A FORMAL FRAMEWORK FOR SECURITY ANALYSIS OF WPA2 PROTOCOL

A thesis submitted in partial fulfilment of the requirements for the degree of Master of Science in Information Security

By:

Asma Abdulmonem Abdullah Terkawi

[Master degree, Naif Arab University, 2019]

Under Supervision of:

Dr.Nisreen Mohammed Innab

Submitted to:

department of Information Security, Computer and Information Security College
Naif Arab University for Security Sciences

May 2019

إطار رسمي للتحليل الأمني لبروتوكول WPA٢

إعداد

أسماء عبد المنعم عبد الله تركاوي

إشراف

د. نسرين محمد عناب

رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في أمن الحاسب والمعلومات

قسم أمن المعلومات

الرياض
١٤٤٠هـ ٢٠١٩م

Table of Contents

List of Figures

List of Abbreviations

IEEE	Institute of Electrical and Electronics Engineers.
WLAN	Wireless Local Area Network.
Pre-RSNA	Pre- Robust Security Network Association.
RSNA	Robust security network Association.
RSN IE	Robust Security Network Information Element.
WEP	Wired Equivalent Privacy.
WPA	Wi-Fi Protected Access.
WPA2	Wi-Fi Protected Access II.
WPA3	Wi-Fi Protected Access III.
AES	Advanced Encryption Standard.
PMK	Pairwise Master Key.
MSK	Master Session Key.
PTK	Pairwise Transient Key.
PSK	Per-shared key.
CCM	Counter with CBC-MAC.
CCMP	Counter-Mode/CBC-Mac Protocol.
WPA-TKIP	Wi-Fi protected access - Temporal Key Integrity Protocol.
CTR	Counter.
EAP	Extensible Authentication Protocol.
EAPOL	Extensible Authentication Protocol Over LAN.
MIC	Message Integrity Code.
MAC	MAC addresses.
TLS	Transport Layer Security.
GTK	Group key handshake.
SSID	Service Set Identifier.
KCK	Key Confirmation Key.
KEK	Key Encryption Key.
TK	Temporal Key.
PRNG	Pseudorandom number generator function.
MitM	Man-In-The-Middle Attack.
KRACK	Key Reinstallation Attack.