การโจมตีและการป้องกันความปลอดภัย บนโครงข่ายโทรศัพท์เคลื่อนที่ยุคที่ 5

SECURITY THREATS AND PREVENTION ON 5G MOBILE NETWORK

เสาวภาคย์ สาสนัส
Saowaphak Sasanus
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) กรุงเทพฯ 10210
National Telecom of Thailand, Bangkok 10210 Thailand

Corresponding E-mail : saowapha@ntplc.co.th

Received Date November 13, 2023
Revised Date December 25, 2024
Accepted Date February 21, 2025

บทคัดย่อ

บทความนี้ศึกษาสถาปัตยกรรมโครงข่ายโทรศัพท์เคลื่อนที่ อุปกรณ์ และฟังก์ชันที่เกี่ยวข้องกับระบบความปลอดภัยยุคต่าง ๆ ศึกษารูปแบบการถูกโจมตีระบบความปลอดภัยโครงข่าย รวมทั้งวิธีการป้องกันและศึกษาประโยชน์จากการพัฒนาโครงข่ายโทรศัพท์เคลื่อนที่ยุคที่ 5 ตลอดจนข้อแนะนำการใช้งานอย่างปลอดภัย โดยวิธีศึกษาเอกสาร ผลการศึกษาพบว่า สถาปัตยกรรมโครงข่ายหลักยุคที่ 1-4 มีอุปกรณ์ที่ช่วยป้องกันความปลอดภัยน้อย แต่เมื่อถึงยุคที่ 5 มีการพัฒนาหลายฟังก์ชันที่ช่วยป้องกันความปลอดภัยให้รวมอยู่ในอุปกรณ์เดียวโดยแยกฟังก์ชันภายในด้วยการจำลองเสมือน สำหรับรูปแบบการโจมตีระบบความปลอดภัยโครงข่าย เช่น ปลอมเป็นคนอื่น หรือโจมตีด้วยการส่งข้อมูลจำนวนมาก สามารถป้องกันได้โดยการติดตั้งฟีเชอร์ความปลอดภัยให้ครบ อัปเดตซอฟต์แวร์เพื่อปรับปรุงเสมอ ส่วนสาเหตุที่สถาปัตยกรรมโครงข่ายยุคที่ 5 มีความปลอดภัยมากขึ้น เนื่องจากมีการเข้ารหัสตลอดทาง เจาะเข้าระบบได้ยาก มีการแบ่งทรัพยากรย่อยในแต่ละอุปกรณ์ แยกวิกฤตการรั่วไหลของข้อมูลในระดับย่อยได้ และมีรูปแบบรวมศูนย์จึงอัปเดตซอฟต์แวร์ง่ายขึ้น ตรวจสอบการโจมตีได้เร็วขึ้น อย่างไรก็ตาม หากฟังก์ชันใดในสถาปัตยกรรมยุคที่ 5 ถูกเจาะ ฟังก์ชันอื่นจะเสี่ยงไปด้วย เช่น มีความเสี่ยงจากการที่มีอินเทอร์เน็ตสรรพสิ่งให้โจมตีจำนวนมาก หรือกรณีตั้งค่าอุปกรณ์ผิดจะทำให้ทรัพยากรย่อยทุกตัวมีความเสี่ยงด้วย

คำสำคัญ: เทคโนโลยีโทรศัพท์เคลื่อนที่ยุคที่ 5 สถาปัตยกรรมโครงข่าย การโจมตีด้านความปลอดภัย เครือข่ายที่กำหนดโดยซอฟต์แวร์

Abstract

This article studies network architecture, covering security system equipment and functions in various generations of mobile network. It also studies different types of security attacks and protection methods as well as the benefits of 5G mobile network development, along with the recommendations for safe installation and use. Through document research method, academic articles, journals, and newspapers were studied. It was found that there was not a lot of equipment for security protection in 1G to 4G wireless cellular network architecture. For the 5G network, functions for security protection were developed and installed in one single device of which the internal functions were separated through virtualization. There were many forms of network attack, e.g. spoofing attack and Denial of Service (DoS). Security breaches can be prevented by installing all security features and always updating them. The 5G network architecture was more secure because data transmission was encrypted end-to-end, making it difficult to be hacked. Resources were subdivided into smaller pieces on each device, allowing the separation of data leakage crisis at a sub-level. Moreover, being a centralized management makes updating software easier and detecting attacks faster. However, when any function was compromised, other functions were also at risk. In addition, there would be a risk from having a large number of Internet of Things (IoT) to attack. In the case of misconfiguration, it might put every sub-resource at risk as well.

Keywords: 5G technology, network architecture, security threats, software defined network

1. บทนำ

ปัจจุบันเทคโนโลยีเครือข่ายโทรศัพท์เคลื่อนที่มีวิวัฒนาการมาถึงยุคที่ 5 (ห้าจี) (Fifth Generation: 5G) ด้วยศักยภาพของเทคโนโลยีที่มีการพัฒนาเพิ่มขึ้นอย่างต่อเนื่อง ทำให้มีการนำเทคโนโลยีมาประยุกต์ใช้ในการให้บริการในลักษณะที่หลากหลายมากขึ้น ไม่เพียงแต่ให้บริการโทรคมนาคมแก่บุคคลทั่วไปเท่านั้น แต่ยังสามารถนำมาให้บริการเพื่อช่วยในการประกอบ ซ่อมแซม หรืออบรมการใช้งานอุปกรณ์ในโรงงานอุตสาหกรรม ดึงข้อมูลหรือสั่งการอุปกรณ์ อินเทอร์เน็ตสรรพสิ่ง (Internet of Things: IoT) สำหรับเมืองอัจฉริยะ (smart city) ให้บริการผ่าตัดทางไกล (telesurgery) หรือควบคุมรถอัตโนมัติ โดยลักษณะการให้บริการดังกล่าวมีความสำคัญมากขึ้น จากเดิมที่ให้บริการเสียง ข้อมูลข่าว สื่อสังคม (social media) การโอนเงินผ่านธนาคารหรือจ่ายบัตรเครดิต และข้อความสั้น (Short Message Service: SMS) เท่านั้น แต่บริการใหม่ ๆ เหล่านี้สามารถเก็บข้อมูลที่มีความสำคัญในเชิงพาณิชย์มากยิ่งขึ้น ประสิทธิภาพการบริการมีผลต่อสุขภาพและการเกิดอุบัติเหตุมากยิ่งขึ้น

เป็นผลให้เกิดความวิตกกังวลเกี่ยวกับความเสถียรของระบบความปลอดภัยในโครงข่ายเป็นอย่างมาก โดยแต่เดิมมิจฉาชีพนำเอาประโยชน์ของเทคโนโลยีใหม่ ๆ ที่เกิดขึ้นมาใช้หลอกลวง ก่อให้เกิดความเสียหายมากในระดับหนึ่ง เช่น การเจาะระบบข้อมูลและนำมาหลอกว่าเป็นพนักงานจากหน่วยงานของรัฐที่น่าเชื่อถือหรือพนักงานธนาคาร ให้ผู้ใช้งานหลงผิด จากนั้นหลอกให้โอนเงินเข้าไปยังเว็บไซต์ที่ติดไวรัส หรือส่งมัลแวร์ (malware) มายังอุปกรณ์ของผู้ใช้งาน เพื่อให้สามารถริโมตคอนโทรล (remote control) อุปกรณ์ของผู้ใช้งานและยักย้ายเงินหรือเก็บข้อมูลลับเกี่ยวกับบัตรเครดิตของผู้ใช้งาน แต่หากเป็นการให้บริการของโทรศัพท์เคลื่อนที่ยุคที่ 5 ลักษณะการหลอกลวงจะรุนแรงยิ่งขึ้น เช่น เกิดการปล้นจี้ข้อมูล การโจมตีทางไซเบอร์ (cyberattack) กับบริษัท โรงงานอุตสาหกรรม โรงพยาบาล หรือเมืองใหญ่ ๆ ซึ่งนอกจากก่อให้เกิดผลกระทบต่อสุขภาพและการเกิดอุบัติเหตุ ในบางครั้งอาจถูกใช้ในการก่อการร้ายอีกด้วย เนื่องจากในอนาคตระบบดิจิทัลจะเป็นตัวควบคุมอุปกรณ์สำคัญหลายอย่าง ดังนั้น ผู้ให้บริการโทรศัพท์เคลื่อนที่โดยเฉพาะอย่างยิ่งยุคที่ 5 จึงจำเป็นต้องดูแลระบบความปลอดภัยเป็นอย่างดี และทำตามระเบียบและกฎเกณฑ์ให้ถูกต้อง

2. วัตถุประสงค์

2.1 ศึกษาสถาปัตยกรรมโครงข่ายโทรศัพท์เคลื่อนที่ยุคต่าง ๆ รวมถึงอุปกรณ์และฟังก์ชันที่เกี่ยวข้องกับระบบความปลอดภัยโครงข่ายโทรศัพท์เคลื่อนที่

2.2 ศึกษารูปแบบการโจมตีระบบความปลอดภัยโครงข่าย รวมทั้งวิธีการป้องกันการโจมตีความปลอดภัย

2.3 ศึกษาประโยชน์จากการพัฒนาสถาปัตยกรรมโครงข่ายโทรศัพท์เคลื่อนที่ยุคที่ 5 และข้อแนะนำการติดตั้งใช้งานให้ปลอดภัย

3. วิธีการศึกษา

ศึกษาเชิงคุณภาพด้วยวิธีวิจัยเอกสาร (documentary research) โดยศึกษาเอกสารทางวิชาการทั้งในประเทศและต่างประเทศ ได้แก่ บทความทางวิชาการ วารสาร หนังสือพิมพ์ และเอกสารที่เกี่ยวข้อง ตั้งแต่ พ.ศ. 2560-2566 จากนั้นนำมาวิเคราะห์สังเคราะห์ตามวัตถุประสงค์ของการศึกษา

4. การทบทวนวรรณกรรม

สถาปัตยกรรมโครงข่ายโทรศัพท์เคลื่อนที่ยุคต่าง ๆ

เทคโนโลยีโทรศัพท์เคลื่อนที่ถูกพัฒนามาจากยุคที่ 1 ถึง 5 ตามลำดับ สำหรับการพัฒนาของสถาปัตยกรรมโครงข่ายเป็นไปดังภาพที่ 1 (Condoluci & Mahmoodi, 2018)

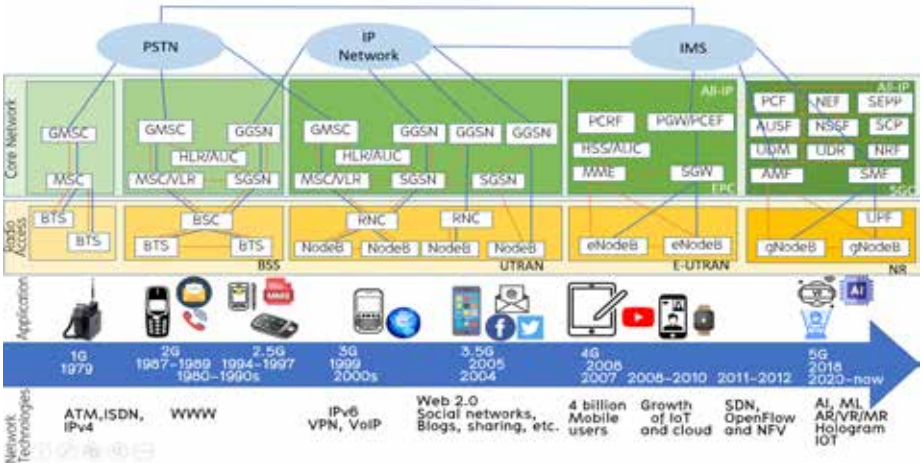
ยุคที่ 1

ในสมัยยุคที่ 1 การสื่อสารเป็นระบบแอนะล็อก (analog) รองรับการให้บริการเสียงอย่างเดียว และสามารถรับส่งทรูพุต (throughput) ได้น้อย ประมาณ 2.4 Kbps เท่านั้น และใช้วิธีเพิ่มประสิทธิภาพการรับส่งข้อมูลในความถี่ที่จำกัดด้วยการใช้ความถี่ซ้ำในระยะห่างที่เหมาะสม สถาปัตยกรรมโครงข่ายประกอบด้วยสถานีฐาน (Base Station: BS) ซึ่งมีหน้าที่ในการรับส่งสัญญาณวิทยุและแปลงให้เป็นสัญญาณทางสาย อีกทั้งจัดการการโทรเข้าออก สำหรับอุปกรณ์ในโครงข่ายหลักประกอบไปด้วยชุมสายโทรศัพท์เคลื่อนที่ (Mobile Switching Center: MSC) ซึ่งทำหน้าที่สลับสาย จัดการการสมัครสมาชิกมือถือ และเชื่อมต่อกับโครงข่ายโทรศัพท์สาธารณะ

ยุคที่ 2

สถาปัตยกรรมโครงข่ายยุคที่ 2 (Global System For Mobile Communication: GSM) ส่งข้อมูลแบบดิจิทัลโดยสามารถรับส่งทรูพุตได้ที่ 13 Kbps สำหรับการรับส่งเสียง และ 9.6 Kbps สำหรับการรับส่งข้อมูลแบบจองเส้นทางล่วงหน้า (circuit switched network) อุปกรณ์ทางฝั่งวิทยุประกอบไปด้วย Base Transceiver Station (BTS) จัดการเฉพาะฟังก์ชันวิทยุ (การส่งและรับสัญญาณ) และ Base Station Controller (BSC) ซึ่งควบคุมกลุ่มของ BTS จัดการการกำหนดเส้นทางการโทร การใช้งานแบบเคลื่อนที่ได้อย่างไร้รอยต่อ และงานประมวลผลการโทรอื่น ๆ

