Volume 2, Issue 1, January 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Need of Secure Voice Encryption and its Methods a Review Paper

Parwinder pal singh
Computer science Engg.
IGCE, PTU Kapurthala

Bhupinder singh
Computer science Engg.
IGCE, PTU Kapurthala

Satinder pal Ahuja
Computer science Engg.
IGCE, PTU Kapurthala

***Abstract*— This paper will give u a information about the voice encryption, what is the need of voice encryption and the different methods to carry out the encryption on voice.In this paers various modes of voice transmission are discussed. Types of voice circuit channels are also discussed in this paper.**

***Keywords*— GSM, Scrambling, Encryption, Data traffic, Digitized.**

I. INTRODUCTION

Voice encryption systems are used to guarantee end-to-end security for speech in real time communication systems such as GSM, VoIP, Telephone, analogue Radio. The term "Encryption" implies more than just **"voice scrambling"** which simply disguise the voice in some manner to reduce the intelligibility of someone monitoring the channel. Most "scramblers" do not use any form of key stream generator that allow any pseudo random changes to the scrambling pattern. The security level of "voice scramblers" is therefore quite low and this approach requires little in terms of counter-measure costs to defeat.

II. NEED OF VOICE ENCRYPTION

1. An easy way a real or perceived threat exists in voice traffic collection from some source that has the technical and financial means to collect and extract information from a communications system.
2. The information on the system is of some value to persons other than the sender and the intended receiver(s), e.g., personal, financial, intelligence, or otherwise information that is sensitive in nature.
3. Today, competitors, hackers, or governmental institutions can intercept any GSM cell call with relatively little effort.

III.Types of Voice Transmissions

A. *Full Duplex* –

Simultaneous, bi-directional traffic between two (or more) users. True full duplex traffic generally requires two, one-way communications links each servicing traffic in opposite directions. An example of a full duplex voice system is the classic analog telephone system that allows two or more users to talk simultaneously to each other.

B. *Half Duplex* –

Non-simultaneous bi-directional traffic between two (or more) users. Half duplex usually relies on cooperation between the users, allowing each to speak in turn. In most half duplex systems, the default mode is 'receive' or 'listen,' with the 'send' or 'talk' mode commanded by the individual users' actions. Some half duplex systems use manually actuated switches (e.g. push-to-talk or 'PTT') to determine when the near end unit will transmit, while other systems use voice actuated microphones (VOXes) that begin transmitting when the VOX circuit detects a signal above its set audio threshold level. In some cases, a mixed mode system is introduced, (e.g., a half duplex radio patch to a full duplex phone system) where the resultant system takes on many of the attributes of a half duplex system.

C. *Voice Channel Attributes* –

Voice channel attributes are typically dependent on whether the voice is digitized or presented in an analog format. Digitized voice channels perform in many respects like digital data channels in that the channel processing performed on the digital voice traffic is identical to that of data traffic. In many multi-channel systems, voice and data signals are intermixed in a multiplexer, and are therefore treated identically within the communications pipeline. Most users of data channels are not overly concerned with data packet delays of up to 2 or 3 seconds. Most users of voice channels (digitized or analog circuits) are critically aware of such delays, and would therefore not appreciate the communications channel postponing audio

presentation while re-sending "voice packets". On the other hand, a voice channel may perform adequately with a fair amount of noise, (bit errors) while although noticeable, would not seriously effect voice intelligibility. A data channel on the other hand may not tolerate any bit errors and may make use of extensive amounts of forward error correction and/or data re-transmissions to detect and correct any errors at the destination data terminal.

D. *Intrusive vs. Non-intrusive Cryptographic Methods*

Most voice systems are made up of various sub systems or 'components' that treat or process voice information. In the case of cryptographic equipment, the introduction of an encipher and decipher process is designed to provide a non-intrusive presence, particularly when the cryptographic equipment is placed in a "PLAIN" mode of operation. This methodology dictates that the user of a system does not detect the presence of a cryptographic subsystem within its architecture. The possible exception may include some additional delay introduced by the signal processing, and occasionally, some additional user functionality (mode selections and indicators). An example of intrusive cryptographic methodology is where additional connections (patches), complex channel establishment procedures (special lines or trunks), or other noticeable features like degraded voice quality or some other measurable voice channel degradation is present.

