บทความวิจัย

ระบบแจ้งเตือนการเชื่อมต่อแอคเซสพอยต์ที่ไม่ถูกต้อง

A Notification System for Illegitimate Access Point Associations

พงศกร ศรีวังสุ, กฤติพงศ์ แสงงาม, อรรถพล สุวรรณษา
ภาควิชาวิทยการคอมพิวเตอร์ คณะวิทยการสารสนเทศ มหาวิทยาลัยมหาสารคาม

บทคัดย่อ

ความปลอดภัยในการเข้าใช้งานเครือข่ายเป็นสิ่งสำคัญต่อผู้ใช้งาน Smartphone โดยเฉพาะผู้ใช้ที่เชื่อมต่อ Wi-Fi ในที่สาธารณะ ในการเข้าสู่ระบบอินเทอร์เน็ตมีโอกาสในการถูกโจมตี จากผู้ไม่ประสงค์ดี เนื่องจากผู้ใช้งานไม่ได้มีความระมัดระวังและสังเกต หรือ มีความรู้เกี่ยวกับ ความปลอดภัยของระบบ Wi-Fi หนึ่งในการโจมตีที่ถูกใช้อย่างแพร่หลายและมีผลของความรุนแรงค่อนข้างสูง คือ การเชื่อมต่อแอคเซสพอยต์ที่ไม่ถูกต้องหรือที่เรียกว่า Rouge Access Point และอีกหนึ่งเทคนิคคือ Evil-Twin ซึ่งผู้ใช้งาน จะได้รับผลเสียต่างๆจากการโจมตีด้วยเทคนิคนี้ เช่น ถูกขโมยข้อมูลส่วนตัวที่สำคัญ

คำสำคัญ: Wireless LAN, Wi-Fi, Rouge Access Point, Evil-Twin, ระบบแจ้งเตือน

1.บทนำ

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

Smartphone เป็นหนึ่งในเป้าหมายการโจมตีของผู้ไม่ประสงค์ดี ที่พยามยามต้องการข้อมูลสำคัญต่างๆ หรือ ข้อมูลทางการเงิน ของผู้ใช้งานไม่ได้คำนึงถึง หรือ ไม่ได้มีความรู้เกี่ยวกับความปลอดภัย

โดยเฉพาะเครือข่าย Wi-Fi เวลาใช้งานในที่สาธารณะ เทคนิคการรบกวนหรือโจมตีต่างๆ สามารถโจมตี อุปกรณ์มือถือผ่านเครือข่ายที่อาจไม่ปลอดภัย เพื่อดักจับข้อมูลมีหลายเทคนิค หนึ่งในเทคนิคนี้คือ เทคนิคการสร้าง Rouge Access Point และ Evil-Twin การทำงานของเทคนิคจะรวดเร็วมาก ทำให้ผู้ใช้งานอาจไม่สามารถรับรู้ถึงการถูกโจมตี หรือ 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

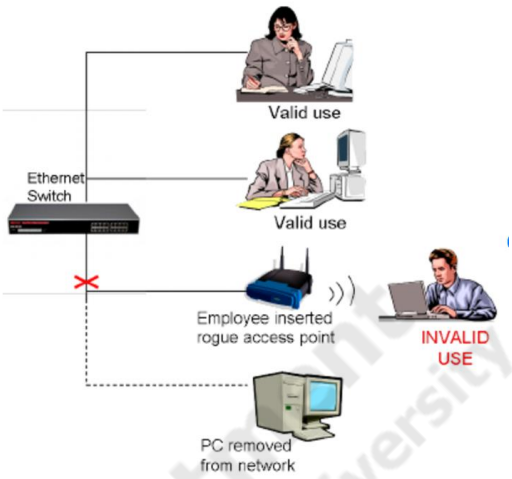
APs อย่าง Rogue Access Point และ Evil-Twin ขณะใช้งานเครือข่าย Wi-Fi หรือ

