PASSWORD-BASED AUTHENTICATION IN WIRELESS LAN

GAN HOCK LAI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Electrical Engineering

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

DECEMBER 2005

To my beloved parents

ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to my research supervisors, P.M. Muhamad Mun'im b. Ahmad Zabidi and Dr. Sulaiman b. Mohd. Nor, for their support and guidance throughout the years.

I also like to thank my mentor, Mr. Thong Foo Hong, and Intel Communication Group Penang for the financial support.

Thanks to the Open Source Software development communities especially to Jouni Malinen, Alan DeKok, Tom Wu, James Carlson and Nick L. Petroni, my achievements would not have been possible without these OSS contributors. I would never forget to thank Taekyoung Kwon, the AMP password protocol designer, for the tips and tricks to implement the protocol.

Finally, I am grateful to my family and friends for the love and support they have given to me.

ABSTRACT

Authentication in wireless LAN can prevent unauthorized parties from gaining access to the network. Preliminary authentication mechanism specified in IEEE 802.11 standard was compromised as the consequence of WEP vulnerabilities. Thus, the wireless LAN enhanced security task group and IETF have introduced the IEEE 802.1X port based network access control and Extensible Authentication Protocol (EAP) to secure wireless LAN authentication session. Re-authentication is another critical issue when a supplicant roams to the neighbouring access point. To retain secure communication session and especially in real time applications, the handoff process must be done within the specified time defined by ITU [50]. The objective of the research is two fields; to propose a password-based public key authentication method and to refine the roaming key management in Inter Access Point Protocol (IAPP) with proactive caching approach for fast and secure handoff process. The proposed authentication method fulfills the mandatory requirements of EAP method for wireless LAN [29]. The authentication methods are compared from the aspects of performance, security and usability. Compared to pre-authentication and proactive key distribution method, the refinement on handoff method provides comparable performance and security with lower computational cost. An experimental test bed was setup to compare the efficiency of the proposed authentication method. The result shows that the proposed authentication execution can be completed at 295ms compared to existing methods like TLS which needs over 1000ms. For handoff process, the result still could not meet the time constraint due to the research scope is only covered roaming key management. Besides, password-based authentication method is inherently ease to deploy, manage and is user friendly.

ABSTRAK

Pengesahan pada LAN wayarles boleh menghalang pihak penceroboh dari mendapat capaian ke rangkaian. Mekanisma pengesahan terdahulu yang dispesifikasi dalam piawaian IEEE 802.11 telah dikompromi akibat kelemahan WEP. Maka, kumpulan kerja keselamatan LAN wayarles dan IETF telah memperkenalkan IEEE 802.1X, kawalan capaian rangkaian berasaskan port dan protokol pengesahan lanjutan (EAP) untuk melindungi sesi pengesahan LAN. Pengesahan semula adalah isu kritikal apabila pengguna membuat perayauan ke titik capaian yang berjiranan. Untuk mengekalkan keselamatan sesi komunikasi dan terutamanya dalam aplikasi masa nyata, proses serahan mesti siap dalam masa yang dicadangkan oleh ITU [50]. Objektif penyelidikan adalah dua bahagian; untuk memperkenalkan satu kaedah pengesahan kata laluan kekunci awam dan untuk memperbaiki pengurusan kekunci pemantauan dalam protokol inter titik capaian (IAPP) dengan cara sorokon proaktif [55] bagi proses serahan yang pantas dan selamat. Kaedah pengesahan yang diperkenalkan memenuhi keperluan mandatori kaedah EAP untuk LAN wayarles [29]. Kaedah-kaedah pengesahan telah dibandingkan berdasarkan aspek prestasi, keselamatan dan kebolehgunaannya. Dibandingkan dengan kaedah pengesahan terdahulu and kaedah taburan kunci proaktif, kaedah serahan yang diperbaiki memberi prestasi dan keselamatan yang setara dengan kos pengiraan yang rendah. Satu ujian bereksperimen telah dijalankan untuk membandingkan kecekapan kaedah pengesahan yang dicadangkan. Keputusan menunjukkan bahawa perlaksanaan pengesahan yang dicadangkan dapat disiapkan dalam masa 295ms berbanding dengan kaedah yang telah ada seperti TLS yang memerlukan lebih daripada 1000ms. Bagi proses serahan, keputusan masih tidak dapat mencapai kekangan masa itu disebabkan oleh skop penyelidikan hanya merangkumi pengurusan kekunci pemantauan sahaja. Selain daripada itu, kaedah pengesahan berasakan kata laluan adalah sangat mudah diguna, diurus dan juga mesra pengguna.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AAA	-	Authentication, Authorization and Accounting
ACK	-	Acknowledgement packet
AES	-	Advance Encryption System
AH	-	Authentication Header
AMP	-	Authentication via Memorable Password (algorithm)
AMSK	-	Application MSK
AP	-	Access Point
AS	-	Authentication Server
AuthA	-	A password-based authentication key exchange algorithm
AVP	-	Attribute-Values Pairs
BSS	-	Basic Service Set
CA	-	Certificate Authority
CCM	-	Counter mode with Cipher-block chaining - Message authentication code
CCMP	-	CCM Protocol
c-DLSE	-	Discrete Logarithm with Short c-Bit Exponents
CDMA	-	Code Division Multiple Access
CHAP	-	Challenge Handshake Authentication Protocol
CF	-	Contention Free
CTS	-	Clear To Send
DIAMETER	-	an AAA protocol
DER	-	Distinguished Encoding Rules
DES	-	Data Encryption Standard
DHCP	-	Dynamic Host Configuration Protocol
DL	-	Discrete Logarithm
DLAMP	-	AMP in DL setting
DS	-	Distribution System

