# การทดสอบช่องโหว่โปรโตคอล WAP2 ด้วยการโจมตีแบบ KRACK กรณีศึกษาอุปกรณ์เครือข่ายไร้สายมหาวิทยาลัยราชภัฏกำแพงเพชร

# The Vulnerability Analysis of WPA2 Protocol by KRACK, a Case Study: Wireless Network Devices of Kamphaeng Phet Rajabhat University

**ศิลป์ณรงค์ ฉวีพัฒน์[1] ,พรนรินทร์ สายกลิ่น[1]**

**Silnaorng Chavipat[1],Ponnarin Saiklin[1]**

[1] อาจารย์ประจำหลักสูตรเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกำแพงเพชร

**บทคัดย่อ**

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาและป้องกันภัยคุกคามจากอุปกรณ์เครือข่ายไร้สายที่เข้ารหัสโปรโตคอล WPA2 ที่อาจจะถูกโจมตีด้วย KRACK เนื่องจากเป็นช่องโหว่ในระดับโปรโตคอล ส่งผลให้อุปกรณ์เครือข่ายไร้สายทุกผลิตภัณฑ์ที่เข้ารหัสด้วยโปรโตคอลดังกล่าว ไม่มีความปลอดภัยต่อการใช้งาน เพื่อเป็นแนวทางในการทดสอบหาช่องโหว่และแนวทางการป้องกัน งานวิจัยนี้ได้นำเสนอหลักการและขั้นตอนต่าง ๆ ในการทดสอบโดยใช้ระบบปฏิบัติการ KALI Linux ที่ติดตั้ง KRACK Script เพื่อใช้เป็นแนวทางในการนำไปป้องกันและปรับปรุงระบบเครือข่ายไร้สายที่ใช้งานอยู่ ให้มีความปลอดภัยและมีประสิทธิภาพมากขึ้นกว่าเดิม

ผลจากการทดสอบพบว่าระบบเครือข่ายไร้สายของมหาวิทยาลัยราชภัฏกำแพงเพชรที่เข้ารหัสด้วยโปรโตคอล WPA2 จำนวน 4 รุ่น พบว่ามีช่องโหว่จาก WPA2 Handshake และถูกโจมตีด้วย KRACK ทั้งหมด ต้องหาแนวทางการแก้ไขและปรับปรุงให้อุปกรณ์เครือข่ายไร้สายมีความปลอดภัยทันที

**คำสำคัญ:** ช่องโหว่ระบบเครือข่ายไร้สาย/ โปรโตคอล WPA2/การโจมตีแบบ KRACK

**Abstract**

This study had objectives to study and protect wireless network devices, implementing the WPA2 protocol, that are vulnerable to Key Reinstallation Attack: KRACK attack. This is a protocol-level issue that puts almost every WPA2 wireless-enabled device, all brands, at risk of attack. To find those loopholes and guidelines for protecting the devices, this study proposed the principles, step by step, in testing the attack using KALI Linux operating system that has KRACK script installed. The testing meant to help preventing and improving the wireless network devices, to be more safe and effective.

The testing results showed that all of the 4 wireless networks of Kamphaeng Phet Rajabhat University, implementing the WPA2 protocol, are vulnerable to KRACK attack through exploiting a handshake of the WPA2 protocol. An immediate security prevention and improvement are needed.