ในยุคที่ 2 มีการนำ Home Location Registration (HLR) ซึ่งใช้เก็บข้อมูลผู้ใช้งาน และ Authentication Center (AUC) ซึ่งใช้เก็บรหัสในการเข้ารหัสข้อมูลมาใช้งานด้วย ทั้งนี้ ในโครงข่ายหลัก 2.5G มีการปรับปรุงให้สามารถรองรับการส่งข้อมูลแบบแพ็กเก็ต (packet switching network) ได้ด้วย รองรับความเร็วที่สูงขึ้นสูงสุดถึง 384 Kbps โดยอุปกรณ์ที่เพิ่มเข้ามาในโครงข่ายหลัก 2.5G ประกอบด้วย Serving GPRS Support Node (SGSN) ซึ่งเราต์ (route) ข้อมูลส่งภายในโครงข่ายด้วยกันเอง และ Gateway GPRS Support Node (GGSN) ที่เราต์ข้อมูลส่งไปยังโครงข่ายภายนอก



ภาพที่ 1 วิวัฒนาการทางโครงข่ายยุคที่ 1-5

ที่มา: Condoluci and Mahmoodi (2018) (ปรับปรุงภาพโดยผู้เขียน)

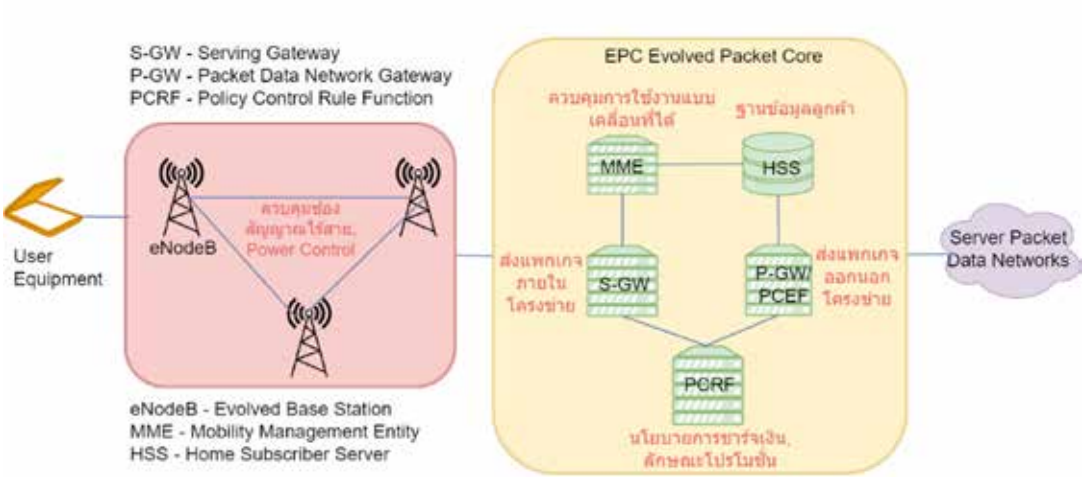
ยุคที่ 3

สถาปัตยกรรมโครงข่ายยุคที่ 3 (Universal Mobile Telecommunication System: UMTS) เป็นยุคที่ผู้ใช้งานสามารถรับส่งข้อมูลได้มากถึง 2 Mbps โดยสถาปัตยกรรมโครงข่ายยุคที่ 2 และ 3 ในส่วนของสถานีฐานและตัวควบคุมสถานีฐานที่มีฟังก์ชันคล้ายคลึงกัน เทียบเคียง BTS ได้กับสถานีฐาน NodeB และตัวควบคุมสถานีฐาน BSC เทียบเคียงได้กับ Radio Network Controller (RNC) โดยในส่วนของโครงข่ายหลักมีลักษณะเหมือนกับยุคที่ 2.5 คือมีอุปกรณ์ SGSN และ GGSN ในการส่งต่อข้อมูลแบบแพ็กเก็ต และยังคงใช้อุปกรณ์ HLR และ AUC ไว้เก็บข้อมูลลูกค้าและรหัสชั่วคราวที่ใช้ในการเข้ารหัสข้อมูลตามลำดับ

ยุคที่ 4

ภาพที่ 2 แสดงสถาปัตยกรรมโครงข่ายยุคที่ 4 ที่ลดลำดับชั้น (hierarchical) ของโครงข่ายยุคที่ 2 และ 3 ลง โดยในส่วนของภาคสัญญาณวิทยุเหลือเพียงอุปกรณ์สถานีฐาน eNodeB ซึ่งยุบรวมอุปกรณ์ สถานีฐาน NodeB และตัวควบคุมระบบสถานีฐาน RNC ในโครงข่ายยุคที่ 3 เข้าด้วยกัน ทำให้สถานีฐาน eNodeB สามารถจัดการทรัพยากรในฝั่งวิทยุโดยไม่จำเป็นต้องขอการตัดสินใจจากอุปกรณ์ในโครงข่ายหลักทุกครั้ง

ในโครงข่ายหลัก อุปกรณ์ Home Subscriber System (HSS) เป็นตัวเก็บข้อมูลลูกค้า ซึ่งส่วนใหญ่จะมีฟังก์ชัน AUC ติดตั้งอยู่ด้วย อุปกรณ์ Mobility Management Entity (MME) ทำหน้าที่จัดการเกี่ยวกับการเคลื่อนที่แบบไร้รอยต่อ ในขณะที่อุปกรณ์ Serving Gateway (S-GW) ทำหน้าที่ในการส่งต่อสัญญาณ (signaling) ที่เกี่ยวข้องกับแทรฟฟิก คอนโทรล (traffic control) ของลูกค้าภายในโครงข่ายเดียวกัน และอุปกรณ์ Packet Gateway (P-GW) ทำหน้าที่ส่งต่อแทรฟฟิก คอนโทรลและข้อมูลของลูกค้าไปยังโครงข่ายอื่น



ภาพที่ 2 สถาปัตยกรรมโครงข่ายยุคที่ 4

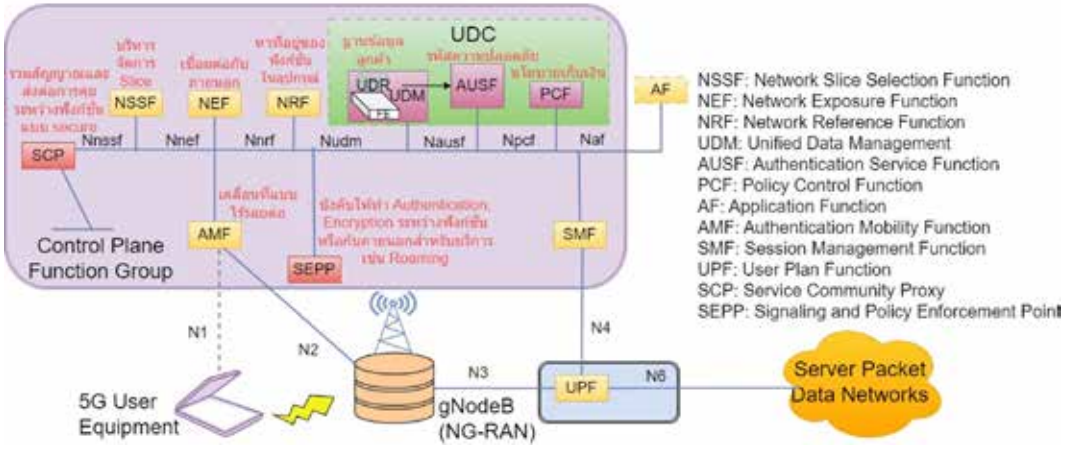
ที่มา: CableFree (n.d.)

ยุคที่ 5

สำหรับสถาปัตยกรรมโครงข่ายยุคที่ 5 เป็นไปดังภาพที่ 3 โดยอุปกรณ์ในโครงข่ายหลักในยุคก่อนจะถูกนำมารวมอยู่ที่อุปกรณ์เดียวกัน[1] โดยแยกเป็นฟังก์ชันภายในสำหรับการจัดการในแต่ละส่วนออกจากกันในลักษณะการจำลองเสมือน (virtualization) โดยสามารถทำได้ทั้งแบบ Virtual Machine (VM)[2] และแบบ containers[3] ส่งผลให้ความหน่วง (latency) ในการรับส่งข้อมูลระหว่างอุปกรณ์ลดลง และลดระดับชั้นในการเชื่อมต่อ

Authentication Mobility Function (AMF) ทำหน้าที่การพิสูจน์ตัวตนและจัดการเรื่องการเคลื่อนที่แบบไร้รอยต่อ ในขณะที่ User Plane Function (UPF) ทำหน้าที่เราต์ข้อมูลแทรฟฟิกของลูกค้า และ Session Management Function (SMF) เป็นตัวจัดการ session ของแทรฟฟิกลูกค้าที่ผ่าน UPF

สำหรับรหัสความปลอดภัยจะถูกเก็บไว้ที่ Authentication Function (AUSF) ในขณะที่โพรไฟล์ (profile) ของลูกค้าและนโยบายการคิดค่าบริการจะเก็บไว้ที่ User Defined Management (UDM) และ Policy Control Function (PCF) ตามลำดับ



ภาพที่ 3 สถาปัตยกรรมโครงข่ายยุคที่ 5

ที่มา: Ghadialy (2018)

การเชื่อมต่อระหว่างอุปกรณ์แบบฟังก์ชันเสมือนต่าง ๆ นั้น อุปกรณ์จำลองสามารถหาที่อยู่ของอุปกรณ์จำลองอื่น ๆ โดยติดต่อฟังก์ชันที่เก็บข้อมูลโครงข่าย (Network Reference Function: NRF) ซึ่งติดต่อกับข้อมูลเนมเซิร์ฟเวอร์ (Domain Name Server: DNS) อีกต่อหนึ่ง แต่อาจมีกรณีที่มีอุปกรณ์แปลกปลอมมาทำหน้าที่

[1] การติดตั้งจริง ฟังก์ชันจะรวมที่อุปกรณ์เดียวกันหรือไม่ขึ้นกับผู้ประกอบการและความเป็นเหตุเป็นผลในการใช้งาน

[2] Virtual Machine (VM) เป็นการจำลองเสมือนของฮาร์ดแวร์ทั้งอัน โดยรวมถึงหน่วยความจำ พื้นที่เก็บข้อมูล เน็ตเวิร์กอินเทอร์เฟซ โดยแต่ละ VM จะแยกออกจากกัน ทำให้ไม่สามารถสื่อสารกันได้โดยตรง เหมาะสำหรับแอปพลิเคชันที่ต้องการการแยกจากกัน เช่น ฐานข้อมูล และเว็บเซิร์ฟเวอร์ การติดตั้งจริงจะรวมที่อุปกรณ์เดียวกันหรือไม่ขึ้นกับผู้ประกอบการและความเป็นเหตุเป็นผลในการใช้งานจริง

[3] containers จำลองเสมือนเฉพาะระบบปฏิบัติการ (OS) ของ physical machine เท่านั้น containers หลาย ๆ ตัวสามารถแชร์ใช้ทรัพยากรของฮาร์ดแวร์ตัวเดียวกัน เช่น หน่วยความจำและพื้นที่เก็บข้อมูลได้ ทั้งนี้ containers ไม่แยกจากกัน ทำให้สามารถสื่อสารกันกับ containers อื่น ๆ ได้โดยตรง เหมาะสำหรับการติดตั้งแอปพลิเคชันที่ต้องการเคลื่อนย้ายได้ง่าย และไม่เสียทรัพยากรในการติดตั้งมากนัก เช่น ไมโครเซอร์วิส

เป็นฟังก์ชันเสมือนในระบบได้ จึงต้องมีอุปกรณ์เสมือนที่เรียกว่า บริการพรอกซีในการสื่อสาร (Service Communication Proxy: SCP) และพรอกซีสำหรับการป้องกันอุปกรณ์ปลายทางให้ปลอดภัย (Secure Edge Protection Proxy: SEPP) ทำหน้าที่เป็นตัวรวมแทรฟฟิกแบบสัญญาณคอนโทรล (signaling) และบังคับใช้นโยบายทางด้านความปลอดภัย ไม่ว่าจะเป็นด้านการตรวจสอบรหัสยืนยันตัวตนหรือการเข้ารหัสข้อมูล signaling[4] ก่อนจะส่งข้อมูลออกไปเพื่อเป็นการทำให้การส่งข้อมูลระหว่างฟังก์ชันต่าง ๆ สามารถใช้งานร่วมกันได้อย่างราบรื่นและปลอดภัย โดย SCP จะเน้นจัดการฟังก์ชันภายในผู้ให้บริการรายเดียวกัน ซึ่งรวมถึงกรณีที่มีผู้ผลิตแตกต่างรายกันในผู้ให้บริการรายนั้น ในขณะที่อุปกรณ์จำลอง SEPP เน้นจัดการฟังก์ชันระหว่างอุปกรณ์เสมือนที่อยู่ภายใต้ผู้ให้บริการโทรศัพท์เคลื่อนที่มากกว่าหนึ่งราย สำหรับบริการดังเช่นโรมมิง (roaming)

อุปกรณ์จำลองทั้งสองตัว (SCP และ SEPP) เป็นศูนย์กลางในการจัดทำ signaling คล้ายกับ Signaling Transfer Point (STP) ในโครงข่ายโทรศัพท์เคลื่อนที่ยุคเก่า ซึ่งทำหน้าที่ส่งต่อหรือเราต์แทรฟฟิก signaling ในโทรศัพท์เคลื่อนที่ยุคที่ 2 และ 3 เหมือนกับฟังก์ชันของอุปกรณ์ Diameter Signaling Controller (DSC) ที่ทำการส่งต่อข้อมูลหรือเราต์ signaling ในโทรศัพท์เคลื่อนที่ยุคที่ 4 ทั้งนี้ SEPP ยังมีหน้าที่ซ่อนรูปแบบการเชื่อมต่อ (topology) เพื่อป้องกันการโจมตีจากอุปกรณ์ภายนอกไปยังอุปกรณ์ใด ๆ ที่สำคัญภายในโครงข่ายอีกด้วย และยังทำหน้าที่บีบอัดหรือดรอปสัญญาณ signaling เพื่อป้องกันกรณีที่แทรฟฟิกเข้ามามากเกินไป ป้องกันการโจมตีด้วยแทรฟฟิกจำนวนมาก ส่งผลให้บริการไม่ได้หรือเกิดความล่าช้า (Henda et al., 2019)