แอคเซสพอยต์ใดๆ ในพื้นที่สาธารณะ เพื่อให้ผู้ใช้มีความระแวดระวังกับการเชื่อมต่อเครือข่าย Wi-Fi ที่ไม่ถูกต้อง อาจจะเกิดขึ้นจากผู้ไม่ประสงค์ดี ทำการโจมตีเครือข่าย ณ ขณะนั้น ซึ่งจะเกิดผลเสียหลายประการตามมาในอนาคต เช่น ข้อมูลหรือความลับต่างๆสูญหาย ไม่ว่าจะเป็นข้อมูลการเงิน ข้อมูลส่วนตัวของผู้ใช้งาน ที่ผู้โจมตีสามารถดักจับได้ โดยการตรวจสอบ illegitimate APs จะดูจากข้อมูล ESSID ID ของ Access Point ใดๆ ในระบบเครือข่าย หากมี ESSID และ BSSID ปรากฏขึ้นโดยไม่ได้รับอนุญาตในระบบ สันนิษฐานได้ ว่ามี Rouge Access Point หรือ Evil-Twin ในระบบเครือข่าย

2.ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

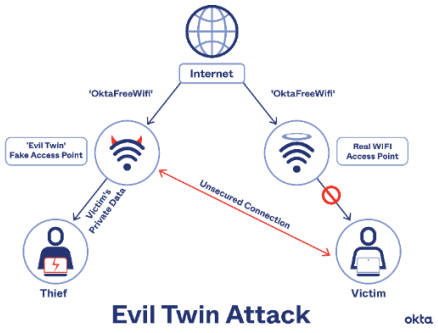
ทฤษฎีที่เกี่ยวข้อง

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



ภาพประกอบที่ 1 Rouge Access Point

Evil Twin [2] เกิดขึ้นเมื่อผู้โจมตีสร้างจุดเชื่อมต่อ Wi-Fi ปลอมโดยหวังว่าผู้ใช้จะเชื่อมต่อกับจุดดังกล่าวแทนที่จะเป็นจุดที่ถูกต้องเมื่อผู้ใช้เชื่อมต่อกับจุดเชื่อมต่อนี้ข้อมูลทั้งหมดที่แชร์กับเครือข่ายจะผ่านผู้โจมตี

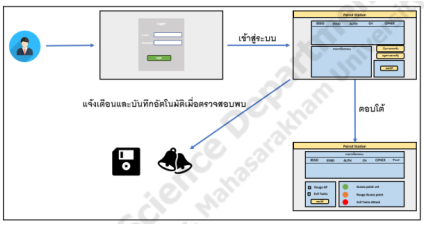


ภาพประกอบที่ 2 Evil-Twin

Detection and Response System Against The Evil Twin Attack [3] เป็นซอฟต์แวร์จากวิทยานิพนธ์ สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยมหาสารคาม ใช้สำหรับติดตั้งภายในองค์กร ใช้งานสำหรับตรวจจับและตอบโต้ ระบบจะทำการตรวจจับโดยการค้นหาข้อมูลของ Access Point ในบริเวณรอบๆ แล้วนำมาเปรียบเทียบกับข้อมูล Access Point ที่ลงทะเบียนไว้ในระบบ หาก

ตรวจพบจะส่งการแจ้งเตือน เป็นการแจ้งเตือนไปยังผู้ดูแลระบบแบบอัตโนมัติโดยแจ้งเตือนไปยัง Line Group ผ่านระบบ Line notification และ Email ที่ลงทะเบียนไว้ในระบบในส่วนข้อมูลของสมาชิก

การป้องกันการโจมตีเบื้องต้นเพื่อป้องกันไม่ให้ผู้ใช้งาน การทำ De-authentication



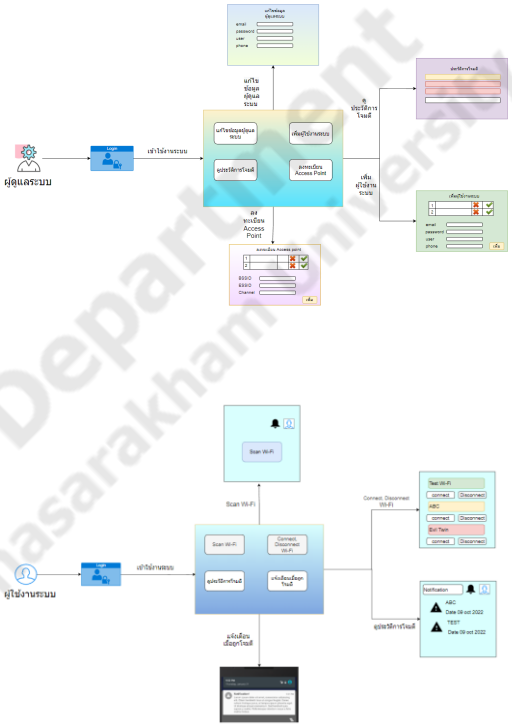
ภาพประกอบที่ 3 Detection and Response System Against The Evil Twin Attack

