ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard for Electronic Transactions

ขมธอ. XX -XXXX

ว่าด้วยการทดสอบการตรวจจับการโจมตีหลอกระบบชีวมิติ

PRESENTATION ATTACK DETECTION TESTING

เวอร์ชัน 0.2

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ICS 35.240.15

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทดสอบการตรวจจับการโจมตีหลอกระบบชีวมิติ

ขมธอ. XX -XXXX

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ พ.ศ. XXXX

คณะทำงานจัดทำมาตรฐานเกี่ยวกับการพิสูจน์และยืนยันตัวตนด้วยเทคโนโลยีชีวมิติ

ที่ปรึกษาคณะทำงาน

ศาสตราจารย์ ดร.วุฒิพงศ์ อารีกุล	มหาวิทยาลัยเกษตรศาสตร์

ประธานคณะทำงาน

นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คณะทำงาน

นางสมศรี หอกันยา	สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	สำนักงานปลัดกระทรวงมหาดไทย
นายสัญชัย เตชนิมิตวัช	กรมการปกครอง
นายณัฏฐา พาชัยยุทธ	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นางสาวอาจารีย์ ศุภพิโรจน์	ธนาคารแห่งประเทศไทย
นายสมเกียรติ วัฒนาประสบสุข	สำนักงานคณะกรรมการกำกับและส่งเสริม การประกอบธุรกิจประกันภัย
นายวิบูลย์ ภัทรพิบูล	สำนักงานคณะกรรมการกำกับหลักทรัพย์ และตลาดหลักทรัพย์
นายศุภกาญจน์ บุญจันทร์	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ศาสตราจารย์ ดร.วิเชียร เปรมชัยสวัสดิ์	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายสืบศักดิ์ สืบภักดี	สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์
นายยศ กิมสวัสดิ์	สมาคมธนาคารไทย
นายณัฐพล โลหชิตพิทักษ์	สมาคมบริษัทหลักทรัพย์ไทย
นายทำนุ อมาตยกุล	สมาคมประกันชีวิตไทย
นางสาวปิยกานต์ ญาณอุดม	สมาคมประกันวินาศภัยไทย

เลขานุการ

นายสมบัติ ชั้นอินทร์งาม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ช่วยเลขานุการ

นายธวัชชัย พริ้งพร้อม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

วิเคราะห์และจัดทำข้อเสนอแนะมาตรฐานฯ
ว่าด้วยการทดสอบสมรรถนะการทำงานเทคโนโลยีชีวมิติ

ดร. อรุชา รุ่งโชคอนันต์	มหาวิทยาลัยเกษตรศาสตร์
ดร. กิตติพล โหราพงศ์	มหาวิทยาลัยเกษตรศาสตร์
นางสาวพลอยนภัส เกิดจิรโรจน์	มหาวิทยาลัยเกษตรศาสตร์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทดสอบการตรวจจับการโจมตีหลอกระบบชีวมิติ ฉบับนี้ จัดทำขึ้นเพื่อเป็นข้อกำหนดและข้อเสนอแนะสำหรับการทดสอบสมรรถนะการทำงานของเทคโนโลยีชีวมิติในการทดสอบสมรรถนะการป้องกันการโจมตีหลอกระบบ เพื่อให้การใช้งานเทคโนโลยีชีวมิติมีความถูกต้องน่าเชื่อถือในระดับสากล มีความมั่นคงปลอดภัย มีธรรมาภิบาล และเกิดประสิทธิภาพสูงสุด

ข้อเสนอแนะมาตรฐานนี้เหมาะกับหน่วยงานภาครัฐหรือภาคเอกชนที่ทำหน้าที่ตรวจสอบสมรรถนะของอัลกอริทึม หรือ ระบบรู้จำชีวมิติ โดยครอบคลุมข้อกำหนดและข้อเสนอแนะสำหรับการทดสอบระดับต่าง ๆ เพื่อให้สอดคล้องกับการนำอัลกอริทึมหรือระบบรู้จำชีวมิติไปประยุกต์ใช้งานทางด้านการบริหารจัดการอัตลักษณ์บุคคล ที่ต้องการใช้เทคโนโลยีชีวมิติในงานภาคบริการประชาชน

โดยมีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทดสอบสมรรถนะการทำงานเทคโนโลยีชีวมิติฉบับนี้ จัดทำขึ้นโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200
E-mail: estandard.center@etda.or.th
Website: www.etda.or.th

คำนำ

การให้บริการประชาชนของภาครัฐหรือภาคเอกชน อาจประกอบด้วยขั้นตอนการพิสูจน์และยืนยันตัวตนที่มีความสำคัญเป็นอย่างยิ่ง รัฐบาลได้ดำเนินงานพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ที่สอดคล้องกับนโยบายอำนวยความสะดวกในการประกอบธุรกิจ และการให้บริการกับประชาชน เพื่อให้เป็นโครงสร้างพื้นฐานทางดิจิทัลที่สำคัญของประเทศ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ได้ร่วมกันกำหนดแนวทางการพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของประเทศ และจัดทำข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์ยืนยันตัวตน ขึ้นประกอบด้วยมาตรฐานทั้งหมดห้าฉบับ คือ ขมธอ. 29 เล่ม 1-2565 [1] ขมธอ. 29 เล่ม 2-2565 [2] ขมธอ. 29 เล่ม 3-2565 [3] ขมธอ. 29 เล่ม 4-2565 [4] และ ขมธอ. 30-2565 [5] โดยมาตรฐานทั้งสี่ฉบับแรกดังกล่าวได้ครอบคลุมการใช้ชีวมิติสำหรับสำหรับการพิสูจน์และยืนยันตัวตนในภาพรวม รวมทั้งการใช้งานชีวมิติสำคัญคือ ใบหน้า ลายนิ้วมือ และลายม่านตา ส่วนเล่มสุดท้าย มาตรฐาน ขมธอ. 30-2565 [5] นั้นเกี่ยวข้องกับการทดสอบสมรรถนะการทำงานของเทคโนโลยีชีวมิติโดยเฉพาะ ซึ่งรวมการทดสอบสมรรถนะการป้องกันการโจมตีหลอกระบบชีวมิติไว้ด้วย

สำหรับข้อเสนอแนะมาตรฐานฉบับนี้ มีจุดมุ่งหมายในการแยกการทดสอบสมรรถนะการป้องกันการโจมตีหลอกระบบชีวมิติ ออกจากการทดสอบสมรรถนะการทำงานของเทคโนโลยีชีวมิติในส่วนของมาตรฐาน ขมธอ. 30-2565 [5] เนื่องจากเป็นคนละส่วนกัน ทำให้ส่วนมาตรฐาน ขมธอ. 30 เล่ม 1 จะเกี่ยวข้องกับการทดสอบสมรรถนะการทำงานของเทคโนโลยีชีวมิติเท่านั้น และมาตรฐานที่แยกเล่มมานี้ จะเรียกว่า ขมธอ. 30 เล่ม 2 ซึ่งจะเกี่ยวข้องกับการทดสอบสมรรถนะการป้องกันการโจมตีหลอกระบบชีวมิติ เพื่อให้มีความถูกต้องน่าเชื่อถือในระดับสากล มีความมั่นคงปลอดภัย และมีธรรมาภิบาล ทั้งนี้การประยุกต์ใช้ข้อเสนอแนะมาตรฐานนี้ จะเป็นไปในภาพรวมเพื่อตรวจสอบสมรรถนะการทำงานของการป้องกันการโจมตีหลอกระบบชีวมิติ โดยในกรณีที่มีหน่วยงานกำกับดูแลเฉพาะของแต่ละภาคส่วนกำหนดมาตรฐานการตรวจสอบสมรรถนะการทำงานของการป้องกันการโจมตีหลอกระบบชีวมิติเป็นการเฉพาะแล้ว ให้ปฏิบัติตามมาตรฐานของหน่วยงานที่กำกับดูแลเหล่านั้น

สารบัญ

สารบัญรูป

หน้า

สารบัญตาราง

หน้า

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทดสอบสมรรถนะการทำงานเทคโนโลยีชีวมิติ

โดยที่เป็นการสมควรกำหนดแนวทางในการทดสอบสมรรถนะการป้องกันการโจมตีหลอกระบบ เพื่อให้การใช้งานเทคโนโลยีชีวมิติมีความถูกต้องน่าเชื่อถือในระดับสากล มีความมั่นคงปลอดภัย มีธรรมาภิบาล และเกิดประสิทธิภาพสูงสุด

อาศัยอำนาจตามความในมาตรา ๕ แห่งพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทดสอบสมรรถนะการทำงานเทคโนโลยีชีวมิติ เลขที่ ขมธอ. ๓๐ เล่ม ๒-๒๕๖๖ ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ตุลาคม พ.ศ. ๒๕๖๖

