Yau, Wei-Chuen; Phan, Raphael C.-W.
Cryptanalysis of a chaotic map-based password-authenticated key agreement protocol using smart cards. (English) Zbl 1345.94090

Summary: Chaotic maps have been applied in the design of authenticated key agreement protocols, which allow communication parties to exchange session keys in an authentic and secure manner. Guo and Chang recently proposed a novel password-authenticated key agreement protocol using smart card based on chaotic maps. They claimed that the protocol achieves the security goal of mutual authentication, as well as other essential security requirements. In this paper, we show that this protocol is susceptible to key-compromise impersonation and parallel session attacks. We also identify two weaknesses in the password change phase of the protocol that leads to authentication with old password and denial of service, respectively.

MSC:
94A60 Cryptography
94A62 Authentication, digital signatures and secret sharing
37E05 Dynamical systems involving maps of the interval
37D45 Strange attractors, chaotic dynamics of systems with hyperbolic behavior
68M10 Network design and communication in computer systems
90B18 Communication networks in operations research

Keywords:
authentication; Chebyshev polynomials; chaotic maps; security

Software:
HMQV

Full Text: DOI

References:
[3] Bellare, M; Pointcheval, D; Rogaway, P; Preneel, B (ed.),Authenticated key exchange secure against dictionary attacks, No. 1807, 139-155, (2000), Berlin · Zbl 1082.94533
[7] Chalkias, K; Baldintesi, F; Hristu-Varsakelis, D; Stephanides, G; Filipe, J (ed.); Obaidat, M (ed.), Two types of key-compromise impersonation attacks against one-pass key establishment protocols, No. 23, 227-238, (2009), Berlin Heidelberg · doi:10.1007/978-3-540-88653-2_7
[11] Dojen, R; Jurcut, A; Coffey, T; Györdi, C; Badica, C (ed.); Mangioni, G (ed.); Carchiolo, V (ed.); Burdescu, DD (ed.), On establishing and fixing a parallel session attack in a security protocol, No. 102, 239-244, (2008), Berlin · Zbl 1188.68070


[36] Phan, RCW; Yao, WC; Goh, BM; Xiong, Y (ed.); Lopez, J (ed.); Wang, H (ed.); Zhou, W (ed.), Analysis of two pairing-based three-party password authenticated key exchange protocols, 102-106, (2009), Gold Coast, Queensland


[40] Sun, DZ; Huai, JP; Sun, JZ; Li, JX; Zhang, JW; Feng, ZY, Improvements of juang ’s password-authenticated key agreement scheme using smart cards, IEEE Trans. Ind. Electron., 56, 2284-2291, (2009) · doi:10.1109/TIE.2009.2016508


Yau, WC; Phan, RCW; Goi, BM; Heng, SH; Lin, D (ed.); Tsudik, G (ed.); Wang, X (ed.), Cryptanalysis of a provably secure cross-realm client-to-client password-authenticated key agreement protocol of CANS '09, No. 7092, 172-184, (2011), Berlin · Zbl 1307.94112


Zhang, Y; Li, C; Li, Q; Zhang, D; Shu, S, Breaking a chaotic image encryption algorithm based on perceptron model, Nonlinear Dyn., 69, 1091-1096, (2012) · Zbl 1254.68118 · doi:10.1007/s11071-012-0329-y


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.