บทที่ 1

บทนำ

1.1 หลักการและเหตุผล

อินเทอร์เน็ต และ Smartphone เป็นสิ่งที่จำเป็นที่อำนวยความสะดวก ต่อการใช้ชีวิตประจำวันของมนุษย์ ผู้ใช้และธุรกิจต่างๆ มีการใช้งาน Smartphone มากขึ้นเรื่อย ๆ สิ่งต้องที่คำนึงถึงเมื่อใช้งานสิ่งเหล่านี้ ก็คือ ความปลอดภัยในระบบ Wi-Fi บน Smartphone ความเสี่ยงของข้อมูลส่วนบุคคลและข้อมูลทางธุรกิจ ที่จะรั่วไหล ทำให้เกิดความเสียหายแก่ผู้ใช้งาน หรือ ทรัพย์สินทางปัญญาของบริษัท

Smartphone เป็นหนึ่งในเป้าหมายการโจมตีของผู้ไม่ประสงค์ดี ที่พยามยามต้องการข้อมูลสำคัญต่างๆ หรือ ข้อมูลทางการเงิน ของผู้ใช้งานไม่ได้คำนึงถึง หรือ ไม่ได้มีความรู้เกี่ยวกับความปลอดภัยโดยเฉพาะเครือข่าย Wi-Fi เวลาใช้งานในที่สาธารณะ

เทคนิคการรบกวนหรือโจมตีต่างๆ สามารถโจมตี อุปกรณ์มือถือผ่านเครือข่ายที่อาจไม่ปลอดภัย เพื่อดักจับข้อมูลมีหลายเทคนิค หนึ่งในเทคนิคนี้คือ เทคนิคการสร้าง Rouge Access Point และ Evil-Twin การทำงานของเทคนิคจะรวดเร็วมาก ทำให้ผู้ใช้งาน อาจไม่สามารถรับรู้ถึงการถูกโจมตีหรือ ว่ามีการดักจับข้อมูลหรือไม่ เพราะเวลาการใช้งาน Wi-Fi จะเหมือนปกติ โดยเทคนิคนี้ดังกล่าวนั้นจะสร้าง ชื่อของ Wi-Fi (ESSID) ให้เหมือนกับ Access Point ตัวจริง ในที่สาธารณะ เพื่อให้เหยื่อ หรือ ผู้งานใช้ ไม่สังเกตและหลงเชื่อไปใช้งาน ซึ่งเป็นการหลอกเหยื่อให้เชื่อมต่อไปยัง Access Point ที่ไม่ถูกต้อง (illegitimate APs)

จากปัญหาดังกล่าว ผู้จัดทำโครงการนี้ต้องการที่จะช่วยแจ้งเตือนเมื่อผู้ใช้ Smartphone เชื่อมต่อไปยัง illegitimate APs อย่าง Rogue Access Point และ Evil-Twin ขณะใช้งานเครือข่าย Wi-Fi หรือแอคเซสพอยต์ใดๆ ในพื้นที่สาธารณะ เพื่อให้ผู้ใช้มีความระแวดระวังกับการเชื่อมต่อเครือข่าย Wi-Fi ที่ไม่ถูกต้อง อาจจะเกิดขึ้นจากผู้ไม่ประสงค์ดี ทำการโจมตีเครือข่าย ณ ขณะนั้น ซึ่งจะเกิดผลเสียหลายประการตามมาในอนาคต เช่น ข้อมูลหรือความลับต่างๆ สูญหาย ไม่ว่าจะเป็นข้อมูลการเงิน ข้อมูลส่วนตัวของผู้ใช้งาน ที่ผู้โจมตีสามารถดักจับได้ โดยการตรวจสอบ illegitimate APs จะดูจากข้อมูล ESSID (Extended Service Set ID) ซึ่งโดยปกติจะเป็นชื่อเครือข่ายไร้สายที่ได้รับอนุญาตในระบบเครือข่ายนั้นๆ และข้อมูล BSSID (Basic Service Set ID) โดยเป็น ID ของ Access Point ใดๆ ในระบบเครือข่าย หากมี ESSID หรือ BSSID ปรากฏขึ้นโดยไม่ได้รับอนุญาตในระบบอาจสันนิษฐานได้ว่ามี Rouge Access Point หรือ Evil-Twin ในระบบเครือข่าย

1.2 วัตถุประสงค์ของโครงงาน

ต้องการพัฒนาแอปพลิเคชันบน Smartphone เพื่อแจ้งเตือนผู้ใช้ เมื่อมีการเชื่อมต่อเข้าสู่แอคเซสพอยต์ที่ไม่ถูกต้อง โดยประกอบไปด้วย Rouge Access Point และ Evil-Twin

