NECTEC
a member of NSTDA

เอกสารเผยแพร่

THINK LIKE ATTACKERS!

เส้นทางสู่ความปลอดภัยทางไซเบอร์สำหรับ IoT

“เข้าใจเส้นทางโจร
เพื่อหาทางป้องกัน”

บทความ | ดร.กลิกา สุขสมบูรณ์

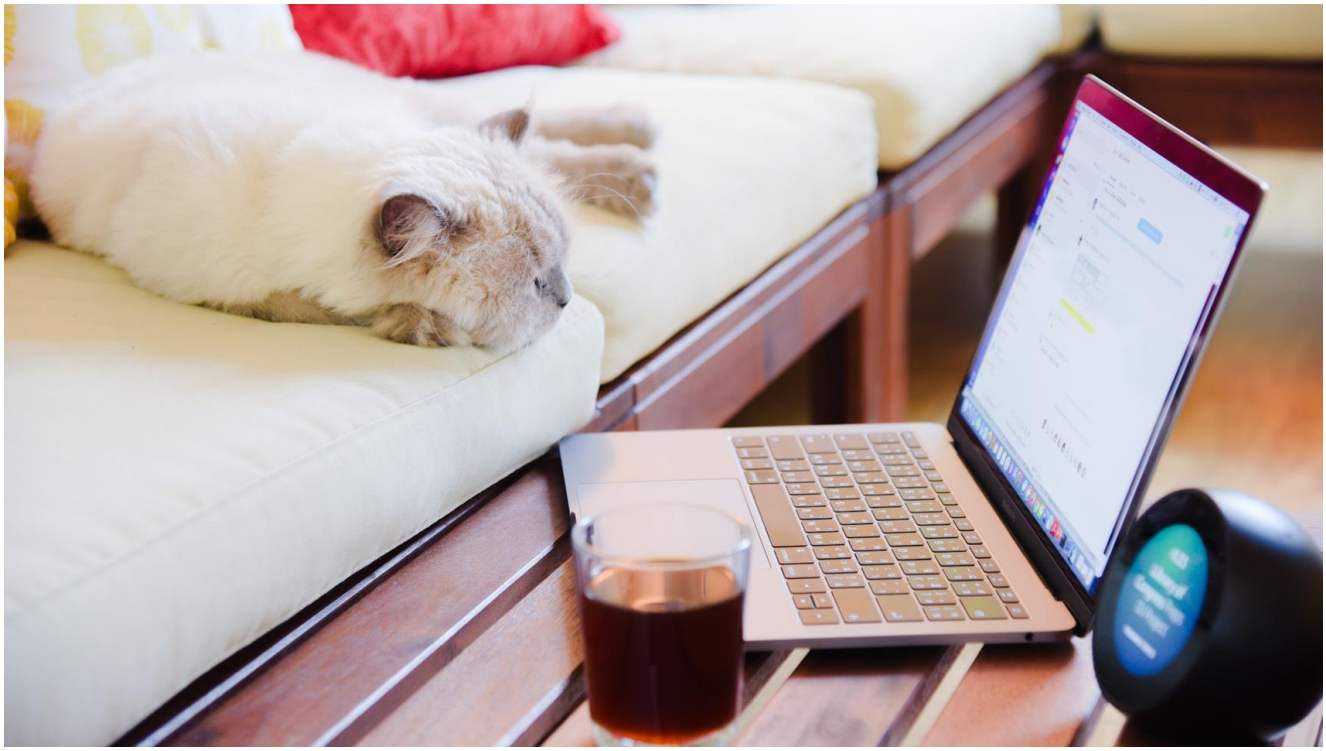
ทีมระบบไซเบอร์-กายภาพ (CPS)
หน่วยทรัพยากรด้านการคำนวณและไซเบอร์-กายภาพ (NCCPI)

THINK LIKE ATTACKERS!

เส้นทางสู่ความปลอดภัยทางไซเบอร์สำหรับ IoT

กลิกา สุขสมบูรณ์

บทนำ



“สรรพสิ่งพูด” หรือ “Things Talk” เป็นคำกล่าวที่ไม่แปลกอีกต่อไปสำหรับยุค 4.0 ซึ่งเป็นยุค Internet of Things (IoT) หรือ *อินเทอร์เน็ตแห่งสรรพสิ่ง* ที่มีใช้กันอย่างแพร่หลาย ตั้งแต่สิ่งต่าง ๆ รอบตัวเราภายในบ้าน ไม่ว่าจะเป็นกล้อง CCTV, ลำโพงอัจฉริยะ, หลอดไฟอัจฉริยะ ไปจนถึงระดับอุตสาหกรรมขนาดใหญ่ หรือแม้แต่ใน ยานอวกาศ “ใช่! คุณฟังไม่ผิด วัตถุในยานอวกาศของนาซ่า (NASA) ก็คุยกับคนบนโลกได้ด้วยเทคโนโลยี IoT เช่น Int-Ball” [1]

