EVALUATION OF QUALITY AND SECURITY OF A VOIP NETWORK BASED ON ASTERISK AND OpenVPN

Dherik Barison, Rodrigo S. Miani and Leonardo de Souza Mendes
School of Electrical and Computer Engineering (FEEC), State University of Campinas, Campinas, Brazil

Keywords: AES, Asterisk, Blowfish, DES, OpenVPN, Security analysis, VoIP, VoIP security.

Abstract: The proposed work is to verify the performance and security of different cryptographic algorithms in a encrypted VPN (Virtual Private Network), created to provide confidentiality in the network VoIP traffic. The performance tests of the algorithms will occur in various network scenarios, simulating some problems like latency, packet loss, out of order packets, among others. The test architecture consists of: use of the SIPp software for communication between clients, an Asterisk server to intermediate the calls and the OpenVPN software, which will be responsible to create the virtual private network and provide the cryptography necessary for this work.

1 INTRODUCTION

When there is an Asterisk (Digium, 2009) server managing the VoIP (Voice over Internet Protocol) calls in a network, sometimes there is the necessity to create some mechanism that can cipher these VoIP communications, because the data interception is a growing concern (Tanenbaum, 2003), once that VoIP technology expands its participation in the world every year (ITU Telecommunication, 2008). However, there is not an official solution to guarantee confidentiality implemented in Asterisk that would solve the security problem of voice packages interception (VOIP-Info, 2008).

One of the available options is the IPSec (IP Security Protocol) protocol, but IPSec is generally complex to be implemented (Kivinen et al., 2005) (Huttunen et al., 2005). Another option is the use of patches that implement cryptography resources to Asterisk, adding functionalities to support security protocols like ZRTP (Zimmerman Real-time Transport Protocol) (Zimmermann et al., 2009) and MIKEY (Multimedia Internet KEYing) (Ignjatic et al., 2006), for example. But some of these solutions may have problems, because none of them were enough tested with Asterisk to be considered reliable and stable.

To solve this problem, a VPN (Virtual Private Network) can be created using SSL through the OpenVPN (The OpenVPN Project, 2009) software. This option has the advantage of being flexible, independent of specific hardware and having an easy installation and management.

However, ciphering data can lead to side effects in communication. The main of these effects is the degradation of VoIP calls' quality, because the function of encrypting and decrypting data creates more latency in the transmission and can decrease the overall quality of VoIP communication when associated with other network problems. To measure the impact of cryptography in the transmission, one should analyzed which conditions the network needs to offer for an encrypted communication of acceptable quality.

Our intention with this work is to analyze these network conditions in which the encrypted VoIP communication may be deprecated, creating different scenarios of network problems. The collected data in our tests will be studied, and we expect to verify if any of the cryptographic algorithms will have a considerable, or sensible, superior performance when compared to others, which should be enough to maintain an acceptable call quality, and check if some of these algorithms will, in the same network conditions, harm the call quality. We will also focus on the test scenarios and if it is possible to predict the quality of a VoIP call according to network problems and the chosen cryptographic algorithm.

The section 2 brings some works related to our own, involving VoIP, OpenVPN, cryptography and quality measure of VoIP calls. In the section 3 we show the methods adopted to do the tests. In the

S. Miani R., Barison D. and de Souza Mendes L. (2009).
EVALUATION OF QUALITY AND SECURITY OF A VOIP NETWORK BASED ON ASTERISK AND OpenVPN.
In *Proceedings of the International Conference on Security and Cryptography*, pages 144-147
DOI: 10.5220/0002228101440147

subsection 3.1 we explain how the VoIP calls will be made. In the subsection 3.2 we talk about OpenVPN and in the subsection 3.3 we talk about cryptography. In the subsection 3.4 we explain how the analysis of VoIP calls is made with the proposed network scenarios in the section 4. Finally, in the subsection 5, we describe the expected results and the way to analyze it.

2 RELATED WORKS

The proposed work is based in Snyder tests (Snyder, 2008). Snyder analyzed the performance of 10 commercial products that create a SSL VPN to protect the VoIP traffic of the network. We made 4 network scenarios with different problems, checking the behavior of each product in each scenario through of the MOS (Mean Opinion Score) obtained.

Miroslav (Miroslav et al., 2008) analyzes the impact in the quality of VoIP calls when the voice data is encrypted with OpenVPN, observing that when the content of calls are encrypted, the network stays more vulnerable to attacks of deny of service, and the performance of VoIP services decreases.

We may say that in concept our work unites the Snyder's tests with methods and tools used by Miroslav. Getting ourselves closer to Snyder's goals, we will check the behavior of the encryption in different network scenarios.

3 METHODS

Initially, some research has been made to evaluate the available tools on market. The tools were chosen by following some criteria: robustness, available documentation and giving priority to those which are open-source whenever possible.

The choices of used protocols and algorithms were based on that same criteria, prioritizing the most used both commercially and along with desktop users.

3.1 VoIP Calls

To reach the work proposal, a software is necessary to send and receive a phone call. The chosen software to do this job was SIPp (Gayraud et al., 2009).