1.3 ขอบเขตของโครงงาน

1.3.1 ขอบเขตของเครื่องมือที่ใช้ในการโจมตีหรือสร้างปัญหา

(1) Rouge Access Point จำลองด้วย Access Point จริงหรือการใช้ Mobile Hotspot

(2) การทดสอบโจมตีระบบบน Test bed ของ ISAN LAB โดยไม่ก่อปัญหากับผู้อื่นและเป็นไปตามหลักจริยธรรมและกฎหมาย

1.3.2 ส่วนประกอบของระบบมี 2 ส่วนหลักๆดังนี้

(1) ส่วนของโมไบล์แอปพลิเคชันสำหรับผู้ใช้งานระบบแจ้งเตือนการเชื่อมต่อเข้าสู่ Rouge Access Point และ Evil-Twin

(2) ส่วนของเว็บแอปพลิเคชันสำหรับผู้ดูแลระบบ โดยประกอบไปด้วย ผู้ดูแลระบบหลัก (default admin account) และ สมาชิกในกลุ่มผู้ดูแลระบบ

1.3.3 ขอบเขตของผู้ใช้งาน ซึ่งแบ่งตามส่วนประกอบของระบบ 2 ส่วนดังนี้

(1) ผู้ใช้งานส่วนของโมไบล์แอปพลิเคชัน

- สามารถสมัครสมาชิก โดยข้อมูลประกอบไปด้วย
  - อีเมลผู้ใช้
  - รหัสผ่าน (ในกรณีผู้ใช้ไม่ได้เชื่อมบัญชี Google)
- การ Login เข้าสู่ระบบ
  - สามารถ Login ด้วย Email, Password และ ป้องกันการ flush ข้อมูลด้วย Captcha
  - สามารถเชื่อมโยงไปยังบัญชี Google เพื่อเข้าสู่ระบบได้
  - เมื่อผู้ใช้งาน Login เข้าสู่ระบบเรียบร้อยแล้ว หากไม่ Logout ระบบจะบันทึก Session การ Login ไว้เพื่อความสะดวกในการใช้งาน
  - สามารถ Logout ได้
- ฟังก์ชันการทำงาน
  - ก่อนใช้งานแอปพลิเคชันครั้งแรก ผู้ใช้ต้อง Login ในเครือข่ายที่ปลอดภัย

เพื่อดึงข้อมูล Access Point ที่ถูกต้องมาเก็บใน Smart Phone และข้อมูลนี้จะถูกนำไปตรวจสอบเมื่อผู้ใช้เริ่มเชื่อมต่อกับ Access Point ใดๆ

- มี Menu Scan Wi-Fi
- แจ้งเตือนเมื่อเชื่อมต่อกับ Evil-Twin หรือ Rouge Access Point
- มี Menu การยกเลิกเชื่อมต่อ Wi-Fi ผ่านแอปพลิเคชัน หากมีการแจ้งเตือนว่ามีการเชื่อมกับ Evil-Twin หรือ Rouge Access Point
- สามารถแก้ไขข้อมูลส่วนตัวได้
- สามารถดูประวัติการแจ้งเตือน โดยข้อมูลประกอบไปด้วย เวลา วันที่ ESSID และ BSSID

o เงื่อนไขการแจ้งเตือนการถูกโจมตี

- เมื่อผู้ใช้เชื่อมต่อ Access Point ใดๆ จะได้รับการแจ้งเตือนเมื่อถูกโจมตีโดยมีเงื่อนไข ดังนี้

1) แทบสีแดง จะขึ้นแสดง Warning ในแอปพลิเคชัน โดยหากตรวจพบว่าเป็น Evil-Twin ซึ่งมี ESSID ที่ลงทะเบียนในระบบแต่ BSSID ไม่ได้ถูกลงทะเบียน

2) แทบสีเหลือง จะขึ้นแสดง Warning ในแอปพลิเคชัน โดยหากตรวจพบว่าเป็น Rouge Access Point ซึ่งมี ESSID และ BSSID ที่ไม่ได้ลงทะเบียนในระบบ

3) แทบสีเขียว คือ Access Point ที่ลงทะเบียนหรือบันทึกข้อมูลลงในระบบแล้วโดย ESSID และ BSSID ตรงกับที่ลงทะเบียน

- การดึงข้อมูล ESSID และ BSSID มาเก็บไว้เพื่อใช้ในการตรวจสอบ Evil-Twin หรือ Rouge Access Point ในการนำแอปพลิเคชันไปใช้งานจริงต้องอยู่ภายใต้เงื่อนไขการเชื่อมต่อระหว่างแอปพลิเคชันกับ Server ผ่าน Protocol HTTPS