สืบเนื่องมาจากการพัฒนาของอุปกรณ์ฮาร์ดแวร์ขนาดเล็กที่มีประสิทธิภาพการคำนวณสูงแต่ราคาถูก การพัฒนาแพลตฟอร์มสำหรับการเชื่อมต่ออุปกรณ์ IoT ให้ใช้งานง่ายและหลากหลายมากขึ้น และการพัฒนาระบบเครือข่ายอินเทอร์เน็ตที่สามารถรองรับการเชื่อมต่อทุกสรรพสิ่งได้อย่างรวดเร็ว ทำให้เรามีอุปกรณ์ IoT แพร่หลายในท้องตลาดที่สามารถเชื่อมต่อถึงกันกับผู้ใช้งานและถูกควบคุมผ่านระบบเครือข่ายอินเทอร์เน็ต และด้วยการเชื่อมต่อที่ครอบคลุมนี้ทำให้ผู้ใช้สามารถเข้าถึงอุปกรณ์ IoT ได้จากทุกหนทุกแห่งถึงแม้ว่าจะอยู่ในอวกาศก็ตาม

แต่แน่นอนว่า การเข้าถึงและควบคุมอุปกรณ์ IoT ได้ง่ายจากที่ใดก็ตามส่งผลให้ IoT กลายเป็นสนามประลองฝีมืออิสระขนาดใหญ่ที่ไร้ข้อจำกัดของ Hacker เปรียบได้ดั่งบุฟเฟต์ที่ใครก็ตามที่เจาะระบบและเข้าควบคุมอุปกรณ์ที่เชื่อมต่ออยู่ในโลกออนไลน์ได้แล้ว จะสามารถใช้ IoT เป็นช่องทางในการก่ออาชญากรรมทางไซเบอร์ได้ ดังจะเห็นได้จากข่าวอุปกรณ์ IoT ถูกใช้เป็นเครื่องมือในการโจมตีทางไซเบอร์ ด้วยเทคนิคการยึดอุปกรณ์ IoT จำนวนหนึ่งเพื่อใช้โจมตีระบบไอทีอื่น เช่น Mirai Bot [2] และ Ransomware Attack [3] เป็นต้น

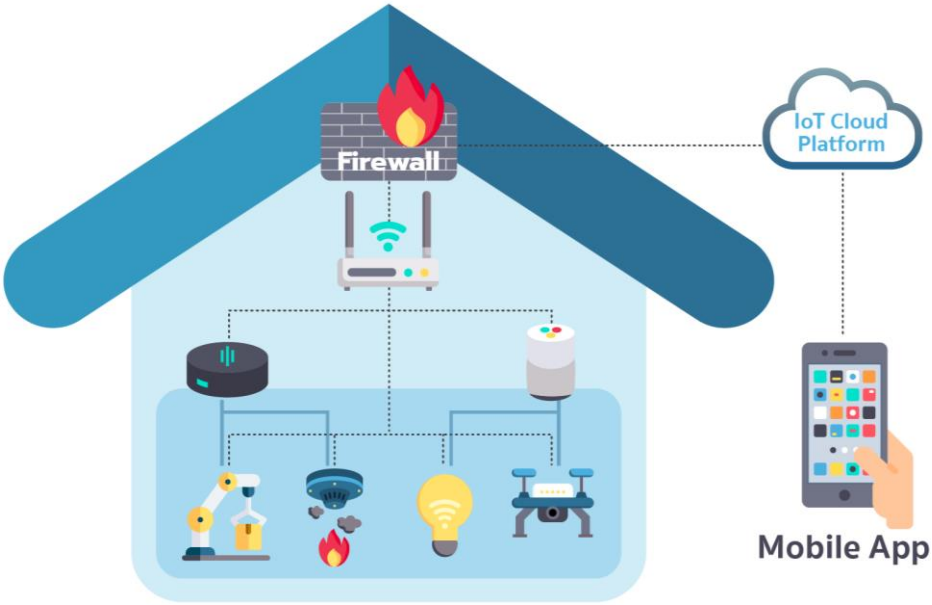
มนต์ขลัง Cyber Security เสื่อม?

