Cryptanalysis and Improvement of the Robust User Authentication Scheme for Wireless Sensor Networks

Yung-Cheng Lee[1,*], Hsin-Yu Lai[2] and Pei-Ju Lee[3]

[1]Department of Security Technology and Management, WuFeng University, Chiayi, Taiwan

[2]Graduate School of OptoMechatronics and Materials, WuFeng University, Chiayi, Taiwan

[3]School of Information Science, University of Pittsburgh, 135 N Bellefield, Pittsburgh, PA 15260

Received 25 July 2012; received in revised form 10 September 2012; accepted 08 October 2012

Abstract

Wireless sensor networks are widely used in industrial process control, human health care, environmental control, vehicular tracking and battlefield surveillance, etc. A wireless sensor network consists of lots of sensor nodes and a gateway node. The sensor node usually communicates with the gateway node and users over an ad hoc wireless network. However, due to the open environments, the wireless sensor networks are vulnerable to variety of security threats. Thus, it is a critical issue to adopt a suitable authentication mechanism for wireless sensor networks to enhance security. In 2009, Vaidya et al. proposed a robust user authentication schemes for wireless sensor networks. In this article, we will show that their scheme is vulnerable to the guessing attack and the impersonation attack. Since it needs a secure channel for communications in password changing phase, their scheme is also inconvenient and expensive for users to update passwords. We also propose an improved scheme to remedy the flaws. The improved scheme withstands the replay attack and off-line guessing attack, and the users can freely update their passwords via public channels.

Keywords: wireless sensor networks, authentication, guessing attack, impersonation attack

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “Wireless sensor networks: A survey,” Computer Networks, vol.38, pp.393-422, 2002.

[2] Z. Benenson, N. Gedicke and O. Raivio, “Realizing robust user authentication in sensor networks,” Workshop on Real-World Wireless Sensor Networks (REALWSN 2005), 2005.

[3] C.Y Chong, S. Kumar, “Sensor networks: evolution, opportunities, and challenges,” Proceedings of the IEEE, vol.91, pp.1247-1256, 2003.

[4] M.L. Das, “Two-factor user authentication in wireless sensor network,” IEEE Transaction on Wireless Communications, vol.8, pp.1086-1090, 2009.

[5] L. Lamport, “Password authentication with insecure communication,” Communications of the ACM, vol.24, pp.770-772, 1981.

[6] I. E. Liao, C. C. Lee and M. S. Hwang, “Security enhancement for a dynamic ID-based remote user authentication scheme,” Proceedings of the IEEE International Conference on Next Generation Web Services Practices (NWeSP 2005), 2005, pp.22-26.

[7] K. Martinez, J.K. Hart, R. Ong, “Environmental sensor networks,” IEEE Computer, vol.37, pp.50-56, 2004.

[8] Z. Tan, “Cryptanalysis of a two-factor user authentication scheme in wireless sensor networks,” Advances in Information Sciences and Service Sciences, vol.3, pp.117-126, 2011.

[*] Corresponding author. E-mail address: yclee@wfu.edu.tw
Tel.: +886-5-2267125

[9] H.-R. Tseng, R.-H. Jan and W. Yang, “An improved dynamic user authentication scheme for wireless sensor networks,” Proceedings of the IEEE Global Telecommunications Conference, GLOBECOM '07, 2007, pp.986-990.

[10] B. Vaidya, M. Chen and J.J.P.C. Rodrigues, "Improved robust user authentication scheme for wireless sensor networks," 2009 Fifth IEEE Conference on Wireless Communication and Sensor Networks (WCSN), 2009, pp.1-6.

[11] B Vaidya, J.S. Silva, J.J. Rodrigues, “Robust dynamic user authentication scheme for wireless sensor networks,” Proceedings of the 5th ACM Symposium on QoS and Security for wireless and mobile networks (Q2SWinet 2009), Tenerife, Spain, 2009, pp.88-91.

[12] K.H.M. Wong, Y. Zheng, J. Cao, and S. Wang, “A dynamic user authentication scheme for wireless sensor networks,” Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC’06), vol.1, 2006, pp.318-327.