(นายชัยชนะ มิตรพันธ์)
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยการทดสอบการตรวจจับการโจมตีหลอกระบบชีวมิติ

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานการทดสอบการตรวจจับการโจมตีหลอกระบบฉบับนี้ เป็นข้อเสนอแนะสำหรับหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชนในประเทศไทย ที่ต้องการเป็นผู้ทดสอบสมรรถนะของระบบรู้จำชีวมิติเพื่อนำไปประยุกต์ใช้กับการพิสูจน์และยืนยันตัวตนสำหรับการให้บริการประชาชนในประเทศไทย ข้อเสนอแนะมาตรฐานฉบับนี้ครอบคลุมการทดสอบสมรรถนะการป้องกันการโจมตีหลอกระบบด้วยชีวมิติปลอม ทำให้การประยุกต์ใช้งานเทคโนโลยีชีวมิติมีความถูกต้องน่าเชื่อถือในระดับสากล มีความมั่นคงปลอดภัย และมีธรรมาภิบาล

ทั้งนี้การประยุกต์ใช้ข้อเสนอแนะมาตรฐานนี้ จะเป็นไปในภาพรวมเพื่อตรวจสอบสมรรถนะการทำงานของการป้องกันการโจมตีหลอกระบบ โดยในกรณีที่มีหน่วยงานกำกับดูแลเฉพาะของแต่ละภาคส่วนกำหนดมาตรฐานการตรวจสอบสมรรถนะการทำงานของการป้องกันการโจมตีหลอกระบบเป็นการเฉพาะแล้ว ให้ปฏิบัติตามมาตรฐานของหน่วยงานที่กำกับดูแลเหล่านั้น

ข้อเสนอแนะมาตรฐานฉบับนี้ อ้างอิงข้อกำหนดเกี่ยวกับการทดสอบตามมาตรฐานสากล คือ ISO/IEC 30107-1:2023 [7] และ ISO/IEC 30107-3:2023 [8] เป็นหลัก และนำข้อกำหนดดังกล่าวมาประยุกต์เป็นแนวทางการทดสอบของประเทศไทยที่สอดคล้องกับมาตรฐานสากล

ในข้อเสนอแนะมาตรฐานฉบับนี้ จะใช้รูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐานและเนื้อหาเชิงให้ข้อมูล ดังต่อไปนี้

- “ต้อง” ใช้ระบุสิ่งที่เป็นข้อกำหนด ซึ่งต้องปฏิบัติตาม
- “ควร” ใช้ระบุสิ่งที่เป็นข้อแนะนำ
- “อาจ” ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 ผู้ปลอมชีวมิติ (biometric imposter) หมายถึง บุคคลผู้ปลอมชีวมิติโดยใช้เครื่องมือโจมตีหลอกเพื่อลวงให้ระบบชีวมิติยอมรับว่าเป็นผู้ลงทะเบียนในระบบ

2.2 ผู้ปกปิดชีวมิติ (biometric concealer) หมายถึง บุคคลผู้ปกปิดชีวมิติโดยใช้เครื่องมือโจมตีหลอกเพื่อลวงให้ระบบชีวมิติไม่ยอมรับว่าเป็นผู้ลงทะเบียนในระบบ

2.3 การโจมตีหลอก (presentation attack) เป็นการแสดงให้กับระบบย่อยเก็บข้อมูลชีวมิติ โดยมีเป้าหมายที่จะหลอกลวงระบบชีวมิติ หรือบุคคลนำเสนอลักษณะเฉพาะชีวมิติปลอมเพื่อหลอกระบบรู้จำชีวมิติอัตโนมัติ

2.4 สิ่งทำหลอก (artifact) หมายถึง สิ่งประดิษฐ์ที่สร้างขึ้นเพื่อเลียนแบบคุณสมบัติของชีวมิติเพื่อใช้ในการหลอกระบบรู้จำชีวมิติ

2.5 เครื่องมือโจมตีหลอก (presentation attack instrument: PAI) หมายถึง สิ่งประดิษฐ์หรืออุปกรณ์ใช้ปลอมแปลงเพื่อแอบอ้างเป็นเจ้าของลักษณะเฉพาะชีวมิติ หรือปลอมแปลงเพื่อหลบหลีกการตรวจสอบลักษณะเฉพาะชีวมิติ

2.6 การตรวจจับการโจมตีหลอก (presentation attack detection: PAD) หมายถึง กระบวนการที่ใช้ตรวจสอบการปลอมแปลงลักษณะเฉพาะชีวมิติของบุคคลที่เข้ามาใช้งานระบบ

2.7 การแสดงแท้จริง (bona fide presentation) การโต้ตอบระหว่างบุคคลตัวจริงผู้ทดสอบระบบ กับระบบย่อยเก็บข้อมูลชีวมิติซึ่งเป็นไปตามนโยบายของระบบชีวมิติ

2.8 รูปแบบการโจมตี (attack type) ส่วนประกอบหรือลักษณะเฉพาะของการโจมตีหลอก รวมถึงเครื่องมือโจมตีหลอกระบบต่างๆ การโจมตีแบบปลอมชีวมิติหรือแบบปกปิดชีวมิติ ระดับของการควบคุม และวิธีต่างๆ ในการตอบโต้กับอุปกรณ์เก็บข้อมูลชีวมิติ

2.9 การมีชีวิต (liveness) หมายถึง สถานะของการมีชีวิต โดยหลักฐานชัดแจ้งคือ ลักษณะเฉพาะทางกายวิภาค การตอบสนองที่ไม่ได้บังคับหรืออัตโนมัติ หน้าที่ของสรีรวิทยา การตอบสนองตามความสมัครใจ พฤติกรรมของบุคคล หรือ หลายส่วนผสมกัน

2.10 การตรวจจับการมีชีวิต (liveness detection) หมายถึง การวัดหรือการวิเคราะห์ลักษณะเฉพาะทางกายวิภาค หรือ การตอบสนองที่ไม่ได้บังคับหรือการตอบสนองตามความสมัครใจ เพื่อที่จะตัดสินว่าข้อมูลชีวมิติที่ได้มาจากบุคคลที่มีชีวิตหรือไม่

2.11 แนวเข้าสู่การทดสอบ (test approach) ทั้งหมดของการพิจารณาและตัวแปรที่เกี่ยวข้องกับการประเมินผลการตรวจจับการโจมตีหลอก

2.12 รายการสำหรับการทดสอบ (item under test: IUT) การสร้างวัตถุเพื่อใช้ในการทดสอบ หรือ กรณีทดสอบ

2.13 เครื่องมือโจมตีหลอกหลากชนิด (presentation attack instrument species: PAIS) ประเภทของเครื่องมือโจมตีหลอก ที่สร้างขึ้นโดยใช้วิธีการปกติ โดยมีพื้นฐานจากลักษณะเฉพาะชีวมิติแบบต่างๆ

2.14 อนุกรมเครื่องมือโจมตีหลอก (presentation attack instrument series: PAIs) ประเภทของเครื่องมือโจมตีหลอก ที่สร้างขึ้นโดยใช้วิธีการปกติ โดยมีพื้นฐานจากลักษณะเฉพาะชีวมิติแบบเดียวกัน

2.15 เป้าหมายของการประเมินผล (target of evaluation: TOE) ผลิตภัณฑ์ไอทีที่จะถูกทดสอบประเมินผลภายใต้บริบทของเกณฑ์ที่กำหนดร่วมกัน

2.16 ศักยภาพในการโจมตี (attack potential) เป็นการวัดขีดความสามารถในการโจมตีเป้าหมายของการประเมินผล (TOE) โดยให้ความเชี่ยวชาญความรู้ของผู้โจมตี ทรัพยากร และ แรงจูงใจ