E. *Throughput Delay*

A measure of total end-to-end time delay that a system introduces to a communications channel, between the signal's point of origin and its point of final reception. The total throughput delay of a system is the sum of all system time delays ranging from coder/decoders (CODEC) or other digitization techniques, signal buffers, signal processing, interleaving techniques (error spreading matrices), signal filters, as well as all propagation delays from the communications path(s). In general, this delay is most noticeable in voice channels, and in particular, full duplex voice channels such as telephone circuits.

III. VOICE ENCRYPTOR.

The two voice encryptor types are generally categorized as either 'analog voice encryptors' or 'digital voice encryptors'.

A. *The Digital Voice Encryptor*

1. The digital voice encryptor treats the voice signal as a digital data stream, and is therefore closer to a data encryptor than a voice encryptor in terms of its performance characteristics. It relies on some method of converting the voice signal into a digital data stream. Once it is digitized, it is then 'Exclusive ORed' with the key stream generator's output bit stream, thus producing the encrypted data stream signal sent out over the channel.
2. The principle disadvantage or limitation of the digital voice encryptor is generally recognized to be that of recovered voice intelligibility and recognition brought on by limitations in voice channel bandwidths. In other words, in order to fit the digitized information into a restrictive audio channel, certain trade-offs of bits-per-second (bps) vs. voice quality need to be addressed. Also, the previously noted problem with retaining digital synchronization on poor quality channels is also generally viewed as a disadvantage of digital voice encryption techniques.
3. One notable advantage of a digital voice encryptor over an analog voice encryptor is that the security level is generally considered to be equal to that of the key stream generator itself. Related to this feature, digital encryption offers the countermeasure attacker an interesting problem, where if designed correctly, the ability to break back the data stream to the key is typically viewed as an "all-or-nothing" challenge. That is, if the key is discovered, all of the traffic for that key period is susceptible to interception. The analog encryptor, again if properly designed, offers a different challenge to an attacker, in that the amount of effort to find the originator's key from the attributes of the captured encrypted analog signal is next to impossible (due to limited key stream 'visibility') and is not an all-or-nothing challenge. The only viable attack against "quality" analog encryption techniques is to attempt to piece together the individual audio segments using individual segment's boundary characteristics. These segment boundary characteristics are not necessarily easy to ascertain, particularly after a signal has been transmitted over a communications channel. Although some degree of success may be achieved over long periods of time, the amount of effort to piece together small segments (seconds) of speech is generally viewed as not worth the signal analysis time (weeks to months) and effort it requires.
4. All digitized voice encryptors use some method of digitizing the voice signal using an analog-to-digital (A/D) process before the signal is encrypted. The principle difference from 'analog' approaches is that the digitized signal is not treated as analog information, but rather is viewed as a true digital bit stream that is subsequently Exclusive-ORed (XOR) with the output of the secure key stream generator. This classical digital decryption method does result in a secured data bit stream with totally pseudo random characteristics. The 'down side' is that a

quality (high bit rate) voice signal, being truly random digital in nature, cannot be re-routed through the D/A (digital to analog) circuitry and be broadcast in the same analog bandwidth channel as the original voice signal. The only way to reduce the channel bandwidth of the signal is to reduce the sampling rate of the analog signal during the A/D process. The obvious result in reducing the sampling rate is that the audio characteristics suffer. A simple A/D converter samples the signal at twice the highest frequency component of the analog signal. If the sampling rate is reduced, then the channel band-width must likewise be reduced. This reduces the channel band pass in proportion to this reduction. To help offset this constraint, voice encoding techniques have been developed that enable the predictable nature of voice signals to be modeled with the end result of greatly reducing the digital rate needed to pass an audio signal. The most common digital voice encryptors use a vocoder (short for voice coder/ decoder) to provide the optimum voice intelligibility for a given channel data capacity. These devices (or software modules) use current and previous states of sampled audio to predict the next sample's state, and then model the deviation from the expected state in far fewer bits than an equivalent direct-sampled A/D converter would need. Most modern voice encryption products use vocoders, to present the best available voice characteristics within constrained channel bandwidths. A 'down side' to vocoders over direct A/D and D/A, is that channel noise attributes and distortions become more pervasive when using a vocoder, since more information is represented by individual bits than in simple A/D and D/A converters. The other 'down side' is that even the best designed voice encoders can require appreciably more bandwidth to pass an equivalent audio quality signal than a straight analog signal (or an analog encrypted signal).