ข่าวการโจมตีทางไซเบอร์ในช่วงไม่กี่ปีที่ผ่านมาสร้างความสงสัยว่า ทำไมระบบรักษาความปลอดภัยทางไซเบอร์ เช่น Firewall ในระบบเครือข่ายสื่อสาร อีกทั้งอุปกรณ์และซอฟต์แวร์ป้องกันด้าน Cyber Security มากมายในท้องตลาดถึงเอาไม่อยู่!! ภายใต้ความชะล่าใจของผู้พิทักษ์ไอทีในการอนุญาตให้นำเอาอุปกรณ์ IoT ที่ไม่ได้มาตรฐานมาติดตั้งไว้ภายในระบบเครือข่ายภายในของตน โดยไม่ได้รับการตรวจสอบให้แน่ใจก่อนว่าไม่ได้กำลังเปิดประตูเชื้อเชิญผู้ไม่หวังดีเข้ามาในระบบ

แท้จริงแล้ว Firewall ในระบบเครือข่ายของเราไม่ได้เสื่อม แต่ Firewall ของเราไม่ได้ป้องกันศึกภายในหากแต่ป้องกันเฉพาะศึกภายนอกที่จะเข้ามาจู่โจมระบบ ดังนั้นการแฝงตัวเข้ามาของภัยคุกคามทางไซเบอร์ในรูปของอุปกรณ์ IoT ซึ่งมีการติดต่อกับ ioT cloud platform และ Mobile Application ที่อยู่ภายนอก เปรียบเสมือนการปูพรมแดงให้ผู้โจมตีเข้ามาล้วงข้อมูลภายในไปได้อย่างง่ายดาย

เข้าใจเส้นทางโจรเพื่อหาทางป้องกัน

การทำความเข้าใจเส้นทางโจร หรือ Think Like Attackers เพื่อหาทางป้องกัน ไม่ได้เป็นแนวคิดใหม่ แนวคิดนี้ใช้ในการรบมาตั้งแต่สมัยโบราณ ดังปรัชญาการรบของซุนวู ที่ว่า *“รู้เขารู้เรา รบร้อยครั้งชนะร้อยครั้ง”* ดังนั้น การคุ้มครองความปลอดภัยทางไซเบอร์ในระบบ IoT จึงเริ่มต้นจากการตรวจสอบเส้นทางการเดินทางของข้อมูลในระบบ IoT ซึ่งจะช่วยแกะรอยทางเข้าของโจรในระบบไซเบอร์ได้ ดังรูปที่ 1.



รูปที่ 1. เส้นทางข้อมูลของระบบ IoT

การเดินทางของข้อมูลในระบบ IoT เริ่มตั้งแต่...

อุปกรณ์ IoT (Hardware) : ภายในอุปกรณ์ IoT ถูกควบคุมด้วยซอฟต์แวร์ฝังตัวที่เรียกกันว่า เฟิร์มแวร์ (Firmware) และช่องทางการปรับบันทึกเฟิร์มแวร์เข้าไปในตัวชิพหรือแผงวงจรของอุปกรณ์ IoT จะกระทำผ่านพอร์ตเชื่อมต่อ หากตัวอุปกรณ์ IoT หรือแผงวงจรของอุปกรณ์ IoT นั้นเปิดช่องทางสำหรับการเชื่อมต่อจากภายนอกไว้ (Backdoor) เช่น Tx-Rx port ช่องทางนี้เป็นช่องทางที่เปิดไว้เพื่อให้ผู้ผลิตหรือผู้ใช้งานเข้าไปอัพเดท Firmware หรือทำการ Reverse engineer firmware binary images ได้ แต่ถ้าหากผู้ผลิตไม่ปิดช่องทางนี้ภายหลังการอัพเดท Firmware ทำให้ Hacker สามารถนำ Firmware ปลอมเข้าไปแฝงตัวในอุปกรณ์ได้ หรือ Hacker อาจดึงข้อมูลบางส่วนที่บันทึกไว้ในอุปกรณ์ IoT ออกมา และโดยมากข้อมูลที่เก็บไว้ในหน่วยความจำของตัวอุปกรณ์มักไม่ถูกเข้ารหัส ซึ่งส่งผลให้เกิดความเสียหายด้านการรั่วไหลของข้อมูลส่วนตัว (Privacy leak)

โพรโทคอล (Protocol) : โพรโทคอลที่ใช้ในการเชื่อมต่ออุปกรณ์ไปบน Cloud หรือ เซิร์ฟเวอร์ของผู้ให้บริการ IoT โดยมากอุปกรณ์ IoT จะส่งข้อมูลผ่านโพรโทคอล MQTT และ HTTP ซึ่งทำให้ข้อมูลที่ส่งไม่ถูกเข้ารหัส ดังนั้นทำให้ผู้โจมตีสามารถเข้าโจมตีโดยขโมยข้อมูลหรือเรียนรู้ข้อมูลที่ตัวอุปกรณ์ส่งและรับจากผู้ใช้ได้ ดังนั้นผู้โจมตี จะเลือกเข้าจู่โจม IoT ที่ใช้ช่องทางการสื่อสารที่อ่อนไหวเป็นเป้าหมายการโจมตีอันดับต้น ๆ