5. ผลการศึกษา

5.1 อุปกรณ์และฟังก์ชันที่เกี่ยวข้องกับระบบความปลอดภัยโครงข่ายโทรศัพท์เคลื่อนที่

ในการศึกษาอุปกรณ์และฟังก์ชันที่เกี่ยวข้องกับระบบความปลอดภัยของโครงข่ายโทรศัพท์เคลื่อนที่ตั้งแต่ยุคแรกเริ่ม (ยุคที่ 1) จนถึงยุคปัจจุบัน (ยุคที่ 5) โดยเปรียบเทียบความแตกต่างของเทคโนโลยีที่ใช้เพื่อรักษาความปลอดภัยของผู้ใช้และข้อมูลในแต่ละยุคสมัย พบข้อมูลดังนี้

ยุคที่ 1

ไม่มีอุปกรณ์ที่ใช้ด้านความปลอดภัยแต่อย่างใด

ยุคที่ 2

Home Location Registration (HLR) ทำหน้าที่เก็บข้อมูลผู้ใช้งาน (IMSI และหมายเลขโทรศัพท์) ส่วนใหญ่จะติดตั้ง Authentication Center (AUC) รวมอยู่ที่อุปกรณ์เดียวกัน มีหน้าที่ในการตรวจสอบรหัสของซิม (SIM Pin) และเก็บรหัสชั่วคราวที่ใช้ในการเข้ารหัสเสียงและข้อความ นอกจากนี้ มีอุปกรณ์อื่น ๆ ที่เกี่ยวข้อง คือ BSC ซึ่งทำหน้าที่ควบคุมการเข้าถึงโครงข่าย

[4] ข้อมูลรหัสยืนยันตัวตนหรือการเข้ารหัสข้อมูลถูกส่งผ่านโพรโทคอล HTTPS

ยุคที่ 3

HLR จัดเก็บข้อมูลผู้ใช้งาน (IMSI และ SIM Pin) และ AUC ตรวจสอบรหัสของซิมและเก็บรหัสที่ใช้เข้ารหัสข้อมูล ในขณะที่ BSC ควบคุมการเข้าถึงโครงข่ายและ NodeB มีทางเลือกที่จะเข้ารหัสข้อมูลลูกค้า

ยุคที่ 4

ในยุคที่ 4 และ 5 Authentication and Authorization Server (AAS) ซึ่งทำหน้าที่ตรวจสอบรหัสผ่านของ SIM (SIM Pin) และ Key and Certificate Management System (KMS) ซึ่งทำหน้าที่จัดการ key และ certificate ถูกนำเข้ามาใช้เพิ่มความปลอดภัยในระบบ โดยฟังก์ชันทั้งสองถูกติดตั้งรวมอยู่ที่ HSS

HSS จะมีฟังก์ชัน Unified Data Repository (UDR) ทำหน้าที่จัดเก็บข้อมูลผู้ใช้ (IMSI, SIM Pin, ข้อมูลการใช้งาน และตำแหน่ง) ติดตั้งรวมอยู่ด้วย สำหรับฟังก์ชันด้านความปลอดภัยอื่น ๆ เช่น Policy and Charging Enforcement Function (PCEF) เป็นฟังก์ชันการทำงานหนึ่งของ P-GW จะทำหน้าที่กรองเนื้อหาและการควบคุมการเข้าถึง ป้องการการโจมตีแบบ DoS

อุปกรณ์อื่น ๆ เช่น Base Station Controller (BSC) ทำการควบคุมการเข้าถึงโครงข่าย ในขณะที่ eNodeB ทำการเข้ารหัสข้อมูลลูกค้า

ยุคที่ 5

ในส่วนของโครงข่ายหลัก AMF จะตรวจสอบว่าผู้ใช้และอุปกรณ์มีสิทธิ์เข้าถึงเครือข่าย 5G หรือไม่ โดยใช้กลไกการพิสูจน์ตัวตน เช่น การระบุตัวตนแบบ EAP (Extensible Authentication Protocol) และจะบังคับใช้นโยบายความปลอดภัยที่กำหนดไว้ เช่น การควบคุมการเข้าถึงบริการ และการจำกัดแบนด์วิดท์ (bandwidth) และสุดท้าย ช่วยในการป้องกันการโจมตีแบบ DoS โดยตรวจจับและกรองการรับส่งข้อมูลที่ผิดปกติ

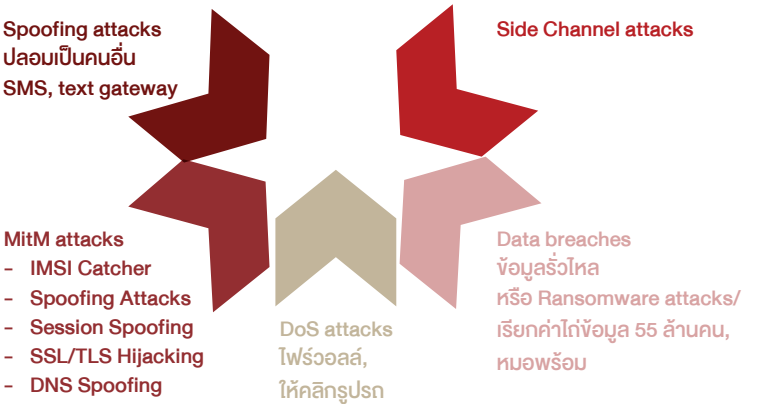
SMF ทำหน้าที่แยกส่วนโครงข่ายออกเป็นชิ้นส่วนเสมือน (network slice) เพื่อรองรับบริการที่หลากหลายและควบคุมการไหลของข้อมูลระหว่าง slice เหล่านี้ ในขณะที่ทำงานดังกล่าวสามารถเข้ารหัสข้อมูลเพื่อป้องกันการดักฟังได้

นอกจากนี้ ยังมี SCP ที่อำนวยความสะดวกในการสื่อสารที่ปลอดภัยและมีประสิทธิภาพระหว่างฟังก์ชันที่แตกต่างกันโดยใช้โพรโทคอล HTTP/2 บังคับใช้นโยบายความปลอดภัยที่กำหนดโดยผู้ให้บริการโครงข่าย เช่น การควบคุมการเข้าถึงผู้ใช้งาน การกรองการรับส่งข้อมูล ใช้โพรโทคอลที่ปลอดภัย เช่น Transport Layer Security (TLS) กับการพิสูจน์ตัวตนแบบสองทางสำหรับการกำหนดเส้นทางข้อความที่ฟังก์ชันต่าง ๆ ในโครงข่ายหลักใช้ และช่วยให้ผู้ปฏิบัติงานสามารถมองเห็นการรับส่งข้อมูลบนเครือข่าย ทำให้สามารถตรวจสอบกิจกรรมที่น่าสงสัยได้

ฟังก์ชันอื่น ๆ เช่น SEPP ทำหน้าที่ตรวจสอบและกรองการรับส่งข้อมูลเพื่อป้องกันภัยคุกคามทางไซเบอร์ เช่น มัลแวร์ (malware) ป้องกันการโจมตีแบบ DoS โดยจำกัดจำนวนการเชื่อมต่อจากอุปกรณ์แต่ละตัว และบังคับใช้นโยบายความปลอดภัยที่กำหนดไว้ เช่น ไฟร์วอลล์ (firewall)

5.2 รูปแบบต่าง ๆ ของการโจมตีและการป้องกันระบบความปลอดภัยระบบโครงข่ายโทรศัพท์เคลื่อนที่

ภัยคุกคามความปลอดภัยในโครงข่ายโทรศัพท์เคลื่อนที่มีอยู่หลายรูปแบบ ดังกรณีที่พบอยู่ทั่วไป โดยเป็นข้อมูลรูปแบบภัยคุกคามที่บางส่วนถูกประมวลมาจาก Vicente (2023)



ภาพที่ 4 ตัวอย่างภัยคุกคามความปลอดภัยในโครงข่ายโทรศัพท์เคลื่อนที่

5.2.1 การโจมตีด้วยการปลอมแปลง (spoofing attack) และแนวทางป้องกัน

5.2.1.1 การโจมตีด้วยการปลอมแปลง

จากทางด้านซ้ายดังภาพที่ 4 เป็นรูปแบบการโจมตีแบบแรกเรียกว่า spoofing attack ซึ่งเป็นรูปแบบที่ปลอมเป็นคนอื่น ซึ่งเป็นกรณีที่เกิดขึ้นมาก พบในข่าวทั่วไปในช่วงที่ผ่านมา การส่งข้อความสั้น หรือ Short Message Service (SMS) ที่มีลิงก์ ซึ่งเมื่อคลิกเข้าไปจะส่งลูกค้าต่อไปยังหน้าเว็บที่ติดมัลแวร์ หรือหากผู้ใช้งานเข้าไปกรอกข้อมูลลับส่วนตัวเข้าไป จะถูกหลอกเอาข้อมูลสำคัญไป สำหรับบริการข้อความสั้นเหล่านี้ ถ้าส่งเป็นจำนวนมาก แต่เดิมผู้ให้บริการใช้วิธีคีย์ข้อมูลที่ส่งพร้อมกับเบอร์โทรศัพท์ที่ต้องการส่งและรับเข้าที่เกตเวย์ที่ใช้ในการส่งข้อความ ซึ่งผู้ร้ายก็จะเลือกใส่เบอร์โทรศัพท์มือถือของเจ้าของที่น่าเชื่อถือเป็นเบอร์โทรศัพท์ของผู้ส่ง เช่น ธนาคาร หรือหน่วยงานราชการ เพื่อหลอกให้เหยื่อหลงเชื่อและกรอกข้อมูลลับที่สำคัญ

5.2.1.2 แนวทางป้องกันการโจมตีด้วยการปลอมแปลง

ปัจจุบันสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) ได้ขอความร่วมมือจากผู้ให้บริการโทรศัพท์เคลื่อนที่เพื่อป้องกันภัย ดังนี้ (สำนักงาน กสทช., 2564)

1) ต้องมีระบบยืนยันตัวตนลูกค้าที่มาซื้อการส่งข้อความสั้นและตรวจสอบได้

2) ต้องไม่ให้ลูกค้ากำหนดข้อความสั้นและชื่อผู้ส่งเองโดยอิสระ ต้องแจ้งให้ทราบก่อน

3) ต้องไม่กำหนดชื่อผู้ส่งเป็นหมายเลขโทรศัพท์ และหากชื่อผู้ส่งตรงหรือคล้ายกับชื่อบริษัท หน่วยงาน หรือเครื่องหมายการค้าที่มีอยู่แล้ว ผู้ให้บริการสามารถขอเอกสารจากลูกค้าในการรับรอง หรือการได้รับความยินยอมให้ใช้ชื่อจากเจ้าของชื่อบริษัท หน่วยงาน หรือเครื่องหมายทางการค้านั้น ๆ ได้

4) ข้อความไม่ควรมีเว็บลิงก์ เพื่อป้องกันไม่ให้ใช้เป็นเครื่องมือการกระทำผิด

5) หากผู้ใช้บริการมือถือมีซิมการ์ดในนามเดียวกันเกิน 6 เบอร์ ให้ลงทะเบียนยืนยันตัวตนกับผู้ให้บริการด้วย มิฉะนั้นอาจถูกระงับการให้บริการได้

5.2.2 การโจมตีแบบ MitM attack และแนวทางป้องกัน

สำหรับแบบที่สอง คือ Man-in-the-Middle (MitM) attack เป็นการโจมตีในลักษณะที่ผู้ร้ายนำตัวมาอยู่ตรงกลางระหว่างการสื่อสารของผู้ใช้งานกับโครงข่าย และทำการดักเอาข้อมูลมาใช้ หรือเข้าไปเปลี่ยนข้อมูลในการสื่อสารนั้น ๆ โดย MitM attack มีหลายรูปแบบย่อย ดังที่แสดงในภาพที่ 5 โดยสามลำดับแรกเป็นการโจมตีโครงข่ายโทรศัพท์เคลื่อนที่โดยตรง และสองลำดับหลังเป็นการโจมตีการใช้งานวายฟาย (Wi-Fi) ซึ่งส่วนใหญ่ผู้ใช้งานต้องการขนถ่าย (offload) ข้อมูลไปใช้ผ่านวายฟายแทนส่งผ่านโทรศัพท์เคลื่อนที่เพื่อลดค่าใช้จ่าย การโจมตีแบบที่ผู้ร้ายอยู่ตรงกลางระหว่างผู้ใช้งานและอุปกรณ์ในโครงข่าย (MitM attack) มีหลายรูปแบบ รายละเอียดแต่ละรูปแบบ ดังนี้

5.2.2.1 การโจมตี MitM แบบปลากระเบน (stingray) และแนวทางป้องกัน

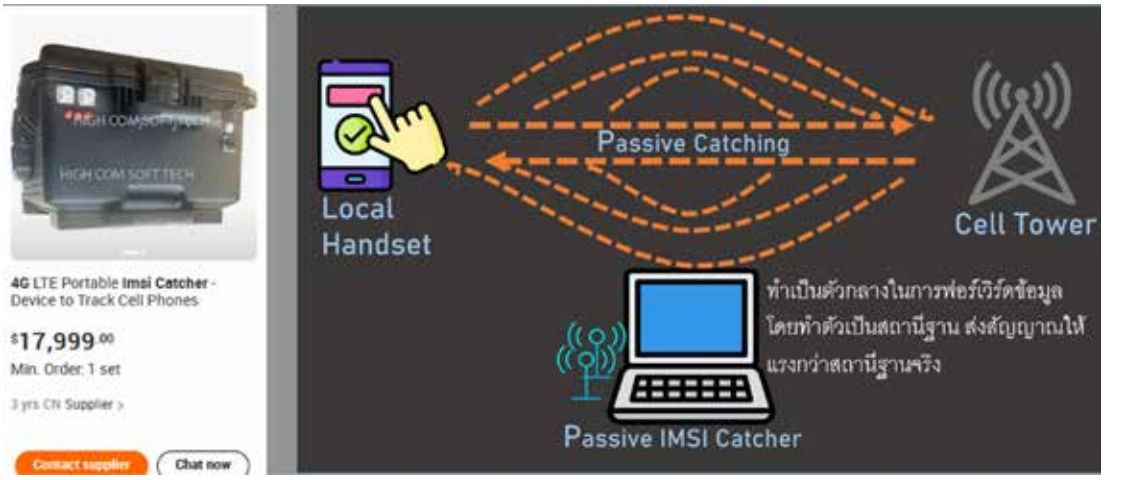
5.2.2.1.1 การโจมตีแบบปลากระเบน

การโจมตีโดยหาทางเข้าไปดึงข้อมูลเลขระบุโทรศัพท์เคลื่อนที่แต่ละเครื่องไว้ ที่เรียกว่า IMSI catcher หรือการโจมตีแบบปลากระเบน ซึ่งได้ชื่อมาจากผลิตภัณฑ์ที่บริษัทฮาริส[5] นำออกมาขาย