2.17 ผู้ประเมินผล (evaluator) หมายถึง

3. อักษรย่อ

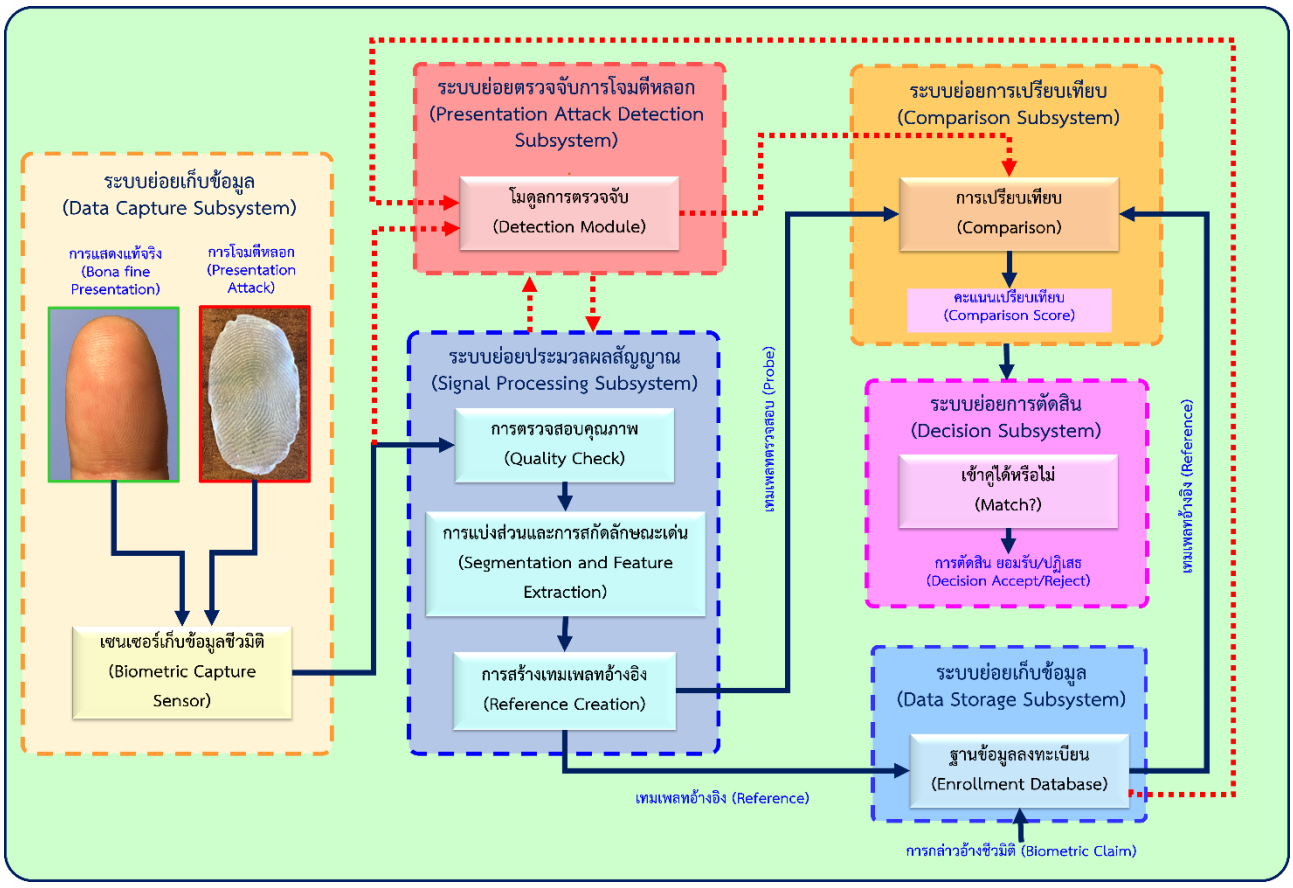
อักษรย่อที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

อักษรย่อ	คำเต็ม	คำภาษาไทย
APAR	Attack Presentation Acquisition Rate	อัตราการเก็บข้อมูลตัวอย่างชีวมิติจากการโจมตีหลอก
APCER	Attack Presentation Classification Error Rate	อัตราความผิดพลาดการจำแนกการโจมตีหลอก
$APCER_{AP}$	Attack Presentation Classification Error Rate at the Given Attack Potential	อัตราความผิดพลาดการจำแนกการโจมตีหลอกที่ระดับการโจมตีที่กำหนด
APNRR	Attack Presentation Non-Response Rate	อัตราการไม่ตอบสนองต่อการโจมตีหลอก
BPCER	Bona fide Classification Error Rate	อัตราความผิดพลาดการจำแนกชีวมิติจริงแท้
BPNRR	Bona Fide Presentation Non-Response Rate	อัตราการไม่ตอบสนองต่อชีวมิติจริงแท้
CAPNIR	Concealer Attack Presentation Non-Identification Rate	อัตราการระบุชีวมิติไม่สำเร็จจากการโจมตีหลอกแบบปกปิดตัวตน
CAPRR	Concealer Attack Presentation Reject Rate	อัตราการปฏิเสธจากการโจมตีหลอกแบบปกปิดตัวตน
DCS-PD	Data Capture Subsystem Processing Duration	ระยะเวลาที่ใช้ในการประมวลผลของระบบย่อยเก็บข้อมูลชีวมิติ
FNIR	False Negative Identification Rate	อัตราการระบุผลลบลวง
FPIR	False Positive Identification Rate	อัตราการระบุผลบวกลวง
FS-PD	Full-System Processing Duration	ระยะเวลาที่ใช้ในการประมวลผลแบบเต็มระบบ
FTAR	Failure-to-Acquire Rate	อัตราการเก็บข้อมูลตัวอย่างชีวมิติล้มเหลว
FTER	Failure-to-Enroll Rate	อัตราการลงทะเบียนล้มเหลว
IAPAR	Impostor Attack Presentation Accept Rate	อัตราการยอมรับการโจมตีหลอกแบบปลอมตัวตน
$IAPAR_{AP}$	Impostor Attack Presentation Accept Rate at The Given Attack Potential	อัตราการยอมรับการโจมตีหลอกแบบปลอมตัวตนที่ระดับการโจมตีที่กำหนด
IAPIR	Impostor Attack Presentation Identification Rate	อัตราการระบุการโจมตีหลอกโดยปลอมชีวมิติ
PA	Presentation Attack	การโจมตีหลอก
PAD	Presentation Attack Detection	การตรวจจับการโจมตีหลอก
PAI	Presentation Attack Instrument	เครื่องมือโจมตีหลอก
PAP	Presentation Attack Protection	การป้องกันการโจมตีหลอก
PS-PD	PAD Subsystem Processing Duration	ระยะเวลาที่ใช้ในการประมวลผลของระบบย่อยตรวจจับการโจมตีหลอก

อักษรย่อ	คำเต็ม	คำภาษาไทย
RIAPAR	Relative Impostor Attack Presentation Accept Rate	อัตราการยอมรับการโจมตีหลอกแบบปลอมตัวตนสัมพัทธ์

4. ภาพรวมระบบตรวจจับการโจมตีหลอกในระบบชีวมิติ

การตรวจจับการโจมตีหลอก (PAD) ในระบบรู้จำชีวมิติ จะมีการเพิ่มเติม*ระบบย่อยตรวจจับการโจมตีหลอก* (presentation attack detection subsystem) เข้าไปในระบบ เพื่อทำงานสอดประสานกับระบบโดยมีรูปแบบดังแสดงอยู่ในรูปที่ 1 ตามมาตรฐาน มาตรฐาน ISO/IEC 30107-1:2023 [7]



รูปที่ 1 ภาพรวมระบบชีวมิติที่มีระบบย่อยการตรวจจับการโจมตีหลอก

ระบบรู้จำชีวมิติที่มีระบบย่อยตรวจจับการโจมตีหลอก มีขั้นตอนการทำงานโดยทั่วไปดังต่อไปนี้

(1) *ระบบย่อยเก็บข้อมูล* (data capture subsystem) จะเก็บข้อมูลตัวอย่างชีวมิติ โดยใช้ *เซนเซอร์เก็บชีวมิติ* (biometric capture sensor) จากนั้นจะป้อนเข้า*ระบบย่อยประมวลผลสัญญาณ* (signal processing subsystem) และป้อนเข้า*ระบบย่อยตรวจจับการโจมตีหลอก* (presentation attack detection subsystem)

(2) *ระบบย่อยประมวลผลสัญญาณ* (signal processing subsystem) ทำหน้าที่ตรวจสอบคุณภาพของข้อมูล

ตัวอย่างชีวมิติ (quality check) ถ้าไม่ผ่านจะทำการเก็บใหม่ ถ้าผ่านจะทำ*การแบ่งส่วน* (segmentation) โดยเอาเฉพาะส่วนที่เกี่ยวข้องกับชีวมิติไปทำ*การสกัดลักษณะเด่น* (feature extraction) ของชีวมิตินั้นๆ หลังจากที่ได้ลักษณะเด่น จะทำการสร้างเทมเพลทอ้างอิงแทนข้อมูลตัวอย่างชีวมิติ (reference creation)

- ในกรณีที่เป็นการลงทะเบียน เทมเพลทอ้างอิงจะถูกเก็บไว้ใน*ระบบย่อยฐานข้อมูลลงทะเบียน* (enrollment database)
- ในกรณีที่เป็นการยืนยันตัวตนหรือระบุตัวตน จะส่งเทมเพลทอ้างอิงไป*ระบบย่อยเปรียบเทียบ* (comparison subsystem)