ข้อมูล (Data) : ข้อมูลที่ถูกส่งจากอุปกรณ์ IoT และถูกจัดเก็บไว้ใน Cloud server หรือตัวอุปกรณ์ไม่ถูกเข้ารหัส ดังนั้น จึงเป็นช่องโหว่ที่ทำให้ผู้ให้บริการ Cloud หรือ Cloud server ถูกโจมตี ผู้โจมตีสามารถล่วงรู้ข้อมูลเหล่านั้นได้ หากไม่มีระบบป้องกันจาก Cloud เอง

ซอฟต์แวร์ (Application) : ตัว Application ที่ใช้ในการสื่อสารระหว่างผู้ใช้และอุปกรณ์ หากมีช่องโหว่ในการรั่วไหลของการปกป้อง Credential ของตัวผู้ใช้ทำให้เกิดความไม่ปลอดภัยและสูญเสียข้อมูลส่วนบุคคลได้ ซึ่งส่วนใหญ่ Credential ของผู้ใช้จะนำมาซึ่งข้อมูลลับที่ใช้ในการเข้าถึงข้อมูลในส่วนอื่น ๆ ได้

รอยรั่วที่พบบ่อย

Hacker ส่วนใหญ่มักจะหาจุดอ่อน หรือรอยรั่วของอุปกรณ์ IoT โดยอาศัยรอยรั่วที่พบได้บ่อย เพราะนี่จะเป็นเส้นทางที่ง่ายที่สุดที่ Hacker จะเลือกโจมตี ทั้งนี้กลุ่มวิจัย OWASP (Open Web Application Secure Project) ได้มีการจัดอันดับช่องโหว่ความไม่ปลอดภัยของ IoT ที่พบบ่อย 10 อันดับแรก ดังนี้

1. พาสเวิร์ดที่คาดเดาได้ง่าย : ในการเข้าถึงอุปกรณ์ IoT นั้น Mobile Application ที่ใช้ในการเชื่อมต่อระหว่างผู้ใช้กับอุปกรณ์จะบังคับให้สร้าง ID และ Password ซึ่งโดยมากผู้ใช้งานจะเลือกใช้พาสเวิร์ดที่คาดเดาได้ง่ายเกินไปเพื่อให้ผู้ใช้งานเองสามารถจำได้ง่าย หรือเป็นพาสเวิร์ดที่มีใช้ทั่วไปซึ่งสามารถหาได้ใน Internet ทำให้ผู้โจมตีอาศัยวิธีการเดาสุ่มจากกลุ่มของพาสเวิร์ดเหล่านั้นในการ crack ทำให้ผู้โจมตีสามารถเข้าควบคุมอุปกรณ์ได้ หรือการตั้งพาสเวิร์ดตาม Password ยอดฮิตซึ่งได้มีการรวบรวมไว้ในอินเทอร์เน็ต ดังนั้น HACKER เพียงสร้าง List ของ Password เหล่าไว้แล้วใช้โปรแกรม crack โดยใช้เวลาเพียงไม่กี่วินาทีก็สามารถเจาะเข้าไปควบคุมอุปกรณ์ได้ทันที

2. เน็ตเวิร์คที่ให้บริการไม่ปลอดภัย : ตัวอย่างเช่น เน็ตเวิร์คที่ให้ใช้ฟรีในบางพื้นที่ เช่น WiFi Access Point ในร้านกาแฟที่ไม่มีการเข้ารหัส ทำให้เปิดโอกาสให้ถูกดักฟังข้อมูลที่ส่งผ่าน Network Gateway นั้นได้

3. ความไม่ปลอดภัยของอินเตอร์เฟสการเชื่อมต่อของระบบ IoT : การเปิดพื้นที่การเชื่อมต่อที่ไม่มีนโยบายการจัดการการเข้าถึงข้อมูล (Access Control) ทำให้การเข้าถึงที่ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลในระบบ IoT ได้ง่าย

4. ไม่มีการอัพเดทเฟิร์มแวร์ของอุปกรณ์ : อุปกรณ์ไม่มีการอัพเดทเฟิร์มแวร์ที่สามารถปิดช่องโหว่การโจมตีใหม่ ๆ ทำให้อุปกรณ์ IoT เหล่านั้นถูกโจมตีได้ เช่น ในกรณีการอัพเดท OS ของอุปกรณ์ หรือ Patch เพื่อปิดช่องโหว่เก่า

5. อุปกรณ์เก่าและไม่ปลอดภัย : อุปกรณ์เก่าและไม่ปลอดภัยโดยมากจะไม่มีระบบป้องกันความปลอดภัยที่ดีทำให้ถูกโจมตีได้ง่าย