วิธีการโจมตีแบบนี้ ดังภาพที่ 5 จะเป็นการใช้ติดตั้งสถานีฐานปลอมที่ทำเป็นตัวกลางในการส่งต่อข้อมูลของผู้ใช้งานไปยังสถานีฐานจริง โดยสถานีฐานปลอมจะส่งสัญญาณให้แรงกว่าปกติ ทำให้โทรศัพท์มือถือเข้าใจผิดและพยายามเชื่อมต่อกับอุปกรณ์สถานีฐานปลอมนี้ ซึ่งเมื่อส่งข้อมูลครั้งแรก ค่า Temporary Mobile Subscriber Identity (TMSI) ซึ่งเป็นค่า IMSI ชั่วคราวที่เอาไว้ใช้เพื่อป้องกันการขโมย IMSI

[5] บริษัทฮาริสปัจจุบันถูกรวมเข้ากับบริษัทแอลทรีเทคโนโลยี (L3 Technologies) มีชื่อใหม่ว่าแอลทรีฮาริสเทคโนโลยี (L3 Harris Technologies)

ในเทคโนโลยีโทรศัพท์เคลื่อนที่ยุคที่ 2 หรือ 3 จะถูกส่งเป็นตัวอักษรที่ไม่ได้ถูกเข้ารหัสไว้ แต่เมื่อผู้ร้ายเก็บเอา TMSI ของผู้ใช้งานไปได้แล้ว จะสามารถหาข้อมูลสำคัญ เช่น ที่อยู่ของผู้ใช้มือถือ หรือส่งข้อความที่มีลิงก์ที่เมื่อผู้ใช้งานคลิกเข้าไปจะทำให้ติดมัลแวร์ได้ หรือนำไปใช้หาข้อมูลการโทรก่อนหน้าเพื่อรู้ข้อมูลลับที่ใช้ในการขู่กรรโชกหรือทำการขโมยตัวตนไปได้ (McDaid, 2019)



ภาพที่ 5 การโจมตีโดยการไปอยู่ตรงกลาง ที่เรียกว่าการโจมตีแบบปลากระเบน

ที่มา: McDaid (2019)

ในปี 2023 (พ.ศ. 2566) มีรายงานว่า คอมพิวเตอร์และฮาร์ดแวร์ราคาถูก ประมาณ 7 ดอลลาร์สหรัฐ หรือ 300 บาท และเพียงเขียนโปรแกรมขึ้นมาเล็กน้อย สามารถใช้เก็บค่า TMSI ได้แล้ว แต่หากไม่มีความรู้ด้านการเขียนโปรแกรม ผู้ร้ายยังสามารถโจมตีได้ง่าย โดยหาซื้ออุปกรณ์สำเร็จที่มีขายบนอินเทอร์เน็ต ราคาเพียงประมาณ 20,000 ดอลลาร์สหรัฐ หรือ 6 แสนบาท ก็สามารถใช้งานโจมตีระบบได้

5.2.2.1.2 แนวทางป้องกันการโจมตีแบบปลากระเบน

เนื่องการโจมตีแบบปลากระเบน สามารถใช้กับโครงข่ายยุคที่ 3 หรือยุคที่ 4 ที่กลับมาใช้โครงข่ายเสียงของยุคที่ 3 แต่ไม่สามารถใช้ได้กับโครงข่ายยุคที่ 5 ซึ่งมีอัลกอริทึม (algorithm) ในการเข้ารหัสและการขอเข้าใช้ระบบสูงกว่า ดังนั้น ผู้ประกอบการควรให้บริการโดยใช้โครงข่ายยุคที่ 4 ที่มีระบบ IP multimedia subsystem ในการให้บริการทางเสียง โดยไม่ต้องกลับไปใช้โครงข่ายยุคที่ 3 ในการให้บริการเสียงหรือบริการมัลติมีเดีย และสนับสนุนด้านส่วนลดอุปกรณ์ปลายทางให้กับผู้ใช้งานเพื่อผลักดันให้ไปใช้โครงข่ายยุคที่ 4 และที่ 5 ได้โดยเร็ว

5.2.2.2 การโจมตี MitM แบบ ReVoLTE และแนวทางป้องกัน

5.2.2.2.1 การโจมตีแบบ ReVoLTE

หากใช้งานโครงข่ายโทรศัพท์เคลื่อนที่ยุคที่ 4 ที่มีการย้อนกลับไปใช้งานโครงข่ายที่ให้บริการเสียงผ่านโครงข่ายยุคเดิมยุคที่ 2 หรือ 3 ซึ่งมีช่องโหว่ทางความปลอดภัยจากการใช้ IMSI catcher เข้าแอบเก็บข้อมูล ทำให้เสี่ยงต่อการโจมตีต่าง ๆ ที่สามารถทำได้บนโครงข่ายยุคที่ 2 หรือ 3 ไปด้วย แต่ในกรณีอื่นที่ใช้เทคนิคการโทรเข้าออกซึ่งเรียกว่า voice over LTE หรือการใช้เสียงผ่านโครงข่ายยุคที่ 4 Long Term Evolution (LTE) จะมีความเสี่ยงต่อการโจมตีในแบบเล่นเสียงซ้ำ ReVoLTE นี้แทน

ReVoLTE เป็นการโจมตีฟังก์ชัน VoLTE ซึ่งใช้งานทั้งในโครงข่ายโทรศัพท์เคลื่อนที่ยุคที่ 4 และยุคที่ 5 พบครั้งแรกในการติดตั้งโครงข่ายที่เยอรมนีในปี 2019 (พ.ศ. 2562) สำหรับกรรมวิธีในการโจมตีมีดังนี้ แรกเริ่มผู้ร้าย (hacker) จะทำการอัดข้อมูลของการโทรระหว่างเป้าหมายกับคนอื่น กรณีดังภาพที่ 6 คือเป็นการโทรคุยกันระหว่างอลิซ (Alice) กับ บ็อบ (Bob) ต่อมาเมื่อเป้าหมายวางโทรศัพท์แล้ว ภายใน 10 วินาที ผู้ร้ายจะโทรเข้าไปยังเครื่องของเป้าหมาย ในกรณีนี้คือ อลิซ หรือ บ็อบ เพื่อชวนพูดคุยด้วยระยะที่ยาวนานกว่าที่เป้าหมายโทรคุยกันในตอนแรก เมื่อจบการสนทนาแล้ว ผู้ร้ายจะถอดรหัสข้อมูลที่โทรกับเป้าหมาย แล้วจึงใช้รหัสนั้นถอดข้อมูลการโทรที่เป้าหมายคุยกันซึ่งได้อัดเสียงไว้ก่อนหน้า (Khandelwal, 2020)

ภาพที่ 6 การโจมตีโดยการไปอยู่ตรงกลาง แบบ ReVoLTE (Replay VoLTE)

ที่มา: Khandelwal (2020)

จากการที่ผู้ร้ายโทรหาเป้าหมายหลังจากการโทรของเป้าหมายกับคู่สนทนาภายในระยะเวลาที่กำหนด 10 วินาที ทำให้สถานีฐานต้องใช้เชื่อมต่อ (connect) ทางสื่อวิทยุ (radio connection) เดิม รหัสที่ใช้ในการเข้ารหัสข้อมูลยังเป็นรหัสเดิม ทำให้สามารถถอดรหัสข้อมูลและทราบรายละเอียดบทสนทนาที่อัดไว้ได้

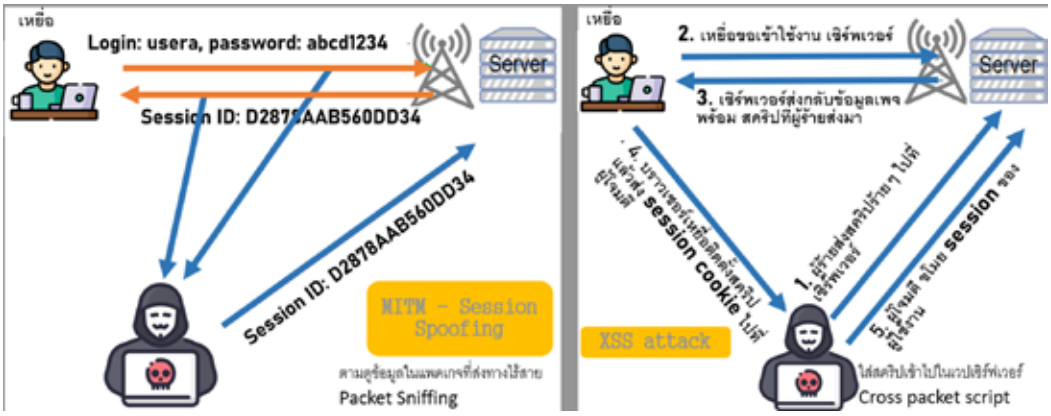
5.2.2.2.2 แนวทางป้องกันการโจมตีแบบ ReVoLTE

หลังจากการค้นพบดังกล่าว มีการแจ้งไปยัง The 3rd Generation Partnership Project (3GPP) ซึ่งเป็นหน่วยงานจัดทำมาตรฐานของโทรศัพท์เคลื่อนที่ด้วยเทคโนโลยียุคที่ 5 ทำให้มีการออกซอฟต์แวร์รุ่นแก้ไขออกมาเพื่อแก้ปัญหารอยรั่วข้อมูล แต่ปัญหาดังกล่าวยังอาจพบได้อีก ขึ้นอยู่กับว่าผู้ให้บริการได้ติดตั้งซอฟต์แวร์รุ่นแก้ไขที่ออกมาแล้วครบหรือไม่ ดังนั้นผู้ให้บริการควรติดตั้งซอฟต์แวร์ให้เป็นเวอร์ชันใหม่อยู่เสมอ

5.2.2.3 การโจมตี MitM แบบขโมยเซสชัน (session spoofing attack) และแนวทางป้องกัน

5.2.2.3.1 การโจมตีแบบขโมยเซสชัน

การโจมตีแบบปลอมแปลงเซสชันนี้ เป็นการโจมตีที่ผู้ร้ายขโมยตัวระบุเซสชัน (session ID) ของผู้ใช้งาน โดยสถานีฐานเป็นอุปกรณ์ที่แจกค่านี้ให้แก่ผู้ใช้บริการโดยฝังไว้ที่ส่วนหัวของข้อมูล เนื่องจากการเข้ารหัสข้อมูลในโครงข่ายโทรศัพท์เคลื่อนที่ยุคที่ 3 เป็นการเข้ารหัสข้อมูลของผู้ใช้งาน ไม่ได้เป็นการเข้ารหัสตัวระบุเซสชัน ดังนั้น เมื่อขโมยค่านี้ไปได้ ผู้ร้ายก็จะปลอมตัวเป็นผู้ใช้งาน ขโมยข้อมูลของผู้ใช้งานจากเว็บไซต์ หรือแอบดูข้อมูลได้ สำหรับตัวระบุเซสชันของโครงข่ายยุคที่ 4 มีการเข้ารหัสแล้ว (Banach, 2019)



ภาพที่ 7 การโจมตีโดยการไปอยู่ตรงกลางแบบขโมยเซสชัน

ที่มา: Banach (2019)

การโจมตีแบบนี้มี 2 วิธีย่อย วิธีที่หนึ่ง ดังภาพที่ 7 ทางซ้าย เรียกว่า การลักลอบขโมยเซสชัน โดยใช้วิธีเก็บข้อมูลแบบ passive คือแอบฟังข้อมูลแล้วนำมาใช้ประโยชน์ในทางมิชอบ ไม่ได้มีการปลอมแปลงหรือเปลี่ยนข้อมูลที่ส่งต่อให้กับเซิร์ฟเวอร์หรือผู้ใช้งาน ส่วนวิธีที่สองเรียกว่า การโจมตีด้วยสคริปต์ข้ามไซต์ (Cross-Site Scripting attack: XSS) โดยผู้ร้ายจะส่งโคด (code) ที่เป็นอันตรายไปยังเว็บไซต์ เมื่อผู้ใช้งานกลับมาใช้งานที่เว็บเซิร์ฟเวอร์อีกครั้งก็จะติดไวรัส และเมื่อเบราว์เซอร์ใช้งานสคริปต์ จะส่งตัวระบุเซสชันไปให้กับผู้ร้าย ซึ่งหลังจากนั้นจะขโมย (hijacks) เซสชันของเหยื่อได้

5.2.2.3.2 แนวทางการป้องกันการโจมตีแบบขโมยเซสชัน

วิธีการป้องกันการโจมตีสามารถทำโดย 1) ยืนยันตัวตนก่อนขอตัวระบุเซสชัน 2) เข้ารหัสตัวระบุเซสชัน และ 3) ระบุการหมดเวลาในการใช้ตัวระบุเซสชันเพื่อให้มีการขอใหม่หลังจากนั้น

5.2.2.4 การโจมตี MITM แบบพ่นยาพิษไปที่ DNS และแนวทางป้องกัน

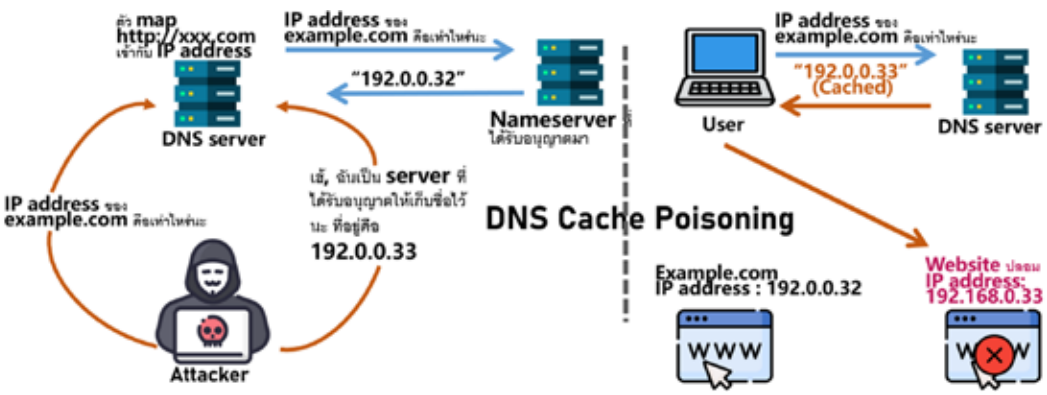
5.2.2.4.1 การโจมตีแบบ DNS cache poisoning