B. *The Analog Voice Encryptor*

Early methods of "analog" encryption were nothing more than voice scramblers with little security to any aggressive attack. The advent of more powerful voice processing circuitry and software allowed more sophisticated voice processing techniques that use a key generator's secure key stream for selecting the given sound segment's permutations. These permutations include band segmentation, sub-band frequency inversions (or non-inversions), and sub-band segment interleaving. The more combinations used, the harder to reconstruct the signal without knowledge of the key generator's key stream. This technique will generally provide a near-plain mode level of voice quality while containing the encrypted channel to within the plain modes voice channel bandwidth. It is common in the newer 'analog' techniques to digitize the signal, but it processes (in many respects) like an analog signal. In this respect, it is a bit of a misnomer to call it 'analog' encryption, however it is done primarily to differentiate it from 'digital' voice encryption techniques (see the discussions below).

1. The analog voice encryptor can be viewed as a hybrid between a digital encryptor and a voice scrambler. It also digitizes the voice signal (often at a data rate much higher than the typical Vocoder), but handles the voice processing in a manner that allows digital-to-analog reconstruction in a bandwidth constrained manner. This means that although the analog voice signal is digitally processed, it retains sufficient voice-like characteristics, that when transmitted out over the channel, maintains the energy within the original voice channel.
2. The digital processing portion of the analog encryptor is generally executed on a high speed digital signal processor (DSP) that handles the digitized audio as sub-elements of the original captured audio. These sub-elements are pseudo randomly manipulated in both time and frequency domains, so that the exported signal has very little of its original voice intelligibility. The destination end processing performs the reverse time and frequency manipulations and reconstructs the audio composite using its DSP.
3. The principle advantage of this approach is the voice quality which is typically much higher than a vocoder-generated product for a given channel bandwidth. Additionally, it operates on far worse channels; noise, multipath, phase distortion, etc. than the digital equivalent encryption system. The degree of security is to a large degree dependent on the level of signal processing and the security of the key stream generator used to set the signal processing's permutation attributes. On one hand, it's extremely difficult to attack the key stream used, particularly if hashing functions are used (that hide the actual key stream output) and the fact that any key stream 'visibility' is very limited. As noted above in the Digital Voice Encryption discussions, this makes a break of the key stream through key analysis extremely improbable.
4. The principle disadvantage of the analog voice encryption technique is in its retention of a finite number of signal permutations. When the number of signal permutations is limited, it may be possible (with a reasonable amount of effort) to achieve some degree of success using signal analysis countermeasures. This approach requires the use of sophisticated signal analysis of the individual encrypted audio segments in an attempt to characterize each to a degree where they can be reconstructed and reorganized in their original orientation and sequential order. However, the ability to reconstruct the signal using brute force methods is

very limited if sophisticated encryption techniques are used, plus the process is too slow to achieve anywhere near real time signal reconstruction. It is therefore an excellent approach for achieving a "tactical" level of voice security, and (depending on the sophistication of signal processing used) can achieve 'strategic' (long term) levels of signal protection.

IV. Voice Circuit Channel Types

A. *Single Channel Full Duplex Encryption*

The most popular application is the secure telephone. It offers end-to-end voice encryption using specialized circuitry and software within the telephone itself. This category of encryption also includes station-to-station voice encryption. It may have the cryptographic device separated from the actual phone instrument by some distance, however, with the advent of microcircuit technology, this approach is not as popular as true end-to-end (phone-to-phone) encryption. The actual method of encryption is typically either analog encryption or digital encryption. Both of these methods will use some sort of Key Generator to produce a secure key stream used by the voice encryptor and decryptor, be it analog encryption or digital encryption.

