



# **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 WPA2

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

١٤٤٠ هـ - ٢٠١٩ م

---

# Table of Contents

Abstract .....	ii
Acknowledgements .....	iv
Statement of Original Authorship .....	v
Table of Contents .....	vii
List of Figures .....	viii
List of Abbreviations.....	ix
<b>Chapter 1: Introduction .....</b>	<b>1</b>
1.1 wireless network .....	1
1.2 objectives .....	2
1.3 Problem statement.....	3
1.4 contribution.....	4
1.5 motivation .....	4
1.6 Thesis organization .....	5
<b>Chapter 2: Background and Literature Review .....</b>	<b>7</b>
2.1 Background knowledge of Wi-fi protected access 2.....	7
2.2 Background knowledge on analysis methods for security protocol.....	18
2.3 Related works.....	20
2.4 Summary .....	24
<b>Chapter 3: Methodology.....</b>	<b>25</b>
3.1 Model Checking.....	25
3.2 Scyther .....	27
3.3 scyther approach .....	28
3.4 Why Scyther?.....	33
<b>Chapter 4: Analysis .....</b>	<b>35</b>
4.1 A formal framework for the verification of 4-way handshake protocol. ....	35
4.2 Formal verification of 4-way handshake protocol.....	40
<b>Chapter 5: Result and Discussion .....</b>	<b>49</b>
5.1 Practical Impact of secrecy vulnerability.....	51
<b>Chapter 6: Conclusion and Future Work.....</b>	<b>54</b>
<b>References .....</b>	<b>56</b>

## List of Figures

Figure 2-1: WPA2 components.....	8
Figure 2-2 : WPA2 Establishment Procedures.....	10
Figure 2-3 : Temporal Key Computation .....	13
Figure 2-4: Pairwise Key Hierarchy.....	14
Figure 2-5: 4-Way handshake protocol.....	15
Figure 3-1: Formal model checking tools comparison [13].....	26
Figure 3-2: Scyther Approach .....	28
Figure 4-1: Aliveness property.....	36
Figure 4-2: Secrecy property.....	36
Figure 4-3: Non-injective synchronization .....	37
Figure 4-4: Non-injective Agreement .....	37
Figure 4-5: Authenticator’s role.....	39
Figure 4-6: Supplicant’s role.....	39
Figure 4-7: A role’s Claims.....	39
Figure 4-8: S role’s Claims .....	40
Figure 4-9: Hierarchy of Authentication properties .....	40
Figure 4-10: Abstract level of 4-Way handshake.....	41
Figure 4-11: Scyther Script .....	44
Figure 4-12: Secret Claim .....	46
Figure 4-13: Authentication Claim .....	46
Figure 5-1 : “Deceiver “attack – Authenticator side.....	50
Figure 5-2: Improved 4-Way handshake.....	52
Figure 5-3: Result after the implementation of the improvement.....	53

## List of Abbreviations

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