AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
ELECTRONICSAND COMMUNICATION DEPARTMENT

Authentication Schemes for Wireless Local Area Networks

A thesis submitted in partial fulfillment of the requirement of the
Ph.D. in Electrical Engineering

By
Ahmed Mettwally AbdElwahed Elnagar
M.Sc. Oct. 2001

Supervised by
Prof. Dr. Adel Ezat Elhenawy
Dr. Ahmed Aly AbdElhafez

Cairo-(2013)

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING

Authentication Schemes for Wireless Local Area Networks

A thesis submitted in partial fulfillment of the requirement of the degree of the
Ph.D. in Electrical Engineering

By
Ahmed Mettwally AbdElwahed Elnagar
M.Sc., in Electrical Engineering
Military Technical Collage –Egyptian Armed Force

EXAMINERS COMMITTEE

Name	**Signature**
Prof. Dr. Adel Ezat Elhenawy	**( )**
Prof. Dr. Elsayed Mostafa Saad	**( )**
Prof. Dr. Mohamed Hassan Abd Elazeem	**( )**
Prof. Dr. Ahmed Aly Abd Elhafez	**( )**

Date: / /

Statement of Original Authorship

This thesis is submitted as a partial fulfillment of Ph.D.degree in electrical engineering, Faculty of Engineering,Ain Shams University.

The author carried out the work included in this thesis , and no part of it has been submitted for a degree or qualification at any other scientific entity .

Signature:

Student name: Ahmed Mettwally AbdElwahed Elnagar

Researcher Data

Name:Ahmed Mettwally Abd Elwahed Elnagar

Date of birth:29/2/1968

Place of birth: Cairo

Academic degree:M.Sc.

Field of specialization: Communication

University issued the decree:Military Technical Collage –Egyptian Armed Force

Date of issuing degree: Oct 2001

Current job:Eng. Col. –Egyptian Armed Force

Abstract

The security has become an important issue in IEEE 802.11 Wireless Local Area Networks (WLANs) and it is always a major concern for their development and those networks based on wireless technology therefore as their security measures increase, the tools and techniques used to attack them from any third party also increase.

WLANs are facing numerous problems linked to security threat issue from the point of view of Authentication, Confidentiality, Data integrity, and Anonymity, which expose legitimate users to several risks. This research addresses the authentication process for wireless Local Area networks, specifically Wi-Fi networks, while other security processes are not within the scope of this research .

The authentication aspect is one of the major challenges in WLAN security issues that proves the identity of a certain entity requesting access to a network to reduce the possibility of illegitimate users to hijack the target network via impersonating a false identity. The 802.1X is a standard securing protocol of the IEEE that acts as an authentication framework for Wi-Fi networks. It's based on the Extensible Authentication Protocol (EAP) protocol and its deployed method.

EAP is a general authentication protocol, it has been widely used for that important aspect, which acts as an envelope consisting of different types of authentication methods that support various authentication procedures. The EAP defines several types of authentication methods for Wi-Fi networks, which can be classified into three categories: Secret-key method (E.g. EAP-MD5, EAP-LEAP), Public-key method (E.g. EAP-TLS), and Tunneled method (E.g. EAP-TTLS, EAP-PEAP).

The Goal of this research is to analyze and show up the flaw of the existing EAP methods and identifying new generic EAP authentication methods. Forward one called EAP-Moderate Weight Extensible Authentication Protocol (EAP-MEAP) belongs to a secret-key methods category, while the later one called EAP- Moderate Transport Layer Security Protocol (EAP-MTLS) belongs to a Public-key methods category according to the classification criteria of this research.

These two generic EAP authentication methods enhanced and developed into several variant forms to satisfy the authentication requirements and they have a proper structure to be implemented and efficient for IEEE802.11WLANs (Wi-Fi and its application domains) as a solution to mitigate and overcome those presented flaws based on their properties. Finally, we have checked and verified the EAP- MEAP

security properties using the specialized model checker AVISPA, which provides formal proofs of the security protocols.