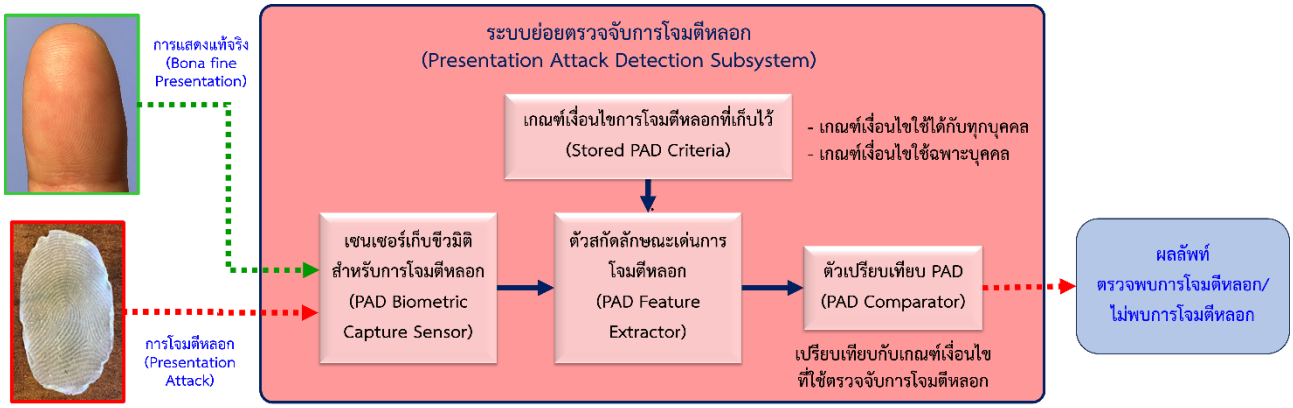
หมายเหตุ: ระบบย่อยประมวลสัญญาณ อาจเชื่อมต่อแลกเปลี่ยนข้อมูลเชิงลึก กับระบบย่อยตรวจจับการโจมตีหลอก โดยลักษณะเด่นของชีวมิติอาจสะท้อนถึงการมีชีวิต หรือการปลอมแปลงชีวมิติได้

(3) *ระบบย่อยเปรียบเทียบ* (comparison subsystem) ทำหน้าที่เปรียบเทียบเทมเพลทอ้างอิงในฐานข้อมูลการลงทะเบียนกับ เทมเพลทอ้างอิงที่ได้จากการสกัดลักษณะเด่นจากข้อมูลตัวอย่างชีวมิติ และมีข้อมูลผลลัพท์จากระบบย่อยตรวจจับการโจมตีหลอกเข้าไปในระบบย่อยเปรียบเทียบนี้ด้วย

- ในกรณีที่เป็นการยืนยันตัวตน ข้อมูลจาก*การกล่าวอ้างชีวมิติ* (biometric claim) จะบ่งชี้ไปที่เทมเพลทอ้างอิงเฉพาะบุคคลในระบบย่อยฐานข้อมูลลงทะเบียน การเปรียบเทียบจะเป็นการเปรียบเทียบระหว่างเทมเพลทจากข้อมูลตัวอย่างชีวมิติและเทมเพลทอ้างอิงเฉพาะที่มีการกล่าวอ้าง
- ในกรณีที่เป็นการระบุตัวตน จะทำการเปรียบเทียบเทมเพลทจากข้อมูลตัวอย่างชีวมิติ กับเทมเพลทอ้างอิงในฐานข้อมูลทั้งหมด

ผลลัพท์ที่ได้จากการเปรียบเทียบจะเป็น*คะแนนเปรียบเทียบ* (comparison score) ซึ่งจะส่งให้*ระบบย่อยการตัดสิน* (decision subsystem)

(4) *ระบบย่อยตัดสิน* (decision subsystem) ทำหน้าที่ตัดสินใจ ไม่ว่าจะเป็นการพิสูจน์ยืนยันตัวตน จะต้องมีเกณฑ์ในการตัดสินว่าจะยอมรับหรือปฏิเสธ หรือ การระบุตัวตน จะต้องมีเกณฑ์ในการตัดสินว่า มีบุคคลนี้ในฐานข้อมูลหรือไม่มี โดยรายละเอียดส่วนนี้ได้อธิบายไว้แล้วใน ขมธอ. 29 เล่ม 1 [1] ผลลัพธ์ที่ได้ไม่ว่าจะเป็นอย่างไร ต้องคำนึงถึงผลลัพท์จากระบบย่อยตรวจจับการโจมตีหลอกเป็นส่วนประกอบในการตัดสินใจ



รูปที่ 2 ภาพรวมระบบย่อยการตรวจจับการโจมตีหลอกในระบบรู้จำชีวมิติ

สำหรับระบบย่อยตรวจจับการโจมตีหลอก มีรูปแบบการทำงานดังแสดงอยู่ในรูปที่ 2 โดยมีขั้นตอนการทำงานโดยทั่วไปดังต่อไปนี้

(1) เก็บข้อมูลตัวอย่างชีวมิติสำหรับระบบตรวจจับการโจมตีหลอก (PAD) จากบุคคล โดยใช้เซนเซอร์เก็บชีวมิติในระบบย่อยเก็บข้อมูลชีวมิติ เซนเซอร์ที่ใช้อาจแตกต่างจากเซนเซอร์ที่ใช้ในการเก็บข้อมูลตัวอย่างชีวมิติ และการเก็บข้อมูลชีวมิติทั้งสองอาจแยกออกจากกัน ระยะเวลาในการเก็บข้อมูลตัวอย่างชีวมิติอาจเพิ่มขึ้นเพื่อให้ได้ข้อมูลเกี่ยวกับการโจมตีหลอก แต่ระยะเวลาที่เพิ่มขึ้นอาจนำไปสู่ความเสี่ยงที่จะถูกโจมตีของระบบชีวมิติได้ง่ายขึ้นและมากขึ้น

(2) *เกณฑ์เงื่อนไขการโจมตีหลอกที่เก็บไว้* (stored PAD criteria) จะเป็นเกณฑ์เงื่อนไขกำหนดเพื่อที่จะตรวจสอบความผิดปกติของลักษณะเด่นของข้อมูลตัวอย่างชีวมิติ โดยเกณฑ์เงื่อนไขจะบ่งชี้ความเป็นไปได้ในการถูกโจมตีหลอก ซึ่งมีได้สองกรณีดังต่อไปนี้

- เกณฑ์เงื่อนไขที่ใช้ได้กับบุคคลทั่วไป
- เกณฑ์เงื่อนไขที่ใช้ได้กับเฉพาะบุคคล

ตัวอย่างเช่น ถ้าใช้การตอบสนองแบบต่างๆ เพื่อตรวจจับการโจมตีหลอก เกณฑ์ที่กำหนดอาจใช้ได้กับทุกบุคคลถ้าเป็นการวัดอย่างหยาบ และใช้ได้กับเฉพาะบุคคลถ้าวัดอย่างละเอียด

(3) *ตัวสกัดลักษณะเด่นการโจมตีหลอก* (PAD feature extractor) เมื่อได้ข้อมูลตัวอย่างชีวมิติ จะป้อนเข้าเพื่อสกัดลักษณะเด่นที่เกี่ยวกับการมีชีวิต ลักษณะความผิดปกติแปลกปลอมที่ไม่ควรมีอยู่ในชีวมิติ หรือการผิดธรรมชาติของชีวมิติ โดยจะใช้เกณฑ์เงื่อนไขการโจมตีหลอกที่เก็บไว้เป็นข้อมูลอ้างอิง

(4) *ตัวเปรียบเทียบการโจมตีหลอก* (PAD comparator) นำลักษณะเด่นที่สกัดได้จากชีวมิติมาพิจารณาเปรียบเทียบกับเกณฑ์เงื่อนไขที่กำหนดในการตรวจจับการโจมตีหลอก ผลลัพธ์ที่ได้จะแสดงผลเป็นตรวจจับได้หรือตรวจจับไม่ได้ หรือเป็นคะแนนความน่าจะเป็นในการถูกโจมตีหลอก ซึ่งคะแนนนี้เป็นผลจากการเปรียบเทียบข้อมูลนี้ หรือรวมกับข้อมูลอื่นๆ จะแจ้งให้ระบบชีวมิติ ยอมรับหรือปฏิเสธ ข้อมูลตัวอย่างชีวมิติ

รูปที่ 1 แสดงตัวอย่างวิธีการใส่ระบบย่อยตรวจจับการโจมตีหลอก หรือระบบย่อย PAD เข้าไปในระบบชีวมิติ แต่การใส่ระบบย่อย PAD มีหลายแบบ คืออาจอยู่ภายในระบบย่อยการประมวลสัญญาณ หรืออยู่หลังระบบย่อยการเปรียบเทียบ หรือระบบย่อยการตัดสิน