**Keywords:** Vulnerability/ Protocol WPA2/ KRACK

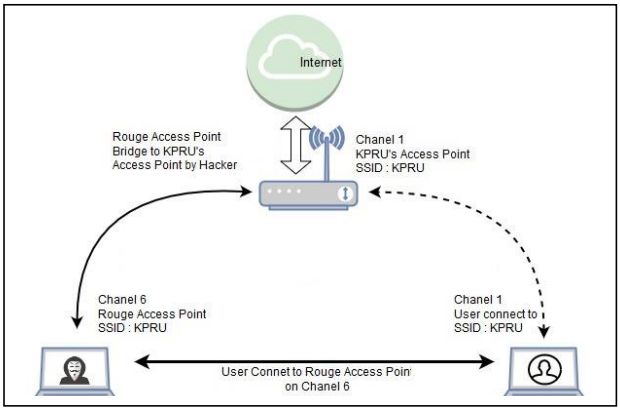
**ความเป็นมาและความสำคัญของปัญหา**

ปัจจุบันระบบเครือข่ายไร้สาย(WiFi) ได้รับความนิยมเป็นอย่างมาก ซึ่งจะพบว่าหน่วยงานขนาดเล็กนิยมติดตั้งระบบเครือข่ายไร้สายทดแทนเดิมคือระบบเครือข่ายแลน(LAN)กันมากขึ้น อย่างไรก็ตามระบบเครือข่ายไร้สายก็คงเป็นระบบการสื่อสารที่มีความปลอดภัยต่ำมากเพราะเป็นการรับส่งข้อมูลผ่านคลื่นวิทยุ ผู้ที่โจมตีสามารถดักจับข้อมูลอยู่ในพื้นที่ที่สัญญาณเครือข่ายไร้สายกระจายมาถึง ก็สามารถดักจับข้อมูลและนำข้อมูลมาวิเคราะห์ได้โดยสะดวก การค้นหาผู้กระทำความผิดสามารถทำได้ยากมาก เนื่องจากเป็นการสื่อสารที่ใช้อากาศเป็นตัวกลางในการกระจายสัญญาณ อีกทั้งไม่จำเป็นต้องเชื่อมต่อเข้าระบบก่อนแต่ประการใด จึงมีผู้ที่โจมตีจำนวนมาก ทำการดักจับข้อมูลและนำเอาข้อมูลดังกล่าวไปใช้ในทางทีมิชอบอยู่เสมอ เพื่อให้การรับส่งข้อมูลระบบในครือข่ายไร้สายมีความมั่นคงปลอดภัยของข้อมูล ได้มีการพัฒนากลไกลการเข้ารหัสข้อมูลเริ่มตั้งแต่ WEP ที่ใช้กุญแจเข้ารหัสขนาด 40 bit ซึ่งต่อมาพบว่ามีช่องโหว่สามารถ HACK ได้โดยง่าย ปี พ.ศ 2546 หน่วยงาน Wi-Fi Alliance ได้เพิ่มขนาดกุญแจเป็น 256 bit และกำหนดมาตรฐานการเข้ารหัสเป็น WPA ที่เข้ารหัสข้อมูลด้วย TKIP และมาตรฐาน WPA2 ที่เข้ารหัสข้อมูลด้วย AES ในปีพ.ศ 2547 โดยมาตรฐานและการเข้ารหัสแบบ WPA2 ได้ถูกใช้มากว่าสิบปี ซึ่งเชื่อกันว่ามีความปลอดภัยและแข็งแกร่งที่สุด จนกระทั่งเมื่อเดือนตุลาคม พ.ศ. 2560 Mathy Vanhoef และ Frank Piessens นักวิจัยจากมหาวิทยาลัย KU Leuven ได้ค้นพบช่องโหว่ของ WPA2 โดยผู้ที่โจมตีทำการปลอมเป็นเครือข่ายไร้สาย แล้วทำการเชื่อมต่อกับผู้ใช้งานอยู่ โดยการรบกวนหรือหยุดการสื่อสารของ ข้อความที่ 3 (Message 3) ซึ่งเป็นกระบวนการการทำงานของ 4-way-handshake ทำให้เครื่องผู้ใช้งานอยู่ได้รับการติดตั้งกุญแจลับชุดใหม่จากเครื่องผู้ที่โจมตีแทนกุญแจลับชุดเดิมที่ใช้อยู่กับเครือข่ายไร้สายก่อนหน้านี้ ซึ่งเป็นการโจมตีรูปแบบที่เรียกว่า man-in-the-middle โดยปกติแล้วกุญแจลับที่ใช้ในกระบวนดังกล่าวจะมีค่าที่ไม่ซ้ำกันและใช้เพียงครั้งเดียว ด้วยช่องโหว่นี้ทำให้ผู้โจมตีสามารถดักจับทราฟฟิกและข้อมูลที่ส่งผ่านระบบเครือข่ายไร้สายได้โดยที่ไม่ต้องทราบรหัสใด ๆทั้งสิ้นรวมทั้งสามารถแทรกแพ็คเก็ตหรือข้อมูลที่เป็นอันตรายไปยังเครื่องผู้ที่ใช้งานได้ด้วย ถึงแม้ว่าจะมีการเปลี่ยนรหัส WPA2 ใหม่แล้วก็ตาม ซึ่งถือว่าเป็นช่องโหว่ที่ร้ายแรงในระดับโปรโตคอล ทำให้อุปกรณ์เครือข่ายไร้สายจากผู้ผลิตต่าง ๆได้รับผลกระทบทั้งหมด[7][8][9] งานวิจัยนี้ได้จัดทำขึ้นเพื่อทดสอบหาช่องโหว่อุปกรณ์เครือข่ายไร้สายที่ติดตั้งภายในมหาวิทยาลัยราชภัฏกำแพงเพชร โดยใช้เทคนิคการโจมตีแบบ KRACK (Key Reinstallation Attacks) จากระบบปฏิบัติการ KALI Linux โดยเนื้อหาถัดไปจะนำเสนอเกี่ยวกับทฤษฎีและหลักการที่นำมาใช้ วรรณกรรมต่าง ๆ ที่เกี่ยวข้อง ขั้นตอนในการดำเนินงานผลที่ได้จากการดำเนินงาน และผลสรุปของงานรวมไปถึงข้อเสนอแนะต่าง ๆ