DSA	-	Digital Signature Algorithm
EAP	-	Extensible Authentication Protocol
EAPoL	-	EAP over LAN
EC	-	Elliptic Curve
ECAMP	-	AMP in Elliptic Curve setting
ECC	-	Elliptic Curve Cryptography
ECDL	-	Elliptic Curve Discrete Logarithm
ECDSA	-	Elliptic Curve Digital Signature Algorithm
ECES	-	Elliptic Curve Encryption Scheme
EKE	-	Encrypted Key Exchange
EMSK	-	Extended Master Session Key
EPS	-	Exponential Password Suite
ESP	-	Encapsulating Security Protocol
ESS	-	Extended Service Set
FAST	-	Flexible Authentication via Secure Tunnel
FIPS	-	Federal Information Processing Standard
GF	-	Galois Field
GRE	-	Generic Routing Encapsulation
GSM	-	Global System for Mobile communication
GTK	-	Group Transient Key
GTKSA	-	Group Transient Key Security Association
GTC	-	Generic Token Card
HMAC	-	keying Hash function for MAC
IAPP	-	Inter Access Point Protocol
IBSS	-	Independent Basic Service Set
ICMP	-	Internet Control Message Protocol
ICV	-	Integrity Check Vector
IEEE	-	Institute of Electrical and Electronics Engineers
IETF	-	Internet Engineering Task Force
IF	-	Integer Factorization
IKE	-	Internet Key Exchange protocol
IP	-	Internet Protocol
IPSec	-	Internet Protocol Security
ISM	-	Instrumentation, Science and Medical

ISO	-	International Standard Organization
ITU	-	International Telecommunication Union
IV	-	Initialization Vector
KCK	-	Key Confirmation Key
KDF	-	Key Derivation Function
KEK	-	Key Encryption Key
L2TP	-	Layer 2 Tunneling Protocol
LAN	-	Local Area Network
LEAP	-	Lightweight EAP
MAC	-	Message Authentication Code
MD4	-	Message Digest 4 standard
MD5	-	Message Digest 5 standard
MIB	-	Management Information Base
MIC	-	Message Integrity Code
MIMO	-	Multi Input Multi Output
MIPS	-	Million Instructions Per Second
MK	-	Master Key
MGF	-	Mask Generation Function
MPM	-	Multiple Precision Multiplication
MPPE	-	Microsoft Point-to-Point Encryption
MSCHAP	-	Microsoft CHAP
MS-CHAPv2	-	Microsoft CHAP version 2
MSB	-	Most Significant Bit
MSK	-	Master Session Key
NAS	-	Network Access Server
OFDM	-	Orthogonal Frequency Division Multiplexing
OSI	-	Open System Interconnection
OTP	-	One-Time Password
PAC	-	Protected Access Credential
PAK	-	Password-Authenticated Key exchange (algorithm)
PAKE	-	Password-Authenticated Key Exchange
PAP	-	Password Authentication Protocol
PC	-	Personal Computer
PEAP	-	Protected EAP

