ความมั่นคงปลอดภัยของ IoT
IoT Security

สรวิศ บุญมี
Sorawit Boonmee
คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยอีสเทิร์นเอเชีย
Faculty of Information Technology, Eastern Asia University

บทคัดย่อ

บทความนี้นำเสนอความสำคัญของความมั่นคงปลอดภัยของอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things--IoT) ซึ่งเป็นเทคโนโลยีที่มีการเติบโตมาโดยตลอด ปัญหาด้านความมั่นคงของ IoT ประเภทของอุปกรณ์ IoT โครงสร้างพื้นฐานของ IoT ตัวอย่างการโจมตีในรูปแบบต่าง ๆ พื้นที่เสี่ยงที่มีโอกาสโดนโจมตี และช่องโหว่ของ IOT 10 อันดับ โดยผู้ที่เกี่ยวข้อง ควรให้ความสำคัญกับความมั่นคง ตั้งแต่ขั้นตอนการออกแบบและการพัฒนาเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นอย่างมากในภายหลัง ดังตัวอย่างการโจมตีของมัลแวร์ Mirai

คำสำคัญ: ความมั่นคงปลอดภัยด้านสารสนเทศ, อินเทอร์เน็ตของสรรพสิ่ง, ไอโอที

Abstract

This article presents the importance of Internet of Things (IoT), a technology that has been grown so far. IoT security issues, type of IoT device, IoT infrastructure, examples of attacks, IoT attack surface areas and IoT top ten risks. IoT stakeholders should focus on security from the design and development stages to prevent potential damage later on, as an example of Mirai malware attacks.

Keywords: information security, internet of things, IoT

บทนำ

นับตั้งแต่คำว่า Internet of Things (IoT) ซึ่งหมายถึง การที่อุปกรณ์อัจฉริยะต่าง ๆ สามารถสื่อสารกันได้ผ่านเครือข่ายอินเทอร์เน็ต ทำให้มนุษย์สามารถสั่งการและควบคุมการใช้งานอุปกรณ์ผ่านทางเครือข่ายอินเทอร์เน็ตได้ ถูกบัญญัติขึ้นมาในปี ค.ศ.1999 (Kullimratchai, 2016) เทคโนโลยีดังกล่าวได้มีการเติบโตและได้รับการจัดอันดับให้เป็นเทคโนโลยีที่น่าจับตามองมาตลอดตั้งแต่แรก Gartner (2017) ซึ่งเป็นบริษัทวิจัยและวิเคราะห์ข้อมูลด้านเทคโนโลยีสารสนเทศชั้นนำของโลกทำนายว่า ภายในปี ค.ศ.2020 อุปกรณ์อิเล็กทรอนิกส์ที่ถูกผลิตขึ้นมาใหม่ร้อยละ 95 จะมีเทคโนโลยี Internet of Things

TechTalkThai (2017) อ้างถึงสถิติจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ซึ่งแสดงให้เห็นว่าเทคโนโลยี IoT ในประเทศไทยยังคงมีโอกาสเติบโตได้อีกมาก โดยจำนวนครัวเรือนที่เชื่อมต่อกับอินเทอร์เน็ตปัจจุบันมีมากถึง 10.7 ล้านครัวเรือน ในขณะที่ภาคการเกษตรมีมูลค่าการส่งออกสูงถึง 1.2 ล้านล้านบาท และจำนวนโรงงานทั่วประเทศมีมากถึงเกือบ 140,000 โรงงาน เหล่านี้ พร้อมที่นำเทคโนโลยี IoT เข้าไปใช้เพื่อก้าวไปสู่ความเป็น Smart Home, Smart Farm และ Smart Factory ในอนาคต

ปัญหาด้านความมั่นคงของ IoT

อุปกรณ์ IoT บางชนิดอาจไม่ได้ถูกออกแบบมาสำหรับใช้กับเครือข่ายอินเทอร์เน็ตตั้งแต่แรก โดยอาจจะถูกออกแบบมาให้ใช้กับเครือข่ายส่วนบุคคล เช่น บลูทูธ จากนั้นเมื่อกระแส IoT ได้รับความนิยม อุปกรณ์เหล่านี้จึงถูกปรับปรุงให้ใช้ได้กับอินเทอร์เน็ตโพรโทคอล และเครือข่ายอินเทอร์เน็ตได้ในที่สุด โดยที่การออกแบบนั้นอาจไม่ได้คำนึงถึงความมั่นคงบนเครือข่ายอินเทอร์เน็ตซึ่งเป็นเครือข่ายสาธารณะมาตั้งแต่แรก

การออกแบบในระยะแรกมักจะมีระบบป้องกันด้านความมั่นคงพื้นฐานอย่างง่าย ๆ และเมื่อพบว่ามีช่องโหว่ก็ปรับปรุงเพิ่มระบบความมั่นคงให้ซับซ้อนมากขึ้น

การปรับปรุงเฟิร์มแวร์เพื่อแก้ไขปัญหา และข้อผิดพลาดต่าง ๆ ที่พบหลังจากติดตั้งใช้งานแล้วโดยมากมักทำได้ยาก หรืออาจจะไม่สามารถทำได้เลยเนื่องจากขาดการสนับสนุนจากผู้ผลิต

