REFERENCES

[1] David Chadwick, "Smartcards Aren't Always The Smart Choice", *IEEE Computer*, December 1999, pp 142-143.

[2] Sharath Pankanti, Ruud M. Bolle and Anil Jain, "Biometrics: The Future of Identification", *Computer Magazine*, February 2000.

[3] Shari Lawrence Pfleeger, "Software Engineering: Theory and Practice", Prentice-Hall International, Inc., 1998.

[4] B. Schneier, "Applied Cryptography Second Edition", John Wiley & Sons, 1996.

[5] L. Gong, M.Lomas, R. Needham, and J. Saltzer, "Protecting Poorly Chosen Secrets From Guessing Attacks", *IEEE Journal on Selected Area in Communication*, vol. 11, no. 5, pp. 648-656, June 1993.

[6] Y. Ding and P. Hoster, "Undetectable On-Line Password Guessing Attacks", *ACM Operating Systems Review*, vol. 29, no. 77-86, Oct. 1995.

[7] RSA Laboratories.
http://www.rsa.com/rsalabs/

[8] Edmund Muth and Unrisky, "Security on the web", Microsoft Security Advisor.
http://www.microsoft.com/security

[9] J.J. Quisquater and L. Guillou, "How to explain zero-knowledge protocols to your children", *In Advances in Cryptology Crypto '89*, pages 628-631, Springer-Verlag, 1990.

[10] RFC2617, HTTP Authentication: Basic and Digest Access Authentication.

[11] Introduction to IIS 5.0 features.
http://www.microsoft.com/windows/server/ Overview/features/web.asp

[12] Bobn M. Bellovin and Michael Merritt, "Limitations of the Kerberos Authentication System", *USENIX*, Winter '91.

[13] Sarvar Patel and Bellcore, "Number Theoretic Attacks On Secure Password Schemes." *IEEE*, 1997.

[14] S. M. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks", *Proceedings of the IEEE. Symposium on Research in Security and Privacy,* Oakland, May 1992.

[15] S. M. Bellovin and M. Merritt, "Augmented Encrypted Key Exchange: a Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise", AT&T Bell Laboratories (c. 1994).

[16] L. Gong, M. Lomas, R. Needham, & J. Saltzer, "Protecting Poorly Chosen Secrets from Guessing Attacks", *IEEE. Journal on Selected Areas in Communications*, Vol. 11, No. 5, June 1993, pp. 648-656.

[17] L. Gong, "Optimal Authentication Protocols Resistant to Password Guessing Attacks", *Proceedings of the 8th IEEE Computer Security Foundations Workshop*, County Kerry, Ireland, June 1995, pp. 24-29.

[18] M. Steiner, G. Tsudik, and M. Waidner, "Refinement and Extension of Encrypted Key Exchange", *Operating Systems Review*, vol. 29, Iss. 3, pp. 22-30 (July 1995).

[19] Thomas Wu, The Secure Remote Password Protocol, "Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium", San Diego, March 1998, pp. 97-111.

[20] Berners-Lee, T., Fielding, R. and H. Frystyk, "Hypertext Transfer Protocol -- HTTP/1.0", *RFC 1945*, May 1996.

[21] Fielding, R., Gettys, J., Mogul, J., Frysyk, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", *RFC 2616*, June 1999.

[22] PKI - PC Webopaedia Definitions and Links.
http://webopedia.internet.com/TERM/P/PKI.html

[23] Government Information Technology Services, Federal Public key Infrastructure.
http://gits-sec.treas.gov/fpki.htm

[24] NIST Public key Infrastructure Program.
http://csrc.ncsl.nist.gov/pki/

[25] The Government of Canada Public key Infrastructure.
http://www.cse.dnd.ca/cse/english/gov.html

[26] The Open Group Public key Infrastructure, Latest Proposals for an HMG PKI.
http://www.opengroup.org/public/tech/security/pki/cki/

[27] Public key Infrastructure (X.509) (PKIX) working group.
http://www.ietf.org/html.charters/pkix-charter.html

[28] Simple Public key Infrastructure (SPKI) working group.
http://www.ietf.org/html.charters/spki-charter.html

[29] The Open Group Public key Infrastructure.
http://www.opengroup.org/security/pki/

[30] What Is...a PKI (public key infrastructure) (a definition)
http://www.whatis.com/pki.htm

[31] VeriSign's Global Affiliate Services
http://www.verisign.com/

[32] E. Rescorla, A. Schiffman, "The Secure HyperText Transfer Protocol (SHTTP)", INTERNET-DRAFT, *Web Transaction Security Working,* May 1996
ftp://www.ripe.net/internet-drafts/draft-ietf-wts-shttp-02.txt

[33] SSL-Talk FAQ.
http://www.consensus.com/security/ssl-talk-faq.html

[34] F. Bergadano, B. Crispo and M. Lomas, "Strong Authentication and Privacy with Standard Browsers."
http://maga.di.unito.it/security/projects/protected/www2/node14.html

[35] R. Morris and K. Thompson, "Password Security: A Case History", *Commmunicatioin of the ACM*, vol.22, no.11, pp 594-597, Nov 1979.