**วัตถุประสงค์ของการวิจัย**

เพื่อทดสอบหาช่องโหว่ของโปรโตคอล WPA2 ซึ่งเป็นโปรโตคอลที่ใช้ในการรักษาความปลอดภัยขอระบบเครือข่ายไร้สาย ที่ใช้กันมาอย่างยาวนานและแพร่หลายและเชื่อกันว่ายังเป็นโปรโตคอลเข้ารหัสที่มีความปลอดภัยสูง

**กรอบแนวคิดการวิจัย**




**ภาพที่ 1** สภาพแวดล้อมของการทดสอบช่องโหว่ของโปรโตคอล WPA 2

**วิธีดำเนินการวิจัย**

ผู้วิจัยได้ติดตั้งระบบปฏิบัติการ Kali Linux และ Script KRACK เพื่อทดสอบหาช่องโหว่ WPA 2 ของอุปกรณ์ระบบเครือข่ายไร้สายที่ติดตั้งภายในมหาวิทยาลัยราชภัฏกำแพงเพชร ซึ่งมีสภาพแวดล้อมในการทดสอบดังภาพที่ 1 และมีรายละเอียดดังนี้ การทดสอบหาช่องโหว่ของโปรโตคอล WPA2 ของระบบเครือข่ายไร้สายนั้นมีอุปกรณ์การทดลองดังนี้

1.เครื่องคอมพิวเตอร์แบบพกพาโดยมีคุณสมบัติโดยย่อดังนี้

1) ติดตั้งระบบปฏิบัติการ Window 64 แบบ 64 Bit

2) ติดตั้งระบบปฏิบัติ Kali Linux แบบเสมือน โดยใช้ Oracle Virtual Box

3) หน่วยประมวลผล Core(TM) i7-6700HQ CPU @ 2.60GHz

4) หน่วยความจำหลักขนาด (RAM) 16 GB

5) หน่วยความจำรองขนาด (HDD) 512 GB

2. อุปกรณ์รับสัญญาณเครือข่ายไร้สาย (Wireless NIC) TPLINK TL-WN722N version 1

3.อุปกรณ์เครือข่ายไร้สายที่ใช้ในการทดสอบหาช่องโหว่จำนวน 4 ผลิตภัณฑ์


**ภาพที่ 2** (ก) อุปกรณ์เครือข่ายไร้สายที่ใช้งานภายในมหาวิทยาลัย (ข.)เครื่องคอมพิวเตอร์ที่ใช้ทดสอบ

การติดตั้ง Script KRACK เพื่อทดสอบช่องโหว่ WPA2 มีขั้นตอนต่าง ๆ ดังนี้

1. ติดตั้งซอฟต์แวร์จำลองโดยใช้ Oracle Virtual Box บนระบบปฏิบัติการ Windows 10 และติดตั้งระบบปฏิบัติการ KALI Linux

2. เปิดหน้าต่าง Terminal บนระบบปฏิบัติการ KALI Linux ให้ทำการ Update และ Download Krackattacks-Scripts โดยใช้คำสั่งดังนี้

- sudo apt update
- apt-get install libnl-3-dev libnl-genl-3-dev pkg-config libssl-dev net-tools git sysfsutils python-scapy python-pycryptodome

3. Download Script จากเว็บไซต์ github โดยใช้คำสั่ง

- git clone https://github.com/vanhoefm/krackattacks-test-ap-ft.git

4.หยุดการทำงานการเข้ารหัสของอุปกรณ์ไร้สายในระดับ Hardware

- ./disable-hwcrypto.sh

5.เมื่อใช้คำสั่งในขั้นตอนที่ 4 เสร็จแล้วให้เริ่มระบบปฏิบัติการ Kali Linux อีกหนึ่งครั้ง