อุปกรณ์ IoT รุ่นเก่าที่มีความมั่นคงต่ำและยังไม่ได้รับการปรับปรุงแก้ไขยังมีการติดตั้งใช้งานอยู่ ทำให้อุปกรณ์ IoT รุ่นใหม่ที่ได้รับการออกแบบให้มีความมั่นคงมาอย่างดีอาจจะไม่สามารถเปิดใช้ระบบความมั่นคงได้อย่างเต็มประสิทธิภาพ เนื่องจากอาจจะทำให้ไม่สามารถทำงานเข้ากับอุปกรณ์ IoT รุ่นเก่าที่ยังคงจำเป็นต้องใช้งานอยู่ได้

ประเภทของอุปกรณ์ IoT

หากใช้บทบาทในการติดต่อสื่อสารผ่านเครือข่ายอินเทอร์เน็ตเป็นเกณฑ์ จะสามารถแบ่งประเภทของอุปกรณ์ IoT ได้ดังนี้

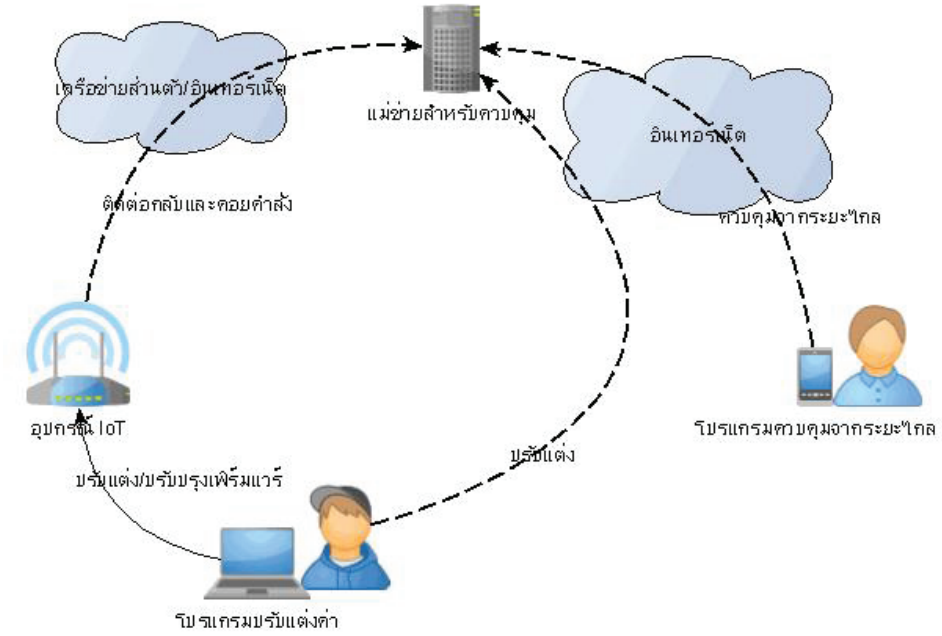
1. แบบลูกข่าย (client type) ซึ่งต้องมีเครื่องแม่ข่ายแยกต่างหากเป็นส่วนประกอบในโครงสร้างพื้นฐานจึงจะทำงานได้ อุปกรณ์ IoT ส่วนใหญ่มักจะทำงานในรูปแบบนี้

2. แบบแม่ข่าย (server type) ซึ่งมีแม่ข่ายรวมอยู่ในตัวอุปกรณ์แล้ว เช่น กล้องไอพี (IP camera) แบบที่มีเว็บเซิร์ฟเวอร์ในตัว

3. แบบ Peer-to-Peer หรือ Mesh คือไม่มีใครเป็นแม่ข่ายหรือลูกข่าย โดยมากใช้ในเครือข่ายแบบ private เช่น ระบบ SCADA

โครงสร้างพื้นฐานของ IoT

โครงสร้างพื้นฐานของ IoT โดยทั่วไปแล้วผู้ใช้งานจะสามารถติดต่อกับอุปกรณ์ IoT ผ่านเครือข่ายอินเทอร์เน็ตโดยใช้โปรแกรมควบคุมจากระยะไกลโดยมีแม่ข่ายเป็นตัวกลางคอยควบคุมการทำงาน นอกจากนี้อุปกรณ์ IoT บางชนิดอาจเพิ่มช่องทางในการติดต่อสื่อสารกับผู้ผลิตเพื่อรองรับการสนับสนุนทางด้านเทคนิคต่าง ๆ เช่น การปรับรุ่นเฟิร์มแวร์ ดังภาพ 1