(2) ผู้ดูแลระบบ

o เพื่อให้ผู้ดูแลระบบจัดการข้อมูลผู้ใช้ และ Access Point ได้ จึงมีเว็บเซิร์ฟเวอร์ให้บริการเว็บแอปพลิเคชันสำหรับผู้ดูแลระบบ โดยมี database เก็บข้อมูลดังนี้

- เก็บข้อมูล BSSID, ESSID และข้อมูล description ของ Access Point เพื่อตรวจสอบความถูกต้องของ Access Point ที่ได้รับอนุญาตในเครือข่าย
- เก็บข้อมูลการลงทะเบียนของผู้ใช้งาน โดยข้อมูลประกอบไปด้วย ชื่อผู้ใช้ อีเมล รหัสผ่าน เบอร์โทรศัพท์ และ ข้อมูล description ของผู้ใช้
- เก็บประวัติการแจ้งเตือน Rouge Access Point และ Evil-Twin โดยข้อมูลประกอบไปด้วย ชื่อผู้ใช้ที่ถูกแจ้งเตือน เวลา วันที่ ESSID และ BSSID

o ส่วนของเว็บแอปพลิเคชันสำหรับผู้ดูแลระบบ ประกอบไปด้วย

1) ผู้ดูแลระบบหลัก (Default Admin Account) ที่มาพร้อมกับระบบ

- ต้อง Login ด้วย Email, Password พร้อมกระบวนการ Captcha หลังจากระบบเริ่มทำงานจำเป็นต้องเปลี่ยน default password

- สามารถ Logout ได้

- มีการทำงาน 2 ส่วน ดังนี้

<u>ส่วนที่หนึ่ง</u>

สามารถลงทะเบียนผู้ใช้ได้ 2 ประเภทคือ 1) ผู้ใช้โมไบล์แอปพลิเคชัน 2) สมาชิกกลุ่มผู้ดูแลระบบ โดยประกอบไปด้วยข้อมูล ดังนี้

1) อีเมล

2) รหัสผ่าน

3) เบอร์โทรศัพท์

4) ข้อมูล description ของผู้ใช้

สามารถแก้ไขข้อมูลของสมาชิกกลุ่มผู้ดูแลระบบได้

<u>ส่วนที่สอง</u>

สามารถดูข้อมูลประวัติการถูกโจมตีของผู้ใช้โมไบล์แอปพลิเคชันได้ ดังนี้

1) วันที่ตรวจพบการโจมตี

2) เวลาที่ตรวจพบการโจมตี

3) ข้อมูล Access Point ของผู้โจมตี ประกอบไปด้วย BSSID, ESSID และอื่นๆที่แอปพลิเคชันบน Smart Phone ของผู้ใช้ดึงข้อมูลมาได้

สามารถบันทึกและแก้ไข BSSID, ESSID, และข้อมูล Access Point ที่ได้รับอนุญาตได้

สามารถจัดการ Log โดยการดูประวัติการโจมตีเป็น วัน/เดือน/ปี และเลือก clear Log ที่ต้องการได้

2) สมาชิกกลุ่มผู้ดูแลระบบที่ถูกเพิ่มโดยผู้ดูแลระบบหลัก

- ต้อง Login ด้วย Email, Password พร้อมกระบวนการ Captcha

- สามารถแก้ไขข้อมูลส่วนตัวได้

- สามารถ Logout ได้

- มีการทำงาน 2 ส่วน ดังนี้

<u>ส่วนที่หนึ่ง</u>

สามารถลงทะเบียนผู้ใช้งานผู้ดูแลระบบได้ โดยประกอบไปด้วยข้อมูล ดังนี้

1) อีเมล

2) รหัสผ่าน

สามารถแก้ไขข้อมูลของผู้ใช้งานได้

ไม่สามารถแก้ไขหรือลบข้อมูลของผู้ดูแลระบบหลักได้

<u>ส่วนที่สอง</u>

สามารถดูข้อมูลประวัติการโจมตีของผู้ใช้งานได้ ดังนี้

1) วันที่ตรวจพบการโจมตี

2) เวลาที่ตรวจพบการโจมตี

3) ข้อมูล Access Point ของผู้โจมตี ประกอบไปด้วย BSSID, ESSID และอื่นๆที่แอปพลิเคชันบน Smart Phone ของผู้ใช้ดึงข้อมูลมาได้

สามารถบันทึกและแก้ไข BSSID, ESSID, และข้อมูล Access Point ที่ได้รับอนุญาตได้

สามารถจัดการ Log โดยการเลือกดูประวัติการโจมตีเป็น วัน/เดือน/ปี ได้ และเลือก clear Log ที่ต้องการได้