PEKM	-	Post EAP Key Management
PEM	-	Privacy Enhanced Mail
PEPKGP	-	Password Entangled Public Key Generation Primitive
PKGP	-	Public Key Generation Primitive
PKI	-	Public Key Infrastructure
PMK	-	Pairwise Master Key
PMKID	-	PMK Identification
PMKSA	-	Pairwise Master Key Security Association
PPP	-	Point-to-Point Protocol
PPTP	-	Point-to-Point Tunneling Protocol
PRF	-	Pseudo-Random Function
PRNG	-	Pseudo-Random Number Generator
PTK	-	Pair-wise Transient Key
PTKSA	-	Pairwise Transient Key Security Association
PUB	-	Publication
PVDGP	-	Password Verification Data Generation Primitive
RADIUS	-	Remote Access Dial-In User Service
RC4	-	Ron Rivest cipher 4
REDP	-	Random Element Derivation Primitive
RFC	-	Request For Comment Internet standard
RK	-	Roaming Key
RSA	-	Rivest-Shamir-Adleman algorithm
RSN	-	Robust Security Network
RTS	-	Request To Send
SHA	-	Secure Hashing Algorithm
SIM	-	Subscriber Identification Module
SNAPI	-	Secure Network Authentication with Password Identification (algorithm)
SNMP	-	Simple Network Management Protocol
SOHO	-	Small Office Home Office
SPEKE	-	Simple Password Exponential Key Exchange
SRP	-	Secure Remote Password
SSID	-	Service Set Identity
SSL	-	Secure Socket Layer

STA	-	wireless Station
STAKeySA	-	Station Key Security Association
SVDP	-	Secret Value Derivation Primitive
TA	-	Transmitter Address
TK	-	Temporal Key
TKIP	-	Temporal Key Integrity Protocol
TLS	-	Transport Layer Security
TTLS	-	Tunneled TLS
TSC	-	TKIP Sequence Counter
TTAK	-	TKIP-mixed Transmit Address and Key
UMTS	-	Universal Mobile Telecommunication System
VoIP	-	Voice over IP
VPN	-	Virtual Private Network
WEP	-	Wired Equivalent Privacy
Wi-Fi	-	Wireless Fidelity
WLAN	-	Wireless Local Area Network
WPA	-	Wi-Fi Protected Access

LIST OF SYMBOLS

a, b	-	Two elliptic curve coefficients
c	-	Length of coverage overlapping region
D	-	Diameter of access point coverage
E	-	An EC defined by two elliptic curve coefficients, a and b
$\#E$	-	Number of points in elliptic curve E
g	-	Element of multiplicative order q in $GF(p)$
g_{p-1}	-	An element of multiplicative order $p-1$ in $GF(p)$
$GF(p)$	-	The Galois Field of order p
$G(x,y)$	-	Point of order q on E over $GF(p)$
id	-	Identity
k	-	A cofactor that is either the value p-1/q in DL domain parameters or the value of $\#E/q$ in EC domain parameters
k_1, k_2	-	Key confirmation data
L	-	Computational Load
p	-	A prime number and the desired field size
q	-	A prime divisor of p-1 and the order of desired group
sk	-	Mutually derived session Key
T	-	Latency
v	-	Password derived data
v	-	Velocity of wireless station
π	-	Hash product of password
x	-	Client Private Key
X	-	Client Public Key
γ	-	Password derived data from Random Element Derivation Primitives
y	-	Server Private Key
Y	-	Server Public Key

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background

1.1.1 Wireless LAN

IEEE 802 community introduced the IEEE 802.11 wireless LAN standard in 1997. The emergence of the standard has taken place over the conventional HiperLAN and HomeRF implementation, which also utilized the same spectrum of 2.4GHz and 5GHz unlicensed ISM band. Throughout these years, wireless LAN technology has gained popularity that can be seen in the incredible growth in wireless LAN products. With the guidance of Wi-Fi Alliance, manufacturers are competing in this industry to produce standard Wi-Fi complaint devices from chipsets to end products like client adaptors and access points.

