.4 GHz.Table 2 Comparative execution times (in seconds) of encryption algorithms in ECB mode on a P-II 266 MHz machine Table 3 Comparative execution times (in seconds) of encryption algorithms in ECB mode on a P-4 2.4 GHz machine .From the results it is easy to observe that Blowfish has an advantage over other algorithms in terms of throughput between the algorithms in stream mode using CBC, but since this paper is more focused on block cipher the results were omitted.The results showed that Blowfish has a very good performance compared to other algorithms. Also it showed that AES has a better performance than 3DES and DES.Amazingly it shows also that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data.encryption algorithms implemented inside .NET framework. Their results are close to the ones shown in Figure(12) & (13).The comparison was performed on the following algorithms: DES, Triple DES (3DES),RC2 and AES (Rijndael). The results shows that AES outperformed other algorithms in both the number of requests processes per second in different user loads, and in the response time in different user-load situations.This section gave an overview of comparison results achieved by other people in the field. Comparison results using .NET implementations In This section also it will describe the simulation environment and the used system components.As mentioned this simulation uses the provided classes in .NET environment to simulate The performance of DES, 3DES and AES (Rijndael). Blowfish implementation used here is the one provided by Markus Hahn under the name Blowfish.NET.This implementation is thoroughly tested and is optimized to give the maximum performance for the algorithm.
The implementation uses managed wrappers for DES, 3DES and Rijndael available in System.Security.Cryptography that wraps unmanaged implementations available in Crypto API. These are DES Crypto Service Provider, Triple DES Crypto Service Provider and

Rijndael Managed respectively. There is only a pure managed implementation of Rijndael available in System.Security.Cryptography, which was used in the tests.

9. Hardware Implementation:

Connection between two PC's

Figure(14) shows how the Hardware is implemented using the following

Mic & speaker:

That's how the analog signal delivered to or out the sound card.

Sound card: Sound card is responsible for converting the analog signal to digital signal and save it as a stream of data into the RAM.

Encryption & decryption layer: In Encryption & decryption layer we will use the blowfish algorithm as the security algorithm, To encrypt and decrypt the input or output data. And put it in an encrypted or decrypted stream.

TAPI: The Telephony Application Programming Interface there are two types TAPI 2.0 and TAPI 3.0 in this project TAPI3.0 is the considered one .

Phase 1 (initialization state)

- To place a call using two PCs you need to create two classes (SAPI and TAPI).
- When you make a call the program create two SAPI objects and one TAPI object in the RAM.
- The MIC take the input signal and convert it from analog to digital as a stream of data that save in the first SAPI object (SAPI x1).
- There is a stream of data coming from the second SAPI object (SAPI x2) that convert from digital to analog in the speaker.
- The TAPI object is responsible for finding connection point that support H.323 then find a port to connect through.

Phase 2 (call state):

- Select destination IP.
- Create call through the TAPI, using selected port.
- Request, reached, connecting, connected.
- When connected :

o create two SAP and encrypt them through encryption layer
o Set encryption type and key.
o Session key will be the result of encrypting a predefined key by a GUID
o exchange ram stream address , to use RTP syn

Phase 3 (Answering the call):

- Connected, Connecting, Accept call.
- create two SAP and one TAP

The MIC take the input signal and convert it from analog to digital as a stream of data that save in the first SAPI object (SAPI x1).

There is a stream of data coming from the second SAPI object (SAPI x2) that convert from digital to analog in the speaker.

The TAPI object is responsible for finding connection point that support H.323 then find a port to connect through.

Performance :

It has been tested by using time counters in the program that the call initialization and key exchange to bring up a session key has taken (1 msec) while the call establishment using a secured layer based on BLOWFISH algorithm has taken around (37 msec) which is very convenient for a VOIP call to be done with the best QOS .