มาตรฐาน ISO/IEC 30107-1:2023 [7] ได้เสนอตัวชี้วัดการประเมินสมรรถนะการป้องกันการโจมตีหลอกระบบในหลายรูปแบบ ได้แก่ ความผิดพลาดในการจำแนกระหว่างชีวมิติจริงกับชีวมิติสังเคราะห์ การไม่ตอบสนองต่อเครื่องมือปลอมแปลง เวลาประมวลผลที่ใช้ หรือตัวชี้วัดอื่น ๆ โดยค่าของตัวชี้วัดทั้งหมดเหล่านี้สามารถนำมาประเมินความปลอดภัยและสมรรถนะของระบบหรือผลิตภัณฑ์เมื่อถูกโจมตีด้วย*เครื่องมือโจมตีหลอกหลากชนิด* (presentation attack instrument species: PAIS)

5. ภาพรวมการประเมินผลการตรวจจับการโจมตีหลอกระบบชีวมิติ

ข้อเสนอแนะมาตรฐานการทดสอบการตรวจจับการโจมตีหลอกระบบชีวมิติ จะเน้นการโจมตีหลอกระบบซึ่งเกิดจากบุคคลสองประเภท คือ *ผู้ปลอมชีวมิติ* (biometric imposter) และ*ผู้ปกปิดชีวมิติ* (biometric concealer) ทั้งสองแบบแตกต่างกันที่ ผู้ปลอมชีวมิติต้องพยายามเอาชนะระบบย่อยตรวจจับการโจมตีหลอก โดยผ่านการตรวจสอบคุณภาพชีวมิติ และการเข้าคู่ในระบบย่อยการเปรียบเทียบ ในขณะที่ผู้ปกปิดชีวมิติไม่จำเป็นต้องจับคู่ผ่าน

ระบบย่อยการเปรียบเทียบ เพียงแค่ระบบไม่สามารถระบุตัวได้ก็เพียงพอ

มาตรฐานฉบับนี้มีเป้าหมายเพื่อที่จะประเมินผล *กลไกตรวจจับการโจมตีหลอกระบบ* (PAD mechanisms) หรือเรียกโดยย่อว่า "**กลไก PAD**" การประเมินผลกลไก PAD และรายงานผล ต้องกำหนดรูปแบบการโจมตีว่าเป็นแบบผู้ปลอมชีวมิติ หรือ ผู้ปกปิดชีวมิติ โดยการประเมินผลกลไกการโจมตีหลอกระบบ หรือเรียกโดยย่อว่า กลไก PAD จะถูกแบ่งออกเป็นสามแบบโดยเพิ่มข้อกำหนดดังต่อไปนี้

(1) การประเมินผลกลไก PAD แบบทั่วไป (generic, broad evaluations of PAD mechanisms) การประเมินผลแบบกว้างๆ ของกลไก PAD ของอุปกรณ์ใดๆ โดยไม่ระบุการประยุกต์ใช้

(2) การประเมินผลกลไก PAD แบบการประยุกต์ใช้เฉพาะ (application-focused evaluations of PAD mechanisms) กำหนดรูปแบบการโจมตีและขอบเขตพิสัยที่ถูกเลือกให้เหมาะสมกับการประยุกต์ใช้งานเฉพาะ

(3) การประเมินผลกลไก PAD แบบเฉพาะผลิตภัณฑ์ (product-specific evaluations of PAD mechanisms) ใช้ในการทดสอบผลิตภัณฑ์ตามสมรรถนะที่ผู้ผลิตสินค้ากล่าวอ้างกับรูปแบบการโจมตีที่กำหนด

การประเมินผลกลไกตรวจจับการโจมตีหลอกระบบและรายงานผล ต้องอธิบายรูปแบบกระบวนการประเมินผลและรูปแบบการโจมตีที่ใช้ทดสอบ

6. ระดับของการประเมินผลของกลไกการตรวจจับการโจมตีหลอกระบบชีวมิติ

การประเมินผลกลไกการโจมตีหลอกระบบ ซึ่งต่อไปนี้จะเรียกโดยย่อว่า "**การประเมินผลกลไก PAD**" ซึ่งกำหนดโดย "**รายการสำหรับการทดสอบ**" หรือเรียกโดยย่อว่า **IUT**

การประเมินผลกลไก PAD และรายงานผล ต้องอธิบายรายละเอียดของ IUT โดยมี องค์ประกอบและการกำหนดค่าต่างๆ ข้อมูลทั้งหมดที่ให้ผู้ตรวจเข้าถึงเกี่ยวกับกลไก PAD โดย IUT จะถูกแบ่งประเภทของระดับการประเมินผลดังต่อไปนี้

(1) ระดับระบบย่อยการตรวจจับการโจมตีหลอก (PAD subsystem level) ระบบย่อยการตรวจจับการโจมตีหลอก หรือ เรียกโดยย่อว่า "**ระบบย่อย PAD**" จะเป็นฮาร์ดแวร์และ/หรือ ซอฟต์แวร์ที่ทำให้กลไก PAD ทำงานได้และแสดงผลการตรวจจับการโจมตีหลอก โดยผู้ประเมินผลสามารถเข้าถึงข้อมูลผลลัพท์ของกลไก PAD ได้ และแสดงผลลัพท์ในลักษณะมุมมองของการประเมิน

(2) ระดับระบบย่อยเก็บข้อมูล (data capture subsystem level) ระบบย่อยเก็บข้อมูลประกอบด้วยฮาร์ดแวร์และ/หรือ ซอฟต์แวร์ที่เชื่อมต่อกับกลไก PAD รวมถึงการตรวจสอบคุณภาพ ซึ่งผู้ประเมินผลไม่จำเป็นต้องเห็นรายละเอียดทั้งหมดอย่างชัดเจน ผู้ประเมินผลไม่จำเป็นต้องทราบว่า ระบบย่อยเก็บข้อมูลใช้กลไก PAD หรือไม่ การเก็บข้อมูลมีจุดประสงค์คือการลงทะเบียนหรือการรู้จำชีวมิติ โดยไม่มีการเปรียบเทียบในระบบย่อยเก็บข้อมูล

(3) ระดับระบบเต็ม (full system level) สำหรับการประเมินผลระบบเต็ม ซึ่งจะเพิ่มเติมจากการประเมินผลระบบย่อย PAD หรือ ระบบย่อยเก็บข้อมูล โดยรวมถึงการเปรียบเทียบชีวมิติในส่วนประกอบทั้งหมดจากต้นจนจบ ในกรณีนี้จะเพิ่มความล้มเหลวในการโจมตีหลอกของ PAI ภายใต้กลไก PAD และ

การตรวจสอบคุณภาพ โดยในระบบเต็มจะมีหนึ่งกลไก PAD หรือมากกว่าในตำแหน่งต่างๆ ของระบบเต็ม

การตรวจสอบคุณภาพในหัวข้อ (2) และ (3) นี้ รวมถึงการตรวจสอบคุณภาพชีวมิติใน การดึงลักษณะเด่นชีวมิติ การแบ่งแยกชีวมิติออกจากพื้นหลัง หรือกระบวนการอัตโนมัติใดๆ ที่เป็นประโยชน์ทำให้ข้อมูลชีวมิติสมบูรณ์

การประเมินผลกลไก PAD และรายงานผล ต้องกำหนดระดับการประเมินผลที่สามารถประยุกต์ได้ตามที่ได้กล่าวข้างต้น คือ ระดับระบบย่อย PAD ระดับระบบย่อยเก็บข้อมูล หรือ ระดับระบบเต็ม ในรายงานผลลัพท์การประเมิน ควรจะอธิบาย ระดับการประเมินที่มีผลอย่างไรต่อการทดสอบ PAD

6.1 หลักปฏิบัติในการประเมินผลกลไก PAD

การประเมินผลกลไก PAD ต้องครอบคลุมรูปแบบการโจมตีหลอก โดยใช้กลุ่มตัวแทนจาก เครื่องมือโจมตีหลอก หรือเรียกโดยย่อว่า “**PAI**” และกลุ่มตัวแทนจาก*บุคคลทดสอบแท้จริง* (bona fide test subjects) สำหรับการทดสอบ

สำหรับกลุ่มตัวแทนจาก PAI การประเมินผลกลไก PAD ควรมีพื้นฐานจากระดับการประเมินที่เหมาะสมและรูปแบบการโจมตีหลอกที่เกี่ยวข้องกัน ทั้งนี้กลไก PAD อาจไม่ได้ถูกออกแบบมาเพื่อรองรับการโจมตีทุกรูปแบบ ตัวอย่างเช่น กลไก PAD ที่ออกแบบมาเพื่อรู้จำลักษณะเฉพาะชีวมิติสังเคราะห์หรือสิ่งทำหลอก (artifacts) จะไม่สามารถตรวจจับการเปลี่ยนแปลงลักษณะเฉพาะชีวมิติได้

