Ouafi, Khaled; **Overbeck, Raphael**; **Vaudenay, Serge**

On the security of HB$^{\#}$ against a man-in-the-middle attack. (English) Zbl 1206.94084

Pieprzyk, Josef (ed.), Advances in cryptology – ASIACRYPT 2008. 14th international conference on the theory and application of cryptology and information security, Melbourne, Australia, December 7–11, 2008. Proceedings. Berlin: Springer (ISBN 978-3-540-89254-0/pbk). Lecture Notes in Computer Science 5350, 108-124 (2008).

Summary: At EuroCrypt '08, *H. Gilbert, M. J. B. Robshaw* and *Y. Seurin* ["HB$^{\#}$: increasing the security and efficiency of HB^{+}", Lect. Notes Comput. Sci. 4965, 361–378 (2008; Zbl 1149.94334)] proposed HB$^{\#}$ to improve on HB^{+} in terms of transmission cost and security against man-in-the-middle attacks. Although the security of HB$^{\#}$ is formally proven against a certain class of man-in-the-middle adversaries, it is only conjectured for the general case. In this paper, we present a general man-in-the-middle attack against HB$^{\#}$ and Random-HB$^{\#}$, which can also be applied to all anterior HB-like protocols, that recovers the shared secret in 2^{25} or 2^{20} authentication rounds for HB$^{\#}$ and 2^{34} or 2^{28} for Random-HB$^{\#}$, depending on the parameter set. We further show that the asymptotic complexity of our attack is polynomial under some conditions on the parameter set which are met on one of those proposed in [loc. cit.].

For the entire collection see [Zbl 1155.94008].

MSC:

94A60 Cryptography
94A62 Authentication, digital signatures and secret sharing

Keywords:

HB; authentication protocols; RFID

Software:

HB-MP

Full Text: DOI

References:

[1] Berlekamp, E.R., McEliece, R., van Tilborg, H.C.A.: On the inherent intractability of certain coding problems (corresp.). IEEE Transactions on Information Theory˜24(3), 384–386 (1978) · Zbl 0377.94018 · doi:10.1109/TIT.1978.1055873

[2] Bringer, J., Chabanne, H.: Trusted-HB: a low-cost version of HB\ +\ secure against man-in-the-middle attacks. CoRR, abs/0802.0603 (2008) · Zbl 1322.94096

[3] Bringer, J., Chabanne, H., Dottax, E.: HB\ +\ \ +\ : a lightweight authentication protocol secure against some attacks. In: Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2006), Lyon, France, June 29, pp. 28–33. IEEE Computer Society, Los Alamitos (2006) · doi:10.1109/SECPERU.2006.10

[4] Duc, D.N., Kim, K.: Securing HB\ +\ against GRS man-in-the-middle attack. In: Institute of Electronics, Information and Communication Engineers, Symposium on Cryptography and Information Security, Sasebo, Japan, January 23-26, p. 123 (2007)

[5] Erdos, P., Rényi, A.: On two problems of information theory. Publ. Math. Inst. Hung. Acad. Sci.˜8(21), 229–243 (1963)

[6] Gilbert, H., Robshaw, M., Sibert, H.: Active attack against HB\ +\ : a provably secure lightweight authentication protocol. IEEE Electronics Letters˜41(21), 1169–1170 (2005) · doi:10.1049/el:20052622

[7] Gilbert, H., Robshaw, M.J.B., Seurin, Y.: Good variants of HB\ +\ are hard to find. In: Tsudik, G. (ed.) FC 2008. LNCS, vol.˜5143, pp. 156–170. Springer, Heidelberg (2008) · Zbl 1175.94079 · doi:10.1007/978-3-540-85230-8_12

[8] Gilbert, H., Robshaw, M.J.B., Seurin, Y.: HB#: Increasing the security and efficiency of HB\ +\ . In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol.˜4965, pp. 361–378. Springer, Heidelberg (2008) · Zbl 1149.94334 · doi:10.1007/978-3-540-78967-3_21

[9] Gilbert, H., Robshaw, M.J.B., Seurin, Y.: HB#: Increasing the security and efficiency of HB\ +\ , full version. Cryptology ePrint Archive, Report 2008/028 (2008) · Zbl 1149.94334

[10] Hammouri, G., Sunar, B.: PUF-HB: A tamper-resilient HB based authentication protocol. In: Bellovin, S.M., Gennaro, R.,

Keromytis, A.D., Yung, M. (eds.) ACNS 2008. LNCS, vol.˜5037, pp. 346–365. Springer, Heidelberg (2008) · Zbl 05288371 · doi:10.1007/978-3-540-68914-0_21

[11] Hopper, N.J., Blum, M.: Secure human identification protocols. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol.˜2248, pp. 52–66. Springer, Heidelberg (2001) · Zbl 1062.94549 · doi:10.1007/3-540-45682-1_4

[12] Juels, A., Weis, S.A.: Authenticating pervasive devices with human protocols. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol.˜3621, pp. 293–308. Springer, Heidelberg (2005) · Zbl 1145.94470 · doi:10.1007/11535218_18

[13] Katz, J., Shin, J.S.: Parallel and concurrent security of the HB and HB\ +\ protocols. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol.˜4004, pp. 73–87. Springer, Heidelberg (2006) · Zbl 1140.94352 · doi:10.1007/11761679_6

[14] Levieil, É., Fouque, P.-A.: An improved LPN algorithm. In: De Prisco, R., Yung, M. (eds.) SCN 2006. LNCS, vol.˜4116, pp. 348–359. Springer, Heidelberg (2006) · Zbl 1152.94434 · doi:10.1007/11832072_24

[15] Munilla, J., Peinado, A.: HB-MP: A further step in the HB-family of lightweight authentication protocols. Computer Networks˜51(9), 2262–2267 (2007) · Zbl 1118.68015 · doi:10.1016/j.comnet.2007.01.011