A high grade secure VoIP using the TEA Encryption Algorithm

Ashraf D. Elbayoumy
Advanced Signals Laboratory
School of Engineering Design & Technology
University of Bradford, BD7 1DP, UK
ademahmo@bradford.ac.uk

Simon J. Shepherd
Advanced Signals Laboratory
School of Engineering Design & Technology
University of Bradford, BD7 1DP, UK
S.J.Shepherd@bradford.ac.uk

Abstract: *Unless a VoIP network is encrypted, anyone with physical access to the office LAN can potentially connect network-monitoring tools and tap into telephone conversations. Unfortunately, the price of this security is a decisive drop in QoS caused by a number of factors. In this paper we present the results of the experimental analysis of the transmission of voice over secure communication links. We present an efficient solution for securing VoIP using the TEA Encryption Algorithm.*

Key words: *VoIP, QoS, TEA.*

1. Introduction

The Internet community agrees that security is one of the key properties that should characterize any ICT (Information and Communication Technology) system and application, with particular emphasis on those that rely on the Internet for their nature, e.g., e-commerce. Unfortunately, security does not come for free and, in general, security and efficiency are conflicting requirements. Confidentiality, integrity and authentication can slow down packet transmission, which may not be acceptable by the application itself. Various aspects have to be considered in order to address the problem of real-time transmission over secure channels. The real-time nature of the problem poses some constraints. In the case of voice transmission, the maximum acceptable delay in packet delivery for optimal voice quality is 150ms, which can be extended up to 200ms in case of encrypted communications. Thus, in a standard VoIP application, after the signal has been digitized, there are 150ms to code the signal using some standard scheme such as ITU standards G.723, G.729…etc, divide it into packets and encapsulate the packets into IP packets, then route the packets on the Internet, and reconstruct the original traffic stream at the destination, where it usually is buffered in order to smooth the jitter. Because of such a timing constraints, voice packets are small (10-50 bytes long payload) in order to guarantee that all above mentioned operations can be performed within the given time constraint. There were many experiments to measure the effect of encryption and decryption on throughput [1][2]. Their results showed that the computationally lighter algorithms achieved better throughput than the more expensive ones.

The Tiny Encryption Algorithm is one of the fastest and most efficient cryptographic algorithms in existence. It was developed by David Wheeler and Roger Needham at the Computer Laboratory of Cambridge University. It is a Feistel cipher, which uses operations from mixed (orthogonal) algebraic groups - XOR, ADD and SHIFT in this case. This is a very clever way of providing Shannon's twin properties of *diffusion* and *confusion*, which are necessary for a secure block cipher, without the explicit need for P-boxes and S-boxes respectively. It encrypts 64 data bits at a time using a 128-bit key. In this paper we present the results of the experimental analysis of the transmission of voice over secure communication links. We introduce the TEA encryption algorithm as a faster and powerful algorithm, which gives us the best compromise between security and efficiency. Our results show that using TEA encryption algorithm saves about 20% of the end-to-end delay compared to all available encryption algorithms. This paper is organized as follows; Section 2 presents a quick overview of VoIP. Section 3 presents the Tiny Encryption Algorithm and summaries its security. Section 4 describes the testbed used for our experiments. Section 5 presents the experimental results of using TEA for securing VoIP. Section 6 concludes the paper and summarizes our findings.

2. Voice over IP

In recent years, we have witnessed a growing interest in the transmission of voice using the packet-based protocols. Voice over Internet protocol (VoIP) is a rapidly growing technology that enables the transport of voice over data

networks such as the public Internet. The following steps are performed:

- Digitization of the analog signal;
- Packet generation of the digital signal according to the TCP-UDP/IP protocols;
- Transmission of the packets on the network;
- Packet reception and analog signal reconstruction at the destination.