In order to transmit an audio sample through SIPp an appropriate codec must be chosen. The chosen codec was G.711 A-Law, a standard created by ITU (International Telecommunications Union) and supported by most of VoIP softwares. The choice of the G.711 codec was based in its popularity, because this codec is supported by most VoIP softwares. An interesting feature of this codec is the low necessity of processing, because the voice compression rate done is one of the lowest among all codecs nowadays, resulting in a better quality of the transmission and lower latency (Hersent et al., 2002). But these advantages are obtained by consuming more network bandwidth, because the G.711 uses a transmission rate of 64 kbits/s to send the data voice, while other codecs, like G.729, use just 8 kbits/s.

We also have the server with Asterisk software installed. Asterisk is a PBX (Private Branch eXchange), created by Digium that allows known phones to communicate, sending calls to each other.

3.2 OpenVPN

OpenVPN is a software that has the ability to create a encrypted VPN. For this, OpenVPN supports a range of cryptographic algorithms, once that it uses for this job a library from another software, the OpenSSL. OpenSSL is an open-source implementation of the SSL and TLS (Transport Layer Security) protocols, so supporting many symmetric, asymmetric and hash algorithms. With this available features, OpenVPN is able to offer security for all the data traveling through VPN, not allowing other people to intercept the information transmitted.

Using OpenVPN to protect the communication can cause delays in the communication, because each package needs to be encrypted in the sender and decrypted in the receiver. An expressive delay can be perceived by the receiver, decreasing the quality of communication. Another issue is the package size, because each encrypted package increases in size, increasing the transmission's need for network bandwidth when compared to an unencrypted transmission of the same data.

Thus, for the mentioned reasons, OpenVPN can negatively influence the transmission, especially in VoIP, but that is a side effect of the provided data confidentiality. In this case, it is recommended to anticipate these problems, ensuring that sufficient network bandwidth will be available and calculating the latency in the network in order to know if it will be increased in account of cryptography enough to forbid a VoIP call with acceptable quality. Our work will verify which network conditions will be necessary for the encrypted VoIP transmission to be deprecated in each network scenario, and if some of the algorithms, even in unfavorable conditions, will have a better performance compared to others and also if there will be guarantee to the quality of VoIP transmission.

3.3 Cryptography

As mentioned previously, the cryptography will be done through OpenVPN. There are lots of symmetric algorithms supported by OpenVPN, but we choose only the algorithms that have the most interesting features for our work. The algorithms chosen to cipher the VoIP calls in this work are AES, DES and BlowFish, that were designed to be block cipher algorithms.

3.3.1 AES

The AES (Advanced Encryption Standard) is a block cipher cryptographic algorithm, created by Vincent Rijmen and Joan Daemen for a competition of the United States government in 2001 (NIST, 2001), which proposal was to choose a new cryptographic algorithm to be the new default algorithm of the north-american government to protect secret documents.

In the test scenario proposed, a 128 bits sized key and 2 operations modes for the AES will be used: the CBC (Cipher-block chaining) and CFB (Cipher feedback).

The objective in using two different operation modes for AES is to discover whether there are significant differences in the use of CBC or CFB mode, because in transmissions in which packages are slightly smaller in size, like in a VoIP communication, the tendency is that a block cipher algorithm, using CFB operation mode, will have a better performance when compared with CBC operation mode (Elbayoumy and Shepherd, 2007).

3.3.2 DES

DES is an algorithm created by IBM in 1976 at the request of the United States government, and support keys with only 56 bits long, which can be broken with brute force attack methods. It is also vulnerable to techniques of linear cryptanalysis since 1993 (Matsui, 1994).

Because of the importance of DES in the past, it will be included in the tests to compare it to newer, faster and more secure cryptographic algorithms.

3.3.3 Blowfish

Blowfish was created in 1993 by Bruce Schneier, and it is the default cryptographic algorithm used by OpenVPN. It is an algorithm considered secure because, as the AES, there are no techniques of cryptanalysis effective against it nowadays (RSA Security, 2009). The key size supported by Blowfish corresponds to all multiples of 8 between 32 and 448 bits, thus showing itself a flexible algorithm concerning key size. In the tests a 128 bits key will be used, which is the default key size of this algorithm.

3.4 Analysis of the Call Quality

When making VoIP calls, we need a method to analyze each call and evaluate its quality. To verify the VoIP transmission quality, we will use the ManageEngine VQManager 6 (AdventNet, 2009), a VoIP monitoring software. This software is commercial, but free and totally functional to monitor up to 10 phones/softphones, compatible with SIP and RTP/RTCP, and that will be enough for our work. The ManageEngine VQManager 6 provides details about the voice communications in the network, like jitter, packet loss, latency and informations directly connected to the call quality, like MOS, that is a metric calculated from the network data, which determines the expected VoIP transmission quality.

4 TEST SCENARIOS

The test scenarios will be used to highlight the differences among the cryptographic algorithms. We will create 4 different network scenarios with different network bandwidth with these problems: packet loss, latency, packets out of order and packet duplication. These network anomalies will be created using the Netem (Hemminger, 2005) tool, available for Linux by the collection of utilities called iproute2. The band limitation will be made by TC (Traffic Control) tool, that also part of iproute2.

