VOICE CHATTING WITH ENCRYPTION

TEAM MEMBERS

- 1. Omar Mohamed Almaghrabi Ali El-gendi.
- 2. Akram Tarek Fouad Kashef.
- 3. Islam Hossam El-din Ibrahim Mohamed.
- 4. Kamal Mohamed Kamal.

AGENDA

- Introduction.
- Problem.
- Solution.
- Results.
- Future Work.
- Demo.

INTRODUCTION

- Security and privacy.
  - this fact rules for all kind of data at any time.
- Communication systems.
  - often seen as possible security leaks for transmitted data even though these systems employ data security techniques.
- Voice encryption systems.
  - used to guarantee end-to-end security for speech in real time communication systems such as GSM, VoIP, Telephone, analogue Radio.

Figure 1 illustrates a possible leak in a kind of network as we use it every day.

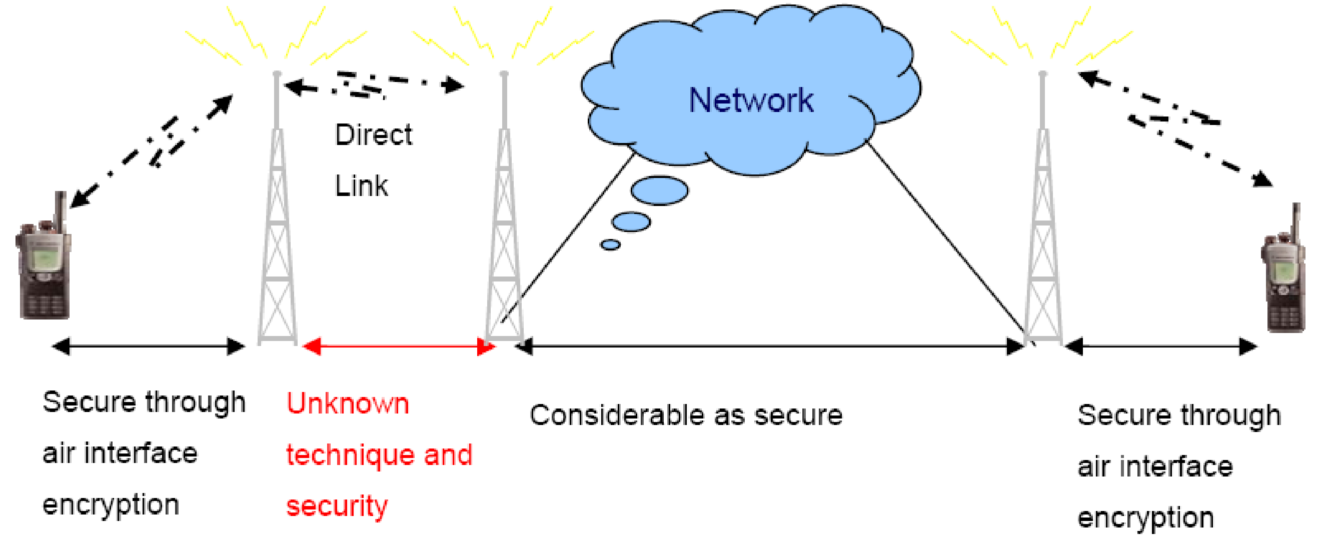

Figure 1: Radio Network with unsecured sectors

PROBLEM

- The main problem in the most voice chat application between end – to – end applications is security.
- It is possible to a third party system to enter the conversation between two users and hear the voice.
- So our main issue in our system is to handle the security threats to make voice conversation more secured.

SOLUTION

- We have designed and implemented a voice chat application between two end points that enables our users to make voice chatting more secured.
- System components :
  - Module 1.
  - Module 2.
  - Module 3.

MODULE 1:

- Real time voice chat application over network using UDP sockets.

MODULE 2:

- Implementing Encoder and Decoder to the voice captured from the microphone at the two end-points

MODULE 3:

- This module handles our main issue Security , it encrypts the voice at the first end-point and decrypt it at the second end-point.

SOLUTION

- Voice chat application.
  - Sockets.
  - Compression/Decompression.
  - Encode/Decode.
  - Encrypt/Decrypt.

SOCKETS

- **An Internet socket is characterized by (IP,PORT NUM,PROTOCOL)**
- Type of sockets.
  - Datagram sockets (UDP). //stream
  - Stream sockets (TCP). //packets
  - Raw sockets.
- How sockets work.

SOCKETS

- A socket is like a handle to a file, which is used to open the path to communicate with another machine. It resembles the file IO, as does the serial communication. Using socket programming, we can have communication between two applications. The applications are typically on different computers or in the same computer. For the two applications to talk to each either on the same or different computers, one application is generally a server that keeps listening to the incoming requests and the other application acts as a client and makes the connection to the server application.

SOCKETS

The server application can either accept or reject the connection. If the server accepts the connection, a dialog can begin between the client and the server. Once the client is done with whatever it needs to do, it can close the connection with the server. Connections are expensive in the sense that servers allow only finite connections to occur. During the time client has an active connection, it can send the data to the server and/or receive the data.

ENCODER

Introduction:

- In our application we use G.711
- **G.711** is an ITU-T standard for audio companding. It is primarily used in telephony.
- Its formal name is *Pulse code modulation (PCM) of voice frequencies.*

- We used two types of encoders/decoders.
    - A-LAW .
    - U-LAW .

A – LAW:

- A-law encoding thus takes a 13-bit signed linear audio sample as input and converts it to an 8 bit value as follow :

Linear input code	Compressed code
s0000000wxyz`a	s000wxyz
s0000001wxyz`a	s001wxyz
s000001wxyz`ab	s010wxyz
s00001wxyz`abc	s011wxyz
s0001wxyz`abcd	s100wxyz
s001wxyz`abcde	s101wxyz
s01wxyz`abcdef	s110wxyz
s1wxyz`abcdefg	s111wxyz

U – LAW:

- µ-law encoding takes a 14-bit signed linear audio sample as input, increases the magnitude by 32 (binary 100000), and converts it to an 8 bit value as follows:

Linear input code	Compressed code
s00000001wxyz`a	s000wxyz
s0000001wxyz`ab	s001wxyz
s000001wxyz`abc	s010wxyz
s00001wxyz`abcd	s011wxyz
s0001wxyz`abcde	s100wxyz
s001wxyz`abcdef	s101wxyz
s01wxyz`abcdefg	s110wxyz
s1wxyz`abcdefgh	s111wxyz

COMPARISON A-LAW TO MU-LAW:

- The µ-law algorithm provides a slightly larger dynamic range than the A-law for small signals. By convention, A-law is used for an international connection if at least one country uses it.

ENCRYPTION

- Using Data Encryption Standard (DES).
  - Stream Cipher.
  - DES objectives.
  - DES weakness

DES ALGORITHM:

- Substitution-permutation algorithm:

– 64-bit input and output blocks

– 56-bit key (with an additional 8 parity bits)

– information data is cycled16 times through a set of substitution and permutation trans- formations: highly non-linear input-output relationship.

DES ALGORITHM:

- Very high throughput rates achievable (upto100Mbits/s)

- Availability of economical hardware to implement DES.

- Low to medium security applications (e.g. secure speech communications)

RESULTS

- Voice chat application using sockets.
- Encoder and Decoder for the voice.
- Encrypt and Decrypt between two end points.

FUTURE WORK

- Implement a plug-in as an intermediate software between all voice chat application eg. Skype , Yahoo , etc..
- Enhance our encryption and decryption algorithm to make a high level security layer.

DEMO