งานวิจัยที่เกี่ยวข้อง

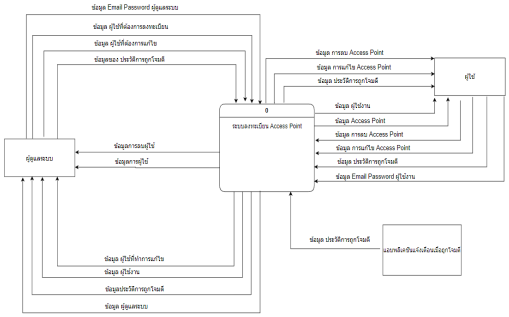
Evil-Twin Detection on Client-Side [4] การเสนอวิธีการตรวจสอบ การโจมตีแบบ Evil Twin ฝั่งผู้ใช้ ด้วยการตรวจ Modulation Coding Scheme (MCS) และ Round Trip Time (RTT) โดยการตรวจสอบเฟรม RTT และ MCS ที่สอดคล้องกัน ผลการจำลองพบว่าสามารถระบุ ET ที่มีอยู่ได้ โดยข้อมูลที่ถูกรวบรวม ระบบจะบันทึกการหน่วงเวลาก่อน 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

3.แผนดำเนินงาน



ภาพประกอบที่ 4 ภาพรวมของระบบ



ภาพประกอบที่ 5 แผนภาพบริบทของระบบ

4.การทดสอบแอปพลิเคชัน

จาการทดสอบระบบการแจ้งเตือนการเชื่อมต่อแอคเซสพอยต์ที่ไม่ถูกต้องพบว่าระบบสามารถแจ้งเตือนเมื่อถูกโจมตีด้วย เทคนิค Evil-Twin และ Rouge Access Point

แอปพลิเคชันสามารถ connect Wi-Fi ที่ต้องการ ได้ในแอปพลิเคชัน มีข้อมูลและสถานะต่างๆ

การทดสอบเว็บไซต์สำหรับลงทะเบียน Access Point ในส่วนของผู้ดูแลระบบที่สามารถลงทะเบียน Access Point ได้ถูกต้องและครบถ้วนทุกฟังก์ชันการทำงาน

5.สรุปผลและข้อเสนอแนะ

5.1 สรุปผลและอภิปาย

มีความจำกัดของระบบที่ไม่สามารถป้องการ ใช้เทคนิค Mac Spoofing และ ไม่สามารถระบุความต่างระหว่าง Rouge Access Point กับ Wi-Fi Hotspot ที่ยังไม่ลงทะเบียนข้อมูล เนื่องจากมีข้อจำกัดในเรื่องของข้อมูลในระบบ Android ฟังกชันต่างๆยังทำงานได้อย่างถูกต้อง ซึ่งได้ประเมิณตวามถึงพอใจของผู้ใช้งาน ซึ่งการออกแบบและการทำงานอยู่ในระดับปานกลาง

5.2 ข้อเสนอแนะ

ใช้ทรัพยากรของระบบเพื่อปรับปรุงประสิทธิภาพของระบบและเว็บไซต์ในการลงทะเบียน Access Point การแจ้งเตือน การตอบสนองหรือความเร็ว พิจารณาการปรับปรุงอินเตอร์เฟซและส่วนติดต่อของเว็บไซต์ลงทะเบียนเพื่อทำให้มันเป็นไปตามความสะดวกและง่ายต่อผู้ใช้ การเพิ่มมาตรการความปลอดภัยและการป้องกันการโจมตีที่อาจเกิดขึ้นต่อระบบแจ้งเตือนแอคเซสพอยต์

6.เอกสารอ้างอิง

1. Evil-Twin-Attack, www.okta.com/identity-101/evil-twin-attack
2. Evil twin attacks and how to prevent, https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks
3. Detection and Response System Against The Evil Twin Attack, http://digital.csmsu.net:8080/library/handle/123456789/138
4. Evil-Twin Detection on Client Side, Songrit Kitisriworapan, Aphirak Jansang, AnanPhonphoem, https://ieeexplore.ieee.org/document/895515