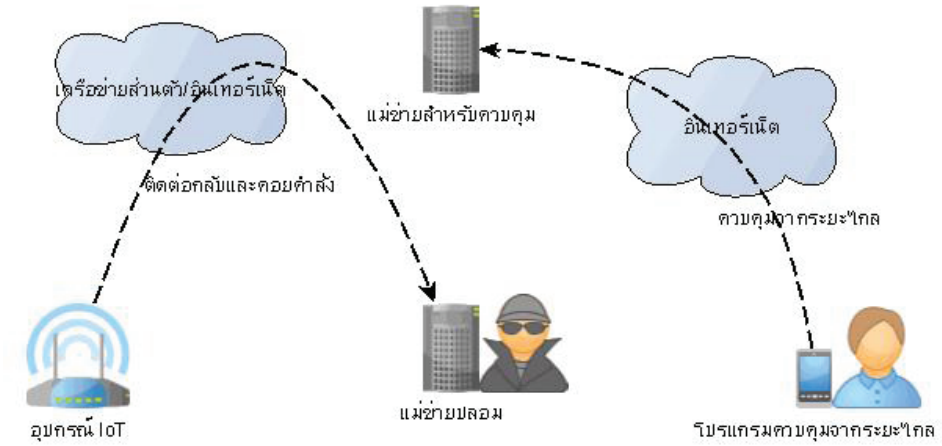


ภาพ 1 โครงสร้างพื้นฐานทั่วไปของ IoT

การโจมตีระบบ IoT

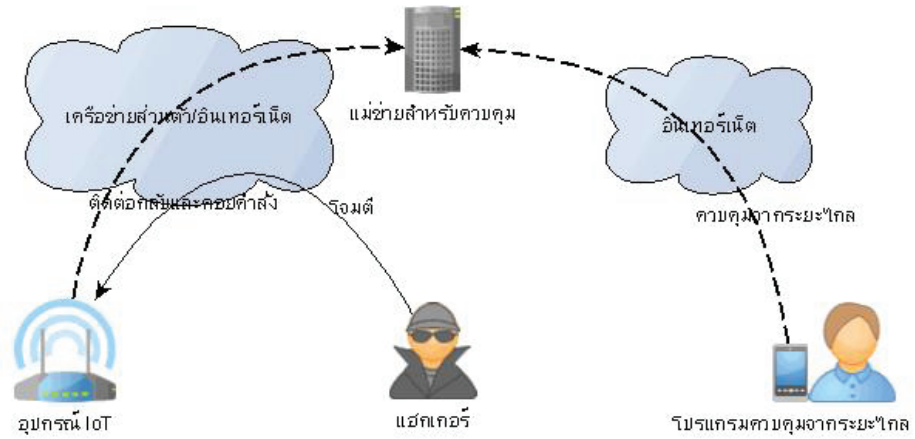
Roongsiriwong (2017) ได้ยกตัวอย่างการโจมตีระบบ IoT ที่มักพบได้โดยทั่วไปในหลายรูปแบบดังต่อไปนี้

1. ปลอมเครื่องแม่ข่ายที่ใช้ควบคุมอุปกรณ์ IoT เนื่องจากอุปกรณ์เหล่านี้อาจไม่ได้ถูกเชื่อมต่อกับเครื่องแม่ข่ายตลอดเวลา แฮกเกอร์อาจจะใช้การทำ DNS Poisoning เพื่อหลอกอุปกรณ์ IoT ให้เชื่อมต่อกับเครื่องแม่ข่ายปลอมของแฮกเกอร์แทน ซึ่งถ้าหากการเชื่อมต่อกับแม่ข่ายตามปกติไม่มีความมั่นคงปลอดภัยเพียงพอ แฮกเกอร์จะสามารถดักข้อมูลในการติดต่อเพื่อเรียนรู้และควบคุมอุปกรณ์ IoT นั้นได้ ดังภาพ 2



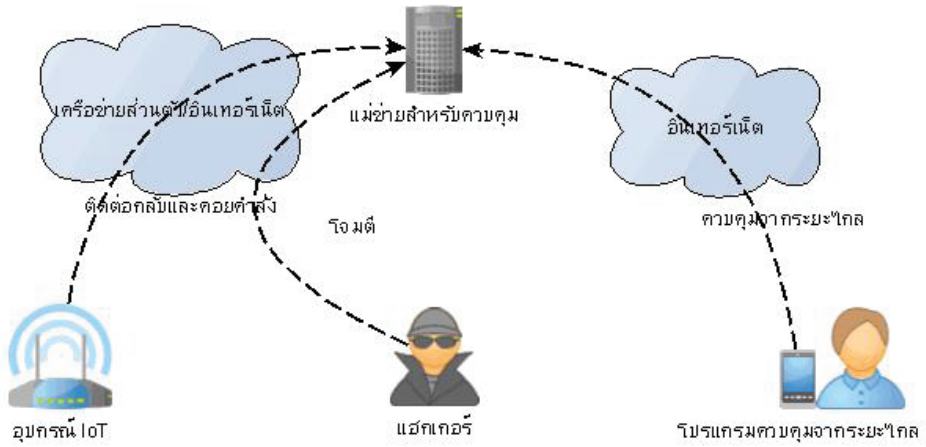
ภาพ 2 โครงสร้างพื้นฐานทั่วไปของ IoT

2. โจมตีอุปกรณ์ IoT โดยตรง โดยอาจใช้การ Reverse Engineering หรือใช้โปรแกรมในการสแกนพอร์ตของอุปกรณ์เพื่อช่วยในการหาช่องโหว่สำหรับใช้โจมตีให้สามารถเข้าควบคุมยึดครองตัวอุปกรณ์ได้โดยเฉพาะอุปกรณ์รุ่นเก่าส่วนใหญ่ที่ไม่ได้ถูกออกแบบโดยให้ความสำคัญกับ ดังภาพ 3



