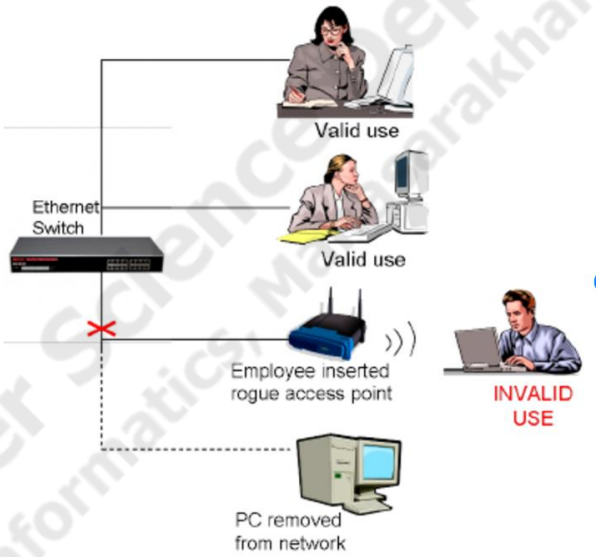
บทที่ 2

ทฤษฎีและระบบงานที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 Rouge Access Point

Rouge Access Point [1] คือ Access Point ใดๆ ก็ตามที่เชื่อมต่อเข้าสู่ Network จริง หรือ Switch ที่ไม่ได้อยู่ในองค์กรนั้นๆ แล้วทำหน้าที่เป็น Access Point ที่ไม่ถูกต้อง ที่พยายามหลอกให้เหยื่อหรือผู้ใช้งานเชื่อมต่อเพื่อวัตถุประสงค์ในการเจาะระบบหรือดักจับข้อมูล หรือ การหลอกให้ผู้ใช้เชื่อว่า มีการให้บริการอินเทอร์ฟรี สำหรับ Wi-Fi



ภาพประกอบที่ 2.1 Rouge Access Point

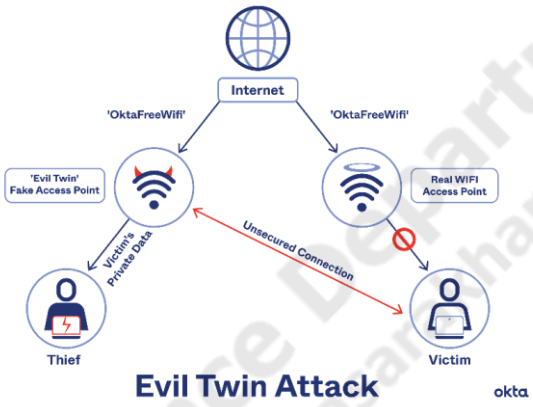
2.1.2 Evil-Twin

Evil-Twin [2] เกิดขึ้นเมื่อผู้โจมตีสร้างจุดเชื่อมต่อ Wi-Fi ปลอมโดยหวังว่าผู้ใช้จะเชื่อมต่อกับจุดดังกล่าวแทนที่จะเป็นจุดที่ถูกต้อง เมื่อผู้ใช้เชื่อมต่อกับจุดเชื่อมต่อนี้ ข้อมูลทั้งหมดที่พวกเขาแชร์กับเครือข่ายจะผ่านผู้โจมตี ผู้โจมตีสามารถสร้าง Evil-Twin ด้วยสมาร์ทโฟน หรืออุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตได้ และซอฟต์แวร์บางตัวที่พร้อมใช้งาน การโจมตีแบบ Evil-Twin นั้นพบได้บ่อยในเครือข่าย Wi-Fi สาธารณะซึ่งไม่ปลอดภัยและทำให้ข้อมูลส่วนตัวมีความเสี่ยง Evil-Twin นั้นมีความอันตรายเพราะเมื่อทำสำเร็จ จะอนุญาตให้ผู้ไม่ประสงค์ดีเข้าถึงอุปกรณ์ของได้ ซึ่งหมายความว่าพวกเขา

สามารถขโมยข้อมูลการเข้าสู่ระบบและข้อมูลส่วนตัวอื่น ๆ รวมถึงข้อมูลทางการเงิน (หากผู้ใช้ทำธุรกรรมทางการเงินเมื่อเชื่อมต่อกับ Wi-Fi)