6 ใช้คำสั่ง sudo vi เพื่อสร้างไฟล์คอนฟิกูเรชัน wpa_supplicant โดยมีตัวอย่างด้านล่างต่อไปนี้เพื่อเชื่อมต่อกับเครือข่ายไร้สายที่ต้องการทดสอบ

```
ctrl_interface=/var/run/wpa_supplicant
network={
ssid="KPRU"
key_mgmt=FT-PSK
psk="password" }
```

โดยกำหนดชื่อ ssid และ psk เป็นค่าเดียวกับอุปกรณ์เครือข่ายไร้สายที่ใช้ทดสอบ ให้บันทึกชื่อไฟเป็น network.conf

7. ทำการ run Script โดยใช้คำสั่งตามลำดับต่อไปนี้

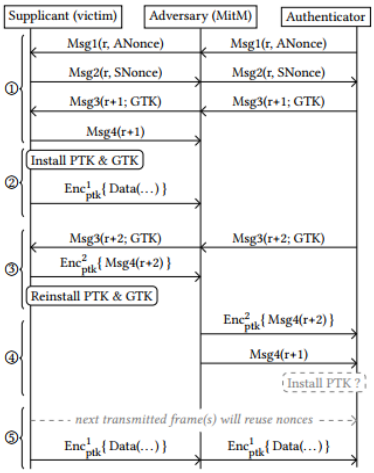
- rm /var/run/wpa_supplicaticant/wlan0
- sudo wpa_supplicant -D nl- 80211i wlan- 0c network.conf

8 ทำการทดสอบเชื่อมต่อเครือข่ายไร้สายที่ตั้งค่า SSID ชื่อ KPRU โดยใช้คำสั่งดังต่อไปนี้

- sudo krack-ft-test.py wpa_supplicant -D nl- 80211i wlan- 0c network.conf

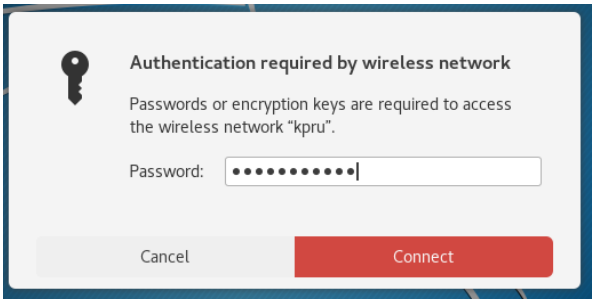
9.ระบบปฏิบัติ Kali Linux จะทำการเชื่อมต่อเครือข่ายไร้สายใหม่อีกครั้งซึ่งจะมีข้อสังเกตว่าจะให้มีการใส่รหัสผ่าน WPA2 ใหม่อีกครั้ง

10. ในงานวิจัยนี้เป็นการทดสอบช่องโหว่ WPA2 โดยใช้ Script KRACK เพื่อตรวจสอบว่ามีการส่ง Message 3 ระหว่างผู้รับ )Client( และผู้ให้บริการ )Access Point (ซ้ำหรือไม่ โดยสังเกตจากค่า IV (initialization vector) และค่า seq (sequence number) โดยในการทดสอบจะเป็นการโจมตีเพื่อขัดจังหวะการแลกเปลี่ยนข้อความที่ 3 ของกระบวนการ 4-way handshake ซึ่งได้ออกแบบการทดลองให้สอดคล้องกับงานวิจัยของ Mathy Vanhoef และ Frank Piessens ดังภาพที่ 3




