第三代行動通訊之安全性研究

薛丁瑋、黃培壎

E-mail: 9607549@mail.dyu.edu.tw

摘 要

使用者身份的隱匿性在UMTS行動網路中，一直是個很重要的研究議題。在UMTS行動網路中，IMSI（International Mobile Subscriber Identity）某些情況下會在無線連結端以明文的方式傳送。也就是說這種作法無法達到對於使用者身份的機密性要求，導致使用者身份會有被竊取與盜用的可能性。為了改善UMTS行動網路架構下使用者身份在某些情況下是以明文的方式傳送，針對這個缺點，在本文中將會提出一個改善使用者身份機密性的方法稱作Integrated Confidentiality Mechanism（ICM）用來克服這個缺點。我們整合RSA公開金鑰加密演算法、MD5演算法等方法而成ICM，利用RSA公開金鑰加密演算法將IMSI加密後傳送，並且利用MD5產生Mobile Ticket來替代原來TMSI（Temporary Mobile Subscriber Identity）的角色。希望能在不需耗費大量計算能力及能量的限制下利用ICM方法達到雙向認證，並使行動用戶在ICM的保護下達成資訊的不可追蹤性及不可辨識性。如此一來可以改善UMTS行動網路中，使用者身份的隱匿性上的缺點提供較好的使用者身份機密性且也不需要大幅度更動UMTS的架構。

關鍵詞 : UMTS，IMSI，RSA公開金鑰加密演算法，TMSI，ICM

目錄

參考文獻

[1] C. J. Mitchell,“ Security for Mobility ”, Publisher: Institute of Electrical Engineers, December 2004 ISBN: 0863413374.

[2] 3rd Generation Partnership Project (3GPP) [Online]. Available: http://www.3gpp.org/ .
[Accessed Nov. 1, 2006].

[3] C. Xenakis and L. Merakos,“ Security in third generation mobile network. ” Computer Communications, vol. 27, no.3, pp. 306-324, Feb. 2006.

[4] G.M. Koien,“ An introduction to access security in UMTS, ” IEEE Wireless Communications, vol. 11, no.1, pp. 8-18, Feb. 2004.

[5] K. Boman, G. Horn, P. Howard, and V. Niemi,“ UMTS security.“ Electronic & Communications Engineering Journal, vol. 14, no. 5, pp. 191-204, Oct. 2002.

[6] 3rd Generation Partnership Project (3Gpp),“ TS33.102-3G security, security architecture V7.0.0 (Release 7), ” Dec. 2005.

[7] D. Kesdogan and C. Palmer,“ Technical challenges of network anonymity, ” Computer Communications, vol. 29, no. 3, pp. 306-324, Feb. 2006.

[8] Barbeau, M.; Robert, J-M.,“ Perfect Identity Concealment in UMTS over Radio Access Links ”, Wireless And Mobile Computing, Networking And Communications, 2005. (WiMob ’ 2005), IEEE International Conference on Vol. 2, 22-24, Page(s):72-77 Aug. 2005.

[9] Sattarzadeh, B.; Asadpour, M.; Jalili, R.,“ Improved User Identity Confidentiality for UMTS Mobile Nerworks, ” Universal Multiservice Networks, 2007. ECUMN ’ 07. Fourth European Conference on Feb. 2007 Page(s):401-409.

[10] C. – S. Park,“ Authentication protocol providing user anonymity and untraceability in wireless mobile communication system, ” Computer

Networks, vol. 44,no. 2, pp. 267-273, Feb. 2004.
[11] A. Menezes, P. van Ooorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
[12] 3rd Generation Partnership Project (3GPP), “ Technical Specification Group Services and System Aspects: Network architecture, Release 6. ” 3GPP TS 23.002 v 6.5.0, 2004.
[13] 3rd Generation Partnership Project (3GPP), “ Technical Specification Group Services and System Aspects: General UMTS architecture, Release 5. ” 3GPP TS 23.101 v 5.0.1, 2003.
[14] 3rd Generation Partnership Project (3GPP), “ Technical Specification Group Services and System Aspects: Numbering, addressing and identification, Release 6. ” 3GPP TS 23.003 v6.4.0, 2004.
[15] 3rd Generation Partnership Project (3GPP), “ Technical Specification Group Services and System Aspects: Organization of subscriber data, Release 6. ” 3GPP TS 23.008 v6.3.0 2004.
[16] Bais, A.; Penzhorn, W.T.; Palensky, P., “ Evaluation of UMTS security architecture and services, ” Industrial Informatics, 2006 IEEE International Conference on Aug. 2006 Page(s):570-575.
[17] B. Vinck, G Horn and K. Muller, “ A viable security architecture for UMTS, ” in ACTS Mobile Summit, Sorrento, Italy, Jun. 1999.
[18] USECA, “ UMTS security architecture AC336/ATEA/WP23/DS/P/08/1, ” USECA project, Deliverable 08, Mar. 2002. [Online]. Available: http://www.isrc.rhul.ac.uk/useca/Deliverables/D08.PDF.
[19] G. M. Koien, “ Privacy enhanced cellular access security, ” in International Conference on Mobile Computing and Networking, Proceedings of the 4th ACM workshop on Wireless security, Cologne, Germany, 2005, pp. 57-66.
[20] G. Godor, B. Varadi and S. Imre, “ Novel authentication algorithm of future networks, ” in International Conference on Networking, International Conference on Systems and International Conference on Mobile Communication and Learning Technologies (ICN/ICONS/MCL ’ 06), IEEE Computer Society, 2006, pp. 80.
[21] http://zh.wikipedia.org/w/index.php?title=RSA&variant=zh-tw [22] http://www.cnblogs.com/anlydo/archive/2005/11/05/269379.aspx [23] http://pwse.kcg.gov.tw/ebook/files/epaper061_3_pa7.doc [24] http://zh.wikipedia.org/wiki/MD5 [25] http://www.encrypter.net/article/encrypt0003.htm [26] http://aflag.77169.com/archives/2005/3049.html