6. ไม่มีการปกป้องคุ้มครองความเป็นส่วนตัวของข้อมูล : อุปกรณ์ไม่มีมาตรการ หรือระบบที่ป้องกันการเข้าถึงข้อมูลส่วนตัวของผู้ใช้ ทำให้ข้อมูลส่วนตัวรั่วไหล

7. ช่องทางการส่งผ่านข้อมูลไม่ปลอดภัยและอุปกรณ์จัดเก็บข้อมูลไม่ปลอดภัย : การส่งข้อมูลของอุปกรณ์ IoT ผ่านช่องทางการสื่อสารที่ไม่ได้ถูกเข้ารหัส เช่น MQTT, HTTP เป็นต้น ทำให้ข้อมูลที่ส่งผ่านช่องทางนี้สามารถถูกดักฟังได้

8. ขาดการจัดการอุปกรณ์ : ขาดการจัดการความปลอดภัยในการดำเนินการบนระบบ IoT และไม่มีระบบมอนิเตอร์ความปลอดภัยทางไซเบอร์

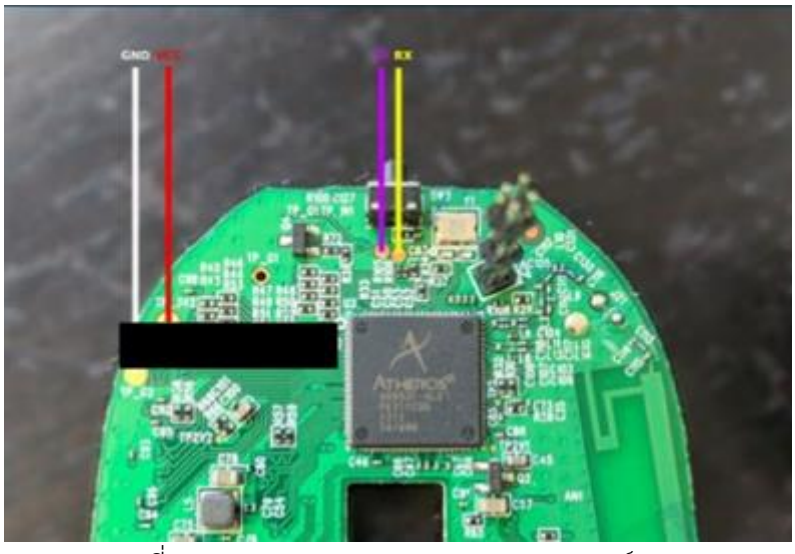
9. การติดตั้งจากโรงงาน Default Setting แบบไม่ปลอดภัย : ช่องโหว่จากการติดตั้ง เช่นการ ตั้งพาสเวิร์ดที่ง่ายเกินไปจากโรงงาน และยากต่อการเปลี่ยนแปลงระบบเพื่อปรับปรุงมาตรการความปลอดภัยจากโรงงาน

10. ขาดการปกป้องบริเวณการโจมตีทางกายภาพ : ง่ายต่อการโจมตีระบบป้องกันทางกายภาพของตัวอุปกรณ์ IoT, ง่ายต่อการเข้าถึง Port การเชื่อมต่อทางกายภาพ และ มีการป้องกันที่อ่อนแอในการเข้าถึงพอร์ตการเชื่อมต่อทางกายภาพ

ทดสอบความปลอดภัยทางไซเบอร์ของอุปกรณ์ IoT ด้วยการ HACK!

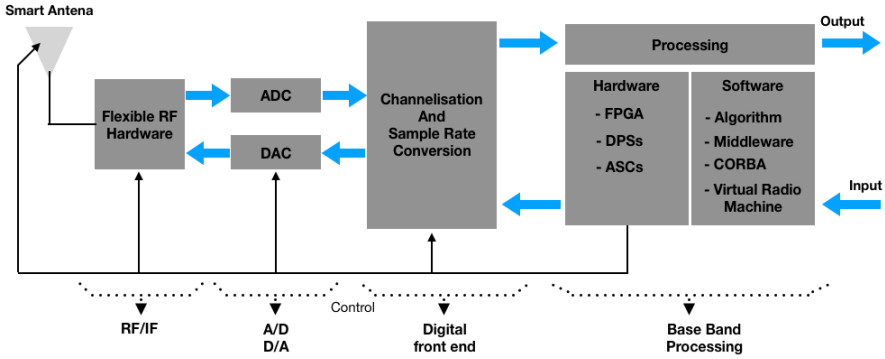
ก่อนที่จะให้ผู้ไม่หวังดีมาโจมตี เราเลือกที่จะทดสอบโจมตีระบบตัวเองก่อน แนวคิดนี้เป็นแนวทางการทดสอบความสามารถในการป้องกันการโดนโจมตีทางไซเบอร์ของอุปกรณ์ หรือที่เรียกว่า Penetration Testing การทดสอบการโจมตีแบ่งเป็น 3 วิธี ได้แก่