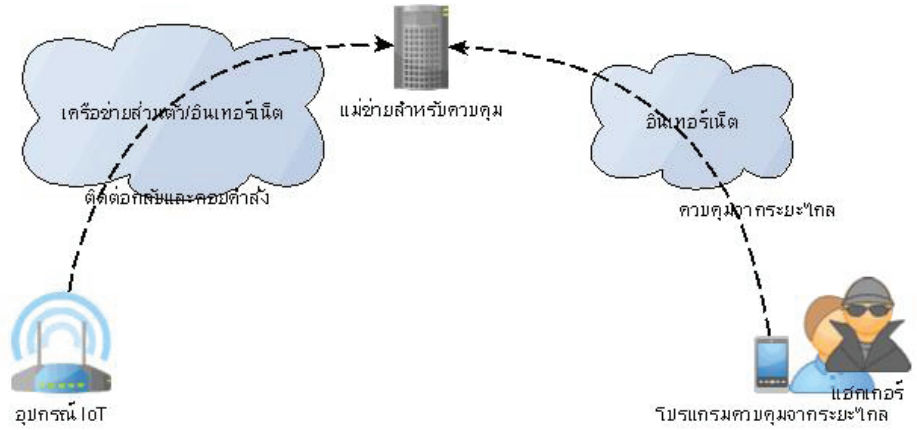
ภาพ 3 การโจมตีอุปกรณ์ IoT โดยตรง

3. โจมตีเครื่องแม่ข่ายที่ควบคุมอุปกรณ์ IoT ซึ่งโดยมากจะใช้เทคโนโลยีเดียวกับเครื่องบริการเว็บปกติ ส่งผลให้ถ้าไม่ได้มีการป้องกันเป็นอย่างดี มักจะมีช่องโหว่ให้ถูกโจมตีโดยเครื่องมืออันทันสมัยได้ง่ายเหมือนเครื่องบริการเว็บทั่วไปดังภาพ 4



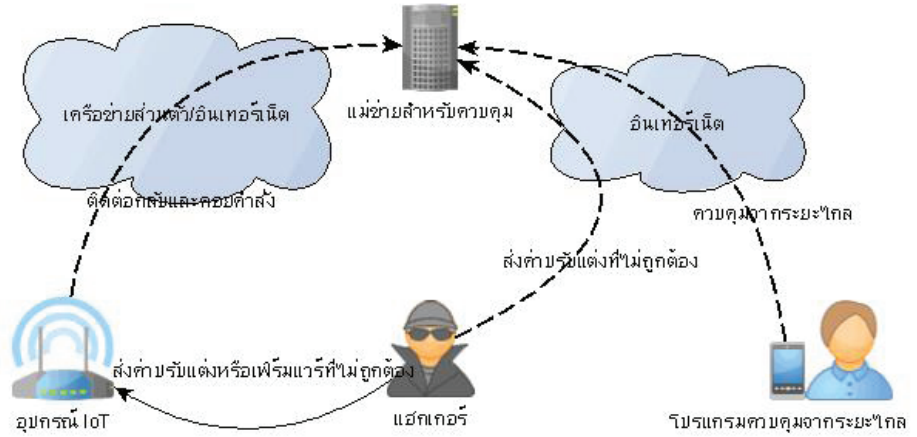
ภาพ 4 โจมตีเครื่องแม่ข่ายที่ควบคุมอุปกรณ์

4. การขโมยสวมรอยเป็นผู้ใช้เพื่อติดต่อกับเครื่องแม่ข่ายควบคุม โดยหากวิธีในการควบคุมการเข้าถึงและติดต่อสื่อสารระหว่างแอปพลิเคชันที่ผู้ใช้กับเครื่องแม่ข่ายที่ควบคุมอุปกรณ์ IoT ไม่มีความมั่นคงและรัดกุมเพียงพอย่อมเปิดโอกาสให้แฮกเกอร์สามารถขโมยสวมรอยเป็นผู้ใช้เพื่อเข้าควบคุมอุปกรณ์ IoT ได้ดังภาพ 5



