

Study on Security of 3G Mobile System

薛丁璋、黃培壘

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

ABSTRACT

User identity concealment in UMTS mobile networks is an important research topic. Under some situations, the IMSI (International Mobile Subscriber Identity) of an user is conveyed in clear text over the wireless interface in UMTS mobile networks. In another word, UMTS is unable to reach the requirement of user identity confidentiality. The UMTS user's identities are possibly stolen and usurped. In order to improve the problem of user ' s identity that is conveyed in clear text in UMTS mobile networks air interfaces, we introduce a method to improved user's identity confidentiality. The method is called ICM (Integrated Confidentiality Mechanism). We integrated RSA public key encryption algorithm with MD5 algorithm into ICM. In ICM, RSA is applied to IMSI encrypting. ICM also use MD5 to produce MT (Mobile ticket). The MT is used in the subsequence authentication process instead of TMSI (Temporary Mobile Subscriber Identity). ICM method also achieve two-way authentication under the restrictions of lack of great computing capability and energy. ICM make mobile users information to be untraceable and can't be distinguished. ICM improve the concealment of user's identity and offers better user's identity confidentiality. Finally, the cost of ICM is low, because ICM only make a minor change of UMTS mobile networks.

Keywords : UMTS, IMSI, RSA public key cryptography, TMSI, ICM.

Table of Contents

封面內頁 簽名頁 授權書.....	iii	中文摘要.....	iv	ABSTRACT.....	v
誌謝.....	vi	目錄.....	vii	圖目錄.....	ix
表目錄.....	x	第一章 緒論.....	1	1.1 前言.....	1
1.2 研究動機與目的.....	3	1.3 論文架構.....	4	第二章 相關文獻.....	6
2.1 IMSI安全性概述.....	6	2.2 改善IMSI暴露在無線端缺點的方法.....	7	2.2.1 Perfect identity concealment[8].....	7
2.2.2 Improved User Identity Confidentiality[9].....	8	2.3 UMTS架構下的身份認證.....	9	2.4 其他相關討論.....	11
第三章 Integrated Confidentiality Mechanism... ..	13	3.1 加密方式.....	14	3.1.1 RSA公開金鑰加密演算法[21].....	14
3.1.2 IMSI加密.....	15	3.2 Mobile Ticket.....	17	3.2.1 MD5 (Message-Digest Algorithm 5) [24]... ..	17
3.2.2 利用MD5產生Mobile Ticket.....	18	3.3 雙向認證與同步.....	21	第四章 安全性與效能比較.....	24
4.1 加密運算效能.....	24	4.1.1 RSA.....	24	4.1.2 MD5.....	25
4.2 安全性比較.....	26	4.3 效能比較.....	27	第五章 結論.....	29
參考文獻.....	31				

REFERENCES

- [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 Networks, " 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 Oorschot 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/A TEA/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>