การโจมตีในอีกรูปแบบหนึ่ง เรียกว่า DNS spoofing เป็นการหลอกผู้ใช้งานว่าอุปกรณ์ปลอมของผู้ร้ายเป็นเซิร์ฟเวอร์ที่บอกชื่อโดเมนที่ผู้ใช้งานต้องการเรียกใช้งาน โดยส่งบันทึกชื่อโดเมน (DNS record) ที่ผิดให้กับผู้ใช้งานโดยตรง หรือให้กับอุปกรณ์เซิร์ฟเวอร์ที่เป็นตัวเก็บชื่อโดเมนจริง ๆ ของระบบ โดย DNS record เป็นชิ้นส่วนของข้อมูลที่จัดเก็บไว้ในเซิร์ฟเวอร์ที่เก็บชื่อโดเมน และบอกเซิร์ฟเวอร์ว่าจะแปลงชื่อโดเมนเป็นที่อยู่ทางอินเทอร์เน็ต (IP address) ได้อย่างไร

โดยทั่วไป ถึงแม้ผู้ใช้งานจะใช้งานแทรฟฟิกผ่านโทรศัพท์มือถือปกติ แต่ส่วนใหญ่เมื่อเข้าไปอยู่ในสถานที่ที่มีจุดเชื่อมต่อวายฟาย ผู้ใช้งานจะเปลี่ยนเป็นเปิดใช้งานวายฟายเพื่อประหยัดค่าใช้จ่ายด้านการรับส่งข้อมูล เช่น ในสถานที่เปิดทั่ว ๆ ไป เช่น ร้านกาแฟหรือโรงแรม

1) DNS spoofing หรือส่งข้อมูล DNS ผิด ๆ ไปให้ผู้ใช้บริการ ทำให้ผู้ใช้บริการเชื่อมต่อไปยังเว็บไซต์ปลอม และอาจเผลอกรอกข้อมูลที่เป็นความลับในการเข้าใช้งานเว็บไซต์นั้น

2) DNS cache poisoning โดยผู้ร้ายปลอมเป็นเว็บเซิร์ฟเวอร์ แล้วแจ้งข้อมูล DNS ที่ผิดให้กับวายฟายเราเตอร์ ทำให้เมื่อผู้ใช้งานเรียกใช้เว็บไซต์ที่ต้องการใช้งาน แทรฟฟิกจะถูกส่งต่อไปยังเว็บเซิร์ฟเวอร์ที่ผู้ร้ายแอบดูอยู่ และถูกหลอกให้กรอกข้อมูลลับ เหมือนกับกรณีของ DNS spoofing (Cloudflare, n.d.)



ภาพที่ 8 การโจมตีโดยการไปอยู่ตรงกลาง แบบ DNS Cache Poisoning (MITM - DNS Cache Poisoning)

ที่มา: Cloudflare (n.d.)

5.2.2.4.2 แนวทางป้องกันการโจมตีแบบ DNS cache poisoning

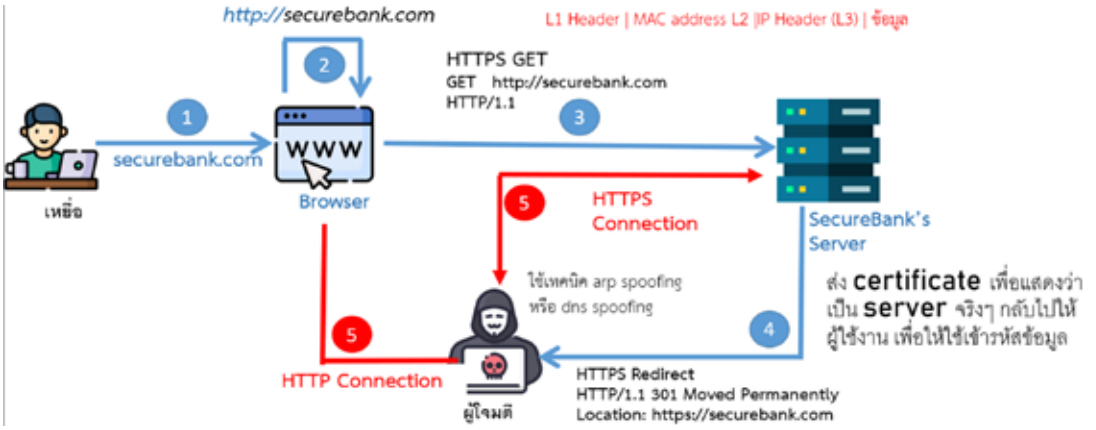
ในกรณีนี้ เพื่อเพิ่มความปลอดภัยของระบบ ผู้ให้บริการโครงข่ายควรติดตั้งการใช้งานโพรโทคอล DNS Security (DNS SEC) ที่มีการใช้ลายเซ็นดิจิทัลเพื่อตรวจสอบบันทึกชื่อโดเมนใด ๆ หรือใช้เทคนิค DNS split ที่มีการใส่บันทึกชื่อโดเมนไว้ที่ DNS เซิร์ฟเวอร์จริงหลาย ๆ ตัวเพื่อป้องกันการถูกพ่นพิษไปยังบันทึกชื่อโดเมน

5.2.2.5 การโจมตี MITM แบบขโมยเซสชัน SSL/TLS hijacking และแนวทางป้องกัน

5.2.2.5.1 การโจมตีแบบ SSL/TLS hijacking

โดยปกติ Secure Sockets Layer (SSL)/Transport Layer Security (TLS) จะถูกเรียกใช้เวลาที่ผู้ใช้งานใช้ Hypertext Transfer Protocol Secure (HTTPS) เพื่อเข้าใช้เว็บไซต์ที่ต้องการความปลอดภัย เช่น เว็บไซต์ธนาคาร เพราะจะมีการเข้ารหัสข้อมูล สำหรับหลักการของโจมตี SSL/TLS เป็นการโจมตีที่ผู้ร้ายเข้าไปแอบฟังและเปลี่ยนแปลงการตกลงกันของโพรโทคอล SSL/TLS handshake ระหว่างผู้ใช้งานกับเซิร์ฟเวอร์เพื่อบังคับให้ผู้ใช้งานเข้าไปที่เว็บปลอมและหลอกเอาข้อมูลลับ (Hossain et al., 2018)

การที่จะโจมตีแบบนี้ได้สำเร็จ สามารถทำได้หลายรูปแบบ จะใช้เทคนิค DNS spoofing หรือ DNS cache poisoning ดังที่อธิบายข้างต้น เมื่อใช้เทคนิคส่งบันทึกชื่อโดเมน (DNS record) ปลอมหลอกผู้ใช้งานว่าเป็นเว็บเซิร์ฟเวอร์ที่ผู้ใช้งานต้องการใช้บริการได้ เว็บไซต์เซิร์ฟเวอร์ปลอมซึ่งไม่รองรับการใช้งาน HTTPS จะตอบกลับเป็น HTTP โดยบางครั้งผู้ใช้งานยอมใช้ HTTP แต่บางกรณีเว็บเซิร์ฟเวอร์ปลอมจะส่งกลับ HTTPS โดยใช้รหัสใหม่ของเว็บปลอมในการส่งข้อมูล ดังนั้น ผู้ใช้งานจำเป็นต้องตรวจดูให้แน่ใจว่าเซิร์ฟเวอร์มีใบรับรอง (certificate) ที่น่าเชื่อถือจริง ๆ ไม่ได้เป็นใบรับรองที่สร้างขึ้นเอง



ภาพที่ 9 การโจมตีโดยการไปอยู่ตรงกลาง แบบขโมย SSL/TLS (SSL/TLS Hijacking)

ที่มา: Hossain et al. (2018)

Address Resolution Protocol (ARP) spoofing จะเป็นอีกเทคนิคที่สามารถนำมาใช้ทำ SSL/TLS hijacking ให้สำเร็จได้เช่นกัน โดย ARP เป็นโพรโทคอลที่ใช้ในการจับคู่ที่อยู่ IP กับที่อยู่ Media Access Control (MAC) Layer 2 เพื่อใช้ส่งข้อมูลในโครงข่ายเดียวกัน การทำ ARP spoofing ก็เป็นการปลอมที่อยู่ของเซิร์ฟเวอร์ในระดับต่ำกว่าชั้น IP layer นั่นเอง

5.2.2.5.2 แนวทางป้องกันการโจมตีแบบ SSL/TLS hijacking

วิธีการป้องกันมีหลายวิธี วิธีแรกคือการใช้ DNSSEC ซึ่งมีการใส่ลายเซ็นดิจิทัลต่อท้ายในข้อมูลบันทึกชื่อโดเมนเพื่อให้แน่ใจว่าตอบมาจากเซิร์ฟเวอร์ที่ได้รับอนุญาต วิธีที่สองคือ การใช้โพรโทคอล IP source guard หรือ ARP reverse เพื่อป้องกันเครือข่ายจากการปลอมแปลง IP หรือ ARP ตามลำดับ ในการตรวจสอบความถูกต้องของที่อยู่ โดยทั้งสองโพรโทคอลทำงานคล้ายคลึงกันคือ พิจารณา IP address ต้นทางของแพ็กเก็ตที่ผูกเข้ากับ MAC address ของอุปกรณ์ที่ได้รับอนุญาตให้ส่งแทรฟฟิก โดยหาก IP address ต้นทางของแพ็กเก็ตไม่ตรงกับ MAC address ของอุปกรณ์ที่ได้รับอนุญาตให้ส่งแทรฟฟิกบนเซกเมนต์ (IP source guard) หรือ Subnet (ARP reverse) นั้น ๆ ตามลำดับ แพ็กเก็ตจะถูกทิ้งไป ทั้งนี้ สามารถใช้ทั้งสองโพรโทคอลร่วมกันเพื่อครอบคลุมยิ่งขึ้น

5.2.3 การโจมตีแบบ DoS attack และแนวทางป้องกัน

5.2.3.1 การโจมตีแบบ DoS attack

การโจมตีโดยส่งข้อมูลจำนวนมาก ๆ (Denial of Service attack: DoS attack) เป็นการที่ผู้ร้ายพยายามส่งแทรฟฟิกเข้ามาในโครงข่ายเป็นจำนวนมาก เพื่อเข้าโจมตีให้เซิร์ฟเวอร์เสียเวลาในการรับอ่านที่อยู่และทิ้งข้อมูลของผู้ร้าย จนไม่สามารถไปให้บริการลูกค้าตามปกติได้ ในกรณีนี้โครงข่ายจะมี ไฟร์วอลล์เพื่อป้องกันคอยตรวจสอบว่าแทรฟฟิกที่เข้ามามีการโจมตีในลักษณะดังกล่าวเข้ามาหรือไม่

5.2.3.2 แนวทางป้องกันการโจมตีแบบ DoS attack

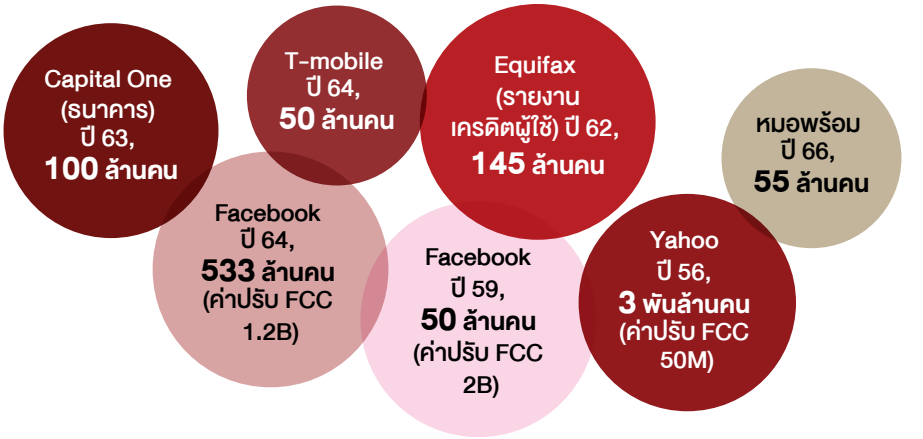
สำหรับการป้องกันการโจมตีในส่วนของเซิร์ฟเวอร์จะใช้วิธีให้คลิกรูปต่าง ๆ เช่น รูปรถ สะพาน เมื่อเข้าหน้าล็อกอินที่ต้องใส่ยูสเซอร์เนม (username) และพาสเวิร์ด (password) เพื่อให้แน่ใจว่าเป็นการร้องขอจากมนุษย์ ไม่ใช่จากบอต (bot)

อุปกรณ์ไฟร์วอลล์ถูกนำมาตรวจจับการโจมตีด้วยแทรฟฟิกจำนวนมาก โดยการนำมาคั่นก่อนแทรฟฟิกเข้าหรือออกจากโครงข่ายด้วยการดรอปทิ้งแทรฟฟิกที่ตรงกับแพทเทิร์นที่กำหนดไว้ ทั้งนี้สามารถทำงานร่วมกันกับอุปกรณ์ป้องกันการบุกรุก (Intrusion Prevention System: IPS) ซึ่งใช้ในเชิงป้องกันด้วยการวางอุปกรณ์ไว้ด้านหลังไฟร์วอลล์และมอนิเตอร์ดูลักษณะแทรฟฟิกที่ผิดปกติอยู่อย่างสม่ำเสมอ (VMWare, n.d.)