1.3.4 ข้อจำกัดของระบบ

(1) ไม่สามารถตรวจจับ Evil-Twin ได้หากผู้โจมตีทำการ Mac Address Spoofing

(2) ระบบจะทำการดึง List ข้อมูล ESSID และ BSSID ก็ต่อเมื่ออยู่ภายใต้เงื่อนไขการเชื่อมต่อที่ปลอดภัยผ่าน Protocol HTTPS

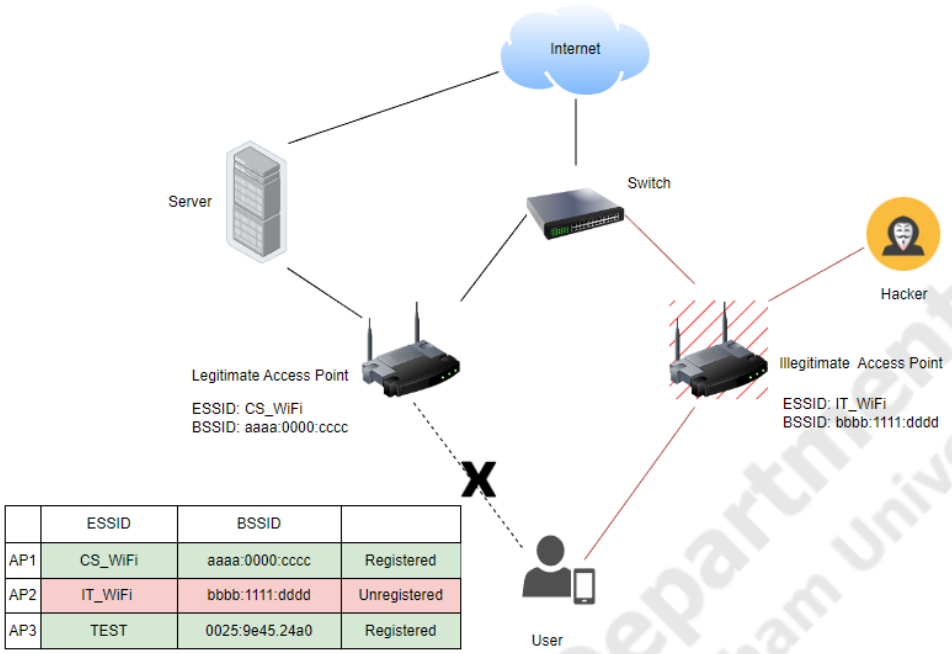
(3) หากแอปพลิเคชันไม่สามารถเชื่อมต่อกับ Server เพื่อที่จะดึงข้อมูลมาตรวจสอบ ESSID และBSSID ได้ จะทำการตรวจสอบข้อมูลล่าสุดกับแอปพลิเคชัน แต่ระบบจะแจ้งเตือนว่า List ของ ESSID และ BSSID อาจจะไม่อัพเดท เนื่องจากไม่สามารถเชื่อมต่อกับ Server ได้

1.4 ภาพรวมของระบบ

การจำลองการเชื่อมต่อเข้าสู่แอคเซสพอยต์ ที่ไม่ถูกต้อง โดยมี 2 เทคนิคหลักๆคือ Rouge Access Point และ Evil-Twin

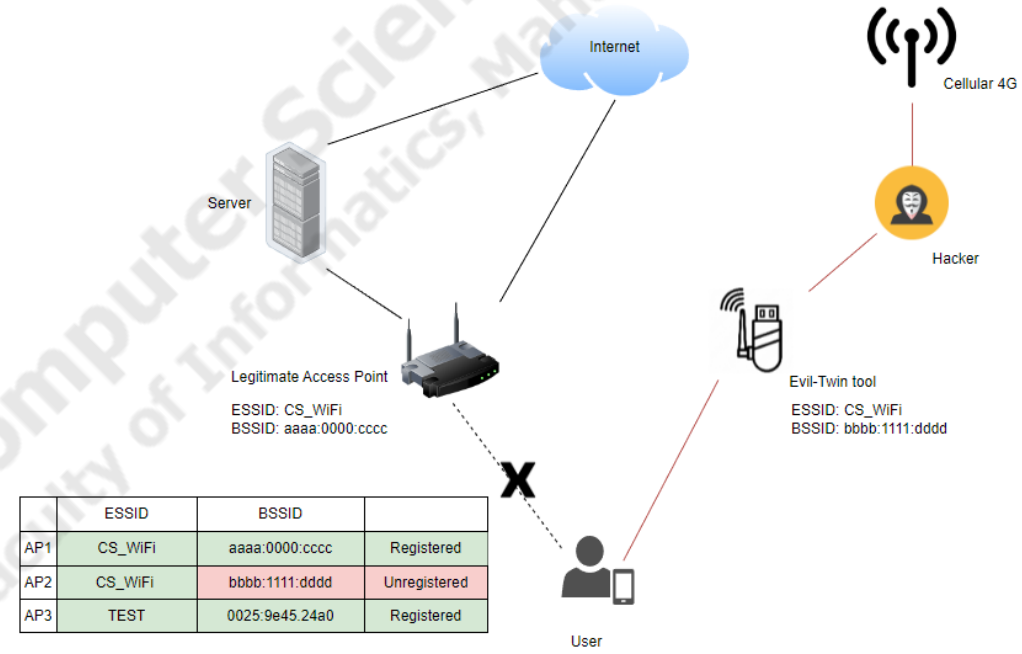
ข้อควรรู้ในภาพรวมของระบบคือ นิยามของ Rouge Access Point ปริญญานิพนธ์นี้ขอกำหนดไว้ดังนี้ Access Point ใดๆ ก็ตามที่เชื่อมต่อเข้าสู่ Network จริง แล้วทำหน้าที่เป็น Access Point ที่ไม่ถูกต้อง โดยมี BSSID และ ESSID ที่ไม่ได้ลงทะเบียนกับระบบ