1.การโจมตีทางฮาร์ดแวร์ : การโจมตีทางฮาร์ดแวร์ เป็นการโจมตีที่อาศัยหาช่องโหว่ของอุปกรณ์ทางกายภาพ โดยหาช่องทางการเชื่อมต่อเข้ากับ Serial port ของ FPGA ของตัวอุปกรณ์ IoT เช่น การใช้ อุปกรณ์ USB to UART โดยการเชื่อมต่อ UART เข้ากับ Tx-Rx port ดังรูปที่ 2 และทำการเชื่อมต่อ USB เข้ากับ USB port ของคอมพิวเตอร์ จากนั้นทำการทดลอง login เข้าสู่ root shell ในอุปกรณ์เพื่อเปลี่ยนเฟิร์มแวร์หรือดึงข้อมูลออกมา หากอุปกรณ์ IoT เปิดพอร์ตสำหรับการ debug ผ่าน debug channel/JTAG ทำให้ผู้โจมตีสามารถเข้าถึงข้อมูลและเปลี่ยนแปลงข้อมูลภายในตัวอุปกรณ์ IoT ได้ นอกจากนี้ อุปกรณ์ฮาร์ดแวร์ที่ใช้สำหรับการโจมตีช่องโหว่ของอุปกรณ์ IoT ทางฮาร์ดแวร์อื่นๆ มีดังตัวอย่างนี้ เช่น HackRF, Facedancer, ChipWhisperer, JTAG เป็นต้น



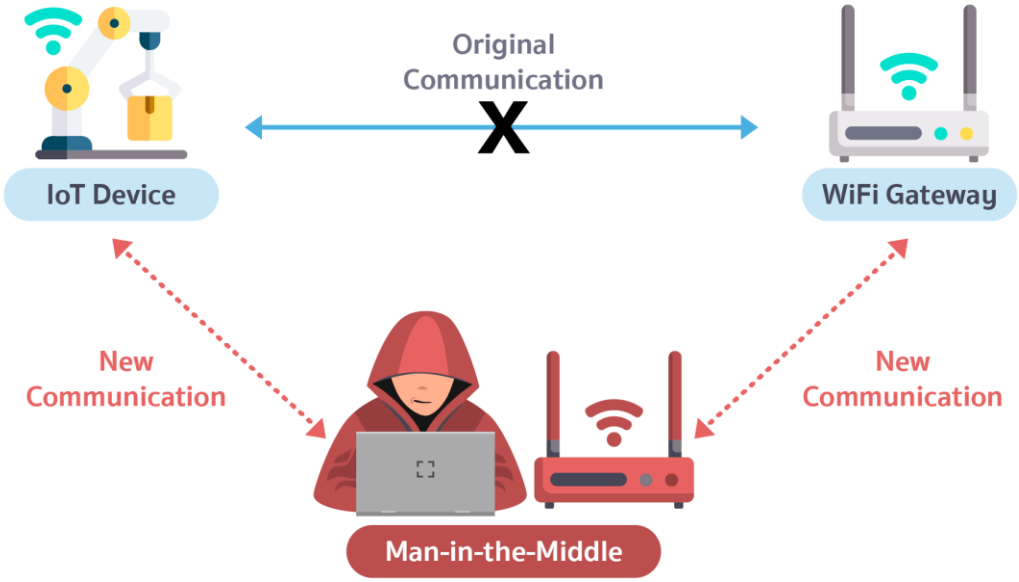
รูปที่ 2. Tx-Rx port แผงวงจรบนแของอุปกรณ์ IoT

2. การทำ Replay radio signal ด้วย Software Define Radio (SDR) : เราสามารถใช้อุปกรณ์ SDR ในการจับ Spectrum ของสัญญาณที่ส่งออกมาจากตัวอุปกรณ์ IoT ขณะทำการเชื่อมต่อกับอุปกรณ์ Mobile application ภายหลังจากจับคลื่นสัญญาณ Radio spectrum แล้ว นำสัญญาที่ได้มา ทำการ Replay ซึ่งทำให้สามารถส่งข้อมูลชุดเดียวกันกับที่อุปกรณ์ควบคุมปลายทางใช้สื่อสารกับอุปกรณ์ IoT ซึ่งถ้าหากอุปกรณ์ IoT ไม่มีการเข้ารหัส หรือเปลี่ยนชุดข้อมูลเข้ารหัสทำให้ การทำ Replay radio signal สามารถเข้าถึงตัวอุปกรณ์แทนอุปกรณ์ของผู้ใช้งานจริงได้ รูปที่ 3. แสดงโครงสร้างของโมดูลการทำงานของอุปกรณ์ SDR