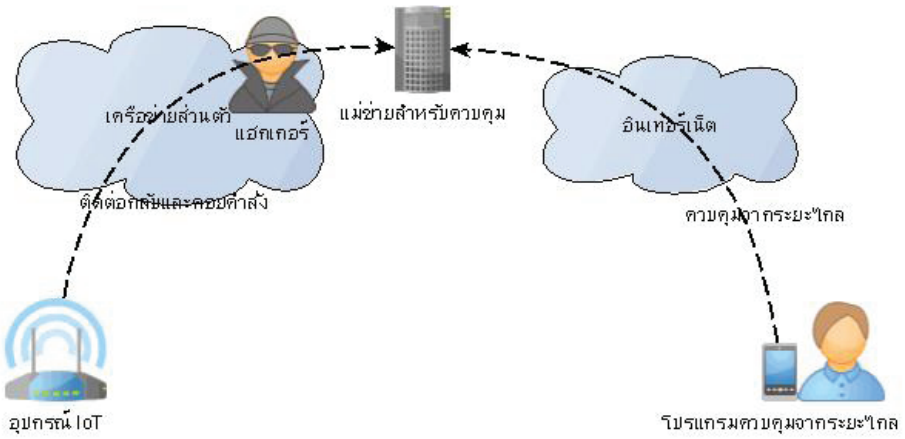
ภาพ 5 การขโมยสวมรอยเป็นผู้ใช้

5. การแอบส่งค่า Configuration หรือเฟิร์มแวร์ ถ้าหากกระบวนการในการปรับเปลี่ยนค่า Configuration หรือเฟิร์มแวร์ไม่รัดกุมมั่นคง แฮกเกอร์อาจจะแอบส่งค่า Configuration หรือเฟิร์มแวร์ที่ได้รับการแก้ไขให้เป็นประโยชน์กับแฮกเกอร์ทำให้สามารถควบคุมอุปกรณ์ IoT ได้โดยไม่ต้องผ่านกระบวนการตรวจสอบด้านความมั่นคงตามปกติ ดังภาพ 6



ภาพ 6 การแอบส่งค่า Configuration หรือเฟิร์มแวร์ที่ไม่เหมาะสม

6. ดักจับข้อมูลผ่านเครือข่ายส่วนตัว แม้ว่าอุปกรณ์ IoT อาจจะไม่ได้เชื่อมต่อกับเครื่องแม่ข่ายผ่านทางเครือข่ายสาธารณะ แต่อาจถูกดักจับข้อมูลผ่านเครือข่ายส่วนตัวได้หากไม่ระมัดระวัง หรือเชื่อว่าเครือข่ายส่วนตัวจะมีความมั่นคงเพียงพอ ดังภาพ 7



ภาพ 7 การดักจับข้อมูลผ่านเครือข่ายส่วนตัว

พื้นที่เสี่ยงที่มีโอกาสโดนโจมตี (IoT attack surface areas)

The Open Web Application Security Project หรือที่เรียกสั้น ๆ ว่า OWASP เป็นองค์กรสากลที่เปรียบเสมือนชุมชนของนักพัฒนาเว็บแอปพลิเคชันทั่วโลกเพื่อการสร้างเว็บแอปพลิเคชันให้มีความปลอดภัย ได้แสดงรายการพื้นที่เสี่ยงที่มีโอกาสโดนโจมตีของระบบ IoT ซึ่งผู้ผลิต ผู้พัฒนา นักวิจัยด้านความมั่นคง และผู้ที่จะนำ IoT ไปใช้งาน ควรทำความเข้าใจเพื่อประกอบการบริหารความเสี่ยงดังต่อไปนี้ (OWASP, 2017)

1. ระบบนิเวศ (ecosystem) เช่น มาตรฐานระหว่างอุปกรณ์ ความมั่นคงในการลงทะเบียนอุปกรณ์

2. หน่วยความจำของอุปกรณ์ (device memory) เช่น ข้อมูลสำคัญอาจไม่ได้ถูกเข้ารหัส

3. การเชื่อมต่อทางกายภาพ (device physical interfaces) เช่น การคัดลอกเฟิร์มแวร์ การเชื่อมต่อผ่าน CLI พอร์ตสำหรับดีบัก

4. การเชื่อมต่อผ่านเว็บ (device web interface) ทำให้สามารถถูกโจมตีได้เช่นเดียวกับเว็บไซต์ทั่วไป เช่น การขโมยข้อมูลรหัสผ่าน การกู้รหัสผ่านง่ายเกินไปไม่มั่นคง

5. เฟิร์มแวร์ของอุปกรณ์ (device firmware) อาจเปิดเผยข้อมูลที่อ่อนไหวต่อความมั่นคง เช่น บัญชีผู้ใช้พิเศษ รหัสผ่าน กุญแจสำหรับการเข้ารหัส

6. การเชื่อมต่อกับเครือข่าย (device network services) อาจจะโดน Denial of Service Buffer Overflow

7. ส่วนติดต่อผู้ดูแลระบบ (administrative interface) มักจะเชื่อมต่อผ่านเว็บ ทำให้สามารถถูกโจมตีได้เช่นเดียวกับเว็บไซต์ทั่วไป

8. การจัดเก็บข้อมูลในเครื่อง (local data storage) อาจไม่ได้เข้ารหัสหรือเข้ารหัสง่ายเกินไป

9. การเชื่อมต่อกับระบบคลาวด์ (cloud web interface) มักจะเชื่อมต่อผ่านเว็บ ทำให้สามารถถูกโจมตีได้เช่นเดียวกับเว็บไซต์ทั่วไป

10. เอพีไอแบ็กเอนด์สำหรับบุคคลที่สาม (third-party backend APIs) อาจเปิดเผยข้อมูลสำคัญ เช่น รุ่นหรือตำแหน่งของอุปกรณ์