When sending voice traffic over IP networks, a number of factors contribute to overall voice quality as perceived by an end user. Some of the most important factors are end-to-end delay in the voice carrier path and degraded voice quality. Among the factors that degrade voice quality are packet loss, delay variation, or jitter, voice compression schemes (CODECs), echo cancellation algorithms. In this paper we focus on end-to-end delay and packet loss. Various factors influence signal delay during a VoIP transmission. The time spent by the CODEC, the device that performs the digitization process, may vary between 0.75-30ms, depending on the coding schemes adopted and the quality of the reproduced signal. The queuing delay (i.e., the time spent by a packet in the router buffers waiting for being routed) may add up to 30 ms. A further delay in the range of 40-70ms, called jitter delay, is introduced by buffering arriving packets so that they can be delivered at a uniform rate.

Table 1 reports the number of phone calls (using VoIP) that can be performed with up to date technology given channels with different bandwidth and different payload per packet.

TABLE I. Number of telephone calls and average delay in ms as a function of channel bandwidth (B/W, from 32Kbps to 10 Mbps) and payload size (10,20, and 40 bytes).

	Payload Size					
	10		**20**		**40**	
B/W	***#calls***	***delay***	***#calls***	***delay***	***#calls***	***delay***
32	0	-	0	-	1	>200
64	0	-	1	100-150	2	150-200
128	1	<100	2	~100	4	150-200
256	2	<100	5	~100	9	~150
512	5	<100	10	<100	18	100-150
1024	11	<100	20	<100	36	100-150
10240	117	<100	214	<100	365	~100

Quality of Service is fundamental to the operation of a VoIP network. Despite all the money VoIP can save users and the network elegance it provides, if it cannot deliver at least the same quality of call setup and voice relay functionality and voice quality as a traditional telephone network, then it will provide little added value. Unfortunately, the implementation of various security measures can degrade QoS.

These complications range from delaying or blocking of call setups by firewalls to encryption-produced latency and delay variation (jitter). QoS issues are central to VoIP security. If QoS were assured, then most of the same security measures currently implemented in today's data networks could be used in VoIP networks. But because of the time-critical nature of VoIP, and its low tolerance for disruption and packet loss, many security measures implemented in traditional data networks just aren't applicable to VoIP in their current form.

3. THE TEA ENCRYPTION ALGORITHM

It is a Feistel type routine although addition and subtraction are used as reversible operators rather than XOR. The routine relies on the alternate use of XOR and ADD to provide non-linearity. A dual shift causes all bits of the key and data to be mixed repeatedly. The number of rounds before a single bit change of the data or key has spread very close to 32 is at most six, so sixteen rounds will suffice (although the authors suggest 32!).

The key is set at 128 bits, which is more than enough to prevent brute force attack for the foreseeable future. The top 5 and bottom four bits are probably slightly weaker than the middle bits. These bits are generated from only two versions of z (or y) instead of three, plus the other y or z. Thus the convergence rate to even diffusion is slower. However the shifting evens this out with perhaps a delay of one or two extra cycles.

The key scheduling uses addition, and is applied to the unshifted z rather than the other uses of the key. In some tests $k[0]$ etc. were changed by addition, but this version is simpler and seems as effective. The number delta, derived from the golden number is used where delta = $\left(\sqrt{5}-1\right)2^{31}$.

A different multiple of delta is used in each round so that no bit of the multiple will not change frequently. The algorithm is not very sensitive to the value of delta. It will be noted that delta turns out to be odd with truncation or nearest rounding, so no extra precautions are needed to ensure that all the digits of sum change.

The use of multiplication is an effective mixer, but needs shifts anyway. It was about twice as slow per cycle on our implementation and more complicated. The algorithm will easily translate into assembly code as long as the exclusive or is an operation. The hardware implementation is not difficult, and is of the same order of complexity as DES, taking into account the double length key.

In the last couple of years (X) TEA has been subject to several differential attacks, to which, surprisingly, TEA emerges less vulnerable than XTEA. Moon et al. [3] use impossible differentials to attack 14-round XTEA, requiring $2^{62.5}$ chosen plaintexts and the computation time of 2^{85} encryptions. The equivalent attack on TEA is on 11-rounds and needs $2^{52.5}$ chosen plaintexts and 2^{84} encryptions.