ความต่างระหว่าง Rouge Access Point และ Evil-Twin

Rouge Access Point คือ จุดเชื่อมต่อที่ไม่ถูกต้อง ที่เชื่อมต่อกับกับเครือข่ายจริงๆ หรือ อยู่ใน network นั้นๆ ในทางตรงกันข้าม Evil-Twin คัดลอกข้อมูลของ Access Point จริงจะพยายามหลอกล่อเหยื่อที่ไม่รับรู้ให้เชื่อมต่อกับลวงเพื่อขโมยข้อมูล ดังนั้น Evil-Twin เป็นอีกหนึ่งรูปแบบของ Rouge Access Point ซึ่งเป็นการโจมตีด้วยเทคนิค Man in the Middle Attack (mitm)

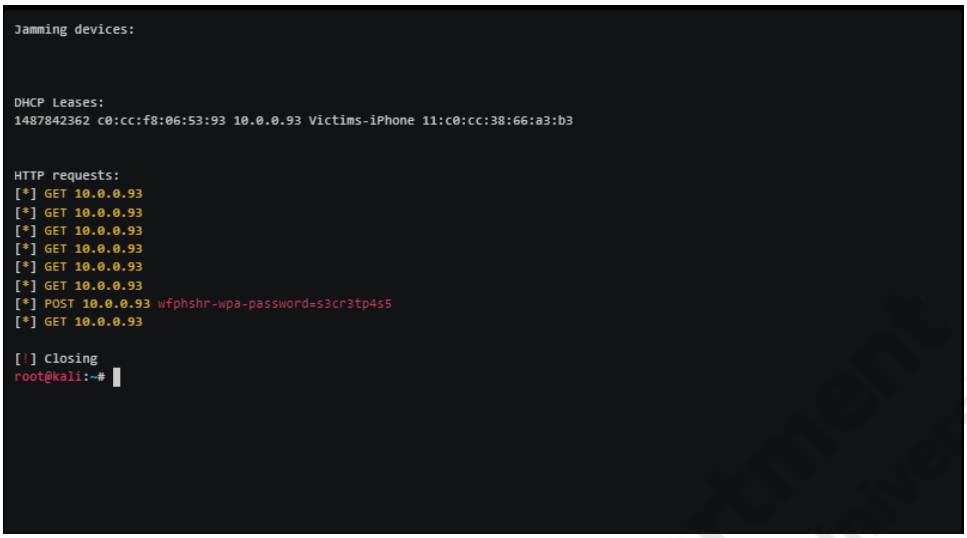


ภาพประกอบที่ 2.2 Evil-Twin

2.1.3 Wi-Fi Phisher

Wi-Fi Phisher [3] เป็น Framework จุดเชื่อมต่อสำหรับการทดสอบความปลอดภัย Wi-Fi การทำงานของ Wi-Fi phisher จะทำการ disconnect ผู้ใช้ที่เชื่อมต่อกับ Access Point อยู่ด้วยการส่ง De-authentication packets ไปยัง AP และเครื่องผู้ใช้ จากนั้นก็จะดักฟังข้อมูลของ AP แล้วปลอมตัวเป็น AP เครื่องนั้นๆ เมื่อเหยื่อพยายามที่จะเชื่อมต่อกับระบบเครือข่าย Wi-Fi ใหม่อีกครั้ง ก็จะมาเชื่อมต่อที่ AP ลวงแทน

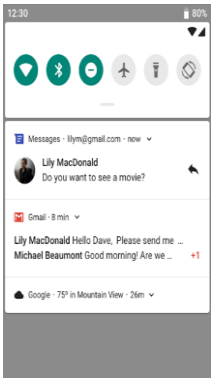
Wi-Fi Phisher มีการติดตั้ง Web Server ขนาดเล็กไว้เพื่อโต้ตอบการร้องขอ HTTP/HTTPS เมื่อไหร่ที่เหยื่อเปิดเว็บไซต์เพื่อเล่นอินเทอร์เน็ต Wi-Fi Phisher จะสร้างหน้าเพจปลอมที่เหมือนจริงขึ้นมาเพื่อแอบถามข้อมูลล็อกอินและรหัสผ่าน เช่น WPA Passphrase สำหรับยืนยันการอัพเกรดเฟิร์มแวร์ของ Router เมื่อเหยื่อใส่รหัสผ่านลงไป ผู้ไม่ประสงค์ดีก็จะได้ข้อมูลรหัสผ่านนั้นทันที ซอฟต์แวร์ Wi-Fi Phisher สามารถทำงานบน Kali Linux และต้องใช้อินเตอร์เฟสสำหรับเชื่อมต่อระบบเครือข่าย Wi-Fi 2 อินเตอร์เฟส ซึ่งหนึ่งอินเตอร์เฟสจะถูกใช้เพื่อปลอมเป็น Access Point