The major benefits of wireless LAN technology is flexibility and mobility. Wireless LAN plays an important role to support some real time applications like Voice over IP (VoIP) in lowering cost and providing higher data throughput. Therefore, evolution of this famous technology is in a rapid progress since it still lacks flexibility and mobility especially in the area of wireless authentication for fast and secure roaming. Currently, wireless LAN technology allows roaming with security disabled. If the security is enabled, mobility is restricted within a Basic Service Set (BSS). When moving away into Extended Service Set (ESS) or to inter ESS, time critical application will suffer from packets drop or even disconnection during the roaming process.

In this thesis, the performance and security problems are described, and the existing and proposed solution are introduced and partially implemented. The thesis evaluates the performance and security of common Extensible Authentication Protocol (EAP) methods and handoff process. It provides wireless implementor a reference to deploy the wireless LAN authentication securely and the handoff process efficiently.

1.1.2 Authentication Technology

Authentication means proving an instance to be genuine. In network security, authentication serves two purposes; to identify between communication parties and to validate originality of data. The process is a lot easier when performed in the real world, where our senses can directly interact with the instance. In virtual network environment, only streams of data are presented to the authenticator.

Authentication is held when the prover asserts his identity using some facts or secret piece of knowledge shared with the authenticator. There are various instances and techniques to prove or identify the assertion of peer identity. The most common authentication instances of human presence are password. When technology evolves, several instances emerged, for example digital certificate, smart card and biometrics.

Techniques of authentication are even designed and developed in a great number of ways. It is based on the ways to apply the cryptography with the instance. For example, challenge handshake authentication protocol (CHAP) schemes, which have been used since earlier 1980's, are hash of password together with random challenge.

Authentication in wireless LAN is a mandatory process. Besides proving the identity of both ends (mutual authentication between client and authentication server), a shared key is generated to protect subsequent communication sessions. However, as stated in security techniques of IEEE 802.11 standard [1] called Wired Equivalent Privacy (WEP), authentication implemented in data link layer with two modes (Open

system authentication and shared key authentication), has been seriously compromised. This is due to implementing authentication only in data link layer without invocation from upper layer, and due to this limitation, the algorithm was unprofessionally designed. Because of the security flaws in authentication algorithm, the security task group has redesigned the algorithm for implementation of IEEE 802.1X standard [2] and Extensible Authentication Protocol (EAP) [3].

1.2 Problem Statement

The WEP protocol is intended to provide data privacy and authenticity for IEEE 802.11 wireless local area network (WLAN) standard. However, improper implementations of the WEP in WLAN have led to this algorithm open to a wide variety of attacks.

The IEEE 802.11i standard [4] has provided a guideline on how to adopt the higher layer authentication and key management schemes. With the flexibility of EAP, proprietary authentication methods has been introduced and implemented, but some of the method like Challenge Handshake Authentication Protocol (CHAP) did not address the limitation of implementing such schemes in wireless environment. This may lead to the implementation vulnerable to attacks or compromising the performance. This is especially when only human memorable password is only used in authenticating server and client. The authentication method must take into consideration dictionary attacks, online guessing attacks or the disclosure of server's password file. Furthermore, the certificate based authentication like Transport Layer Security [30, 31, 36] is hardly deployed. It is also incumbent end users to check the validity of certificate. Certificate based authentication authenticates the certificate holder and not the user itself. In other word, stolen certificate with private key allows the thief impersonating the certificate holder. Token based authentication methods like SecurID [69] would probably increase the cost of security investment, because token card (smart card) and reader devices are expensive. It is not practicable in public wireless LAN when portability is required.