11. กลไกการปรับปรุงระบบ (update mechanism) หากไม่มีการตรวจสอบให้ดีอาจถูกเปลี่ยนแปลงแก้ไขซอฟต์แวร์จนกลายเป็นมัลแวร์ได้

12. แอปพลิเคชันบนมือถือ (mobile application) ถูกพัฒนาอย่างไม่มั่นคง เช่น เก็บข้อมูลอย่างไม่มั่นคงปลอดภัย

13. เอพีไอแบ็กเอนด์สำหรับผู้ผลิต (vendor backend APIs) เช่น อาจมีการควบคุมการเข้าถึงหรือการยืนยันตัวตนที่ไม่รัดกุมเพียงพอ

14. การสื่อสารของระบบนิเวศ (ecosystem communication) เช่น การตรวจสอบสุขภาพของอุปกรณ์

15. การจราจรในเครือข่าย (network traffic) เช่น LAN หรือแบบไร้สาย

16. การยืนยันตัวตนและตรวจสอบสิทธิ์ (authentication) เช่น session key, token, cookie

17. ความเป็นส่วนตัว (privacy) เช่น ข้อมูลผู้ใช้ ตำแหน่งอุปกรณ์

18. ฮาร์ดแวร์ (เซนเซอร์) อาจถูกเจาะหรือทำลายได้

จะเห็นได้ว่าพื้นที่เสี่ยงที่มีโอกาสโดนโจมตีมีจำนวนมาก จึงควรลดพื้นที่เสี่ยงเหล่านี้ให้เหลือที่จำเป็นที่สุด และพิจารณาเลือกใช้เทคโนโลยีด้านความมั่นคงสารสนเทศที่เหมาะสมมาป้องกัน เช่น การเข้ารหัส Two-factor authentication เป็นต้น

ช่องโหว่ของ IOT 10 อันดับ

OWASP ได้ทำการจัดอันดับช่องโหว่ IoT 10 อันดับแรก (TechTalkThai, 2015) เพื่อเป็นแนวทางสำหรับการป้องกัน ดังนี้

1. เว็บอินเตอร์เฟสที่ไม่มั่นคงปลอดภัย (insecure web interface) คือ เว็บที่มีระบบลงทะเบียนผู้ใช้ไม่รัดกุม เช่น ชื่อผู้ใช้หรือรหัสผ่านง่ายเกินไป ไม่มีระบบห้ามล็อกอินเมื่อใส่รหัสผ่านผิดเกิน 5 ครั้ง เป็นต้น รวมทั้งไม่มีระบบป้องกัน XSS, SQL Injection และ CSRF ส่งผลให้ข้อมูลอาจถูกขโมย หรืออุปกรณ์อาจถูกแย่งสิทธิ์ควบคุมได้

การป้องกัน ควรเปลี่ยนชื่อผู้ใช้และรหัสผ่านเริ่มต้นได้ มีการป้องกันการเดารหัสผ่าน และประเมินความมั่นคงของโปรแกรมประยุกต์บนเว็บ

2. การพิสูจน์ตัวตน/การกำหนดสิทธิ์ไม่เพียงพอ (insufficient authentication) แฮกเกอร์สามารถเดารหัสผ่าน โดยใช้กลไกของ Password Recovery ที่ไม่มั่นคงปลอดภัย หรือระบบ Access Control ที่ไม่แข็งแกร่งในการเจาะเข้าสู่ระบบ ส่งผลให้ข้อมูลอาจถูกขโมย หรืออุปกรณ์อาจถูกแย่งสิทธิ์ควบคุมได้

การป้องกัน บังคับใช้รหัสผ่านที่เดาได้ยาก ใช้กลไกของ Password Recovery ที่มั่นคงปลอดภัย ใช้การยืนยันตนเองสองระดับ (two-factor authentication)

3. บริการด้านเครือข่ายไม่มั่นคงปลอดภัย (insecure network services) ระบบให้บริการเครือข่ายมีช่องโหว่ต่อการถูกโจมตี หรือช่วยให้แฮกเกอร์มีช่องทางในการโจมตีอุปกรณ์ต่าง ๆ ส่งผลให้อาจถูกโจมตีแบบ DoS หรือ Buffer Overflow ได้

การป้องกัน เปิด port ให้น้อยที่สุด ไม่ใช้ UPnP ทบทวนบริการเครือข่ายที่จำเป็นทั้งหมดว่าช่องโหว่หรือไม่

4. การเข้ารหัสข้อมูลไม่แข็งแกร่ง (lack of transport encryption) แฮกเกอร์สามารถแอบดูข้อมูลที่ส่งผ่านระบบเครือข่ายได้ ส่งผลให้ข้อมูลสำคัญถูกขโมยหรือเปิดเผยสู่โลกภายนอก