5.2.4 การโจมตีแบบ data breaches และแนวทางป้องกัน

5.2.4.1 การโจมตีแบบ data breaches

เป็นการรั่วไหลของข้อมูล (data breaches) ซึ่งโดยทั่วไปผู้ร้ายก็จะนำข้อมูลไปใช้เพื่อเอาเงินออกมาจากธนาคารหรือบัตรเครดิต แต่ถ้าข้อมูลรั่วไหลจำนวนมาก เรียกว่า การโจมตีเพื่อเรียกค่าไถ่ (ransomware attacks) ผู้ร้ายจะนำเอาการรั่วไหลของข้อมูลมาขู่กรรโชกเพื่อให้โอนเงินให้ สำหรับกรณีตัวอย่างการเรียกค่าไถ่ ดังภาพที่ 10



ภาพที่ 10 ตัวอย่างกรณีการโจมตีแบบเรียกค่าไถ่

- พ.ศ. 2556-2559 ข้อมูลของลูกค้า Yahoo ซึ่งให้บริการอีเมลรั่วไหลมากกว่า 3 พันล้านราย (Stempel, 2019)
- พ.ศ. 2562 Equifax ซึ่งเป็นบริษัทเอเจนซีที่รายงานเครดิตของผู้ใช้งานบัตรเครดิต มีข้อมูลรั่วไหลมากกว่า 145 ล้านราย (Cowley, 2019)
- พ.ศ. 2563 ธนาคาร Capital One ทำข้อมูลลูกค้า 100 ล้านคนรั่วไหล (Neto et al., 2020)
- พ.ศ. 2564 ผู้ให้บริการโทรศัพท์เคลื่อนที่ T-mobile ทำข้อมูลลูกค้า 50 ล้านคนรั่วไหล (Reichert, 2023)
- ในปีเดียวกัน พ.ศ. 2564 เฟซบุ๊ก (Facebook) ทำให้มีข้อมูลผู้ใช้งานมากกว่า 533 ล้านคนรั่วไหล (Powell, 2022)

การรั่วไหลเหล่านี้ มีทั้งข้อมูลทั่ว ๆ ไป เช่น ชื่อ ที่อยู่ รวมทั้งข้อมูลสำคัญ ๆ เช่น เลขประกันสังคมของสหรัฐอเมริกาที่สำคัญคล้ายกับบัตรประชาชนของไทย ข้อมูลบัตรเครดิต และอื่น ๆ

นอกจากนั้น ใน ค.ศ. 2016 (พ.ศ. 2559) มีข้อมูลรั่วไหลเกิดจากการที่บริษัทแคมบริดจ์อนาไลติกนำเอาคำถามทางการเมืองไปโพสต์ที่เฟซบุ๊ก และเมื่อผู้ใช้งานประมาณ 2 แสนกว่าคน คลิกเข้าไปตอบคำถามจะมีการขอผู้ใช้งานอนุญาตให้สามารถเข้าถึงชื่อเพื่อนได้ ทำให้ได้ข้อมูลของประชาชนมากกว่า 87 ล้านคน และต่อมาข้อมูลดังกล่าวถูกนำมาใช้ในการวิเคราะห์และใช้ในการทำแคมเพน (campaign) ทางการเมืองของนายโดนัลด์ ทรัมป์ และมีผู้คาดการณ์ว่าเป็นผลทำให้เขาชนะการเลือกตั้งตำแหน่งประธานาธิบดีไปได้ในปีนั้น (Zialcita, 2019)

ประเทศไทยมีกรณีข้อมูลรั่วไหลมากกว่า 55 ล้านคนเช่นกัน พบในเดือนเมษายน พ.ศ. 2566 ซึ่งคาดว่ามาจากแอปพลิเคชันหมอพร้อม ซึ่งให้บริการทางการแพทย์ มีการพัฒนาและใช้อย่างแพร่หลายจากการระบาดของโรคติดเชื้อไวรัสโคโรนา พ.ศ. 2562 โดยจากการสืบสวนพบว่า ผู้ต้องหาได้ข้อมูลมาจากที่ขายบนเว็บมืด (บีบีซี, 2566)

5.2.4.2 แนวทางป้องกันการโจมตีแบบ data breaches

องค์กรใหญ่ ๆ สามารถป้องกันการรั่วไหลของข้อมูลได้ดังนี้ (Holmes, n.d.)

1) ตั้งระบบให้ผู้ใช้ตั้งค่าพาสเวิร์ดเป็นคำที่ยากต่อการคาดเดา และต้องขอเข้าใช้งานโดยผ่านระบบแบบหลายแฟกเตอร์ (multi-factor authentication) ซึ่งเพิ่มการยืนยันตัวตนผ่านมือถือและเทียบลายนิ้วมือ

2) อัปเดตซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดเสมอ

3) ใช้ลิงก์เข้าเว็บที่ป้อนพาสเวิร์ดเป็นลิงก์ที่ปลอดภัยโดยใช้ HTTPS เสมอ

4) ให้ความรู้ด้านความปลอดภัยกับพนักงาน และ

5) สร้างแผนตอบสนองหากข้อมูลรั่วไหล

5.2.5 การโจมตีแบบด้านข้าง (side channel attack) และแนวทางป้องกัน

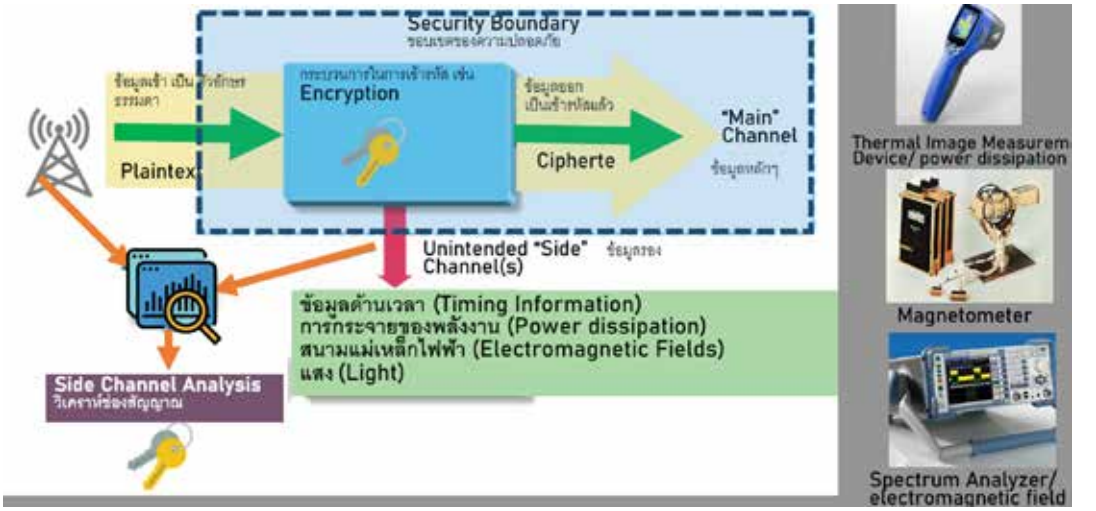
5.2.5.1 การโจมตีแบบด้านข้าง

แบบที่ห้า เป็นการโจมตีด้านข้าง ดังภาพที่ 11 (Gamaarachchi & Ganegoda, 2018) ในการเข้ารหัสข้อมูลหนึ่ง ๆ ผู้ร้ายสามารถนำข้อมูลที่เกี่ยวกับตัวฮาร์ดแวร์อุปกรณ์มาใช้ในการวิเคราะห์ เนื่องจากการส่งข้อมูลที่เข้ารหัสที่ต่างกัน จะเกิดการกระจายของพลังงาน สนามแม่เหล็กไฟฟ้า แสงที่ส่งออกมา หรือแม้แต่ระยะเวลาที่ส่งข้อมูลที่ต่างกัน ผู้ร้ายอาจจะใช้เครื่องมือในการวัดพลังงาน (magnetometer) เพื่อวัดสนามแม่เหล็กไฟฟ้า หรือใช้เครื่องมือเก็บภาพการกระจายความร้อน (thermal image) และกระจายตัวของแสงเพื่อนำมาวิเคราะห์เพื่อหากุญแจ (key) ของการเข้ารหัสได้

การโจมตีแบบด้านข้างเกิดขึ้นมาหลายครั้ง และเกิดขึ้นได้กับเครื่องโทรศัพท์มือถือหลายรุ่น ทั้งระบบปฏิบัติการแอนดรอยด์และไอโอเอส โดยการโจมตีส่วนใหญ่ต้องสามารถเข้าถึงอุปกรณ์โทรศัพท์มือถือของเหยื่อได้จึงจะสามารถดึงข้อมูลได้ แต่ในบางครั้ง อาจทำตัวเป็นสถานีฐานปลอมเพื่อวัดพลังงานจากโทรศัพท์มือถือในระยะไกลได้เช่นกัน

สำหรับตัวอย่างการโจมตีที่จะอธิบายถึงต่อไปนี้ เป็นการโจมตีโดยใช้เวลาในการส่งข้อมูลที่เข้ารหัสแล้วมาวิเคราะห์ ใน พ.ศ. 2562 มหาวิทยาลัยเพอร์ดู (Purdue University) และมหาวิทยาลัยไอโอวา (University of Iowa) ศึกษาการใช้เทคนิคการโจมตีแบบตอร์ปิโด (TRacking via Paging mEssage DistributiOn: ToRPEDO) ซึ่งใช้ประโยชน์จากตารางเวลาที่แน่นอนที่สถานีฐานใช้ส่งและที่โทรศัพท์มือถือใช้ในการตรวจสอบการส่ง paging ซึ่งตารางเวลานี้จะขึ้นอยู่กับค่าตัวชี้เฟรม (paging frame index) ที่เซตค่าขึ้นกับข้อมูลเลขระบุโทรศัพท์มือถือ (International Mobile Subscriber Identity: IMSI) (Hussain et al., 2019)

การโทรหาเหยื่อบ่อย ๆ จะทำให้สถานีฐานส่ง paging ไปยังโทรศัพท์มือถือเพื่อระบุตำแหน่ง ผู้ร้ายจะสามารถตรวจดูได้ว่าช่วงเวลาใดมีการส่ง paging และเป็นผลให้ทราบถึงเลข IMSI บางส่วนด้วย ซึ่งผู้ร้ายสามารถทำการโจมตีได้โดยส่ง paging ปลอมในช่วงเวลานั้น เพื่อทำให้สถานีฐานไม่สามารถติดต่อโทรศัพท์มือถือของเหยื่อได้ และหากผู้ร้ายทำการโจมตีในรูปแบบอื่นเพิ่มเติม จะทราบค่า IMSI ทั้งหมดและสามารถเข้าโจมตีในรูปแบบอื่นเพิ่มเติมได้อีก เช่น ปลอมตัวเป็นเหยื่อและเข้าเก็บข้อมูลสำคัญ ๆ ของเหยื่อได้



ภาพที่ 11 การโจมตีทางด้านข้าง

ที่มา: Gamaarachchi and Ganegoda (2018)

นอกจากวิธีดังกล่าว ผู้ร้ายสามารถทำตัวเป็นสถานีฐานปลอมและจำลองข้อมูล paging ส่งไปที่โทรศัพท์มือถือ โดยใช้การเข้ารหัสหลายรหัส แล้ววัดเวลาที่โทรศัพท์มือถือถอดรหัสได้สำเร็จของแต่ละรหัส ก่อนนำไปเปรียบเทียบกับเวลาที่ใช้ในการถอดรหัสข้อมูล paging ที่มาจากสถานีฐานของจริง เพื่อจะทราบได้ว่ารหัสที่สถานีฐานที่แท้จริงใช้นั้นคือรหัสอะไร (Gamaarachchi & Ganegoda, 2018)

5.2.5.2 แนวทางป้องกันการโจมตีแบบด้านข้าง

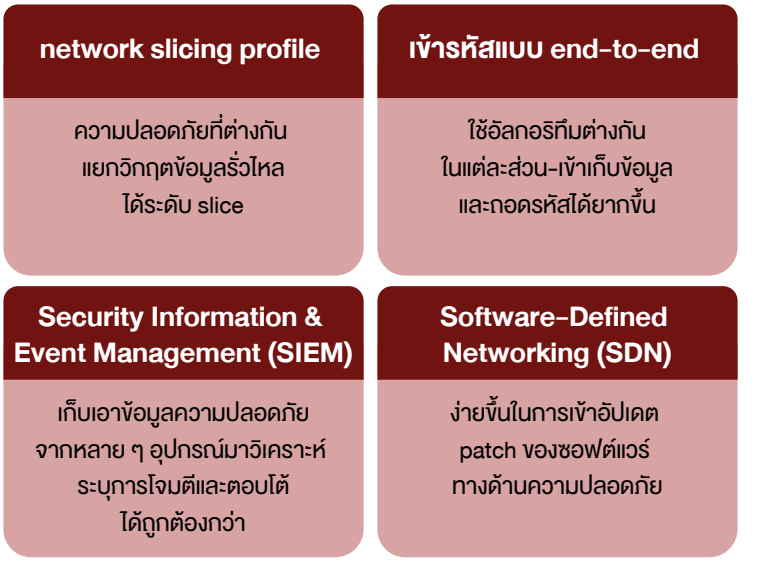
การโจมตีด้านข้างมีประสิทธิภาพสูงมาก สามารถโจมตีโทรศัพท์เคลื่อนที่ได้ทุกรุ่น ในขณะเดียวกัน หากผู้ให้บริการต้องการป้องกันการโจมตีด้านข้างในรูปแบบของการนำเอาเวลาการเข้ารหัสข้อมูลมาวิเคราะห์ ผู้ให้บริการสามารถใส่ค่าตัวแปรของเวลาที่ใช้ในการส่งข้อมูล paging เพิ่มได้ แต่โดยทั่วไปแล้วผู้ให้บริการอาจจะไม่ได้ติดตั้งค่าตัวแปรดังกล่าว เนื่องจากความยุ่งยากและทรัพยากรที่ต้องใช้เพิ่มขึ้น และข้อมูลส่วนใหญ่ไม่ได้ต้องการความปลอดภัยมากนัก อย่างไรก็ตาม ควรพิจารณาติดตั้งค่าตัวแปรดังกล่าว หากออกแพ็กเกจโพรโมชันสำหรับหน่วยงานหรือผู้ใช้บริการที่ต้องการส่งข้อมูลที่ต้องการความปลอดภัยขั้นสูง