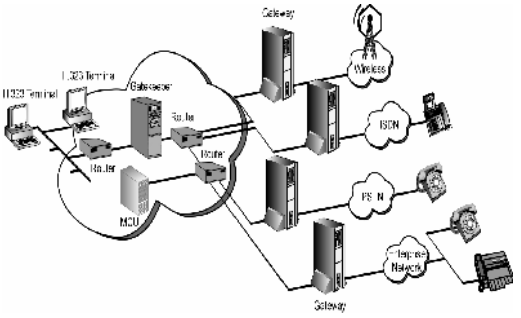

Figure (1): *H.323 Architecture*

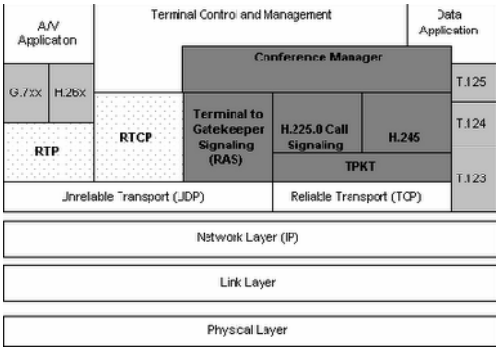

Figure (2): *H.323 Protocol Stack*

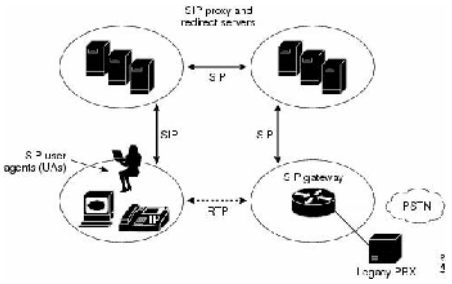

Figure (3): *SIP Architecture*

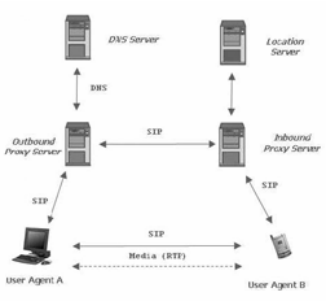

Figure (4): *MGCP Architecture*

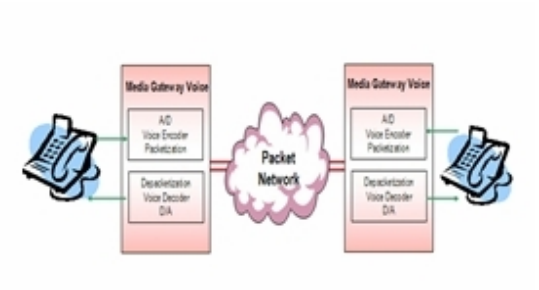

Figure (5): *A/D – D/A Voice conversion*

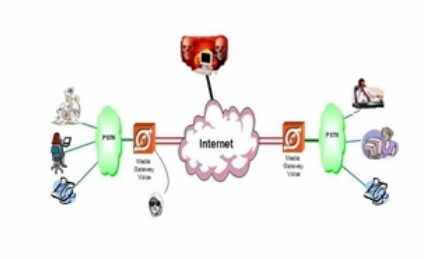

Figure (6): *Eaves dropping*

Figure (7): *encryption algorithm*

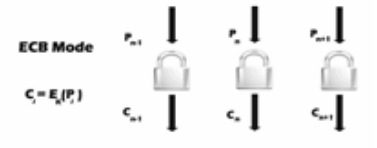

Figure (8): *Block Cipher ECB Mode.*

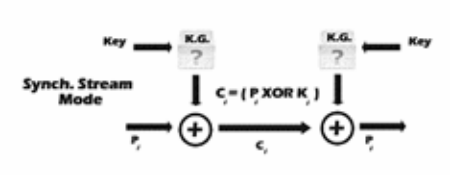

Figure (9): *Stream Cipher (Simple Mode)*

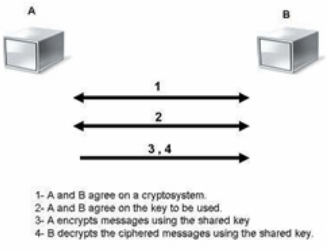

Figure (10): *Symmetric Encryption*

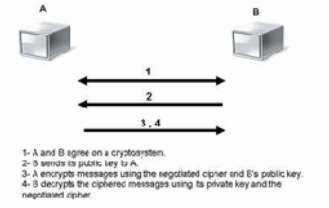

Figure (11): *Asymmetric Encryption*

Figure (12): *Comparison results using .NET implementations*

Figure (13): *Comparison results using .NET implementations*

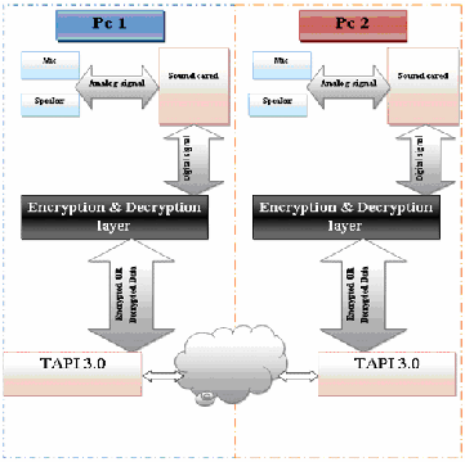

Figure (14): *Hardware Implementation*

Table (1): *Comparison results using Crypto++*

Algorithm	Megabytes(2^20 bytes) Processed	Time Taken	MB/Second
Blowfish	256	3.976	64.386
Rijndael (128-bit key)	256	4.196	61.010
Rijndael (192-bit key)	256	4.817	53.145
Rijndael (256-bit key)	256	5.308	48.229
Rijndael (128) CTR	256	4.436	57.710
Rijndael (128) OFB	256	4.837	52.925
Rijndael (128) CFB	256	5.378	47.601
Rijndael (128) CBC	256	4.617	55.447
DES	128	5.998	21.340
(3DES)DES-XEX3	128	6.159	20.783
(3DES)DES-EDE3	64	6.499	9.848

Table (2): *ECB mode on a P-II 266*

Input Size (bytes)	DES	3DES	AES	BF
20,527	24	72	39	19
36,002	48	123	74	35
45,911	57	158	94	46
59,852	74	202	125	58
69,545	83	243	143	67
137,325	160	461	285	136
158,959	190	543	324	158
166,364	198	569	355	162
191,383	227	655	378	176
232,398	276	799	460	219
Average Time	134	383	228	108
Bytes/sec	835	292	491	1,036

Table (3): *ECB mode on a P-4 2.4*

Input Size (bytes)	DES	3DES	AES	BF
20,527	2	7	4	2
36,002	4	13	6	3
45,911	5	17	8	4