หลังจากรูปแบบถูกกำหนด ควรกำหนดจำนวนและขอบเขตของ PAI ที่จะถูกประเมินให้ชัดเจน โดยเน้นการสร้างรูปแบบการโจมตีเฉพาะให้สำเร็จและสามารถทำซ้ำได้ โดยใช้จำนวนทดสอบที่ไม่จำเป็นต้องมากเกินไป

ผู้ประเมินผลต้องกำหนดตัวแปรของการโจมตีหลอก ที่แสดงลักษณะสมบูรณ์ตามขอบเขตของปฏิกิริยาตอบโต้ระหว่างผู้แสดง PAI กับ IUT ซึ่งรวมทั้งกรอบเวลาของการโจมตีหลอก

กลุ่มตัวแทนจากบุคคลทดสอบแท้จริง จำเป็นต้องใช้ในการหาความถี่ที่กลไก PAD ทำงานผิดพลาดโดยตรวจจับบุคคลทดสอบแท้จริงกลายเป็นผู้โจมตีหลอกระบบ ซึ่งเป็นส่วนสำคัญของการทดสอบ PAD อัตราความความผิดพลาดที่สูงของการตรวจจับผิด จะทำให้ลดความน่าเชื่อถือในการนำมาใช้ประโยชน์ของระบบที่ถูกทดสอบ

ตัวแทนการแสดงแท้จริง ควรพิจารณาเลือกบุคคลมาทดสอบและจำนวนบุคคลที่ใช้สำหรับกลุ่มบุคคลแท้จริง ควรใช้วิธีใน ISO/IEC 19795-1 โดยเฉพาะจำนวนบุคคลแท้จริง ควรเกินจำนวนตามกฎเลข 30 ตาม ขมธอ. 30 เล่ม 1-2566

ในการประเมินกลไก PAD ผู้ประเมินผลต้องกำหนด*การแสดงแท้จริง* (bona fide presentation) และบุคคลตัวแทนทดสอบตามเป้าหมายประชากรที่จะประยุกต์ใช้งาน ผู้ประเมินผลต้องให้พื้นฐานของเหตุผลสำหรับข้อกำหนดเหล่านี้

การกำหนดการแสดงแท้จริงและ*บุคคลทดสอบแทน* (representative test subject) เป็นงานที่ท้าทายในการประเมินผลกลไก PAD ในบางกรณีผู้ประเมินสามารถกำหนดการแสดงแท้จริงและบุคคลทดสอบแทน ที่อยู่ในกรอบที่ผู้ผลิตกำหนดได้ แต่ในบางกรณีที่มีการประยุกต์ใช้งานบางอย่าง การแสดงแท้จริงและบุคคลทดสอบแทนที่กระทำต่ออุปกรณ์เก็บข้อมูล อาจมีพฤติกรรมหรือเงื่อนไขที่ทำให้กว้างไปกว่ากรอบที่ผู้ผลิตกำหนด เช่น บริษัทต้องการให้ผู้ใช้ลายนิ้วมือทดสอบต้องมีนิ้วที่สะอาด แต่ในทางปฏิบัติการทดสอบจริง อาจมี

บุคคลที่นิ้วไม่สะอาดปะปนมา ทำให้ค่าปฏิเสธผิดพลาดสูง หรือ อัตราการไม่สามารถลงทะเบียนได้สูง ซึ่งจะเกี่ยวพันโดยตรงกับ การทดสอบ PAD เนื่องจากความผิดพลาดในการจำแนกการแสดงแท้จริง จะพบได้บ่อยกว่าเมื่อบุคคลทดสอบมีการปฏิสัมพันธ์กับอุปกรณ์เก็บข้อมูลชีวมิติในลักษณะที่นิ้วสกปรก ในขณะที่การลงทะเบียนที่เหมาะสมตามที่บริษัทผู้ผลิตกำหนดต้องการนิ้วมือที่สะอาดนั้น สอดคล้องกับข้อกำหนดบริษัทเพียงเล็กน้อยและไม่ให้ความสำคัญ

6.2 การประเมินผลระบบย่อย PAD

การประเมินผลระบบย่อย PAD เป็นการวัดความสามารถของระบบย่อย PAD ที่สามารถตรวจจับโดยจำแนกทั้งการโจมตีหลอกและการแสดงแท้จริงออกจากกันได้อย่างถูกต้อง การโจมตีหลอกที่ได้ผลจะทำให้ระบบย่อยจำแนกผิดเป็นการแสดงแท้จริง

การประเมินผลระบบย่อย PAD สามารถมุ่งเน้นในประสิทธิผลในอุปกรณ์เก็บชีวมิติ ซึ่งโดยทั่วไปเป็นฮาร์ดแวร์ หรือ เฟิร์มแวร์ภายใน โดยประเมินในรูปแบบการปฏิเสธการเก็บตัวอย่างชีวมิติ รวมทั้งในกรณีที่มีหรือ ไม่มีสัญญาณบ่งชี้ปฏิเสธอัตโนมัติ การประเมินผลจะมุ่งเน้นไปที่การปฏิเสธ PAI ต่างๆ ที่ใช้ โดยผลลัพท์ที่ได้จากระบบย่อย PAD อาจเป็น ผ่าน/ไม่ผ่าน สำหรับแต่ละ PAI ที่ใช้ทดสอบ

อีกทางเลือกหนึ่งของการประเมินผลระบบย่อย PAD จะมุ่งเน้นไปที่ประสิทธิผลของอัลกอริทึม PAD โดยการประเมินผลระบบย่อย PAD ลักษณะนี้สามารถทำกับฐานข้อมูลในภายหลังการเก็บข้อมูลได้โดยไม่ต้องกระทำต่อหน้าบุคคลทดสอบ โดยระบบย่อย PAD จะตัดสินว่าตัวอย่างชีวมิติมาจากการโจมตีหลอกหรือไม่ โดยทั่วไปการทดสอบจะใช้ฐานข้อมูลที่เก็บมาล่วงหน้า ซึ่งคล้ายคลึงกับการประเมินผลสมรรถนะระบบชีวมิติ

ถ้าระบบย่อย PAD ตอบกลับเป็น คะแนน PAD อัตราความผิดพลาดผลลบลวง และ อัตราความผิดพลาดผลบวกลวง สามารถแสดงในรูปแบบฟังก์ชันของค่าเทรชโฮลด์สำหรับตัดสินใจ เช่น เส้นโค้ง DET

6.3 การประเมินผลระบบย่อยเก็บข้อมูล

ในระบบย่อยเก็บข้อมูล การโจมตีหลอกอาจล้มเหลวด้วยหลายสาเหตุที่ไม่ใช่เกิดจากการตรวจพบในระบบย่อย PAD ตัวอย่างเช่น ระบบย่อยเก็บข้อมูลไม่ตอบสนองต่อการโจมตีหลอก หรือการโจมตีหลอกไม่ผ่านระบบย่อยคุณภาพ

ในระบบย่อยเก็บข้อมูลที่ไม่มีกลไก PAD หรือ ผู้ประเมินผลไม่สามารถเข้าถึงผลลัพท์ของกลไก PAD ได้ สิ่งที่พอจะทำได้คือ ดูผลว่าระบบย่อยเก็บข้อมูลสามารถเก็บข้อมูลตัวอย่างได้หรือไม่ การโจมตีหลอกที่มีประสิทธิผลจะเอาชนะทั้งระบบย่อย PAD (ถ้ามีและทำงานอยู่) และระบบย่อยคุณภาพ และสามารถเก็บข้อมูลชีวมิติได้

6.4 การประเมินผลระบบเต็ม

การประเมินผลระบบเต็ม เป็นการเพิ่มส่วนระบบย่อยเปรียบเทียบเข้าไปกับ IUT โดยการให้คะแนนเปรียบเทียบ หรือ รายการบุคคล ดังแสดงในรูปที่ 1

การประเมินระบบเต็ม ขึ้นอยู่กับแนวทางการทำให้เกิดผล ซึ่งจะครอบคลุมกรณีต่างๆ ดังต่อไปนี้

(1) ระบบย่อย PAD ระบบย่อยเก็บข้อมูล และระบบย่อยเปรียบเทียบ (PAD subsystem, data capture subsystem and comparison subsystem) (สำหรับ IUT ที่ผลลัพท์ของกลไก PAD ถูกเข้าถึงได้โดยผู้ประเมินผล) ในการประเมินผลแบบนี้ การทดสอบจะเป็นไปตามแผนการทดสอบที่รู้ตัวผู้โจมตีที่อยู่ในกลุ่มบุคคลทดสอบ การโจมตีหลอกจะพยายามที่จะล้มล้างระบบย่อย PAD ระบบย่อยเก็บข้อมูล และระบบย่อยเปรียบเทียบ การโจมตีหลอกที่ประสบผลสำเร็จจะผ่านระบบย่อย PAD และระบบย่อยเก็บข้อมูล โดยเก็บข้อมูลชีวมิติตัวอย่างได้ และข้อมูลตัวอย่างชีวมิติจะถูกส่งไปประมวลผลที่ระบบย่อยเปรียบเทียบ