รูปที่ 3. โครงสร้างโมดูลภายในของ Software Define Radio (SDR) [4]

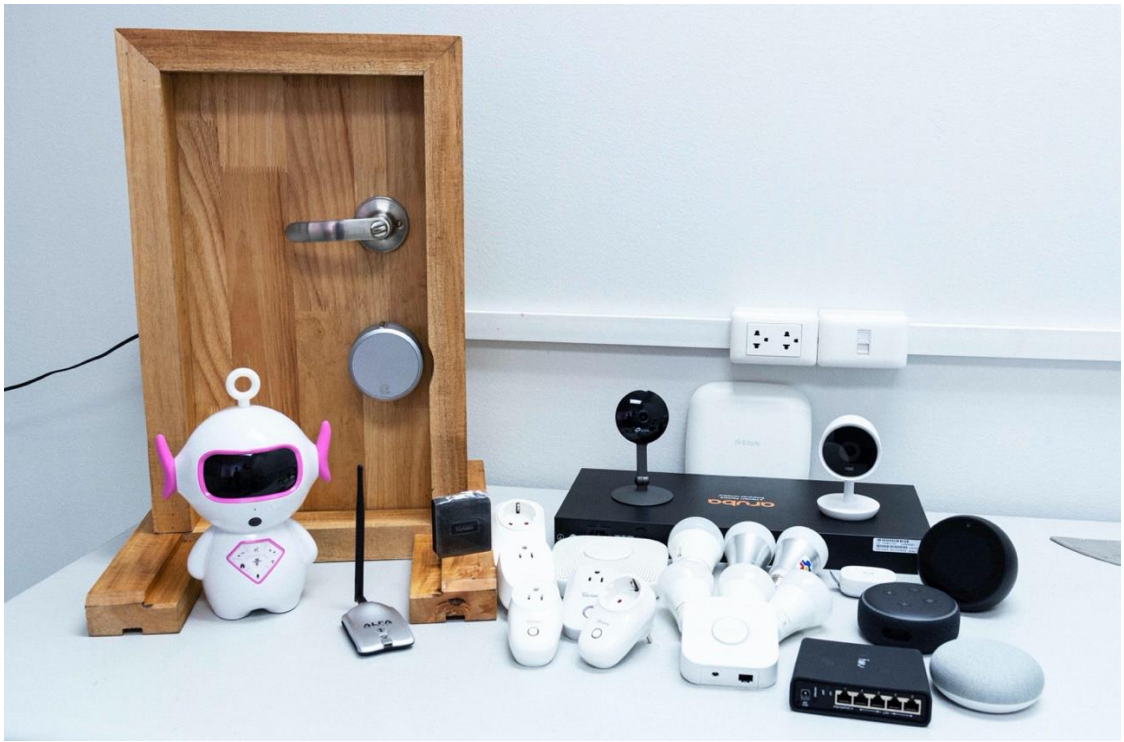
3. การโจมตีแบบ Man-in-the-Middle (MITM) : การโจมตีแบบ MITM เป็นการโจมตีโดยการปลอมตัวเป็นตัวกลางในการเชื่อมต่อระหว่างอุปกรณ์ IoT ไปยัง WiFi gateway หรือ Cloud server โดยเทคนิคการปลอมตัวเป็นตัวกลางในการเชื่อมต่อสามารถทำได้หลายรูปแบบ เช่น การปลอมแปลงชื่อ SSID ของ WiFi gateway เทคนิคนี้สามารถทำได้โดยเครื่องมือสแกน SSID เช่น อุปกรณ์ WiFi Pineapple โดยผู้โจมตีจะสามารถเลือก WiFi gateway ที่เป็นเป้าหมายได้แล้วทำการขัดขวางการเชื่อมต่อของอุปกรณ์ IoT กับอุปกรณ์เดิม และทำให้อุปกรณ์ IoT ทำ (Deauthentication) ด้วยการทำ two-way handshake กับอุปกรณ์ WiFi Pineapple ซึ่งทำหน้าที่เป็น WiFi gateway ปลอม และ WiFi Pineapple จะทำหน้าที่ส่งต่อแพ็คเกจไปยัง WiFi gateway เดิม การโจมตีเช่นนี้จะทำให้เกิดความหน่วงของการส่งข้อมูลซึ่งอาจทำให้ผู้ถูกโจมตีตระหนักรู้ได้ว่ากำลังถูกโจมตี แต่อย่างไรก็ตาม ผู้โจมตีรูปแบบนี้สามารถเรียนรู้ข้อมูลที่ถูกส่งมาได้ นอกจากนั้นผู้โจมตีอาจจะเปลี่ยนแปลงข้อมูลที่ส่งไปยัง WiFi gateway ได้ หากข้อมูลที่ส่งไม่ถูกเข้ารหัส หากในกรณีที่อุปกรณ์ IoT ใช้โพรโทคอล MQTT ในการส่ง ซึ่งข้อมูลที่ส่งจะไม่ถูกเข้ารหัส และอุปกรณ์ IoT ได้ทำการส่งข้อมูลผ่าน MQTT broker ทำให้ผู้โจมตีสามารถดักจับข้อมูลได้และปลอมตัวเป็น MQTT broker ปลอม รูปที่ 4. แสดงตัวอย่างการโจมตีแบบ MITM