Key Words

Wireless network, WLAN Authentication protocols, EAP Methods, HLPSL, EAP-MEAP ,AVISPA, SPAN,EAP-MTLS, EAP-TLS, LEAP,WLAN Threats, CAS+.

ACKNOWLEDGMENTS

I would like to thank my supervisor Prof. Dr. ADEL ELHENAWY for his guidances and advices, and most of all, his felicitous direction that I should research on authentication protocols for wireless local area networks, before that I was obsessed with the cryptographic algorithms study. It was truly the correct decision for my research and has led me to achieve the result in this thesis.

I would also like to offer my heartfelt thanks to my associate supervisor Dr. AHMED A. ABD EL-HAFEZ. He consistently and kindly guided me; he did not draw my rein but brought me up to develop my ideas with passion and inspiration.

Great thanks to my two parents, my dead father was my tutor and gave me a steady support in the early stage of my PhD course, my mother was encouraging me and always gives me energetic advices throughout my PhD research.

I would also like to present my heartfelt thanks to my associate brother for his strong support when I need.

Final thanks go to my wife for her understanding and encouragement, who helped me through many tough times, also my two sons with an ever-bright smile on their faces encouraged and helped me when I was struggling with my stressful last year.

List of Abbreviations

3G	Third Generation Mobile Phone Network.
A5/1, 2, 3	Encryption Algorithms.
AAA server	Authentication Authorization and Accounting server.
ACK	Acknowledgement.
AES	Advanced Encryption System.
AP	Access Point.
AS	Authentication Server.
AVISPA	Automated Validation of Internet Security Protocols and Applications.
BSS	Basic Service set.
BSSID	BSS Identifier.
CAs	Certification Authorities.
CAS+	Protocols Specifying Language.
CBC-CTR mode	Cipher Block Chaining- Counter mode
CBC-MAC	Cipher Block Chaining -Message Authentication Code.
CCK	Complementary Code Keying modulation .
CCMP	Counter-mode/CBC-MAC Protocol.
CF	Coordination Function .
CIA	Confidentiality, Integrity and Authenticity.
CL-AtSe	Constraint-Logic-based Attack Searcher .
CRC-32	Cycle Redundancy Check 32.
CSMA- CA	Carrier Sense Multiple Access- Collision

	Avoidance.
CSMA-CD	Carrier Sense Multiple Access- Collision Detection.
CTR mode	Counter mode .
CTS	Clear To Send.
DCF	Distributed Co-ordination Function .
DFS	Dynamic Frequency Selection.
DHCP	Dynamic Host Configuration Protocol.
DLL	Data Link Layer .
DOS	Denial of Service.
DS	Distribution System .
DSL	Digital Subscriber Line.
DSS	Distribution System Services .
DSSS	DirectSequence Spread Spectrum
EAP	Extensible Authentication Protocol.
EAP-LEAP	EAP-Light Weight Extensible Authentication Protocol.
EAP-MD5	EAP- Message Digest- 5.
EAP-MEAP	EAP-Moderate Weight Extensible Authentication Protocol
EAP-MTLS	EAP- Moderate Transport Layer Security.
EAPOL	EAP over LAN.
EAP-PEAP	EAP-Protected Extensible Authentication Protocol.
EAP-TLS	EAP- Transport Layer Security.

EAP-TTLS	EAP-Tunneled Transport Layer Security.
EDCA	Enhanced Distributed Channel Access.
EDGE	Enhanced Data rates for GSM Evolution.
ESS	Extended Service Set.
FCC	Federal Communications Commission.
FIFO	First-In First-Out
FTP	File Transfer Protocol .
GPRS	General Packet Radio Service.
GSM	Global System for Mobile.
HCCA	HCF Controlled Channel Access.
HCF	Hybrid Coordination Function.
HLPSL	High Level Protocols Specification Language.
HLPSL2IF	High Level Protocols Specification Language To Intermidiate Formate.
HSDPA	High Speed Downlink Packet Access.
HTTP	Hypertext Transfer Protocol .
IAPP	Inter Access Point Protocol .
IBSS	Independent BSS .
IEEE	Institute of Electrical and Electronics Engineers.
IEEE 802.11	WLAN standard defined by the IEEE.
IEEE 802.1X	WLAN securing standard defined by the IEEE .
IEEE802. 11	WLAN(Wi-Fi) standard defined by the IEEE.
IETF	Internet Engineers Task Force .
IF	Intermediate Format .
IPSec	Internet Protocol Security.