TEA and XTEA are analysed for differential and truncated differential weaknesses in [4]. An ordinary differential attack can break 15 rounds of XTEA with 2^{59} chosen plaintexts. Truncated differentials of probability 1 are used in an attack on 17-round TEA (1920 chosen plaintexts and $2^{123.37}$ time complexity) and 23-round XTEA ($2^{20.55}$ chosen plaintexts and $2^{120.65}$ time complexity).

The best attack to date on XTEA is a related-key differential attack on 27 rounds [5]. The attack requires $2^{20.5}$ chosen-plaintexts under a related key-pair and has a time complexity of $2^{115.15}$ 27-round XTEA encryptions.

4. Experimental Environment

In this section we describe the environment where most of the experiments described in section 5 were performed. An active VoIP QoS measurement is performed with software that simulates VoIP streams between two hosts connected via an IP network. The measurement data consists of a stream transmitted round-trip between two hosts, see "Fig. 1". The stream consists of N packets of size S bytes that are transmitted at intervals of T milliseconds. This is very flexible approach since the parameters S and T can be chosen to correspond to any codec with any packetization scenario.

For example, by choosing S=200 bytes and T=20ms, we can simulate the transmission of G.711 speech data grouped into 20 ms frames, one frame per packet. By virtue of the round-trip test, the measurement simulates a full-duplex VoIP stream on the network level.

The measurement packets are marked with a transmission timestamp and sequence number (TS1, SEQ1) immediately prior to transmission. Once the packets are received by the host, another timestamp and sequence number (TS2, SEQ2) is added to the data packet and it is transmitted back. Upon reception of the packet, the original sender adds a third timestamp (TS3).). Using these data, the round-trip delay of a single packet is computed from the equation:

$$d = \alpha(TS_3 - TS_1) \qquad (1)$$

where α is a scaling factor such that milliseconds result from the computation. Measurement software was implemented with C-language using windows sockets API and run on Pentium II laptops.

Figure 1. Packets are transmitted from Host 1 to Host 2 and back to Host 1.

5. Experimental Results

We now investigate the impact of different encryption algorithms to encrypt the payload on the packet size and the delay. We consider the cryptographic algorithms DES, 3DES, IDEA, TEA (all implemented in software). Our experiments show that the crypto-engine is a serious bottleneck in the transmission of real-time traffic and the best performance is achieved by TEA.

A. Packet size:

Our results show that the impact of different encryption algorithms on the packet size is negligible; especially as the packet size increases. "Fig. 2" shows the percentage increase in packet size as a function of the original packet size for DES, 3DES, IDEA (top line) and for TEA (bottom line).

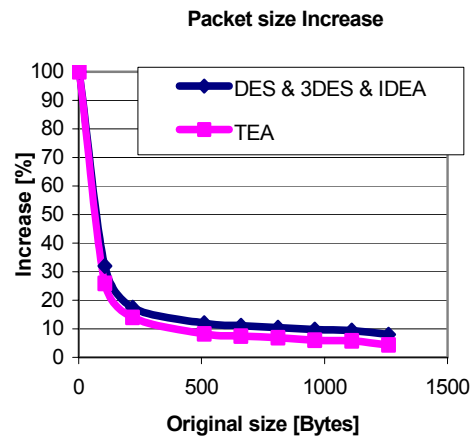

Figure 2. Packet size increase for two sets of cryptographic functions, as a function of packet size in bytes.

The packet size increase has negative effects not only on the bandwidth usage but it also impacts on the transmission delay, router internal delays, queuing delay, thus affecting jitter and overall packet delay.

B. Crypto-engine:

In order to measure the maximum encoding rate, when different algorithms are used, we performed the following experiments. We considered the cryptographic algorithms DES, 3DES, IDEA, TEA (all implemented in software) and for each case we generated 4 packet flows with packets of size 60, 100, 250, 1000 bytes, respectively. Each flow starts from 0 pps and increases its rate of 25 pps every 30 s in order to saturate the crypto-engine. "Fig. 3" graphs the measured throughput as a function of the global traffic flow.