**ภาพที่ 3** ขั้นตอนการโจมตีเพื่อขัดจังหวะการแลกเปลี่ยนข้อความที่ 3 ของกระบวนการ 4-way handshake

โดยปกติแล้วถ้าหากไม่มีข้อผิดพลาดในการสื่อสารการรับส่งข้อมูลข่าวสารจากฝั่งผู้รับ (Client) ก็สามารถรับ Message 3 จาก จากฝั่งผู้ให้บริการ (Access Point)ได้อย่างถูกต้องครบถ้วน ในกรณีที่มีเกิดมีข้อผิดพลาดใด ๆ ที่ฝั่งผู้รับ (Client) ทำให้ไม่ได้รับข้อมูลข่าวสารจาก Message 3 จากฝั่งผู้ให้บริการ (Access Point) หลายครั้ง ผู้รับ (Client) จะถูกบังคับให้มีการล้างค่าที่จำเป็นในกระบวนการเข้ารหัสเพื่อจัดการข้อผิดพลาดต่าง ๆที่เกิดขึ้นในกระบวนการรับส่งข้อมูลและบังคับให้เข้ารหัสด้วยกุญแจเดิมซ้ำอีกครั้ง ซึ่งขั้นตอนดังกล่าว หากมีผู้โจมตีสามารถบังคับไม่ให้ผู้รับ (Client) ได้รับ Message 3 ได้อย่างถูกต้อง เพื่อให้เกิดเงื่อนไขการส่ง Message 3 ซ้ำ ทำให้อุปกรณ์ที่ใช้งานอยู่บนเครือข่ายไร้สายที่เข้ารหัสใหม่อีกครั้งหนึ่ง ซึ่งการเปลี่ยนแปลงค่าดังกล่าวจะมีผลต่อความปลอดภัยของข้อมูลที่มีการเข้ารหัส ส่งผลให้ผู้โจมตีสามารถถอดรหัสข้อมูลดูทราฟฟิกได้โดยไม่ต้องใช้รหัสผ่านใด ๆทั้งสิ้นซึ่งการโจมตีแบบ KRACK ทำให้อุปกรณ์เครือข่ายไร้สายที่เข้ารหัสตามมาตรฐานแบบ WPA1 และ WPA2 แบบ WPA-TKIP , AES-CCMP และ AES GCMP และสามารถสอดแทรก Packet ปลอมเข้าไปยังข้อมูลของผู้ใช้งานบนเครือข่ายไร้สายได้อีกด้วยในกรณีที่ใช้การเข้ารหัสแบบ AES-CCMPดังนั้นจากที่ได้กล่าวไปแล้วเราการโจมตีแบบ KRACK (Key Reinstallation Attack) คือการติดตั้งคีย์ลับที่ผ่านการโจมตีมาแล้วใหม่อีกครั้ง โดยมีตัวอย่างดังภาพ




**ภาพที่ 4** การร้องขอรหัสผ่านใหม่อีกครั้ง

จากภาพจะเป็นการบังคับให้ใส่รหัสผ่าน WPA2 อีกหลายครั้งจนกว่าจะบังคับให้เครื่องผู้ใช้งานเชื่อมต่อกับเครือข่ายไร้สายของผู้ที่โจมตี

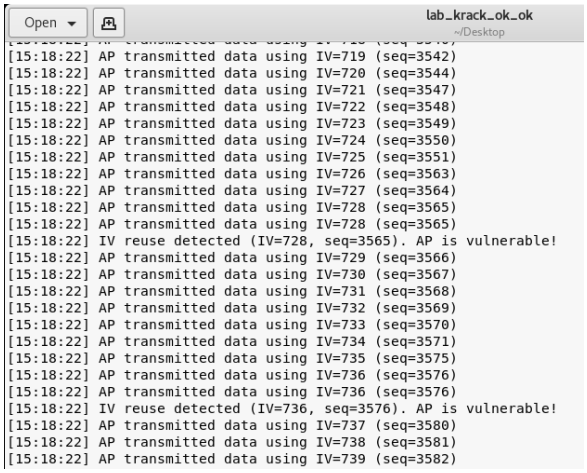
**ผลการทดสอบช่องโหว่ WPA2 ของอุปกรณ์เครือข่ายไร้สาย**

ผลการทดสอบการโจมตีแบบ โดยใช้เทคนิคการโจมตีแบบ KRACK (Key Reinstallation Attacks) กับอุปกรณ์เครือข่ายไร้สายที่ใช้ในมหาวิทยาลัยราชภัฏกำแพงเพชรจำนวน 4 รุ่น ที่เข้ารหัสการรักษาความปลอดภัยแบบ WPA2 มีช่องโหว่ทั้ง 4 รุ่น ซึ่งผลการทดสอบดังตารางที่ 1