[36] Simple Digest Security Scheme.
http://www.w3.org/Protocols/HTTP/digest_specification.html

[37] W. Diffie abd M.E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, v. IT-22, n. 6, Nov 1976, pp. 644-654.

[38] J. Steiner, B. C. Neuman, and J.I. Schiller, "Kerberos: An authentication service for open network systems", in *Proc. Winter USENIX Conference*, (Dallas), 1988.

[39] D. Jablon, "Strong Password-Only Authenticated Key Exchange", *Computer Communication Review*, vol. 26, no. 5, pp. 5-26, October 1996.

[40] P. C. van Oorschot, M. J. Wiener, "On Diffie-Hellman Key Agreement with Short Exponents", *Proceedings of Eurocrypt '96*, Springer-Verlag, May 1996.

[41] Security Dynamics Ltd.
http://www.securitydynamics.com

[42] Haller, N., and R. Atkinson, "On Internet Authentication", *RFC 1704*, Bell Communications Research and Naval Research Laboratory, October 1994.

[43] Haller, N., "The S/KEY One-Time Password System", *RFC 1760*, February 1995

[44] Lamport, L., "Password Authentication with Insecure Communication", *Communications of the ACM 24.11*, November 1981, 770-772.

[45] European Committee for Banking Standards, "Biometrics: A Snapshot of Current Activity", November 1996.

[46] SAC Technology's Ltd.
http://www.sacman.com/biometrics_explained

[47] Tim Hudson, "SSLeay FAQ".
http://www.psy.uq.oz.au/~ftp/Crypto

[48] Integrity Sciences Ltd.
http://www.IntegritySciences.com

[49] SSLeay
http://www.rsasecurity.com/products/bsafe/sslc.html

[50] Warwick Ford, "Computer Communications Security", Prentice Hall, pp 109-147.

[51] About password.
http://www.webdon.com/vitas/psw.htm

[52] Carl Ellison and Bruce Schneier, "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure".
http://www.counterpane.com

[53] H. Krawczyk, M. Bellare, and R. Canetti, "RFC 2104: HMAC: Keyed-Hashing for Message Authentication", IETF, February 1997.

[54] B. Kaliski, editor, "PKCS #5 v2.0: Password-Based Cryptography Standard, RSA Laboratories", Second Draft, December 10, 1998.

[55] J. Tardo & K. Alagappan, "SPX: Global authentication using public key certificates", Proceedings of I.E.E.E. Computer Society Symposium on Research in Security and Privacy, Oakland, pp. 232-244, May 1991.

[56] C. Ellison, "Establishing Identity Without Certification Authorities", Proceedings of the Sixth Annual USENIX Security Symposium, San Jose, July 1996, pp. 67-76.

[57] What Is...bootstrapping (a definition). *http://www.whatis.com/bootstrapping.htm*

[58] W. Richard Stevens, "UNIX Network Programming Volume 1", Prentice-Hall International, Inc., Second Edition, 1998.

[59] J. Reynolds and J. Postel, "RFC1700: Assigned Numbers", October 1994.

[60] Stefan Lucks, "Open Key Exchange: How to Defeat dictionary attacks without encrypting public keys", The Security Protocol Workshop '97, Ecole Normale Superieure, April 7-9, 1997.

[61] Simple Nomad, "The Hack FAQ", September 6, 1999.

[62] Chris Mitchell, "Identity verification". *http://isg.rhbnc.ac.uk/cjm/Chris_Mitchell.htm*

[63] Gary McGraw, "Smartcards, Java cards and security", developer.com journal: tech focus, January 19, 1998.

[64] Ross Anderson and Markus Kuhn, "Tamper Resistance - a Cautionary Note", The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18-21, 1996, pp 1-11.

[65] J. Wray, "RFC 1509: Generic Security Service API: C-bindings", Digital Equipment Corporation, September 1993.

[66] Jim Kerstetter, "Entrust, VeriSign clear path to PKI", PC Week Online, June 14, 1999.

[67] David Clark, "Toward a New Generation of Simpler PCs", Computer Magazine, December 1999, pp 17-19.

[68] S. Bradner, "RFC 2026: The Internet Standards Process -- Revision 3", Harvard University, October 1996.