Evil-Twin เกิดจากการใช้งานเครื่องมือของ Hacker ที่อาจจะไม่เชื่อมเข้าต่อกับ Network จริง โดย ESSID เหมือนกัน เช่น Wi-Fi phisher , Aircrack-ng



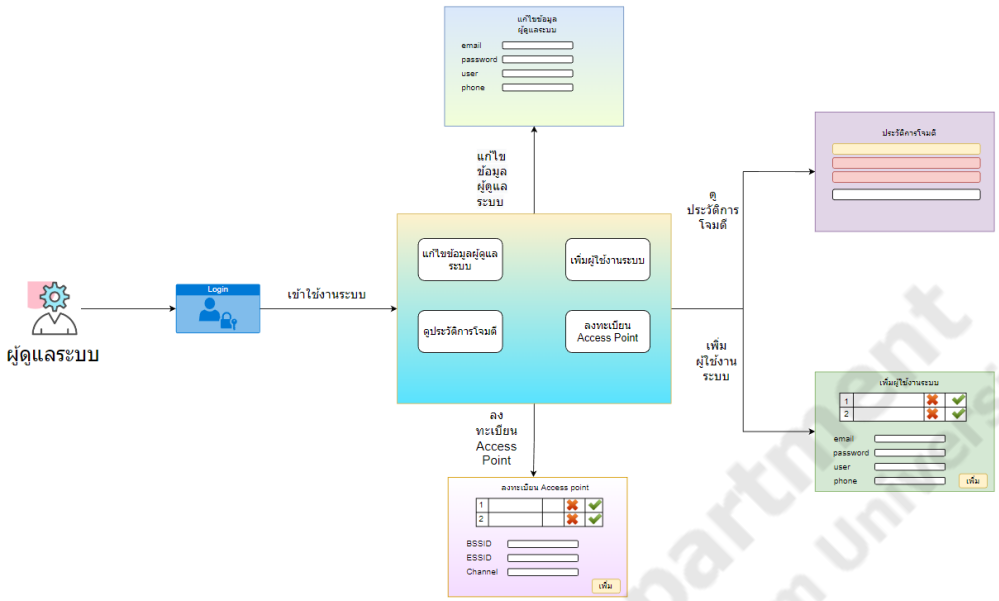
	ESSID	BSSID	
AP1	CS_WiFi	aaaa:0000:cccc	Registered
AP2	IT_WiFi	bbbb:1111:dddd	Unregistered
AP3	TEST	0025:9e45.24a0	Registered