IR	Infrared.
ISM	Industrial, Scientific and Medical Band.
IV	Initialization Vector.
Kc	Dynamic Shard Secret Key .
Kc new	New Dynamic Shard Secret Key.
Ke	Session Encryption Key.
Ke new	New Session Encryption Key.
Ks	Pre-Shard Static Secret Key .
LAN	Local Area Network.
LBT	Listening Before Talking .
LLC	Logical Link Control .
MAC	Message Authentication Code.
MAC address	Media Access Control address.
MAC layer	Medium Access Control layer.
MIC	Message Integrity Code.
MIMO	Multiple Input Multiple Output.
MIS	Management Information Systems.
MITM attack	Man-In-The-Middle attack
MPDUs	MAC frames/packet data units.
MSC	Message Sequence Charts .
MSCHAP	Microsoft Challenge Handshake Authentication Protocol .
MSCHAP2	Microsoft Challenge Handshake Authentication Protocol version 2.
MSDU	MAC Service Data Unit

OFDM	Orthogonal Frequency Division Multiplexing.
OFMC	On-the-Fly Model-Checker
OSA	Open System Authentication.
PAE	Port Access Entity .
PBCC	Packet Binary Convolutional Coding modulation.
PBNAC	Port-Based Network Access Control
PCF	Point Coordination Function.
PDA	Personal Digital Assistant .
PHY	Physical Layer.
PIN	Personal Identification Number.
PLCP	Physical Layer Convergence Procedure Sublayer .
PMD	Physical Medium Dependent Sublayer.
POP3	Post Office Protocol 3.
PRNG	Pseudo Random Number Generator.
PSK	Pre-Shared Key.
QoS	Quality of Service .
RADIUS	Remote Authentication Dial In User Service.
RC4 algorithm	Rivest Cipher 4 algorithm.
RF	Radio Frequency.
Rn	Special Random Number.
Rn new	New Special Random Number.
RSA algorithm	Ron **R**ivest , Adi **S**hamir, and Leonard **A**dleman algorithm.
RNS	Robust Network Security .
RTS	Request To Send.

S, C	Challenge Random Number Pairs .
SATMC	SAT-based Model-Checker.
SID	Session Identify.
SIM	Subscriber Identity Module.
SKA	Shared Key Authentication.
SML	Simple Method LAN.
SMTP	Simple Mail Transfer Protocol.
SNR	Signal-to-noise ratio.
SPAN	Security Protocol Animator for AVISPA.
SS	Station Services .
SSID	Service Set Identifier
SSL protocol	Secure Socket Layer protocol'
STAs	Wireless Stations.
TA4SP	A tree Automata tool based on Automatic Approximations for the Analysis Of Security Protocols .
TKIP	Temporal Key Integrity Protocol .
TLA	Temporal Logic of Actions .
TPC	Transmission Power Control .
UMTS	Universal Mobile Telecommunications System.
U-NII	Unlicensed National Information Infrastructure Band
VoIP	Voice over IP.
VPN	Virtual Private Network.
VSAT	Very Small Aperture Terminal.

WEP	Wired Equivalent Privacy.
Wi- Fi	Wireless Fidelity Network
Wi- MAX	Worldwide Interoperability- Microwave Access
WLAN	Wireless Local Area Networks.
WPA	Wi-Fi Protected Access.
WPA2	Wi-Fi Protected Access 2.

List of Tables