B. *Multi-channel full duplex*

Multi-channel type systems are often encrypted on a station-to-station basis using digital trunk encryption methods. Analog trunks (frequency division multiplexed, multi-channel voice circuits) are seldom if ever "bulk" encrypted due to the extremely high digital sampling rates required and the complexities involved in producing an acceptable voice quality deciphered signal. Digital voice trunks are often encrypted in the same way as digital data trunks. The architecture of a system dictates where the selected encryption device is placed, typically between the voice channel multiplex/ demultiplex equipment and the communications link, (e.g., radio equipment). As in data bulk encrypted channels, the level of security for station-to-station encryption techniques is a function of the degree of physical security of the individual physical channels between the multiplexer equipment and the individual audio channel, (e.g., telephone) instrument. In general, if you can't guarantee the security of the physical links to the end instruments, you should select end-to-end encryption rather than bulk (trunk) station-to-station encryption.

C. *Single Channel Half Duplex*

These systems are generally found on radio channels with push-to-talk features used to send voice traffic across the radio link. Occasionally, data encryptors are found on radio channels, however, many poor quality, (e.g., long distance HF) radio channels will not support reliable, real-time digitized voice exchanges at rates above 600 bits per second (bps). The audio encoders operating at 600bps are not generally acceptable to users who are used to voice recognition and 'plain mode' voice quality. For this reason, 'analog' voice encryption schemes are generally preferred on poor quality radio channels (and even on noisy, poor quality telephone channels). Another attribute of 'analog' encryptors is that they generally accommodate burst noise and channel fade outs without the problem of 'losing sync' experienced on 'digital' voice encryption products.

V. Cryptography in Mobile network

A. Crypto Phones can be split in two main categories: 2G and 3G.Cryptech 2G phones make use of the GSM standard mobile channel, which means that it establishes the secure connection through a CSD data channel which most mobile operators provide free on their lines.

Fig. 1. Encryption or cryptography in GSM network.

B. Cryptech 3G phones make use of 3rd generation internet mobile connections such as UMTS, GPRS or even WiFi, establishing an encrypted voice connection through a proprietary Internet Data Protocols similar to VoIP (Voice over IP).

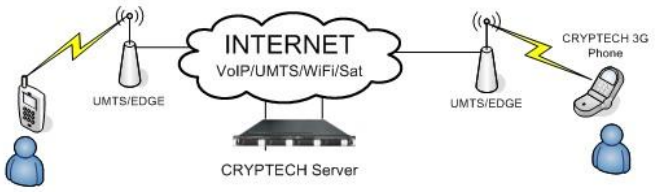

Fig. 2 Encryption or cryptography through internet .

VI. CONCLUSIONS

As outlaid before, encryption often refers to digital technologies, in fact, if you hear about data security and encryption in context with modern technologies, you barely talk about something else but digital encryption. "Digital encryption" can be seen as a much stronger method of protecting speech communications than "analogue scrambling". The big advantage of digital encryption is that it does not matter what kind of signal is encrypted. That makes digital encryption quite powerful because you can create one standard to handle e.g. text, audio, video and every other kind of data. Certainly, digital encryption takes always the same start point, the analogue to digital conversation, however in voice encryption things are a bit different.

ACKNOWLEDGMENT

Firstly, the author is very grateful to Er. Bhupinder singh, Dean Student Welfare, for his support to write this paper.

The author is very thankful to Er. Satinder pal Ahuja, the Head of Department of Compuer science in Indo Global College of Engineering, for his motivation and support during the paper.

REFERENCES

[1] William R. Bennett, (Fellow IEEE); *"Secret Telephony as a Historical Example of Spread-Spectrum Communications,"*IEEE Transactions on Communications, Vol. COM-31, No. 1, January 1983.
[2] D. Minoli and E. Minoli, *Delivering Voice over IP Networks*, New York: John Wiley & Sons, 1998.
[3] Prof. Dr. Heiko Knospe; Script: *„Cryptography" Winter Term 2006/07*; FHCologne
[4] Steven W. Smith; "*The Scientist and Engineer's Guide to Digital SignalProcessing"* copyright ©1997-1998 by. www.DSPguide.com
[5] CES Communications Ltd; „INTRODUCTION TO VOICE SECURITY" http://www.cescomm.co.nz/
[6] http://en.wikipedia.org/wiki/Voice_frequency.