The 4 scenarios were divided in “bad”, “regular”, “good” and “excellent”, with different features. These features were determined by measurements of the network conditions in hotels, Wi-Fi hot-spots, and others locales (Snyder, 2008). The scenarios are:

- Bad: the band is limited to 0.1Mbps, with 60 milliseconds latency, 20 milliseconds jitter, packet loss of 2%, 1% packets out of order, 1% duplicated packets, and a congestion every 20 seconds of 30% packet loss and 1.000 milliseconds latency;
- Regular: the band is limited to 0.5Mbps, with 60 milliseconds latency, 20 milliseconds jitter, packet loss of 2%, 1% packets out of order, 1% duplicated packages, and a congestion every 20 seconds of 30% packet loss and 1.000 milliseconds latency;
- Good: the band is limited to 0.5Mbps, with 45 milliseconds latency, 10 milliseconds jitter,

packet loss of 0.25%, 1% packets out of order, 1% duplicated packages, and without congestion;

- Excellent: in this scenario we will not introduce any kind of network problem. The network band will be of 100 Mbps without latency, packets loss, fails or congestion.

5 EXPECTED RESULTS

Because of the problems that Asterisk has in ensuring the security of VoIP communication, we thought of the solution as adopting a encrypted virtual private network. However, we do not know exactly what is the impact of each cryptographic algorithm in VoIP communication quality in different network scenarios. Thus, we expect to know by the end of the tests which of the tested cryptographic algorithms will have a superior performance, and will have a sufficient performance to ensure the privacy and quality of the voice communication.

Another goal is to verify how each network scenario, described in section 4, will be behave in the tests. The idea is to adjust the scenario features and to separate a specific set for them, for so we can predict when a communication probably will be deprecated depending on the cryptographic algorithm.

REFERENCES

AdventNet (2009). Manageengine vqmanager. [online] [Accessed 9th February 2009] Available from World Wide Web: http://manageengine.adventnet.com/products/vqmanager/.

Digium (2009). Asterisk. [online] [Accessed 9th February 2009] Available from World Wide Web: http://www.asterisk.org.

Elbayoumy, A. D. and Shepherd, S. J. (2007). Stream or block cipher for securing voip? *International Journal of Network Security*, 5(2):128 – 133.

Gayraud, R., Jacques, O., and contributors (2009). SIPp. [online] [Accessed 10th January 2009] Available from World Wide Web: http://sipp.sourceforge.net/.

Hemminger, S. (2005). Network Emulation with NetEm. In *In the Proceedings of Linux Conference AU*.

Hersent, O., Guine, D., and Petit, J.-P. (2002). *Telefonia IP: Comunicação multimídia baseada em Pacotes*. Addison Wesley, São Paulo, trad. 1 ed. edition.

Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and Stenberg, M. (2005). UDP Encapsulation of IPsec ESP Packets. RFC 3948.

Ignjatic, D., Dondeti, L., Audet, F., and Lin, P. (2006). MIKEY-RSA-R: An Additional Mode of Key Distribution in Multimedia Internet KEYing (MIKEY). RFC 4738.

ITU Telecommunication (2008). European voip market growth: The empire strikes back. [online] [Accessed 9th February 2009] Available from World Wide Web: http://www.itu.int/ITU-D/ict/newslog/European+VoIP+Market+Growth+The+Empire+Strikes+Back.aspx.

Kivinen, T., Swander, B., Huttunen, A., and Volpe, V. (2005). Negotiation of NAT-Traversal in the IKE. RFC 3947.

Matsui, M. (1994). Linear cryptanalysis method for des cipher. In *EUROCRYPT '93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pages 386–397, Secaucus, NJ, USA. Springer-Verlag New York, Inc.

Miroslav, V., Alessandro, R., and Antonio, N. (2008). Performance comparision of secure and insecure voip environments. In *TERENA Networking Conference*.

NIST (2001). Specification for the advanced encryption standard (AES). Federal Information Processing Standards Publication 197.

RSA Security (2009). What are some other block ciphers? [online] [Accessed 15th February 2009] Available from World Wide Web: http://www.rsa.com/rsalabs/node.asp?id=2254.

Snyder, J. (2008). Test shows voip call quality can improve with ssl vpn links. [online] [Accessed 9th February 2009] Available from World Wide Web: http://www.networkworld.com/reviews/2006/022006-ssl-voip-test.html.

Tanenbaum, A. S. (2003). *Network Computers*. Prentice Hall, New Jersey, 4 ed. edition.

The OpenVPN Project (2009). Openvpn. [online] [Accessed 9th February 2009] Available from World Wide Web: http://openvpn.net/.

VOIP-Info (2008). Asterisk encryption. [online] [Accessed 03th March 2009] Available from World Wide Web: http://www.voip-info.org/wiki/view/Asterisk+encryption.

Zimmermann, P., Johnston, A., and Callas, J. (2009). Zrtp: Media path key agreement for secure rtp. Internet-Draft (work in progress).