การป้องกัน ใช้ SSL/TLS และ มาตรฐานการเข้ารหัสที่เป็นที่ยอมรับ

5. นโยบายความเป็นส่วนบุคคล (privacy concerns) แฮกเกอร์ใช้การโจมตีที่หลากหลาย เช่น ข้อ 1-4 ในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้ที่ไม่ได้ถูกป้องกันอย่างแน่นหนาเพียงพอ ส่งผลให้ข้อมูลส่วนตัวถูกขโมยหรือเปิดเผยสู่ภายนอก

การป้องกัน เก็บข้อมูลผู้ใช้ให้น้อยที่สุด ไม่ควรระบุตัวตนได้ และให้เลือกข้อมูลที่จะเก็บได้

6. คลาวด์อินเตอร์เฟสไม่มั่นคงปลอดภัย (insecure cloud interface) แฮกเกอร์ใช้การโจมตีที่หลากหลาย เช่น ข้อ 1-4 ในการเข้าถึงข้อมูลหรือเข้าควบคุมระบบผ่านทางคลาวด์เว็บไซต์ ส่งผลให้ข้อมูลอาจถูกขโมย หรืออุปกรณ์อาจถูกแย่งสิทธิ์ควบคุมได้

การป้องกัน ประเมินความมั่นคงของระบบคลาวด์ ใช้การยืนยันตนเองสองระดับ บังคับใช้รหัสผ่านที่เดาได้ยาก

7. โมบายล์อินเตอร์เฟสไม่มั่นคงปลอดภัย (insecure mobile interface) แฮกเกอร์ใช้การโจมตีที่หลากหลาย เช่น ข้อ 1-4 ในการเข้าถึงข้อมูลหรือเข้าควบคุมระบบผ่านทางอินเตอร์เฟสของอุปกรณ์โมบายล์ ส่งผลให้ข้อมูลอาจถูกขโมย หรืออุปกรณ์อาจถูกแย่งสิทธิ์ควบคุมได้

การป้องกัน มีการป้องกันการเดารหัสผ่าน ใช้การยืนยันตนเองสองระดับ บังคับใช้รหัสผ่านที่เดาได้ยาก

8. การตั้งค่าความมั่นคงปลอดภัยไม่ดีพอ (insufficient security configurability) อุปกรณ์มีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลและการควบคุมไม่ดีพอ แฮกเกอร์สามารถใช้ช่องโหว่เรื่องการเข้ารหัสหรือการใช้รหัสผ่านที่ง่ายจนเกินไปในการโจมตีอุปกรณ์หรือเข้าถึงข้อมูลสำคัญได้ ส่งผลให้อุปกรณ์ถูกเจาะเพื่อขโมยข้อมูลออกไปได้

การป้องกัน มีการบันทึก log ด้านความมั่นคง ใช้การเข้ารหัส มีการเตือนผู้ใช้เมื่อเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคง

9. ซอฟต์แวร์/เฟิร์มแวร์ไม่มั่นคงปลอดภัย (insecure software/firmware) แฮกเกอร์สามารถตรวจจับการอัพเดทผ่านช่องทางที่ไม่ได้เข้ารหัสได้ ทำให้แฮกเกอร์สามารถส่งปลอมแปลงไฟล์อัพเดทผ่านทางการทำ DNS Hijacking ได้ นอกจากนี้ แฮกเกอร์สามารถตรวจสอบข้อมูลของการอัพเดท ซึ่งทำให้ทราบได้ว่าซอฟต์แวร์หรือเฟิร์มแวร์ในปัจจุบันมีช่องโหว่อะไรอยู่บ้าง ส่งผลให้ข้อมูลอาจถูกขโมย หรืออุปกรณ์อาจถูกแย่งสิทธิ์ควบคุมได้

การป้องกัน ควรเข้ารหัสและใช้ลายเซ็นดิจิทัลในการตรวจสอบการปลอมแปลง เครื่องแม่ข่ายที่ใช้เผยแพร่ซอฟต์แวร์ควรมีความมั่นคง

10. ปัญหาเชิงกายภาพของอุปกรณ์รักษาความมั่นคงปลอดภัย (poor physical security) อุปกรณ์รักษาความมั่นคงปลอดภัยไม่ได้ปิดกั้นหรือควบคุมการใช้ USB, SD Card หรืออุปกรณ์เก็บข้อมูลประเภทอื่น ๆ ซึ่งอาจถูกใช้เป็นช่องทางในการเข้าถึงระบบปฏิบัติการหรือข้อมูลที่ถูกเก็บไว้ในอุปกรณ์ได้ ส่งผลให้อุปกรณ์ถูกเจาะเพื่อขโมยข้อมูลออกไปได้

การป้องกัน ใช้ USB ให้น้อยสุด ป้องกันเฟิร์มแวร์ของอุปกรณ์อย่าให้เข้าถึงง่าย ๆ ผ่าน USB ควรให้จำกัดความสามารถในการจัดการผ่านช่องทางที่มีความเสี่ยงมากได้