(2) ระบบย่อยเก็บข้อมูลและระบบย่อยเปรียบเทียบ (Data capture subsystem and comparison subsystem) (สำหรับ IUT ที่ผลลัพท์ของกลไก PAD ไม่สามารถเข้าถึงได้โดยผู้ประเมินผล) ในการประเมินผลแบบนี้ การทดสอบจะเป็นไปตามแผนการทดสอบที่รู้ตัวผู้โจมตีที่อยู่ในกลุ่มบุคคลทดสอบ การโจมตีหลอกจะพยายามที่จะล้มล้าง ระบบย่อยเก็บข้อมูลและระบบย่อยเปรียบเทียบ การโจมตีหลอกที่ประสบผลสำเร็จจะผ่านระบบย่อยเก็บข้อมูล โดยเก็บข้อมูลชีวมิติตัวอย่างได้ และข้อมูลตัวอย่างชีวมิติจะถูกส่งไปประมวลผลที่ระบบย่อยเปรียบเทียบ

(3) ระบบย่อย PAD และระบบย่อยเปรียบเทียบ (PAD subsystem and comparison subsystem) (สำหรับ IUT ที่คลังข้อมูลตัวอย่างถูกประเมินในรูปแบบออฟไลน์) ในการประเมินผลแบบนี้ การทดสอบจะเกี่ยวข้องกับการทดสอบเทคโนโลยีด้วยตัวอย่างการโจมตีหลอกจากคลังข้อมูลที่เก็บไว้ก่อนหน้า

(4) ระบบย่อยเปรียบเทียบ (Comparison subsystem) (สำหรับ IUT ที่ผลลัพท์จากตัวเปรียบเทียบและผลลัพท์จากกลไก PAD ได้ผลลัพท์ที่ไม่แตกต่างกัน)

เป้าหมายของผู้โจมตีในการประเมินระบบเต็มเป็นอันตรายมาก เนื่องจากผลลัพท์ของระบบย่อยเปรียบเทียบจะสามารถควบคุมให้การโจมตีประสบผลสำเร็จได้ สิ่งที่ควรพิจารณามีดังต่อไปนี้

- ระบบยืนยันตัวตน (Verification system) ในกรณีของโจมตีแบบผู้ปลอมชีวมิติ หรือผู้พยายามเข้าถึง ความล้มเหลวในการจับคู่ (เช่น การปฏิเสธ PAI โดยตัวเปรียบเทียบ) ถูกพิจารณาให้เป็นผลลัพท์ที่ประสบความสำเร็จจากมุมมองของผู้ออกแบบระบบ

- ระบบระบุผลบวก (Positive identification system) ในกรณีของโจมตีแบบผู้ปลอมชีวมิติ หรือผู้พยายามเข้าถึง ความล้มเหลวในการให้ผลตัวระบุเป้าหมาย (targeted identifier) (เช่น ตัวเปรียบเทียบไม่สามารถจับคู่ของ PAI กับเป้าหมายที่ลงทะเบียนไว้ได้) ถูกพิจารณาให้เป็นผลลัพท์ที่ประสบความสำเร็จจากมุมมองของผู้ออกแบบระบบ

- ระบบระบุผลลบ (Negative identification system) ในกรณีของโจมตีแบบผู้ปกปิดชีวมิติ การให้ผลตัวระบุ (identifier) ที่เกี่ยวข้องกับอัตลักษณ์ของผู้ปกปิดชีวมิติ (เช่น ตัวเปรียบเทียบสามารถจับคู่ลักษณะเฉพาะของผู้ปกปิดที่ลงทะเบียนไว้ได้) ถูกพิจารณาให้เป็นผลลัพท์ที่ประสบความสำเร็จจากมุมมองของผู้ออกแบบระบบ

7. การวัดสำหรับการประเมินผลระบบชีวมิติที่มีกลไกการตรวจจับการโจมตีหลอก

สมรรถนะของกลไกการตรวจจับการโจมตีหลอก (PAD) สามารถวัดได้โดยใช้การวัดอัตราความผิดพลาดในการ

แบ่งกลุ่ม อัตราการไม่ตอบสนอง และอัตราการวัดอื่นๆ สำหรับบทนี้จะกล่าวถึงการวัดที่ใช้ในการทดสอบต่างๆ ตาม ISO/IEC 19795-1 หรือ ขมธอ. 30 เล่ม 1 ซึ่งจะให้ภาพรวมเกี่ยวกับการรายงานความต้องการเกี่ยวกับการวัดสมรรถนะระบบชีวมิติสำหรับผู้ใช้ที่มีการแสดงชีวมิติแท้จริง

การประเมินกลไก PAD ต้องรายงานดังต่อไปนี้

- จำนวนของเครื่องมือโจมตีหลอก (PAI) จำนวนชนิดเครื่องมือโจมตีหลอก (PAIs) และจำนวนอนุกรมเครื่องมือโจมตีหลอก (PAIS) ที่ใช้ในการประเมินผล
- จำนวนของบุคคลที่ใช้ทดสอบ รวมทั้ง จำนวนผู้แสดง PAI ไม่สามารถใช้สิ่งทำหลอก และ จำนวนบุคคลทดสอบไม่สามารถแสดงลักษณะเฉพาะชีวมิติที่ไม่สอดคล้องกับที่ลงทะเบียนไว้
- จำนวนต้นกำเนิด PAI ได้มาจากเจ้าของชีวมิติ
- จำนวนเครื่องมือโจมตีหลอกซึ่งสร้างขึ้น ต่อต้นกำเนิด PAI สำหรับแต่ละ PAIS
- จำนวนของวัสดุที่ใช้ทดสอบ
- คำอธิบายเกี่ยวกับข้อมูลเอาท์พุตจากกลไก PAD
- การจัดลำดับสำหรับการแสดงแต่ละบุคคลด้วย PAI และ ไม่ใช้ PAI และใช้ผู้แสดง PAI หรือบุคคลทดสอบเหล่านี้ทดสอบซ้ำหรือไม่
- การจัดลำดับการแสดงต่อ PAD ที่เปิดใช้งานระบบ และไม่เปิดใช้งานระบบ
- ผู้ทดสอบถูกใช้ทดสอบซ้ำหรือไม่

เพื่อที่จะทำรายการบัญชีให้เต็มขอบเขตของบทบาทที่แตกต่างและที่อาจจะทับซ้อนในการทดสอบ PAD ผู้ทำการทดลอง ต้อง ใส่ข้อมูลต่อไปนี้ ในรายงานการทดสอบ

- กำหนดวัตถุประสงค์และความรับผิดชอบของบทบาทต่างๆ เหล่านี้ในการทดสอบ PAD
    - ผู้รับการทดสอบ โดยทำการแสดงชีวมิติจริงแท้ และ พยายามแสดงลักษณะเฉพาะชีวมิติที่ไม่สอดคล้องกับที่ลงทะเบียนไว้
    - ผู้แสดง PAI (PAI presenter)
    - ต้นกำเนิด PAI (PAI source)
    - ผู้ประดิษฐ์ PAI (PAI creator)
- กล่าวถึงบทบาทของวัสดุกับผลการทดสอบ และให้ข้อมูลพื้นฐานเพื่อยืนยันผลทดสอบ
- ระบุถึงจำนวนของบุคคลที่ทำแต่ละหน้าที่ในการทดสอบ ตัวอย่างเช่น ใช้ห้าบุคคลเป็นต้นกำเนิดของ PAI ในการทดสอบ
- แต่ละบทบาทหน้าที่ อธิบายระดับของประสบการณ์ของแต่ละบุคคลในการโจมตีหลอก
- บันทึกเหตุการณ์ที่เกิดขึ้นซึ่งแต่ละบุคคลทำหน้าที่หลายบทบาท อาทิ ผู้เป็นต้นกำเนิด PAI และเป็นผู้แสดง

PAI ด้วย

ในการทดสอบ มีความจำเป็นต้องลงทะเบียนผู้เป็นต้นกำเนิด PAI เป็นผู้อ้างอิงจริงแท้ (bona-fide reference) หรือเป็นผู้ที่อยู่ในระบบตัวจริง

สำหรับการประเมินผลระบบเต็มสำหรับการโจมตีหลอกโดยผู้ปลอมชีวมิติ ผู้แสดง PAI ต้องไม่ทำการแสดงชีวมิติตนเองในกรณีที่บุคคลเหล่านี้ได้ลงทะเบียนเป็นผู้อ้างอิงจริงแท้ ซึ่งจะทำให้ผู้แสดง PAI ซึ่งเป็นเจ้าของลักษณะเฉพาะจริงแท้ถูกเปรียบเทียบกับ PAI ทำให้ทำลายผลการทดสอบ