Roaming is another issue that gradually gains attention from wireless communities where implementation for the security as well as the performance must be taken into account. ITU [50] has recommended the handoff latency must less than 50ms in order to provide seamless roaming for real-time connection oriented application. By using current wireless LAN devices, this figure is not achievable because latency is mainly contributed by the station scanning phase. Latency in re-authentication phase can be avoided by employing a pre-authentication which is defined in IEEE 802.11i standard [4]. However, this method overloads the authentication server resource that has to handle enormous pre-authentication request. The existing proprietary solution achieves the desired performance but needs addition of roaming server to be implemented.

Based on the above, the identified problems can be defined as follows:

i) Deployment and management of the existing authentication methods (certificate based and token based) are very cumbersome.
ii) There is lack of strong password-only method for EAP authentication in wireless LAN. Although there are about forty EAP methods, some of the password-only methods are not safe to use as standalone method [5], while others are related to the issue of intellectual property and patent restriction.
iii) Pre-authentication method highly loads the authentication server resource. Other solutions like Cisco Centralized Key Management (CCKM) [70] need extra network infrastructure.

1.3 Objectives of Research

Based on the above problems, the objectives of research are:

i) Study the existing security implementations and its' performance impact on wireless LAN.
ii) Propose a more secure and better performance password-based authentication algorithm.

iii) Propose a more secure and lightweight wireless LAN handoff method.

iv) Implement and evaluate the performance of authentication algorithm and wireless LAN handoff method.

1.4 Scope of Work

The research scope is focused on:

i) Development of the password-based authentication method on top of EAP used in communication between wireless client and authentication server.

ii) Linux operating system will become the platform for the authentication algorithm (software) implementation, where open source software FreeRADIUS, HostAP, xsupplicant and wpa_supplicant is deployed to be the authentication server, access point and wireless client respectively.

iii) Security of authentication methods is evaluated based on the known threats in wireless LAN.

iv) Performance of authentication methods is evaluated and compared through implementation and theory.

v) Optimization of handoff process is based on Inter Access Point Protocol (IAPP) by introducing extra key management technique.

vi) The handoff process is just a theoretical proposal.

1.5 Research Contributions

The contributions of this research are identified as:

1. *Enriching the study of security and performance of common authentication methods and the proposed password-based authentication.*

2. *Implementation of a proposed password-based authentication as an EAP method.*
3. *A study of security and performance of handoff technique.*

1.6 Thesis Outline

This thesis presents the latest wireless LAN security technology, from conceptual theory to a practical implementation. Two main contribution areas, authentication and handoff, are emphasized throughout the thesis.

In chapter 1, the latest evolution in wireless technologies is described. The problems of current wireless LAN technology, which led to the motivation of this research, are also presented. Research objectives, scope of work and area of contribution are stated.

Chapter 2 describes current status of wireless LAN security in details. This includes information about amendments by the standard body on wireless LAN standard, brief explanation on previous standard, the main security flaws in the previous standard and brief overview on new wireless LAN security standard. Other security mechanism is also explained briefly. Later in the chapter, how public key cryptography is used in conjunction with password authentication and key agreement, and application of concept of Zero Knowledge Password Proof are discussed.

Chapter 3 explains and compares the authentication methods from various aspects. At the beginning of this chapter, the aims and goals of choosing an authentication method are defined, where three main aspects are considered. Existing and the proposed authentication methods are described in details in the last section. Their advantage and disadvantage compared with the proposed method are discussed and summarized.

Chapter 4 contains the answers on performance and security requirements in the wireless LAN handoff process. Comparison on a few existing techniques used to

achieve the goals is made according to the handoff latency, security strength and hardware processing power consumption. The thesis introduces an enhanced version to the existing technique by using extra key management process during full authentication phase. However this is a theoretical proposal. Implementation of the handoff technique is based on the standard recommendation. The result aids to obtain an estimated value of the proposed technique.

Chapter 5 illustrates the project implementation. The components and configuration of the test bed is demonstrated. It proceeds to discuss the research methodology and project execution. Finally, method of data collection and the results is shown with the relevant discussion.

Chapter 6 summarizes and concludes the research. It concludes the security strength of the proposed authentication method, and the need of future maintenance and management for client and server. It also discusses the remaining security issues that may lead to security breach. The thesis suggests the alignment with pre-release standards to enable interoperability in future work. Additional network infrastructure like user database must be supplemented to RADIUS server as the path to build a comprehensive network.

enrollment session. Moreover, security practice recommends that STA should validate the domain parameters received on every authentication session although it is a set static of value.