รูปที่ 4. การโจมตีแบบ Man-in-the-Middle

นอกจากวิธีการโจมตีแบบต่าง ๆ ข้างต้นแล้ว ซอฟต์แวร์ตัวช่วยสำหรับทดสอบช่องโหว่ของอุปกรณ์ IoT ได้แก่

- ซอฟต์แวร์สำหรับ Web testing เช่น ZAP, Acunetix
- ซอฟต์แวร์สำหรับ Firmware analysis เช่น firmwalker, FACT firmware-analysis-toolkit
- ซอฟต์แวร์สำหรับ Bug finder เช่น Flawfinder, Metasploit, Framework
- ซอฟต์แวร์สำหรับ Binary reversing เช่น IDA, Pro radare2, binaryninja
- ซอฟต์แวร์สำหรับ Port scanner เช่น Nessus professional



รูปที่ 5. อุปกรณ์ IoT ที่นำมาทดสอบ

บทสรุป

บทความนี้ได้นำเสนอเส้นทางสู่ความปลอดภัยทางไซเบอร์สำหรับ IoT โดยอาศัยแนวคิดแบบ Hacker การวิเคราะห์ระเบียบวิธีการโจมตีความปลอดภัยทางไซเบอร์ของอุปกรณ์ IoT โดยทำตัวเสมือนเป็น Hacker เพื่อช่วยในการจำลองวิธีการตรวจสอบความปลอดภัยทางไซเบอร์ของอุปกรณ์ IoT ในเบื้องต้นให้กับผู้ผลิตและพัฒนาอุปกรณ์ IoT รวมไปถึงเป็นแนวทางการตรวจสอบความปลอดภัยของอุปกรณ์ IoT โดยผู้ใช้เองได้ การวิเคราะห์เบื้องต้นนี้สามารถทำได้ใน 2 ส่วน คือ 1. การศึกษาช่องโหว่ความปลอดภัยจากการวิเคราะห์ทางกายภาพและวิธีการสื่อสารระหว่างอุปกรณ์ IoT กับ Mobile Application และ 2. การศึกษาช่องโหว่ความปลอดภัยด้วยวิธีการโจมตี (Hacking) การทดสอบในกรณีศึกษากับอุปกรณ์ IoT บางประเภทพบว่ามีช่องโหว่ความปลอดภัยซึ่งทำให้อุปกรณ์สามารถถูกโจมตีทางไซเบอร์ได้ทั้งทางกายภาพ (Hardware) และ ทางช่องทางการสื่อสาร (Communication channel) โดยช่องโหว่ความปลอดภัยที่เกิดขึ้นเนื่องจากอุปกรณ์ IoT ใช้โพรโทคอลที่ไม่ได้ผ่านการเข้ารหัสช่องสัญญาณ SSL/TLS ในการสื่อสารเพื่อการควบคุมและสั่งการผ่าน Mobile Application ไปยังตัวอุปกรณ์ ซึ่งทำให้ข้อมูล Credential ของตัวอุปกรณ์รั่วไหลจากการถูกดักจับแพ็คเกจได้ และส่งผลกระทบต่อความปลอดภัยและการถูกโจมตีด้วยวิธีอื่นได้

อ้างอิง

[1] First disclosure of images taken by the Kibo's internal drone "Int-Ball". [เข้าถึงเมื่อ 11 มิถุนายน 2563]. เข้าถึงได้จาก https://iss.jaxa.jp/en/kiboexp/news/170714_int_ball_en.html.

[2] Breaking Down Mirai: An IoT DDoS Botnet Analysis. [เข้าถึงเมื่อ 11 มิถุนายน 2563]. เข้าถึงได้จาก https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/.

[3] Honda Global Operation Halted by Randsomware Attack. [เข้าถึงเมื่อ 11 มิถุนายน. 2563]. เข้าถึงได้จาก https://techcrunch.com/2020/06/09/honda-ransomware-snake/.

[4] “File:SDR et WF.svg”, [online access], . [เข้าถึงเมื่อ 1 มีนาคม 2563]. เข้าถึงได้จาก https://commons.wikimedia.org/w/index.php?curid=8831874.