Title (en)

WLAN SESSION MANAGEMENT TECHNIQUES WITH SECURE REKEYING AND LOGOFF

Title (de)

WLAN-SITZUNGSVERWALTUNGSTECHNIKEN MIT SICHEREM REKEYING UND LOGOFF

Title (fr)

TECHNIQUES DE GESTION DE SESSION WLAN AVEC RECHRIFFREMENT SECURISE ET FERMETURE DE SESSION

Publication

EP 1606899 A4 20111102 (EN)

Application

EP 04719770 A 20040311

Priority

- US 2004007403 W 20040311
- US 45454203 P 20030314

Abstract (en)

[origin: WO2004084458A2] The invention provides a method for improving the security of a mobile terminal in a WLAN environment by installing two shared secrets instead of one shared secret, the initial session key, on both the wireless user machine and the WLAN access point during the user authentication phase. One of the shared secrets is used as the initial session key and the other is used as a secure seed. Since the initial authentication is secure, these two keys are not known to a would be hacker. Although the initial session key may eventually be cracked by the would be hacker, the secure seed remains secure as it is not used in any insecure communication.

IPC 1-7

H04H 1/00; H04L 9/00

IPC 8 full level

H04H 20/00 (2008.01); **H04L 9/00** (2006.01); **H04L 9/08** (2006.01); **H04L 9/30** (2006.01); **H04L 9/32** (2006.01); **H04L 12/28** (2006.01); H04L 12/56 (2006.01)

IPC 8 main group level

H04L (2006.01)

CPC (source: EP KR)

H04L 9/0844 (2013.01 - EP KR); **H04L 9/0891** (2013.01 - EP KR); **H04L 9/30** (2013.01 - KR); **H04L 63/0428** (2013.01 - EP KR); **H04L 63/06** (2013.01 - EP KR); **H04W 12/04** (2013.01 - EP KR); **H04W 12/35** (2021.01 - EP); H04L 2209/80 (2013.01 - EP KR); H04L 2463/061 (2013.01 - EP); H04W 12/06 (2013.01 - EP); H04W 84/12 (2013.01 - EP)

Citation (search report)

- [I] SALOWEY CISCO P ERONEN NOKIA J: "EAP Key Derivation for Multiple Applications; draft-salowey-eap-key-deriv-00.txt", IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, 1 February 2003 (2003-02-01), XP015005137, ISSN: 0000-0004
- [A] "An initial Security Analysis of the IEEE 802.1X Standard", 1 January 2002 (2002-01-01), XP055007968, Retrieved from the Internet <URL:http://www.cs.umd.edu/~waa/1x.pdf> [retrieved on 20110923]
- See references of WO 2004084458A2

Designated contracting state (EPC)

DE FR GB IT

DOCDB simple family (publication)

WO 2004084458 A2 20040930; **WO 2004084458 A3 20041118**; CN 1759550 A 20060412; CN 1874222 A 20061206; EP 1606899 A2 20051221; EP 1606899 A4 20111102; JP 2006180561 A 20060706; JP 2006520571 A 20060907; KR 20050116821 A 20051213; KR 20060053003 A 20060519; MX PA05009804 A 20060519; MY 135833 A 20080731

DOCDB simple family (application)

US 2004007403 W 20040311; CN 200480006315 A 20040311; CN 200610092552 A 20040311; EP 04719770 A 20040311; JP 2006077107 A 20060320; JP 2006507069 A 20040311; KR 20057017159 A 20050913; KR 20067005624 A 20060322; MX PA05009804 A 20040311; MY PI20040889 A 20040313