The straight line is the throughput for transmission of packets in the clear, therefore it increases linearly with

traffic. The figure shows that when encryption is performed, throughput levels off or decreases after reaching a maximum value, which depends on the algorithm. It also shows that longer packets significantly improve the crypto-engine performance. The best performance is achieved by TEA, then IDEA, DES, and the last is 3DES.

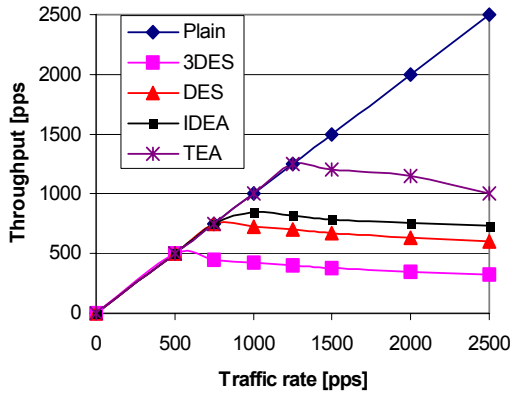

Figure 3. Throughput of the crypto-engine in pps as a function of linearly increasing traffic in pps for plain and encrypted traffic.

The negative slope throughput exhibits after reaching the maximum is due to packets discarded by the engine because it is saturated. Discarded packets contribute to lower the quality of the signal during the reconstruction phase.

In order to evaluate the effect of the payload encryption using different cryptographic algorithms on the end-to-end delay and the QoS degradation we implement the mean opinion score (MOS) test. In voice communications, particularly Internet telephony, MOS provides a numerical measure of the quality of human speech at the destination end of the circuit. The scheme uses subjective tests (opinionated scores) that are mathematically averaged to obtain a quantitative indicator of the system performance. It ranges from 1 to 5, 1 being the worst case. All traffic streams in our test are using G.711 PCM CODEC.

TABLE 2. Different cryptographic algorithms and their MOS.

Encryption Algorithm	MOS
NONE	4.1
DES	3.15
3DES	3.01
TEA	3.5
IDEA	3.25

As Table 2 shows, the best MOS for a secure communication link is in the surroundings of 3.5 and is achieved by the TEA algorithm.

6. Conclusion

Security is a serious bottleneck for the future of VoIP. Because of the time-critical nature of VoIP most of the same security measures currently implemented in today's data networks could not be used in VoIP networks. In this paper we have presented an efficient solution for securing VoIP using the TEA Encryption Algorithm. All our objective and subjective tests show that the best performance of transmitting voice over secure communications links is achieved by TEA.

References

[1] R. Barbieri, D. Bruschi, E. Rosti, "Voice over IPsec: Analysis and Solutions", Computer Security Applications Conference, 2002. Proceedings. 18th Annual, 9-13 Dec. 2002.

[2] O. Elkeelany, Performance "Analysis of IPsec Protocol: Encryption and Authentication", University of Missouri-Kansas City, 2002.

[3] D. Hong, Y. Ko, D. Chang, W. Lee, and J. Lim, "Differentail cryptanalysis of XTEA", Technical Report TR03_13, Center for the Information Security and Technologies (CIST), Seoul, Korea, 2003a.

[4] Y. Ko, S. Hong, W. Lee, S. Lee, and J. Lim, "Related key differential attacks on 26 rounds of XTEA and full rounds of GOST", In Proceedings of FSE '04, Lecture Notes in Computer Science, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004.

[5] D. Moon, K. Hwang, W. Lee, S. Lee, and J. Lim, "Impossible differential cryptanalysis of reduced round XTEA and TEA", Lecture Notes in Computer Science, 2365: 49-60, 2002. ISSN 0302-9743.

[6] M. Marjalaakso, "Security Requirements and Constraints of VoIP", Technical Report, Dept. of Electrical Engineering and Telecommunications, Helsinki University of Technology, 2001.

[7] R. Perlman, "Analysis of the IPsec Key Exchange Standard", Sun Microsystems Laboratories, 2001.

[8] B. Schneier. Applied cryptography: "Protocols, Algorithms, and Source Code in C", John Wiley & Sons, Inc., 2nd Edition, 1996.

[9] U.Black, "Voice over IP", Pretice Hall, 1999.