นอกจากนี้ ยังมีวิธีการป้องกันอื่น ๆ ดังต่อไปนี้ ได้แก่ 1) บังคับใช้เลขระบุโทรศัพท์เคลื่อนที่ชั่วคราวที่เปลี่ยนอยู่เสมอ 2) เปลี่ยนความถี่ที่ใช้ในการส่งเรื่อย ๆ เพื่อให้ยากต่อการคาดเดาและเข้าเก็บข้อมูล 3) สุ่มเปลี่ยนตารางเวลาการส่ง paging หรือสร้าง paging ที่ไม่จำเป็นเพื่อสร้างความสับสนให้กับผู้ร้าย (Singla et al., 2020; Vreman et al., 2019) และ 4) พัฒนาโพรโทคอล ที่เข้มงวดต่อการขอเข้าใช้งาน (authentication) ให้มากขึ้นในอนาคตเพื่อจำกัดการถูกโจมตีแบบด้านข้างจากผู้ร้าย

5.3 ข้อแนะนำการติดตั้งใช้งานเพื่อความปลอดภัย

5.3.1 การรักษาความปลอดภัยในโครงข่ายยุคที่ 5

การรักษาความปลอดภัยในโครงข่ายยุคที่ 5 แบบไม่พึ่งโครงข่ายยุคก่อน หรือที่เรียกว่าแบบ standalone หากพิจารณาสถาปัตยกรรมโครงข่ายจะพบว่า ประโยชน์ของโครงข่ายยุคที่ 5 แบบ standalone จะเหนือกว่าโครงข่ายยุคก่อน ดังภาพที่ 12 และภาพที่ 13 อย่างไรก็ตาม มีความเสี่ยงกับระบบความปลอดภัยบางอย่างเพิ่มขึ้น ดังนี้



ภาพที่ 12 ฟีเชอร์ความปลอดภัยในโครงข่ายยุคที่ 5 แบบ standalone ที่เพิ่มขึ้น

ภาพที่ 13 ช่องโหว่ความปลอดภัยในโครงข่ายยุคที่ 5 แบบ standalone

5.3.1.1 เสี่ยงต่อการโจมตีช่องทางด้านข้างยิ่งขึ้น การโจมตีช่องด้านข้างใช้ประโยชน์จากคุณสมบัติทางกายภาพของอุปกรณ์หรือระบบเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ไม่ว่าจะด้วยการวิเคราะห์พลังงานหรือเวลาที่อุปกรณ์ใช้ในการดำเนินการเข้ารหัส จะสามารถอนุมานรหัสลับที่ใช้เข้ารหัสข้อมูลได้

การโจมตีด้านข้าง มีในโครงข่ายยุคก่อน ๆ อยู่แล้ว และใช้หลักการเดียวกัน แต่สำหรับเทคโนโลยีโทรศัพท์เคลื่อนที่ยุคที่ 5 ที่เป็นอุปกรณ์รุ่นใหม่จะมีความเสี่ยงในการทดลองถูกเจาะระบบมากกว่า เนื่องจากเป็นการใช้ฮาร์ดแวร์รุ่นใหม่ มีฟังก์ชันเครือข่ายและโพรโทคอลที่ใช้ที่หลากหลาย ทำให้มีความละเอียด

(sensitivity) ในการใช้งานพลังงานที่จะนำมาใช้เจาะระบบมากกว่า อีกทั้งอุปกรณ์ที่ใช้เจาะระบบมีความสามารถในการเก็บแคช (cache) ข้อมูลสูงกว่า ความสามารถในการคำนวณที่รวดเร็วกว่า และเข้าถึงแบนด์วิดท์ที่กว้างกว่าที่ทำให้สัญญาณรบกวนมีผลน้อยลงอีกด้วย (Lavaud et al., 2021)

5.3.1.2 โครงข่ายยุคที่ 5 มีการเปลี่ยนแปลงที่สำคัญ คือ การใช้ซอฟต์แวร์กำหนดเครือข่าย (SDN) และติดตั้งไว้บนคลาวด์ อุปกรณ์ในโครงข่ายหลายอุปกรณ์ถูกมารวมกันในคลาวด์ ซึ่งโดยหลักการแล้วเป็นการช่วยลดความหน่วงและเพิ่มความสามารถในการปรับขนาด (scalability) หรือรองรับการใช้งานอุปกรณ์จำนวนมาก แต่การทำเช่นนี้ หากผู้ร้ายสามารถเข้าถึงเจาะฟังก์ชันใด ๆ ในคลาวด์ได้ ก็จะทำให้ฟังก์ชันอื่น ๆ ในโครงข่ายหลักมีความเสี่ยงไปด้วย โดยปัญหาของความสามารถในการควบคุมแบบเป็นศูนย์รวมได้ถูกระบุไว้ในงานศึกษาของ Angelo Bjerre et al. (2023)

5.3.1.3 เมื่อโครงข่ายหลักบนคลาวด์มีฟังก์ชันเพิ่มขึ้นจำนวนมาก จึงเป็นการเพิ่มความเสี่ยงให้มีฟังก์ชันหรือจุดที่จะเข้าโจมตีที่เพิ่มขึ้นด้วย

5.3.1.4 โครงข่ายยุคที่ 5 สามารถเชื่อมต่ออุปกรณ์ IoT ได้จำนวนมาก ซึ่งโดยปกติอุปกรณ์ IoT มักติดตั้งไว้ในที่ที่เข้าถึงง่าย และหากผู้ร้ายสามารถเข้าถึงและควบคุมอุปกรณ์ได้ จะมีโอกาสเข้าเจาะโครงข่ายแบบริโมตคอนโทรลจากช่องโหว่ของอุปกรณ์ IoT เหล่านี้ด้วย ซึ่งอันตรายมาก

5.3.1.5 ความเสี่ยงประการสุดท้าย ถึงแม้ว่าความสามารถในการทำ network slicing จะมีข้อดีในการดูแลปัญหาความปลอดภัยได้เฉพาะแต่ละ slice มากกว่า แต่การคอนฟิก (configure) ค่าผิด เช่น การใช้รหัสหรือพารามิเตอร์ทางความปลอดภัยสำหรับหลาย slice เป็นค่าเดียวกัน จะทำให้เกิดวิกฤตได้อย่างหนักมากกว่า โดยข้อมูลทางความปลอดภัยที่ได้จาก slice หนึ่งซึ่งใช้สำหรับแทรฟฟิกที่ไม่สำคัญ อาจจะสามารถนำไปใช้ในการเจาะอีก slice หนึ่งซึ่งใช้กับแทรฟฟิกสำคัญมาก ๆ ได้ด้วย

จากความเสี่ยงข้างต้น จึงมีข้อแนะนำเพื่อความปลอดภัยของอุปกรณ์และเครือข่ายดังนี้

5.3.2 การรักษาความปลอดภัยสำหรับโครงข่าย

5.3.2.1 อัปเดตซอฟต์แวร์ ตรวจสอบให้แน่ใจว่าระบบปฏิบัติการและแอปพลิเคชันได้รับการอัปเดตล่าสุดอยู่เสมอ การอัปเดตเหล่านี้มักมีการแก้ไขช่องโหว่ด้านความปลอดภัยที่ตรวจสอบพบมาก่อนแล้ว

5.3.2.2 จัดหาและใช้ฟังก์ชันทางโครงข่ายหลักที่บังคับให้ใช้นโยบายทางด้านความปลอดภัย เช่น ฟังก์ชัน SCP และ SEPP เพื่อให้ทุกฟังก์ชันในโครงข่ายมีความปลอดภัย

5.3.2.3 แบ่งส่วนของโครงข่ายที่สามารถเข้าถึงโดยอุปกรณ์ IoT ให้มีสิทธิเข้าถึงได้น้อยกว่าอุปกรณ์ชนิดอื่น เนื่องจากมีความเสี่ยงในการโดนเจาะระบบจากการเข้าถึงด้วยอุปกรณ์เหล่านี้มากกว่า

5.3.2.4 ตรวจสอบค่าคอนฟิกของ slice ต่าง ๆ อยู่อย่างสม่ำเสมอ หลีกเลี่ยงการใช้รหัสผ่านเดียวกันในการคอนฟิก slice ที่มีระดับความสำคัญต่างกัน และแนะนำให้ผู้ตรวจสอบและผู้คอนฟิกเป็นคนละคนกัน

5.3.2.5 ใช้รหัสผ่านที่รัดกุม ตั้งค่ารหัสผ่านที่คาดเดายากสำหรับอุปกรณ์และโครงข่าย และหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับบัญชีหลายบัญชี

5.3.2.6 ติดตั้งซอฟต์แวร์หรืออุปกรณ์ที่ช่วยในการตรวจจับและป้องกันไวรัส หรือการเจาะระบบรูปแบบต่าง ๆ เช่น Intrusion Prevention System (IPS)

5.3.3 การรักษาความปลอดภัยสำหรับผู้ใช้งาน

5.3.3.1 ระมัดระวังโทรศัพท์มือถือของตน หากสูญหาย ควรปรับเปลี่ยนรหัสผ่านใหม่ทันทีที่ได้กลับคืนมา

5.3.3.2 ระวังการคลิก หลีกเลี่ยงการคลิกลิงก์หรือสิ่งที่แนบมาในข้อความอีเมลหรือข้อความที่น่าสงสัย เพราะอาจนำไปสู่มัลแวร์หรือเว็บไซต์ฟิชชิง (phishing)

5.3.3.3 ดาวน์โหลดแอปพลิเคชันจากแหล่งที่เชื่อถือได้ โดยดาวน์โหลดแอปพลิเคชันจาก App Store หรือ Google Play Store เท่านั้น หลีกเลี่ยงการติดตั้งแอปพลิเคชันจากแหล่งที่ไม่รู้จัก

5.3.3.4 เปิดใช้งานการตรวจสอบสิทธิ์แบบสองปัจจัย (2FA) ในกรณีที่เป็นไปได้ ควรเปิดใช้งาน 2FA บนบัญชีของผู้ใช้งาน การใช้งาน 2FA จะเพิ่มชั้นความปลอดภัยเพิ่มเติม โดยต้องใส่รหัสจากโทรศัพท์มือถือหรืออุปกรณ์อื่นเพิ่มเติมนอกเหนือจากรหัสผ่านเมื่อผู้ใช้งานต้องการเข้าสู่ระบบ

5.3.3.5 ใช้โครงข่ายที่ปลอดภัย หากจำเป็นต้องใช้วายฟายสาธารณะ ให้ใช้เครือข่ายส่วนบุคคลเสมือน (Virtual Private Network: VPN) เพื่อเข้ารหัสการรับส่งข้อมูล โดย VPN จะเข้ารหัสการรับส่งข้อมูลของผู้ใช้งานและช่วยปกป้องข้อมูลจากการสอดแนม

5.3.3.6 ปิดใช้งานวายฟายเมื่อไม่ใช้งาน การปิดวายฟายบนอุปกรณ์เมื่อไม่ได้ใช้งาน ช่วยป้องกันไม่ให้ผู้โจมตีสามารถสแกนอุปกรณ์ได้

5.3.3.7 เลือกใช้เว็บไซต์ที่มีระบบรักษาความปลอดภัย โดยสังเกตที่อยู่เว็บไซต์ที่ขึ้นต้นด้วย HTTPS

6. การอภิปรายผล

ประโยชน์จากการพัฒนาสถาปัตยกรรมโครงข่ายโทรศัพท์เคลื่อนที่ยุคที่ 5 พบว่า โครงข่ายยุคที่ 5 แบบ standalone ใช้โครงข่ายหลักและสถานีฐานยุคที่ 5 อย่างเดียว ทำให้มีฟีเซอร์ (feature) การเข้ารหัสตลอดทางจากฝั่งเครื่องผู้ส่งไปยังฝั่งเครื่องผู้รับ ส่งผลให้ในการลักลอบเข้าถึงข้อมูลทำได้ยากขึ้น นอกจากนั้น

สามารถแบ่งชั้นของโครงข่าย (network slicing) ซึ่งเป็นการแบ่งทรัพยากรย่อย ๆ ในแต่ละอุปกรณ์ แต่ละ slice มีระดับความปลอดภัย (security profile) ที่แตกต่างกัน สามารถแยกความวิกฤตในการที่ข้อมูลรั่วไหลได้แต่ละระดับ slice อีกทั้งการเปลี่ยนแปลงอุปกรณ์ในโครงข่ายหลักไปเป็นการติดตั้งแบบซอฟต์แวร์กำหนดเครือข่าย (Software Defined Network: SDN) ซึ่งทำให้การอัปเดตซอฟต์แวร์ทำได้ง่ายขึ้นและเป็นศูนย์รวม ทำให้แน่ใจว่าอุปกรณ์โครงข่ายจะได้รับการอัปเดตซอฟต์แวร์รุ่นแก้ไข (software patch) เพื่อป้องกันไวรัสและมัลแวร์ สำหรับความยืดหยุ่นและความสามารถในการควบคุมแบบเป็นศูนย์รวมของ SDN ทำให้ผู้ดูแลระบบตรวจสอบการโจมตีระบบได้เร็วขึ้น สอดคล้องกับงานศึกษาของ Liyanage et al. (2017) และยังมีแนวโน้มที่จะมีการนำเอาปัญญาประดิษฐ์มาใช้ในการตรวจสอบรูปแบบของข้อมูลที่เก็บได้จากตัวจัดการข้อมูลความปลอดภัยและเหตุการณ์ด้านความปลอดภัย (Security Information and Event Management: SIEM) ทำให้การวิเคราะห์ปัญหาที่เกิดจากความปลอดภัยทำได้ดีกว่าโครงข่ายโทรศัพท์เคลื่อนที่ยุคก่อน ๆ (Broth, 2023; Liyanage et al., 2017) จึงสรุปได้ว่า โครงข่ายยุคที่ 5 มีความปลอดภัยมากขึ้นจากการแบ่งทรัพยากรย่อยในแต่ละอุปกรณ์ ทำให้แยกวิกฤตการรั่วไหลของข้อมูลในระดับย่อยได้ เจาะระบบได้ยากขึ้น การดูแลเป็นศูนย์รวมและอัปเดตซอฟต์แวร์ง่ายขึ้น ทำให้ตรวจสอบการโจมตีได้เร็วขึ้น แต่เมื่อฟังก์ชันใด ๆ ถูกโจมตี ฟังก์ชันอื่น ๆ จะเสี่ยงไปด้วย และมีความเสี่ยงที่โดนโจมตี IoT ได้มาก อีกทั้งหากตั้งค่าอุปกรณ์ผิด ทุกทรัพยากรย่อยจะมีความเสี่ยงไปด้วย