Third, a more complete framework should be defined to integrate other password-based authentication (proposed to IEEE P1363.2 standard) as the EAP methods. This option increase the flexibility and availability of the provided EAP authentication services in AS. For further optimization on the performance of IEEE 802.1x authentication, it is suggested to implement 3-Pass AMP protocol and SRP6 protocol (with optimized message ordering) that take advantage from fewer protocol steps. Enhancement on coding of the authentication algorithm with pre-computation ability will also decrease the latency.

REFERENCE

[1] Institute of Electrical and Electronics Engineers (1997), *Wireless LAN Medium Access Control and Physical Layer Specifications*, IEEE Std 802.11-1997.

[2] Institute of Electrical and Electronics Engineers (2001), *Port-based Network Access Control*, IEEE Std 802.1X-2001.

[3] Internet Engineering Task Force (1998), *PPP Extensible Authentication Protocol (EAP)*, RFC 2284.

[4] Institute of Electrical and Electronics Engineers (2004), *Wireless LAN Medium Access Control and Physical Layer Specifications (Amendment 6: Medium Access Control Security Enhancements)*, IEEE Std 802.11i-2004.

[5] Internet Engineering Task Force (2004), *Extensible Authentication Protocol (EAP)*, RFC 3748 (obsoletes RFC 2284).

[6] S.Fluhrer, I.Mantin and A.Shamir (2001), *Weaknesses in the Key Scheduling Algorithm of RC4*, SAC'2001.

[7] S.Fluhrer, I.Mantin and A.Shamir (2002), *Attacks on RC4 and WEP*.

[8] M. Bellare, D. Pointcheval, P. Rogaway (2000), *Authenticated Key Exchange Secure against Dictionary Attacks*, Advances in Cryptography – Eurocrypt 2000 Proceedings, Lecture Notes in Computer Science Vol. 1807.

[9] J.Carlson, B. Aboba, H. Haverinen (July 2001), *EAP SRP-SHA1 Authentication Protocol (draft-ietf-pppext-eap-srp-03.txt)*, Network Working Group, Internet Draft.

[10] William Stallings (2003), *Cryptography and Network Security: Principles and Practice*, third edition, Prentice Hall.

[11] Arunesh Mishra, William A. Arbaugh (6 Feb 2002), *An Initial Security Analysis of the IEEE 802.1x standard*, University of Maryland.

[12] Bruce Schneier (1996), *Applied Cryptography second edition: protocol, algorithm and source code*, John Wiley & Sons Inc.

[13] Stephanie Delaune, Florent Jacquemard (2004), *A Theory of Dictionary Attack and its Complexity*, France telecommunication R&D.

[14] C.P. Schorr (1991), *Efficient Signature Generation for Smart Card*, journal of cryptology, vol. 4, n. 3, 161-174.

[15] Victor Boyko, Philip MacKenzie, Sarvar Patel (14-18 May 2000), *Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman*, Advance in Cryptography – EUROCRYPT 2000, Preneel, B., (Ed.).

[16] Philip MacKenzie, Ram Swaminathan (30 July 1999), *Secure Network Authentication with Password Identification*, Submission to IEEE P1363a.

[17] Mihir Bellare, Philip Rogaway (14 March 2000), *The AuthA Protocol for Password-Based Authenticated Key Exchange*, Contribution to IEEE P1363.

[18] Thomas Wu (11 November 1997), *The Secure Remote Password Protocol*, Computer Science Department Stanford University.

[19] Taekyoung Kwon (November 2003), *Summary of AMP (Authentication and key agreement via Memorable Passwords)*, Revised submission to IEEE P1363.2, submission to IEEE P1363 Working Group.

[20] Philip MacKenzie (19 July 2001), *On the Security of the SPEKE Password-Authenticated Key Exchange Protocol*, Cryptology ePrint Achieve: Report 2001/057.

[21] Internet Engineering Task Force (1998), *PPP Challenge Handshake Authentication Protocol (CHAP)*, RFC 1994.

