The Study of Enhancing RTP Security

蕭丞堯、黃培壝

E-mail: 9509674@mail.dyu.edu.tw

ABSTRACT

This paper proposes a technique to improve the security of VoIP. The proposed method applies both the voice sample inter-leaving and the payload encryption to protect the voice content. Because the proposed method slices the digital voice data and rearranging their order according a pseudo random number, the voice is hard to be recognized while they are captured by the third parties. In addition, the payload was encrypted by DES encryption algorithm to prevent the important voice data are vulnerable to Internet hackers. In order to control the delay, the proposed method use 64 bits DES encryption. The double protections make sure that important voice message hard to be eavesdropped. In short, this paper provides a real-time voice data security and packet payload encryption to RTP. The proposed approach is verified by software simulation and statistical measures on a testing voice data. The numeric result shows that it outperforms other methods in delay and security level.

Keywords : VoIP, security, RTP, inter-leaving, DES

Table of Contents

REFERENCES

[1] 陳彥學（2000），“ 資料安全理論與實務 ”，文魁資訊，台北， 初版，頁2-28 – 2-29。

[2] 粘添壽，吳順裕（2004），“ 資訊與網路安全技術 ”，旗標出版 股份有限公司，台北，初版，頁4-22 – 4-25。

[3] 賴溪松，韓亮，張真誠（2003），”近代密碼學及其應用 ”，旗 標出版股份有限公司，初版，頁4-24 – 4-25。

[4] 鍾慶豐（2002），”近代網路安全與編碼機制原理、實作 ”，儒 林圖書有限公司，台北，初版，頁5-34 – 5-35。

[5] Goode, B. （ 2002 ） , Voice over Internet protocol (VoIP), Proceedings of the IEEE, Volume 90, Issue 9, Sept. 2002 Page(s):1495 – 151.

[6] M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman. （2004）, The Secure Real-time Transport Protocol (SRTP), RFC 3711.

[7] Daniel Collins （2003）, Carrier Grade Voice Over IP,second edition, McGraw-Hill Companies, inc, United States. Page(s):3 – 24.

[8] Guo, J.-I.; Yen, J.-C.; Pai, H.-F.（2002）, New voice over Internet protocol technique with hierarchical data security protection, Vision, Image and Signal Processing, IEE Proceedings, Volume 149, Issue 4, Aug. 2002 Page(s):237 – 243.

[9] P. Jones （2001）, US secure Hash Algorithm 1 (SHA1), RFC3174. D. Eastlake, 3rd.

[10] Li, C., Li, S., Zhang, D., Chen, G.,（2006）, Cryptanalysis of a data security protection scheme for VoIP, Vision, Image and Signal Processing, IEE Proceedings, Volume 153, Issue 1, Feb. 2006 Page(s):1 – 10.

[11] Colin Perkins （2003）, RTP: Audio and Video for the Internet, Addison Wesley, Boston. Chapter 13.

[12] Barbieri, R.; Bruschi, D.; Rosti, E. （2002）,Voice over IPsec: analysis and solutions, Computer Security Applications Conference, 2002. Proceedings. 18th Annual, Page(s):261 – 270.

[13] H. Schulzrinne（1996）, RTP Profile for Audio and Video Conferences with Minimal Control, RFC 1890. Audio-Video Transport Working

Group.

[14] H. Schulzrinne, S. Casner R. Frederick and V. Jacobson. （2003）, RTP:A Transport Protocol for Real-Time Applications, RFC 3550.