**ตารางที่ 1** ผลการทดสอบการโจมตีช่องโหว่ WPA2 โดยใช้เทคนิคการโจมตีแบบ KRACK

| ลำดับที่ | ผลิตภัณฑ์อุปกรณ์ | รุ่น | ค่า IV | ค่า seq |
|---|---|---|---|---|
| 1 | Linksys | WAP54G | ซ้ำ | ซ้ำ |
| 2 | Linksys | WRT54GL | ซ้ำ | ซ้ำ |
| 3 | Engenius | EAP350 | ซ้ำ | ซ้ำ |
| 4 | Engenius | EAP300 | ซ้ำ | ซ้ำ |

จากตารางที่ 1 จะเห็นได้ว่าผลการทดสอบการโจมตีช่องโหว่ WPA2 โดยใช้เทคนิคการโจมตีแบบ KRACK กับอุปกรณ์เครือข่ายไร้สายจำนวน 2 ผลิตภัณฑ์ 4 รุ่นพบว่ามีค่า Initialization Vector และค่า sequence number มีค่าซ้ำ ซึ่งจะส่งผลให้อุปกรณ์เครือข่ายไร้สาย ดังกล่าวที่ติดตั้งใช้งานอยู่ภายในมหาวิทยาลัยราชภัฏกำแพงเพชรไม่มีความปลอดภัยในการให้บริการ โดยจะมีผลการทดสอบตามตัวอย่างดังภาพที่ 5




**ภาพที่ 5** ลักษณะผลการทดสอบที่พบของการโจมตีแบบ KRACK

จากภาพที่ 5 จะเห็นได้ว่าค่า IV ลำดับที่ 728 ,736 กับค่า seq ลำดับที่ 3565,3576 มีค่าซ้ำ โดยมีข้อความแจ้งจาก ระบบปฏิบัติการ Kali Linux ที่ติดตั้ง Script Krack ว่า ชุดลำดับดังกล่าวเป็นช่องโหว่

**การป้องกันและการแก้ไข**

สามารถป้องกันได้โดยการอัพเดตเฟิร์มแวร์ของของอุปกรณ์เครือข่ายไร้สายที่ใช้งานอยู่ โดยติดต่อและปฏิบัติตามคำแนะนำของเว็บไซต์ผู้ผลิตอุปกรณ์เครือข่ายไร้สาย ผู้วิจัยได้ทดลองเข้าไปยังเว็บไซต์ผู้ผลิตพบว่าเว็บไซต์ของผู้ผลิต Engenius อยู่ระหว่างจัดทำ Firmware เพื่อแก้ไขปัญหาช่องโหว่ KRACK WPA2 ของอุปกรณ์เครือข่าย

ไร้สายและแจ้งว่าจะให้ Download ได้ในเวลาอันใกล้นี้ ในขณะที่เว็บไซต์ของผู้ผลิต Linksys ยังไม่มี Firmware แก้ไขช่องโหว่ WPA2 แต่อย่างใด

**สรุปผลการวิจัย**

การศึกษางานวิจัยนี้ เป็นการศึกษาถึงหลักการโจมตีและหาช่องโหว่ของอุปกรณ์เครือข่ายไร้สายที่เข้ารหัสด้วย WPA2 ของ โดยใช้ Krack Script เป็นการทดสอบการโจมตีแบบ Man-in-the-Middle ผลการทดสอบทำให้ผู้รับข่าวสารไม่ได้รับ Message3 จากผู้ส่ง ทำให้เกิดการส่ง Message3 ซ้ำเกิดขึ้น โดยอัลกอรึทึมการเข้ารหัสแบบ WPA2 มีองค์ประกอบอยู่สองส่วนคือกระบวนการเข้ารหัสหรือคีย์ลับ และค่า initialization vector (IV) ซึ่งค่าดังกล่าวจะเป็นหมายเลขลำดับที่ไม่มีทางซ้ำกันและมีค่าเพิ่มขึ้นตลอด เมื่อมีการส่ง Message3 ซ้ำเกิดขึ้น จะทำให้กระบวนการเข้ารหัสหรือคีย์ลับ จะถูกล้างค่าเป็นค่าเริ่มต้นหรือมีค่าเป็น 0 และเครื่องที่ผู้ใช้งานจะถูกบังคับให้เข้ารหัสเดิมซ้ำจากผู้ที่โจมตี ทำให้ไม่มีค่า initialization vector (IV) หรือเป็นค่าซ้ำนั้นเอง โดยจะส่งผลให้ผู้โจมตีสามารถสามารถถอดรหัสหรือดักจับข้อมูลได้โดยไม่ต้องใช้รหัสใด ๆทั้งสิ้น ถึงแม้ว่าจะมีการเปลี่ยนรหัส WPA2 ก็ไม่สามารถช่วยให้ระบบมีความปลอดภัย โดยแนวทางการแก้ไข ผู้ใช้ที่ใช้งานหรือผู้ดูแลระบบสามารถแก้ไขได้โดยการอัพเดต Firmware รวมทั้งปฏิบัติคำแนะนำ จากผู้ผลิตอุปกรณ์เครือข่ายไร้สายได้โดยตรง ถึงแม้ว่า WPA2 จะถูกค้นพบว่ามีช่องโหว่ แต่ก็ยังมีข้อจำกัดคือผู้ที่จะโจมตีต้องเข้าถึงหรืออยู่ในรัศมีที่สามารถเชื่อมต่อของอุปกรณ์เครือข่ายไร้สายนั้นถึงจะสามารถโจมตีโดยอาศัยช่องโหว่ดังกล่าวนี้ได้ นอกจากนี้การใช้งาน HTTPS และ VPN ช่วยลดผลกระทบจากช่องโหว่ดังกล่าวได้อีกทางหนึ่ง

