加強 RTP 協定安全性之探討

蕭丞堯、黃培壎

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

摘 要

本文採用亂序及加密技術來增加網際網路語音服務（Voice over Internet Protocol, VoIP）之安全性，以簡單的運算加強即時傳輸協定 （Real time transport protocol, RTP）的安全性並且在處理速度上有 良好的表現。本文的研究概念是基於即時傳輸協定封包特性作探 討，研究如何加強其安全性。本文所提出對於提升資料安全性的方 法有：採用亂序將原始聲音取樣作群組切割並將順序以不規則的方 式放置，達成將原始語音資料失真的效果，讓竊聽者對資料辨識度 降低；使用DES 加密演算法技術提高封包負載資料的機密性，降 低竊聽風險。採用本方法可以提供即時性的資料安全性以及封包資 料加密。文中將會描述聲音透過此安全性技術所呈現的效果，並且 評估本文所提出的安全性及效率。

關鍵詞 : 網路電話、安全性、即時傳輸協定、亂序、DES 加密演算法

目錄

參考文獻

[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.