[22] S. Bellovin, M. Merritt (1992), *Encrypted Key Exchange: Password-based Protocols Secure Against Dictionary Attacks*, ACM/IEEE Symposium on Research in Security and Privacy.

[23] Oded Goldreich (3 December 2002), *Zero Knowledge Twenty Years after Its Invention*, Department of Computer Science and Applied Mathematics Weizmann Institute of Science, Rehovot, Israel.

[24] National Institute of Standards of Technology (NIST), Federal Information Processing Standard Publication (FIPS) (27 January 2000), *Digital Signature Standard (DSS)*, FIPS PUB 186-2.

[25] Taekyoung Kwon (May 2000), *Ultimate Solution to Authentication via Memorable Password*, Contribution to the IEEE P1363 study group for Future PKC Standard.

[26] Taekyoung Kwon (2003), *Practical Authenticated Key Agreement using Password*, School of Computer Engineering, Sejong University, Seoul Korea.

[27] Taekyoung Kwon (2004), *Addendum to Summary of AMP (Authentication and key agreement via Memorable Passwords)*, Revised submission to IEEE P1363.2, submission to IEEE P1363 Working Group.

[28] Internet Engineering Task Force (2000), *The SRP Authentication and Key Exchange System*, RFC 2945.

[29] Dorothy Stanley, Jesse Walker and Bernard Aboba (10 August 2004), *EAP methods requirement for Wireless LANs (draft-walker-ieee802-req-04.txt)*, Network Working Group, Internet Draft.

[30] Internet Engineering Task Force (1999), *The TLS Protocol*, RFC 2246.

[31] Internet Engineering Task Force (1999), *Transport Layer Security (TLS) Extensions*, RFC 3546.

[32] Ashwin Palekar *et al*. (15 October 2004), *Protected EAP Protocol (PEAP) version 2 (draft-josefsson-pppext-eap-tls-eap-10.txt)*, EAP Working Group, INTERNET-DRAFT.

[33] H. Andersson *et al.* (23 February 2002), *Protected EAP Protocol (PEAP) (draft-josefsson-pppext-eap-tls-eap-02.txt)*, PPPEXT Working Group, INTERNET-DRAFT.

[34] Paul Funk *et al.* (October 2004), *TLS Inner Application Extension (TLS/IA) (draft-funk-tls-inner-application-extension-00.txt)*, TLS Working Group, Internet-Draft.

[35] Paul Funk *et al.* (April 2004), *EAP Tunneled TLS Authentication Protocol (EAP-TTLS) (draft-ietf-pppext-eap-ttls-04.txt)*, PPPEXT Working Group, Internet-Draft.

[36] Internet Engineering Task Force (October 1999), *PPP EAP TLS Authentication Protocol*, RFC 2716.

[37] Internet Engineering Task Force (1992), *PPP Authentication Protocols*, RFC 1334.

[38] Internet Engineering Task Force (1996), *PPP Challenge Handshake Authentication Protocol (CHAP)*, RFC 1994.

[39] Internet Engineering Task Force (2000), *Microsoft PPP CHAP Extensions*, Version 2, RFC 2759.

[40] Institute of Electrical and Electronics Engineers (2004), *Draft Standard Specifications for Password-based Public Key Cryptographic Techniques*, IEEE P1363.2.

[41] International Standard Organization (November 2003), *Information technology – Security techniques - Key management - Part 4: Mechanisms based on weak secrets*, ISO/IEC 3rd WD 11770-4.

[42] Internet Engineering Task Force (June 2000), *Remote Authentication Dial In User Service (RADIUS)*, RFC 2865.

[43] D. Taylor, T. Wu and T. Perrin, *Using SRP for TLS Authentication (draft-ietf-tls-srp-05)*, TLS working group, Internet Draft, October 2003.

[44] B. Aboba *et al.* (November 2004), *Extensible Authentication Protocol (EAP) Key Management Framework (draft-ietf-eap-keying-04.txt)*, EAP Working Group, Internet Draft.

[45] E. Rescorla (March 2004), *A Survey of Authentication Mechanisms (draft-iab-auth-mech-03.txt)*, Internet Draft.