ตัวอย่างภัยคุกคามที่เกี่ยวข้องกับ IoT

ในปี ค.ศ.2016 (TechTalkThai, 2016) โทรจัน Mirai เน้นพุ่งเป้าที่ Router, DVR, WebIP Camera, Linux Servers และอุปกรณ์ Internet of Things ที่ประมวลผลผ่าน Busybox โดยแฮกเกอร์จะค้นหาอุปกรณ์ที่ใช้รหัสผ่านดั้งเดิมจากโรงงานและเข้าควบคุมอุปกรณ์นั้น ๆ ผ่านทาง Telnet หรือ SSH จากนั้นจึงทำการปล่อยมัลแวร์เข้าไปเพื่อทำหน้าที่เป็น Botnet ควบคุมอุปกรณ์ให้รับคำสั่งตามที่ แฮกเกอร์ต้องการ

Mirai เป็นมัลแวร์ที่มีพัฒนามาจากโทรจัน Bashlite หรือ Gafgyt, Torlus ซึ่งสามารถบังคับให้อุปกรณ์ทำการโจมตีแบบ DDoS ไปยังเป้าหมายได้หลายวิธี เช่น UDP, DNS และ HTTP Floods, UDP Floods over GRE และ TCP Floods หลากหลายรูปแบบ เป็นต้น และเมื่อปริมาณอุปกรณ์ IoT มีจำนวนมหาศาลทั่วโลก จึงทำให้สามารถโจมตีแบบ DDoS ขนาดใหญ่ระดับ 600 Gbps ได้สำเร็จ

อุปกรณ์ที่ติดมัลแวร์ Mirai สามารถจัดการแก้ไขเบื้องต้นได้ด้วยการรีสตาร์ทอุปกรณ์ เพื่อลบมัลแวร์ออกจากหน่วยความจำ แต่อุปกรณ์เหล่านั้นก็อาจติดมัลแวร์ได้อีกหลังจากรีสตาร์ท เนื่องจากยังใช้รหัสผ่านดั้งเดิมจากโรงงาน ดังนั้นควรทำการเปลี่ยนรหัสผ่านใหม่ให้มีความแข็งแกร่ง ไม่ควรอนุญาตให้ตั้งค่าอุปกรณ์ผ่านอินเทอร์เน็ต หากเป็นอุปกรณ์ IoT ที่ใช้แค่ในองค์กรก็ควรไม่ให้มีการเชื่อมต่อกับเครือข่ายสาธารณะอย่างอินเทอร์เน็ต และถ้าต้องเชื่อมต่อกับอินเทอร์เน็ตก็ควรเปิดให้ใช้งานได้เฉพาะพอร์ตที่จำเป็นรวมถึงเปลี่ยนหมายเลขพอร์ตใหม่ให้ต่างจากค่าเริ่มต้นถ้าเป็นไปได้

บทสรุป

Internet of Things (IoT) เป็นเทคโนโลยีที่มีความสำคัญและได้รับความนิยมใช้งานมากขึ้นเรื่อย ๆ เนื่องจากอำนวยความสะดวกและนำไปใช้ประโยชน์ได้อย่างกว้างขวาง หากผู้ที่เกี่ยวข้อง ไม่ว่าจะเป็นผู้ผลิต นักพัฒนา หรือผู้ใช้ไม่คำนึงถึงความมั่นคงปลอดภัย ซึ่งไม่ได้จำกัดเพียงแค่ตัวอุปกรณ์เท่านั้น แต่รวมถึงสภาพ

แวดล้อม โครงสร้างพื้นฐานที่เกี่ยวข้อง รูปแบบการโจมตี พื้นที่เสี่ยงที่มีโอกาสโดนโจมตี และการป้องกันช่องโหว่ต่าง ๆ ตามที่ OWASP แนะนำตั้งแต่ขั้นตอนออกแบบและพัฒนาแล้ว ก็อาจส่งผลให้เกิดความเสียหายเป็นวงกว้างอย่างมากในภายหลังเนื่องจำนวนอุปกรณ์ IoT ที่มีปริมาณมหาศาล ดังตัวอย่างมัลแวร์ Mirai ที่เกิดขึ้น

References

Gartner. (2017). *Gartner top strategic predictions for 2018 and beyond*. Retrieved form https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2018-and-beyond/

Kullimratchai, P. (2016). Internet of things: Current technology trends for future. *EAU Heritage Journal: Science and Technology*, *10*(1), 29-36. (in Thai)

OWASP. (2017). *IoT attack surface areas project*. Retrieved form https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Attack_Surface_Areas

Roongsiriwong, N. (2017). *Embedded system security learning from banking and payment industry.* Retrieved form https://www.slideshare.net/narudomr/embedded-system-security-learning-from-banking-and-payment-industry

TechTalkThai. (2015). *Top 10 threats on the internet of things*. Retrieved form https://www.techtalkthai.com/top-10-owasp-internet-of-things-2014/ (in Thai)

TechTalkThai. (2016). *Found Mirai IoT DDoS botnet source code published on hack forums*. Retrieved form https://www.techtalkthai.com/mirai-iot-ddos-botnet-source-code-leaked/ (in Thai)

TechTalkThai. (2017). *G-ABLE reveals 5 technologies to transform business to watch in 2018*. Retrieved form https://www.techtalkthai.com/5-disruptive-technologies-in-thailand-2018/ (in Thai)