ภาพประกอบที่ 1.1 Rouge Access Point

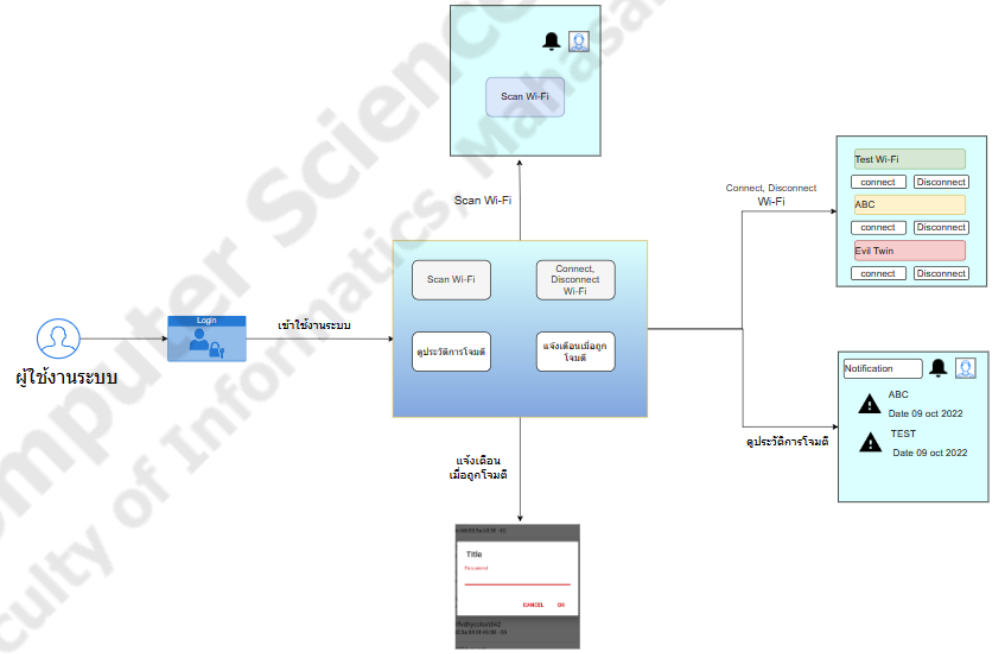


	ESSID	BSSID	
AP1	CS_WiFi	aaaa:0000:cccc	Registered
AP2	CS_WiFi	bbbb:1111:dddd	Unregistered
AP3	TEST	0025:9e45.24a0	Registered

ภาพประกอบที่ 1.2 Evil-Twin



ภาพประกอบที่ 1.3 ภาพรวมเว็บไซต์



ภาพประกอบที่ 1.4 ภาพรวมระบบ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

แจ้งเตือนและหาวิธีป้องกันข้อมูลให้แก่ผู้ใช้งาน หรือ องค์กร ธุรกิจต่างๆ
ให้ความรู้เกี่ยวกับความปลอดภัยบนเครือข่าย Wi-Fi ให้ได้มากที่สุด แก่ผู้ใช้งาน

1.6 อุปกรณ์และเครื่องมือที่ใช้ในการดำเนินงาน

1.6.1 ฮาร์ดแวร์

Computer spec

CPU: core i5 10400f

Ram: 16 GB

SSD: M.2 250 GB

VGA: GTX 1050 Ti

Laptop spec

CPU: core i5

Ram: 12 GB

SSD: M.2 250 GB

VGA: Intel HD 4000

1.6.2 ซอฟต์แวร์

OS: Oracle VM VirtualBox Kali Linux

1.6.3 โปรแกรมสำหรับเขียนโค้ด

Visual studio code

Android studio code

Flutter

1.6.4 อุปกรณ์และเครื่องมือที่ใช้ในการทดสอบ

Linksys WRT 1200 AC

D-Link DES-1016D

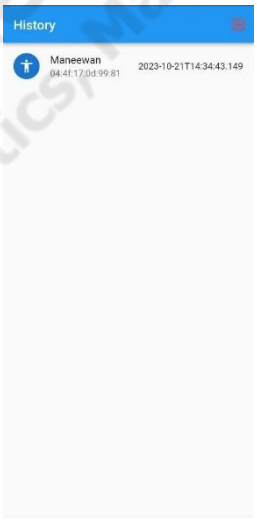
1.7 แผนการดำเนินงาน

โครงงานปริญญานิพนธ์ฉบับนี้ ดำเนินงาน ณ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม ระหว่างเดือน มกราคม 2566 ถึง ตุลาคม 2566

ตารางที่ 1.1 ตารางแผนการดำเนินงาน

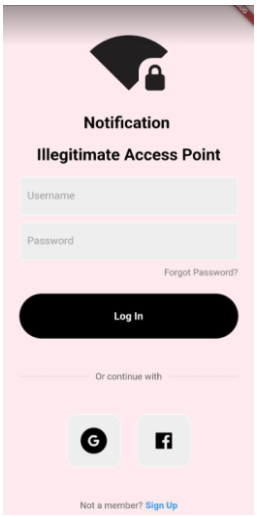
กิจกรรม	เดือน											
	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.
1. ศึกษาและรวบรวมข้อมูล												
2. วิเคราะห์และกำหนดขอบเขต												
3. ออกแบบระบบ												
4. พัฒนาโปรแกรม												
5. ทดสอบระบบ												
6. ทำรายงานสรุป												
7. นำเสนอโครงงาน												