7. ข้อสรุป

สถาปัตยกรรมโครงข่ายยุคที่ 5 รวมเอาอุปกรณ์ในโครงข่ายหลักยุคก่อนไว้ที่อุปกรณ์เดียวกัน โดยแยกฟังก์ชันภายในออกจากกันด้วยการจำลองเสมือน อุปกรณ์ที่มีความสำคัญต่อระบบความปลอดภัยประกอบไปด้วยฟังก์ชันที่มีอยู่ในโครงข่ายยุคก่อน เช่น AUSF ซึ่งเก็บรหัสความปลอดภัย UDM ที่เก็บโพรไฟล์ของลูกค้า และ PCF ที่เก็บนโยบายการคิดค่าบริการ และฟังก์ชันที่เพิ่มเติมขึ้นมา เช่น SCP และ SEPP ซึ่งทำหน้าที่เป็นตัวรวมแทรฟฟิกแบบ signaling และบังคับใช้นโยบายทางด้านความปลอดภัย โดย SCP จัดการฟังก์ชันภายในผู้ให้บริการรายเดียวกัน ในขณะที่ SEPP จัดการแทรฟฟิกโรมมิง โดยมีความเสี่ยงต่อการโจมตีระบบแบบต่าง ๆ พร้อมแนวทางและวิธีป้องกันดังนี้

1) การส่งข้อความปลอมเป็นคนอื่น ป้องกันโดยให้ผู้บริการเข้มงวดในการตรวจสอบและยืนยันชื่อผู้ส่งและข้อความไม่ควรมีลิงก์ภายในซึ่งสามารถอำนวยความสะดวกในการทำความผิด

2) การส่งข้อมูลจำนวนมาก ทำให้ใช้งานระบบไม่ได้ ป้องกันโดยการติดตั้งไฟร์วอลล์และระบบป้องกันผู้บุกรุก

3) การรั่วไหลของข้อมูล ป้องกันโดยระบบกำหนดให้ใช้คำยากตั้งค่ารหัสผ่านและต้องขอเข้าใช้งานโดยผ่านระบบแบบหลายแฟกเตอร์ อีกทั้งใช้โพรโทคอลที่ปลอดภัย และทำแผนตอบสนองหากข้อมูลรั่วไหล

4) โจมตีด้านข้าง ป้องกันโดยการตั้งค่าตัวแปรและส่งแทรฟฟิกแบบรวม เพื่อให้ยากต่อการคาดเดา

5) การโจมตีแบบไปอยู่ตรงกลาง ประกอบด้วย แบบปลากระเบนที่ไม่สามารถโจมตีได้ในโครงข่ายยุคที่ 5 ซึ่งมีกระบวนการเข้ารหัสและขอเข้าใช้งานที่เข้มงวดกว่า การเล่นเสียงซ้ำซึ่งมีการออกซอฟต์แวร์รุ่นแก้ไขมาแก้ไขปัญหาแล้ว ผู้ประกอบการควรติดตั้งซอฟต์แวร์ให้เป็นรุ่นล่าสุด ส่วนการปลอมแปลงเซสชัน การพ่นพิษไปที่ DNS และการขโมยเซสชัน ป้องกันด้วยการเข้ารหัสตัวระบุเซสชัน และเปิดใช้ DNSSEC

โดยภาพรวมแล้ว เทคโนโลยียุคที่ 5 เป็นเทคโนโลยีใหม่ที่มีแนวโน้มดี แต่ก็ยังมีความท้าทายด้านความปลอดภัยใหม่ ๆ ที่ผู้ให้บริการจำเป็นต้องจัดการเพื่อรักษาความปลอดภัยของเครือข่าย ผู้ให้บริการควรทำงานร่วมกับผู้ผลิตอุปกรณ์ เพื่อติดตั้งฟีเซอร์หรือโพรโทคอลต่าง ๆ ด้านความปลอดภัยให้แน่ใจว่าระบบนิเวศน์ทั้งหมดมีความปลอดภัย ติดตามข้อมูลล่าสุดเกี่ยวกับภัยคุกคาม ติดตั้งและอัปเดตซอฟต์แวร์ความปลอดภัยทันทีที่พร้อมใช้งาน และทดสอบเครือข่ายเพื่อหาช่องโหว่ด้านความปลอดภัยเป็นประจำ เพื่อตรวจหากิจกรรมที่น่าสงสัยอย่างสม่ำเสมอ

8. ข้อเสนอแนะ

8.1 ข้อเสนอแนะสำหรับการศึกษาในอนาคต

ศึกษาพัฒนาวิธีที่จะทำให้ฟังก์ชันอื่น ๆ ในโครงข่ายหลักปลอดภัย ถึงแม้ว่าฟังก์ชันใดจะถูกโจมตี และพัฒนาซอฟต์แวร์ ฟีเซอร์ ที่ใช้ปัญญาประดิษฐ์มาช่วยในการตรวจสอบการตั้งค่าทรัพยากรย่อย ๆ ที่ผิดพลาด โดยแนะนำการแก้ไขให้อัตโนมัติ และช่วยในการตรวจสอบการโจมตีได้รวดเร็วขึ้น

8.2 ข้อเสนอแนะเชิงนโยบายสำหรับกิจการสื่อสารดิจิทัล

8.2.1 เสนอให้มีการจัดทำนโยบายการสร้างความมั่นคงปลอดภัยไซเบอร์ (cyber security) ในระบบโครงข่ายโทรศัพท์เคลื่อนที่ยุคที่ 5

8.2.2 เสนอให้หน่วยงานที่เกี่ยวข้องมีมาตรการให้ผู้ให้บริการโทรศัพท์เคลื่อนที่ บริหารจัดการซอฟต์แวร์ในอุปกรณ์ที่ผลิตและจำหน่ายแล้ว เช่น ตรวจสอบความถูกต้องในเชิงของความปลอดภัยสำหรับการติดตั้งค่าอุปกรณ์ในระดับทรัพยากรย่อย หรือการเข้ารหัสแบบ end-to-end ได้โดยอัตโนมัติ การนำปัญญาประดิษฐ์มาใช้ในการตรวจสอบการโจมตีได้รวดเร็วยิ่งขึ้น

รายการเอกสารอ้างอิง

บีบีซี. (2566, 31 มีนาคม). *9near: จับกุม จ่าสิบโท แฮกเกอร์ที่อ้างมีข้อมูลคนไทย 55 ล้านคนได้แล้ว.* BBC Thai. https://www.bbc.com/thai/articles/cq5z3w5lwdxo

สำนักงาน กสทช. (2564, 28 ตุลาคม). *สำนักงาน กสทช. ยกระดับมาตรการจัดการปัญหา SMS หลอกลวง เข้มลงโทษทางปกครองกับผู้ให้บริการเนื้อหาที่ปล่อยให้มี SMS หลวกลวงส่งไปยังประชาชน พร้อมส่งเรื่องให้ บช. สอท. ดำเนินคดีตามกฎหมายกับมิจฉาชีพ ส่วน ก. ดีอีเอส จะดำเนินการเอาผิดกับมิจฉาชีพตาม พ.ร.บ.คอมพิวเตอร์ฯ.* https://www.nbtc.go.th/News/Information/51123.aspx

Angelo Bjerre, S., Wøidemann Klæbel Blomsterberg, M., & Andersen, B. (2023). 5G Attacks and Countermeasures. *Proceedings of 25th International Symposium on Wireless Personal Multimedia Communications. WPMC* (pp. 285-290). Herning: Denmark. IEEE. https://doi.org/10.1109/WPMC55625.2022.10014962

Banach, Z. (2019, August 22). *What Is Session Hijacking: Your Quick Guide to Session Hijacking Attacks.* Invicti. https://www.invicti.com/blog/web-security/session-hijacking/

Broth, J. (2023, April 18). *The Role of Next Gen SIEM in the Era of IoT and 5G.* ITBriefcase. https://www.itbriefcase.net/the-role-of-next-gen-siem-in-the-era-of-IoT-and-5g

CableFree. (n.d.). *LTE Interfaces. Explaining the Interfaces in LTE.* https://www.cablefree.net/wirelesstechnology/4glte/lte-interfaces/

Cloudflare. (n.d.). *What is DNS cache poisoning? | DNS spoofing.* https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

Condoluci, M. & Mahmoodi, T. (2018, December 9). Softwarization and virtualization in 5G mobile networks: Benefits, trends and challenges. *Computer Networks, 146,* 65-84. https://doi.org/10.1016/j.comnet.2018.09.005

Cowley, S. (2019, July 22). Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement. *The New York Times.* https://www.nytimes.com/2019/07/22/business/equifax-settlement.html

Gamaarachchi, H., & Ganegoda, H. (2018, January 3). *Power Analysis Based Side Channel Attack.* [Unpublished manuscript]. arXiv. https://doi.org/10.48550/arXiv.1801.00932

Ghadialy, Z. (2018, February 9). *Tutorial: Service Based Architecture (SBA) for 5G Core (5GC).* The 3G4G Blog. https://blog.3g4g.co.uk/2018/02/tutorial-service-based-architecture-sba.html

Henda, N. B., Wifvesson, M., & Jost, C. (2019, July 17). *An Overview of the 3GPP 5G Security Standard.* Ericsson. https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview

Holmes, D. (n.d.). *What is a Data Breach?.* Fortinet. https://www.fortinet.com/resources/cyberglossary/data-breach

Hossain, M. S., Paul, A., Hasan, H. I., & Atiquzzaman, M. (2018). Survey of the Protection Mechanisms to the SSL-based Session Hijacking Attacks. *Network Protocols and Algorithms, 10*(1), 83. https://doi.org/10.5296/npa.v10i1.12478

Hussain, S. R., Echeverria, M., Chowdhury, O., Li, N., & Bertino, E. (2019, February 24-27). Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. *The 26th Network and Distributed System Security Symposium 2019. NDSS 2019.* San Diego, CA: USA. SyNSec Lab. https://synsec-den.github.io/publications/privacy-attacks-to-the-4g-and-5g-cellular-paging-protocols-using-side-channel-information/

Khandelwal, S. (2020, August 13). *New Attack Lets Hackers Decrypt VoLTE Encryption to Spy on Phone Calls.* The Hacker News. https://thehackernews.com/2020/08/a-team-of-academic-researcherswho.html

Lavaud, C., Gerzaguet, R., Gautier, M., Berder, O., Nogues, E., & Molton, S. (2021). Whispering Devices: A survey on how side-channels lead to compromised information. *Journal of Hardware and Systems Security, 5*(2), 143-168. https://doi.org/10.1007/s41635-021-00112-6

Liyanage, M., Ahmad, I., Okwuibe, J., Ylianttila, M., Kabir, H., Santos, J. L., Kantola, R., Perez, O. L., Itzazelaia, M. U., & Montes De Oca, E. (2017). Enhancing Security of Software Defined Mobile Networks. *IEEE Access, 5,* 9422–9438. https://doi.org/10.1109/ACCESS.2017.2701416

McDaid, C. (2019, August 19). *Understanding and Detecting IMSI catcher around the world.* ENEA. https://www.enea.com/insights/adaptive-mobile-imsi-catchers/

Neto, N. N., Madnick, S. E., Moraes G. de Paula, A., & Malara Borges, N. (2020, January 1). *A Case Study of the Capital One Data Breach* [Unpublished manuscript]. SSRN. http://dx.doi.org/10.2139/ssrn.3542567

Powell, O. (2022, November 29). *Meta fined US$275 million following enquiry into April 2021 data leak.* Cyber Security Hub. https://www.cshub.com/data/news/meta-fined-us275-million-following-enquiry-into-april-2021-data-leak

Reichert, C. (2023, May 1). *T-Mobile Announces Another Data Breach.* CNET. https://www.cnet.com/tech/mobile/t-mobile-announces-another-data-breach/

Singla, A., Hussain, S. R., Chowdhury, O., Bertino, E., & Li, N. (2020). Protecting the 4G and 5G Cellular Paging Protocols against Security and Privacy Attacks. *Proceedings on Privacy Enhancing Technologies, 2020*(1), 126-142. https://doi.org/10.2478/popets-2020-0008

Stempel, J. (2019, April 10). *Yahoo strikes $117.5 million data breach settlement after earlier accord rejected.* Reuters. https://www.reuters.com/article/idUSKCN1RL1GX/#:~:text=Yahoo%20strikes%20%24117.5%20million%20data%20breach%20settlement%20after%20earlier%20accord%20rejected,-By%20Jonathan%20Stempel&text=(Reuters)%20%2D%20Yahoo%20has%20struck,largest%20data%20breach%20in%20history

Vicente, V. (2023, May 16). *7 Types of Information Security Incidents and How to Respond.* AuditBoard. https://www.auditboard.com/blog/types-of-information-security-incidents/

VMWare. (n.d.). *What is Intrusion Prevention System?.* https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html#:~:text=An%20intrusion%20prevention%20system%20(IPS,it%2C%20when%20it%20does%20occur

Vreman, N., Pates, R., Krüger, K., Fohler, G., & Maggio, M. (2019). Minimizing Side-Channel Attack Vulnerability via Schedule Randomization. *2019 IEEE 58th Conference on Decision and Control (CDC)* (pp. 2928-2933). Nice: France. IEEE https://doi.org/10.1109/CDC40024.2019.9030144.

Zialcita, P. (2019, October 30). *Facebook Pays $643,000 Fine For Role In Cambridge Analytica Scandal.* npr. https://www.npr.org/2019/10/30/774749376/facebook-pays-643-000-fine-for-role-in-cambridge-analytica-scandal