**อภิปรายผลการวิจัย**

การศึกษางานวิจัยนี้ เป็นการศึกษาถึงหลักการโจมตีและหาช่องโหว่ของอุปกรณ์เครือข่ายไร้สายที่เข้ารหัสด้วย WPA2 ของ โดยใช้ Krack Script เป็นการทดสอบการโจมตีแบบ man-in-the-middle ผลการทดสอบทำให้ผู้รับข่าวสารไม่ได้รับ Message3 จากผู้ส่ง ทำให้เกิดการส่ง Message3 ซ้ำเกิดขึ้น โดยอัลกอรึทึมการเข้ารหัสแบบ WPA2 มีองค์ประกอบอยู่สองส่วนคือกระบวนการเข้ารหัสหรือคีย์ลับ และค่า initialization vector (IV) ซึ่งค่าดังกล่าวจะเป็นหมายเลขลำดับที่ไม่มีทางซ้ำกันและมีค่าเพิ่มขึ้นตลอด เมื่อมีการส่ง Message3 ซ้ำเกิดขึ้น จะทำให้กระบวนการเข้ารหัสหรือคีย์ลับ จะถูกล้างค่าเป็นค่าเริ่มต้นหรือมีค่าเป็น 0 และเครื่องที่ผู้ใช้งานจะถูกบังคับให้เข้ารหัสเดิมซ้ำจากผู้ที่โจมตี ทำให้ไม่มีค่า initialization vector (IV) หรือเป็นค่าซ้ำนั้นเอง โดยจะส่งผลให้ผู้โจมตีสามารถสามารถถอดรหัสหรือดักจับข้อมูลได้โดยไม่ต้องใช้รหัสใด ๆทั้งสิ้น ถึงแม้ว่าจะมีการเปลี่ยนรหัส WPA2 ก็ไม่สามารถช่วยให้ระบบมีความปลอดภัย โดยแนวทางการแก้ไข ผู้ใช้ที่ใช้งานหรือผู้ดูแลระบบสามารถแก้ไขได้โดยการอัพเดตเฟิร์มแวร์ รวมทั้งปฏิบัติคำแนะนำ จากผู้ผลิตอุปกรณ์เครือข่ายไร้สายได้โดยตรง ถึงแม้ว่า WPA2 จะถูกค้นพบว่ามีช่องโหว่ แต่ก็ยังมีข้อจำกัดคือผู้ที่จะโจมตีต้องเข้าถึงหรืออยู่ในรัศมีที่สามารถเชื่อมต่อของอุปกรณ์เครือข่ายไร้สายนั้นถึงจะสามารถโจมตีโดยอาศัยช่องโหว่ดังกล่าวนี้ได้ นอกจากนี้การใช้งาน HTTPS และ VPN ช่วยลดผลกระทบจากช่องโหว่ดังกล่าวได้อีกทางหนึ่ง

**ข้อเสนอแนะ**

**ข้อเสนอแนะในการทำวิจัยครั้งต่อไป**

ในการทดลองครั้งนี้ยังไม่มี Firmware ออกมาแก้ไขดังนั้นควรจะทำการทดสอบอีกครั้งหลังจากที่ได้มีการอัพเดต Firmware จากผู้ผลิตอีกครั้งหนึ่ง และควรจะทดสอบในรูปแบบการโจมตีในลักษณะของเชื่อมต่อแบบ VPN และการใช้งานแบบ HTTP,HTTPS ทั้งก่อนและหลังอัพเดต Firmware

