References

[1] IEEE, “LAN MAN Standards of the IEEE Computer Society. Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specification. IEEE Standard 802.11, 1997 Edition”, 1997.

[2] IEEE, “LAN MAN Standards of the IEEE Computer Society. Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specification (2.4 GHz). IEEE Standard 802.11g”, 2003.

[3] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.

[4] The AirSnort project homepage, 2002. http://airsnort.sourceforge.net.

[5] IEEE 802.11 Wireless Local Area Networks: The working group for WLAN standards. Available homepage from http://grouper.ieee.org/groups/802/11/, 2003.

[6] IEEE, “LAN MAN Standards of the IEEE Computer Society. Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specification for enhanced security. IEEE Unproved Draft P802.11i/D3.0”, 2003.

[7] IEEE, “Standard for Local and Metropolitan Area Networks: Standard for Port-Based Network Access Control. IEEE Standard 802.1x”, March 2001.

[8] A. Wool, “Lightweight Key Management for IEEE 802.11 Wireless LANs with Key Refresh and Host Revocation”, IEEE 802.11 TGi Working Group, July 2002.

[9] N. Shankar, W.A. Arbaugh, and K. Zhang, “A Transparent Key Management Scheme for Wireless LANs Using DHCP”, Tech. Rep. HPL-2001-227, HP Laboratories, 2001.

[10] G. Schafer, M. Eyrich, “A Simple Key Distribution Method for IEEE 802.11 Encryption Keys”, In Proc. Workshop on Mobile Communication over Wireless LAN: Research and Applications, Vienna, Austria, September 2001.

[11] R.L. Rivest, "The RC4 encryption algorithm", RSA Data Security Inc., (proprietary), March 1992.

[12] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, Internet Engineering Task Force(IETF), October 1999.

[13] C. Rigney and et. al, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, Internet Engineering Task Force(IETF), April 1997.

[14] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, Internet Engineering Task Force(IETF), March 1998.

[15] W. Simpson, "The Point-to-Point Protocol (PPP)", RFC 1661, Internet Engineering Task Force(IETF), July 1994.

[16] W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, Internet Engineering Task Force(IETF), August 1996.

[17] R. Rivest, "The MD5 Message-Digest Algorithm", RFC 1321, Internet Engineering Task Force(IETF), April 1992.

[18] N. Haller, C. Metz, "A One-Time Password System", RFC 1938, Internet Engineering Task Force(IETF), May 1996.

[19] T. Dierks, C. Allen, "The TLS Protocol Version 1.0", RFC 2246, Internet Engineering Task Force(IETF), January 1999.

[20] Federal Information Processing Standards (FIPS) Publication 197, "Specification for the Advanced Encryption Standard (AES)", National Institute of Standards and Technology (NIST), US Department of Commerce, Washington D.C., November 2001.

[21] R. Rivest, "The MD4 Message-Digest Algorithm", RFC 1320, Internet Engineering Task Force(IETF), April 1992.

[22] Federal Information Processing Standards (FIPS) Publication 180-1, "Secure Hash Standard", National Institute of Standards and Technology (NIST), US Department of Commerce, Washington D.C., April 1995.

[23] A. Stubblefield, J. Ioannidis, and A. D. Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP", In Proc. 9th Network and Distributed System Security Symposium (NDSS '02), The Internet Society, 2002.

[24] The OpenSSL project homepage, 2003. http://www.openssl.org.

[25] T. H. Cormen, C. E. Leiserson, and R. L. Rivest, "Introduction To Algorithms", pages 834-836. MIT Press, Massachusetts Institute of Technology, Cambridge, Massachusetts, 1996.