59,852	7	23	11	6
69,545	9	26	13	7
137,325	17	51	26	14
158,959	20	60	30	16
166,364	21	62	31	17
191,383	24	72	36	19
232,398	30	87	44	24
Average Time	14	42	21	11
Bytes/sec	7,988	2,663	5,320	10,167

10. Conclusions:

The results show that the Blowfish has a better performance than Other common encryption algorithms . Since the Blowfish has not shown yet any known security Weakness so far, which makes it an excellent candidate to be considered as a standard encryption algorithm.AES showed poor performance results compared to other Algorithms since it requires more processing power. Using CBC mode has added extra Processing time, but overall it was relatively negligible especially for certain application That requires more secure encryption to a relatively large data blocks.

References:

1. [RFC2828],"Internet Security Glossary", http://www.faqs.org/rfcs/rfc2828.html
2. [Nadeem2005]Aamer Nadeem et al, "A performance Comparison of Data Encryption Algorithms", IEEE 2005
3. [Earle2005] "Wireless Security Handbook,". Auerbach Publications 2005
4. [Dhawan2002] Priya Dhawan., "Performance Comparison: Security Design Choices," Microsoft Developer Network October 2002. http://msdn2.microsoft.com/enus/ library/ms978415.aspx
5. [Edney2003]," Real 802.11 Security: Wi-Fi Protected Access and 802.11i ,". Addison Wesley 2003
6. [Wikipedia-BC] "Block Cipher", http://en.wikipedia.org/wiki/Block_cipher
7. [Hardjono2005]," Security In Wireless LANS And MANS ,". Artech House Publishers 2005
8. [TropSoft] "DES Overview", http://www.tropsoft.com/strongenc/des.htm [Explains how DES works in details, features and weaknesses]
9. [Bruce1996] BRUCE SCHNEIER, "Applied Cryptography" , John Wiley & Sons, Inc 1996
10. [Crypto++]"Crypto++ benchmark", http://www.eskimo.com/~weidai/benchmarks.html [Results of comparing tens of encryption algorithms using different settings].
11. [BlowFish.NET] "Coder's Lagoon",http://www.hotpixel.net/software.html [List of resources to be used under GNU]