**เอกสารอ้างอิง**

ชนัญญา สุวรรณศร และ นวพร วิสิฐพงศ์พันธ์.(2553). การวิเคราะห์ช่องโหว่ของเครือข่ายไร้สายมาตรฐาน 802.11n. **การประชุมวิชาการระดับชาติ 2553 The 6th National Conference on Computing and Information Technology** (น.317).กรุงเทพฯ:มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ธีระ เอี่ยมศรีตระกูล. (2560). **ความปลอดภัยในการใช้งานเครือข่ายไร้สาย ตอนที่ 1**. สืบค้นเมื่อวันที่ 15 ตุลาคม 2560,จากเว็บไซต์ http://www.nidprotech.com/main/2017/07/31/ความปลอดภัยในการใช้งาน.

บงการ หอมนาน และสุธิดา วัฒนาชัย .(2547). AES-CCMP มาตรการรักษาความปลอดภัยตัวจริงสำหรับ Wireless Network. **ฐานข้อมูลบทความอาจารย์มหาวิทยาลัยธุรกิจบัณฑิต**.สืบค้น 20 พฤศจิกายน 2560,จาก http://liblog.dpu.ac.th/article/detail01view.php?arid=414.

ปรีดี ฤกษ์วลีกุล.(ม.ป.ป).**เตือนภัย! พบ KRACK โจมตีช่องโหว่ WPA2.**สืบค้นเมื่อวันที่ 18 พฤศจิกายน 2560,จากเว็บไซต์ https://www.beartai.com/news/itnews/199833.

พิกุลทอง แก้วดวงตา และ ศิรปัฐช์ บุญครอง.(2556). การวัดประสิทธิภาพของการรักษาความมั่นคงบนเครือข่ายท้องถิ่นไร้สายด้วย Back Track.ใน **การประชุมวิชาการระดับชาติ 2556 The 9th National Conference on Computing and Information Technology** (น.480). กรุงเทพฯ: มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.

มหาวิทยาลัยศรีนครินทร์วิโรฒน์. (2547). **ระบบเครือข่ายไวเลสแลน.** สืบค้นเมื่อวันที่ 15 ตุลาคม 2560, จากเว็บไซต์ http://wise.swu.ac.th/Default.aspx?tabid=3438.

วิรินทร์ เมฆประดิษฐสิน.(2558). **ระบบรักษาความปลอดภัยเครือข่ายไร้สาย (3).**สืบค้นเมื่อวันที่ 21 กันยายน 2560,จากเว็บไซต์ https://th-th.facebook.com/virintr/posts/617025115108028.

สุเมธ จิตภักดีบดินทร์.(2557). การโจมตีเพื่อปลอมแปลงข้อมูลของเว็บเพจบนเครือข่ายไร้สายและวิธีป้องกัน. **สารนิพนธ์วิทยาศาสตร์มหาบัณฑิต.**มหาวิทยาลัยเทคโนโลยีมหานคร.

Arif Sari, Mehmet Karay.(2015).**Comparative Analysis of Wireless Security Protocols: WEP vs WPA. Network and System Sciences,** 8(12). Retrieved October 12,2016, form http://www.scirp.org/journal/ijcns http://dx.doi.org/10.4236/ijcns.2015.812043

Khasawneh M,Kajman I,Alkhudaidy R,Althubyani A. (2014). A Survey on Wi-Fi Protocols: WPA and WPA2, **Proceedings of the 2014 International Conference on Security in Computer Networks and Distributed Systems** (pp.496-511).Trivandrum:Indian Institute of Information Technology and Management.

Mathy Vanhoef, Frank Piessens. (2017). Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, **Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security,** (pp.1313-1328). New York: ACM Publications

Samia Alblwi, Khalil Shujaee. (2017). A Survey on Wireless Security Protocol WPA2, **Proceedings of the 2017 International Conference on Security and Management** (pp.12-17). California:The American Council on Science and Education.

Vipin Poddar , Hitesh Choudhary. (2014). A Comparative Analysis of Wireless Security Protocols (WEP and WPA2). **International Journal on AdHoc Networking Systems, 4(3)**. Retrieved October 16,2016 , form http://www.airccse.org/journal/ijans/papers/4314ijans01.pdf