ภาพประกอบที่ 2.3 Wi-Fi Phisher

2.1.4 Notification

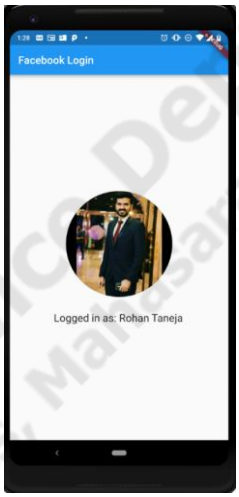
Notification [4] เป็นหนึ่งในช่องทางของแอนดรอยด์ที่เปิดให้แอปพลิเคชันสามารถส่งข้อความให้ผู้ใช้เห็นได้ โดยผู้ใช้ไม่จำเป็นต้องเปิดแอปพลิเคชันขึ้นมา และผู้ใช้ก็สามารถสั่งงานบางอย่างผ่าน Notification ได้ การแจ้งเตือนแบบพุชคือข้อความที่ปรากฏขึ้นบนอุปกรณ์พกพา เช่น คะแนนกีฬา คำเชิญไปงานแฟลชเซลล์ หรือคูปองสำหรับดาวน์โหลด ผู้เผยแพร่แอปพลิเคชันสามารถส่งได้ทุกเมื่อเนื่องจากผู้ใช้ไม่จำเป็นต้องอยู่ในแอปพลิเคชันหรือใช้อุปกรณ์ของตนเพื่อรับ การแจ้งเตือนแบบพุชดูเหมือนข้อความ SMS และการแจ้งเตือนทางมือถือ แต่เข้าถึงได้เฉพาะผู้ใช้ที่ติดตั้งแอปพลิเคชันของคุณแพลตฟอร์มมือถือทั้งหมด iOS, Android, และ Windows – มีบริการของตัวเองเพื่อรองรับการพุช



ภาพประกอบที่ 2.4 Notification Android

2.1.5 Flutter Login Facebook

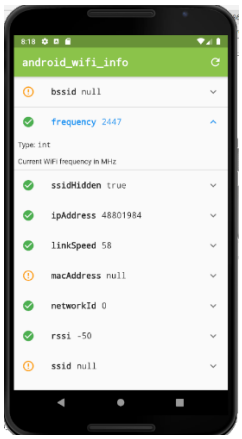
Flutter Login Facebook [5] คือชุดคำสั่งช่วยให้ผู้ใช้เข้าสู่ระบบแอปพลิเคชันด้วย การเข้าสู่ระบบด้วย Facebook เมื่อเข้าสู่แอปพลิเคชันด้วย Facebook ผู้ใช้สามารถให้สิทธิ์การอนุญาตแก่แอปพลิเคชันเพื่อให้รับข้อมูลหรือดำเนินการบางอย่างบน Facebook แทนผู้ใช้ได้การเข้าสู่ระบบนี้สามารถใช้ได้บน iOS, Android, เว็บ, แอปพลิเคชันบนเดสก์ท็อป และอุปกรณ์ต่างๆ เช่น สมาร์ททีวี และอุปกรณ์เชื่อมต่ออินเทอร์เน็ตต่าง ๆ สามารถใช้การเข้าสู่ระบบด้วย Facebook ได้ง่าย ๆ เพื่อการยืนยันตัวตนหรือเพื่อทั้งการยืนยันตัวตนและการเข้าถึงข้อมูลการแจ้งเตือนเมื่อผู้ใช้เข้าสู่ระบบผ่าน Facebook โดยการกดปุ่มที่อยู่บนหน้าแอปพลิเคชัน จะเรียกใช้ชุดคำสั่งของ Facebook ในการเข้าสู่ระบบและใช้สิทธิ์อนุญาตในการเข้าสู่ระบบ



ภาพประกอบที่ 2.5 Flutter Login Facebook

2.1.6 Wi-Fi Scan Flutter

Wi-Fi Scan Flutter [6] เป็น API ของ Flutter ที่ช่วยเก็บข้อมูลต่างของ Wi-Fi และ Access Point ต่างๆให้เรียกดู ใน mobile Application (Android)