1.8 ตัวอย่างแอปพลิเคชัน



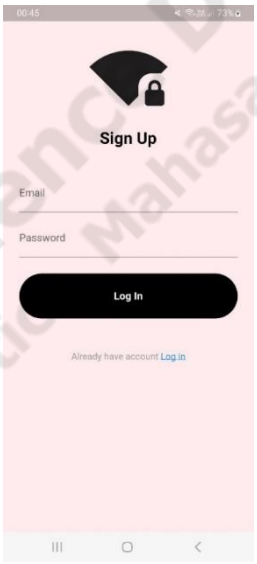
ภาพประกอบที่ 1.5 History

ผู้ใช้สามารถดูรายละเอียดการแจ้งเตือน ประวัติการถูกโจมตี และ ข้อมูล วัน เวลา ชื่อ ESSID ของ Rouge Access Point สามารถกด Disconnect หรือ Connect ได้ผ่านตัวแอปพลิเคชัน Login Page



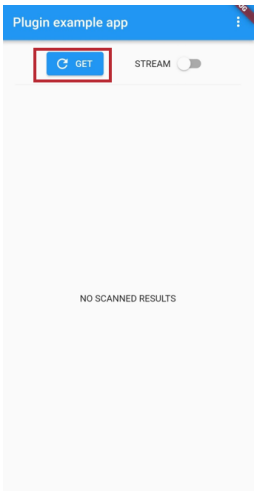
ภาพประกอบที่ 1.6 การ Login

ผู้ใช้ Login ด้วย Email หรือ Login ด้วยการเชื่อมโยงไปยังบัญชี Facebook หรือ Google Account



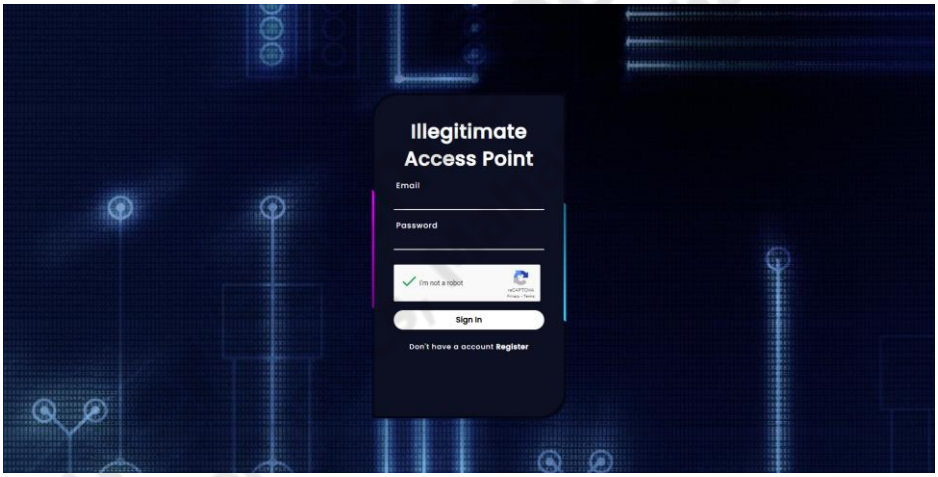
ภาพประกอบที่ 1.7 การสมัครสมาชิก

ผู้ใช้จะต้องสมัครสมาชิกด้วย Email เพื่อทำเข้าใช้งานแอปพลิเคชัน



ภาพประกอบที่ 1.8 Main Menu

ผู้ใช้สามารถดู Wi-Fi บริเวณรอบๆ ที่สแกนได้ หรือ Connect ผ่านในตัวแอปพลิเคชัน

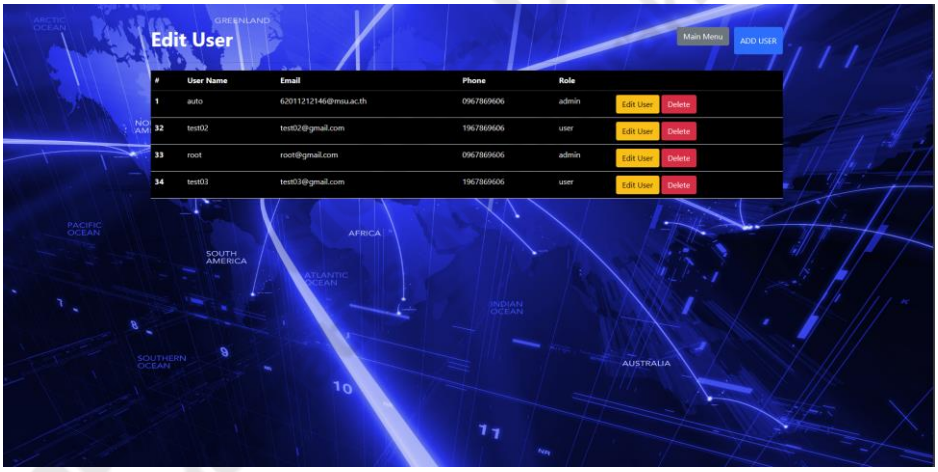


ภาพประกอบที่ 1.9 Login Website

ผู้ใช้จะต้องลงทะเบียนข้อมูลผู้ใช้งานและต้อง Login ด้วย Email และต้องทำ Google reCAPTCHA ถึงจะเข้าระบบได้