[46] Joshua Wright (2003), *Weaknesses in LEAP Challenge/Response (asleap)*, Defcon.

[47] Internet Engineering Task Force (April 2004), *Determining Strength For Public Keys Used For Exchanging Symmetric Keys*, RFC 3766.

[48] T. Wu (October 2002), *SRP6: Improvements and Refinements to the Secure Remote Password Protocol*, Arcot System.

[49] R. Gennaro (August 2000), *An Improved Pseudo-Random Generator Based on the Discrete Logarithm Problem*, IBM T.J. Watson Research Center.

[50] International Telecommunication Union (1988), *General Characteristic of International Telephone Connections and International Telephone Circuit*, ITU-TG.114.

[51] N. Cam-Winget *et al.* (February 2004), *EAP Flexible Authentication via Secure Tunneling (EAP-FAST) (draft-cam-winget-eap-fast-00.txt)*, Internet Draft.

[52] Internet Engineering Task Force (March 2001), *Microsoft Point-To-Point Encryption (MPPE) Protocol*, RFC 3078.

[53] A. Mishra, M. Shin and W. A. Arbaugh (January 2003), *Proactive Key Distribution to support fast and secure roaming*, IEEE 802.11-03/084-r1.

[54] B. Aboba (2003), *Fast Handoff Issues*, IEEE 802.11-03/115r0.

[55] Institute of Electrical and Electronics Engineers (2003), *IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation*, IEEE Std 802.11F-2003.

[56] W.A.Arbaugh and B. Aboba (October 2003), *Handoff Extension to RADIUS (draft-irtf-aaaarch-handoff-04.txt)*, Internet Draft.

[57] R. Moskowitz (May 2003), *PMK Plumbing for Fast Roaming via the Neighborhood Graph*, IEEE 802.11-03/411r2.

[58] B. Aboba and D. Simon (March 2003), *EAP Keying Framework (draft-aboba-pppext-key-problem-06.txt)*, Internet Draft.

[59] J. Walker and E. Qi (May 2004), *Pre-Keying*, IEEE 802.11-04/0476r0.

[60] B. Aboba and D. Harkins (2004), *Post-EAP Key Management Protocol (PEKM)*, IEEE 802.11-04/1186r0.

[61] Institute of Electrical and Electronics Engineers (July 2003), *Draft Standard Specifications for Public Key Cryptography – Amendment 1: Additional Techniques*, IEEE P1363a/D12.

[62] Institute of Electrical and Electronics Engineers (2000), *Standard Specifications for Public Key Cryptography*, IEEE P1363.

[63] S. Goldwasser and M. Bellare (August 2001), *Lecture Notes on Cryptography*, Cambridge, Massachusetts.

[64] B. Aboba *et al.*, (March 2004), *Thinking About the Site Report*, IEEE 802.11-04/0412r0.

[65] B. Aboba, D. Stanley and J. Walker (November 2004), *802.11 Keying Requirements*, IEEE 802.11-04/1498r0.

[66] Internet Engineering Task Force (September 2003), *RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)*, RFC 3579.

[67] Internet Engineering Task Force (September 2003), *Diameter Base Protocol*, RFC 3588.

[68] Internet Engineering Task Force (September 1993), *The Kerberos Network Authentication Service (V5)*, RFC 1510.

[69] Internet Engineering Task Force (April 2000), *The SecurID® SASL mechanism*, RFC 2808.

[70] Bruce McMurdo (2004), *Cisco Fast Secure Roaming,* Cisco Aironet 350 Application Note*,* Cisco Systems, Inc.

[71] J. Edney and W. A. Arbaugh (2003), *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, Addison-Wesley Professional.

[72] J. McGregor (2004), *The weakest link*, DNS Ltd: white paper.

[73] Interlink Network, Inc (2003), *EAP Methods for Wireless Authentication*, ItPapers: white paper.

[74] D.V. Bailey *et al.* (August 1999), *Cryptography in Modern Systems*, WPI-ECE Department and DSP R&D Center, Texas Intrument Inc.

[75] D. Boneh and H. Shacham, Fast Variants of RSA, CryptoBytes RSA Laboratories, 2002 Vol 5, No 1, Page 1-28.