ภาพประกอบที่ 2.6 WiFi Scan Flutter

2.1.7 Evil-Twin Detection on Client-Side

Evil-Twin Detection on Client-Side [7] การเสนอวิธีการตรวจสอบ การโจมตีแบบ Evil Twin ฝั่งผู้ใช้ ด้วยการตรวจ Modulation Coding Scheme (MCS) และ Round Trip Time (RTT) โดยการตรวจสอบเฟรม RTT และ MCS ที่สอดคล้องกัน ผลการจำลองพบว่าสามารถระบุ ET ที่มีอยู่ได้ โดยข้อมูลที่ถูกรวบรวม ระบบจะบันทึกการหน่วงเวลาก่อน โดยส่งรอบการตรวจสอบ ถ้าความแตกต่างของดีเลย์เกินมาตราฐาน ระบบจะรายงานการตรวจหา ET ที่มีอยู่

ความน่าเชื่อถือของการตรวจจับ ET ขึ้นอยู่กับปริมาณข้อมูล RTT เพื่อให้ได้รับค่า RTT ที่แตกต่างกันในปริมาณที่เพียงพอ ผู้ใช้ต้องย้ายไปรอบๆ ตำแหน่งปัจจุบัน สำหรับการย้ายแต่ละครั้ง ทั้ง RTT และ MCS ที่เกี่ยวข้องจะถูกรวบรวมและเปรียบเทียบกับสถานที่อื่นๆ ในสมมติฐาน ด้วยค่า MCS เดียวกัน ค่า RTT ควรใกล้เคียงกัน มิฉะนั้น อาจเกิดการเชื่อมต่อแบบดับเบิ้ลฮอป ซึ่งหมายความว่า ET ในพื้นที่สำรวจอาจมีอยู่

2.2 ระบบงานที่เกี่ยวข้อง

2.2.1 Detection and Response System Against The Evil Twin Attack

Detection and Response System Against The Evil Twin Attack [8] เป็นซอฟต์แวร์จากวิทยานิพนธ์ สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยมหาสารคาม ใช้สำหรับติดตั้งภายในองค์กร ใช้งานสำหรับตรวจจับและตอบโต้ ระบบจะทำการตรวจจับโดยการค้นหาข้อมูลของ Access Point ในบริเวณรอบๆ แล้วนำมาเปรียบเทียบกับข้อมูล Access Point ที่ลงทะเบียนไว้ในระบบ หากตรวจพบจะส่งการแจ้งเตือน

หากตรวจพบการโจมตีจะจำแนกออกเป็น 3 ประเภทและแบ่งเป็น 3 สีคือ

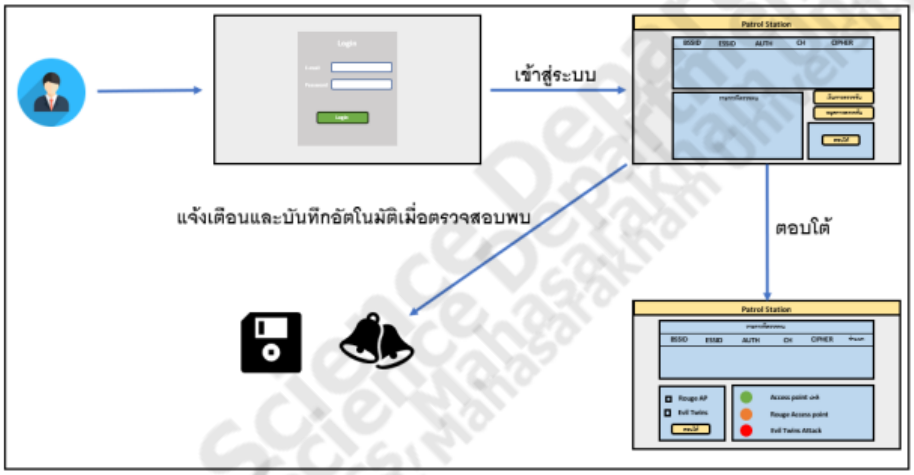
สีเขียว คือ Access Point ที่ตรวจพบ ที่ลงทะเบียนไว้ในระบบโดย จำแนกได้จาก การเปรียบเทียบ จาก ESSID และ BSSID ตรงกับที่ลงทะเบียนไว้ในระบบ

สีส้ม คือ Access Point ที่ตรวจพบ ที่ไม่ได้ลงทะเบียนไว้ในระบบ

สีแดง คือ Access Point ที่ตรวจพบ ที่จงใจทำการโจมตี การที่มี ESSID ตรงกับข้อมูลของ Access Point ที่มีการลงทะเบียนกับระบบ แต่มี BSSID ไม่ตรงกับข้อมูล Access Point ที่ลงทะเบียนไว้ในระบบ

การแจ้งเตือนเป็นการแจ้งเตือนไปยังผู้ดูแลระบบแบบอัตโนมัติโดยแจ้งเตือนไปยัง Line Group ผ่านระบบ Line notification และ Email ที่ลงทะเบียนไว้ในระบบในส่วนข้อมูลของสมาชิก