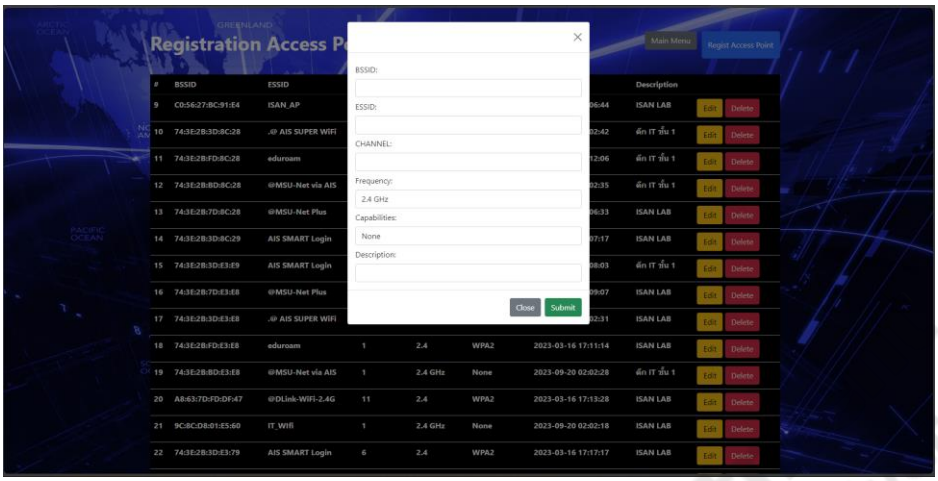
ภาพประกอบที่ 1.10 Menu Page

หน้าเมนูต่างๆของเว็บไซต์ที่มีให้ใช้งานโดยจะมี 3 เมนู ให้ใช้งานคือ 1.การเพิ่มและแก้ไขข้อมูลผู้ใช้งาน 2.การลงทะเบียนข้อมูล Access Point 3.การดูประวัติการถูกโจมตี



ภาพประกอบที่ 1.11 หน้าต่างแก้ไขข้อมูลผู้ใช้

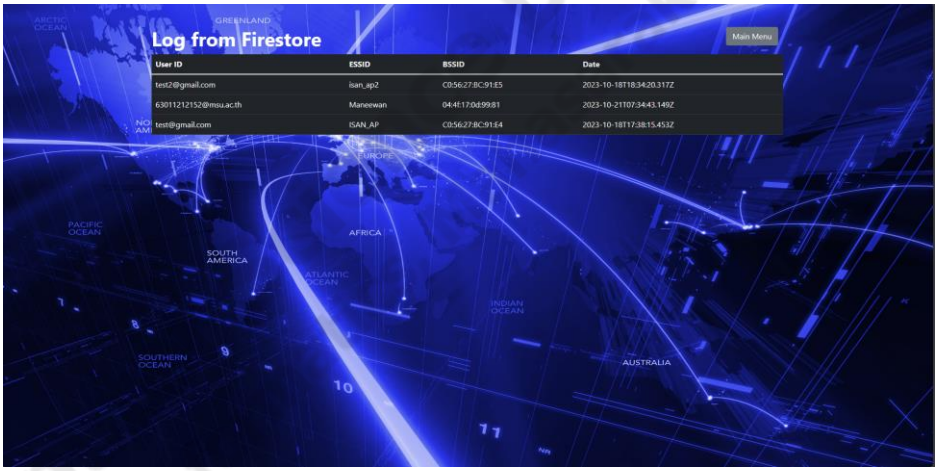
หน้าต่างการแก้ไขข้อมูลผู้ใช้ทั้งหมด โดยจะมีปุ่มให้ Add User แก้ไขข้อมูลของ User และการลบบัญชีของผู้ใช้



ภาพประกอบที่ 1.12 Register Access Point

การกรอกข้อมูลต่างๆเพื่อลงทะเบียน Access Point โดยจะมีข้อมูลให้กรอกดังนี้

1.BSSID 2.ESSID 3.Channel 4.Frequency 5.Capabilities 6.Description



ภาพประกอบที่ 1.13 History Log

การเก็บประวัติข้อมูลเมื่อถูกโจมตีจะดึงข้อมูลมาจาก Firebase และ สามารถค้นหาด้วย วัน ที่ เวลา ที่ถูกโจมตี