การป้องกันการโจมตีเบื้องต้นเพื่อป้องกันไม่ให้ผู้ใช้งาน การทำ De-authentication



ภาพประกอบที่ 2.7 Detection and Response System Against The Evil Twin Attack

2.2.2 Fing Application

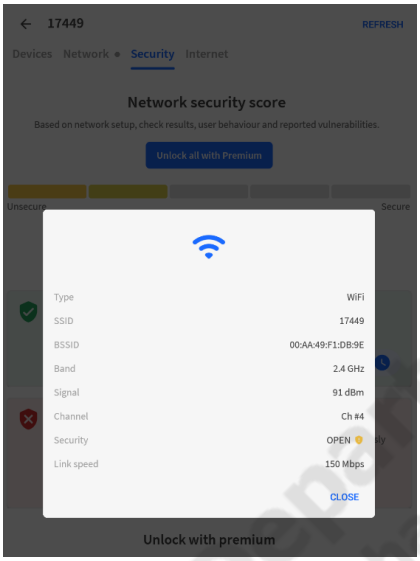
Fing Application [9] ที่ค้นหาผู้ใช้ Wi-Fi ที่กำลังบุกรุกกล้องของโทรศัพท์มือถือและซ่องโหว่ Fing เป็นเครื่องสแกนเครือข่าย อุปกรณ์ทั้งหมดที่เชื่อมต่อกับ Wi-Fi และระบุอุปกรณ์เหล่านั้นด้วยเทคโนโลยีที่จดสิทธิบัตรของเราซึ่งใช้โดยผู้ผลิตเราเตอร์และ บริษัท ป้องกันไวรัสทั่วโลก

1. เรียกใช้การทดสอบความเร็วอินเทอร์เน็ต Wi-Fi และเซลลูล่าร์ความเร็วในการดาวน์โหลดและการวิเคราะห์ความเร็วในการอัปโหลด

2. สแกนเครือข่ายด้วยเครื่องสแกนเครือข่าย Wi-Fi และ LAN ของ Fing และค้นหาอุปกรณ์ทั้งหมดที่เชื่อมต่อกับเครือข่ายใดก็ได้

3. รับการจดจำอุปกรณ์ที่แม่นยำที่สุดของที่อยู่ IP ที่อยู่ MAC ชื่ออุปกรณ์รุ่นผู้จำหน่ายและผู้ผลิต

4. รวมถึงการสแกนพอร์ต ping อุปกรณ์ traceroute และการค้นหา DNS
5. รับการแจ้งเตือนความปลอดภัยเครือข่ายและอุปกรณ์ไปยังโทรศัพท์และอีเมล



ภาพประกอบที่ 2.8 Fing Application

2.3 ตารางเปรียบเทียบ

ตารางที่ 2.1 ตารางเปรียบเทียบระบบที่เกี่ยวข้อง

ฟังก์ชั่นการทำงาน	Detail	Fing	Detection and Response System Against The Evil Twin Attack	ระบบที่พัฒนา
Login	เข้าสู่ระบบเพื่อใช้งาน	✓	✓	✓
การสมัครสมาชิก	สมัครสมาชิกก่อนเข้าใช้งานระบบ	✓	✓	✓
การแจ้งเตือน	แจ้งเตือนไปยังผู้ใช้งานเมื่อถูกการโจมตีด้วยเทคนิค Evil-Twin	✓	✓	✓

ตารางที่ 2.1 ตารางเปรียบเทียบระบบที่เกี่ยวข้อง (ต่อ)

ฟังก์ชั่นการทำงาน	Detail	Fing	Detection and Response System Against The Evil Twin Attack	ระบบที่พัฒนา
connect Wi-Fi	เชื่อมต่อ Wi-Fi ภายในแอปพลิเคชัน			✓
Disconnect Wi-Fi	ยกเลิกเชื่อมต่อ Wi-Fi ภายในแอปพลิเคชัน			✓
Response Evil-Twin Attack	ตอบโต้การโจมตีด้วยเทคนิค Evil-Twin		✓	
Resolve Client Data of Access Point	กู้คืนข้อมูล Client ที่ล้มเหลว		✓	
Detect Evil-Twin Attack	ตรวจสอบ Access Point ที่เป็นการโจมตีด้วยเทคนิค Evil-Twin		✓	✓
Detect Rouge Access Point	ตรวจสอบ Access Point ที่ไม่ได้ลงทะเบียน (Rouge Access Point)		✓	✓