สำหรับการประเมินผลระบบเต็มสำหรับการโจมตีหลอกโดยผู้ปกปิดชีวมิติ ผู้แสดง PAI ต้องทำการลงทะเบียนในระบบ ซึ่งจำเป็นเพื่อที่จะตรวจสอบได้ว่า ผู้แสดง PAI สามารถปกปิดลักษณะเฉพาะชีวมิติของตนเองได้อย่างถูกต้อง

รายงานการทดสอบ ต้องอธิบายการใช้เครื่องจักร หรือ หรือ กลไกอัตโนมัติ ที่เป็น ผู้แสดง PAI หรือ เป็นต้นกำเนิดของ PAI

ในกรณีที่จำนวนตัวอย่างจำกัดและมีจำนวนน้อย การวัดสมรรถนะดังต่อไปนี้อาจไม่ประสบผลทางด้านสถิติ

7.1 การวัดสำหรับการประเมินผลระบบย่อย PAD

การประเมินผลระบบย่อย PAD เป็นการวัดความสามารถของระบบย่อย PAD ที่สามารถตรวจจับการโจมตีหลอกและการแสดงแท้จริง ได้อย่างถูกต้อง

7.1.1 การวัดการจำแนก

ทั้งอัตราความผิดพลาดการจำแนกการโจมตีหลอก (Attack Presentation Classification Error Rate) หรือเรียกโดยย่อว่า “**APCER**” และอัตราความผิดพลาดการจำแนกชีวมิติจริงแท้ (Bona fide Classification Error Rate) หรือเรียกโดยย่อว่า “**BPCER**” จะต้องรายงานในการประเมินผลระบบย่อย PAD

ในการประเมินผลระบบย่อย PAD การวัดสมรรถนะสำหรับการโจมตีหลอกต้องคำนวณและรายงานผล APCER ผู้ประเมินผลต้องรายงานในรูปแบบที่ การตัดสินใจของ PAD และคะแนนจะถูกใช้ในการจำแนกการแสดงชีวมิติ

APCER สำหรับ PAIS ต้องคำนวณโดยใช้ สมการที่ (1)

$$R_{APCE,P} = 1 - \left(\frac{1}{N_P}\right)\sum_{i=1}^{N_P} Res_i \qquad (1)$$

โดยที่

$R_{APCE,P}$ คือ อัตราความผิดพลาดการจำแนกการโจมตีหลอก หรือ APCER สำหรับ PAIS ที่ใช้

N_P คือ จำนวนการโจมตีหลอกทั้งหมดของเครื่องมือแต่ละชนิดที่ใช้ในการทดสอบ

Res_i คือ ผลลัพธ์การจำแนกของการโจมตีหลอกครั้งที่ i โดยมีค่าเป็น 1 เมื่อจำแนกว่าเป็นการโจมตีหลอกและมีค่า 0 เมื่อจำแนกว่าเป็นชีวมิติจริงแท้

การประเมินผลของกลไก PAD ต้องรายงานจำนวนที่ระบบย่อย PAD สามารถจำแนกการโจมตีหลอก ได้อย่างถูกต้องและผิดพลาดเป็นจำนวนทั้งหมดเท่าไร โดย PAIS โดย PAIs โดยบุคคลทดสอบ และโดยต้นกำเนิด PAI

เมื่อพิจารณาว่าระบบย่อย PAD สามารถตรวจจับ PAIS ที่มีศักยภาพในการโจมตี (attack potential) ที่กำหนด หมายถึง อัตราความผิดพลาดสูงที่สุดที่จำแนกการโจมตีหลอกเป็นชีวมิติจริงแท้จากเครื่องมือการโจมตีหลอกทุกประเภทของระดับการโจมตีที่กำหนดและระดับการโจมตีที่ต่ำกว่าทั้งหมด โดย APCER ของ PAIS ที่ประสบความสำเร็จสูงสุดภายใต้ศักยภาพในการโจมตีที่กำหนด ควรจะใช้สมการที่ (2)

$$R_{APCE,AP} = \max_{P \in A_{AP}} \left(R_{APCE,AP} \right) \quad (2)$$

โดยที่

$R_{APCE,AP}$ คือ อัตราความผิดพลาดการจำแนกการโจมตีหลอก หรือ APCER สำหรับ PAIS ที่ประสบความสำเร็จในการโจมตีหลอกมากที่สุด ภายใต้ศักยภาพในการโจมตีที่กำหนด

A_{AP} คือ เซ็ตย่อยของ PAIS ที่มีศักยภาพในการโจมตีเทียบเท่าหรือต่ำกว่า x หรือ ประเภทเครื่องมือการโจมตีหลอกทั้งหมดของระดับการโจมตีที่กำหนดและระดับการโจมตีที่ต่ำกว่าทั้งหมด

P คือ PAIS

ที่ระดับระบบย่อย PAD การวัดสมรรถนะสำหรับกลุ่มที่แสดงชีวมิติจริงแท้ โดยเก็บที่เป้าหมายการประเมินผล ต้องถูกคำนวณและรายงานในรูปแบบของ BPCER ซึ่งคำนวณโดยใช้สมการที่ (3)

$$R_{BPCE} = \frac{\sum_{i=1}^{N_{BF}} Res_i}{N_P} \quad (3)$$

โดยที่

R_{BPCE} คือ อัตราความผิดพลาดการจำแนกชีวมิติจริงแท้ หรือ BPCER

N_{BF} คือ จำนวนชีวมิติจริงแท้ทั้งหมดที่ใช้ในการทดสอบ

Res_i คือ ผลลัพธ์การจำแนกของการโจมตีหลอกครั้งที่ i โดยมีค่าเป็น 1 เมื่อจำแนกว่าเป็นการโจมตีหลอกและมีค่า 0 เมื่อจำแนกว่าเป็นชีวมิติจริงแท้

7.1.2 การวัดการไม่ตอบสนอง

ผู้ประเมินผลต้องรายงานอัตราการไม่ตอบสนอง สำหรับระบบย่อย PAD โดยใช้การวัดดังต่อไปนี้

(1) *อัตราการไม่ตอบสนองต่อการโจมตีหลอก* (APNRR) หมายถึง อัตราที่ระบบย่อยตรวจจับการโจมตีหลอกไม่ตอบสนอง (ใช่/ไม่ใช่) เมื่อทำการโจมตีหลอก ซึ่งคำนวณได้จากการนำจำนวนครั้งการโจมตีหลอกที่ระบบไม่ตอบสนอง หารด้วยจำนวนครั้งการโจมตีหลอกทั้งหมด

(2) *อัตราการไม่ตอบสนองต่อชีวมิติจริงแท้* (BPNRR) หมายถึง อัตราที่ระบบย่อยตรวจจับการโจมตีหลอกไม่ตอบสนอง (ใช่/ไม่ใช่) เมื่อทำการแสดงชีวมิติจริงแท้ ซึ่งคำนวณได้จากการนำจำนวนครั้งการแสดงชีวมิติจริงแท้ที่ระบบไม่ตอบสนอง หารด้วยจำนวนครั้งการแสดงชีวมิติจริงแท้ทั้งหมด

7.1.3 การวัดประสิทธิภาพ

ค่าตัวชี้วัดนิยามโดยระยะเวลาที่ใช้ในการประมวลผลของระบบย่อยตรวจจับการโจมตีหลอก (PAD subsystem processing duration: PS-PD) ซึ่งคำนวณเป็นช่วงเวลาเฉลี่ย และควรรายงานแยกระหว่างการโจมตีหลอกและการแสดงชีวมิติจริงแท้ โดยการคำนวณจะไม่รวมกรณีที่ระบบไม่ตอบสนอง

7.1.4 สรุป

การรายงานสมรรถนะการตรวจจับการโจมตีหลอกของระบบย่อยตรวจจับการโจมตีหลอก ต้องรายงานข้อมูลต่าง ๆ ในตารางที่ 1

ตารางที่ 1 รายละเอียดสมรรถนะการตรวจจับการโจมตีหลอกของระบบย่อยตรวจจับการโจมตีหลอก

ระบบย่อย	ตัวชี้วัด		ชนิดชีวมิติที่แสดง	การรายงาน
ระบบย่อยตรวจจับการโจมตีหลอก PAD subsystem	APCER	อัตราความผิดพลาดการจำแนกการโจมตีหลอก	โจมตีหลอก	บังคับ
	BPCER	อัตราความผิดพลาดการจำแนกชีวมิติจริงแท้	ชีวมิติจริงแท้	บังคับ
	APNRR	อัตราการไม่ตอบสนองต่อการโจมตีหลอก	โจมตีหลอก	บังคับ
	BPNRR	อัตราการไม่ตอบสนองต่อชีวมิติจริงแท้	ชีวมิติจริงแท้	บังคับ
	$APCER_{AP}$	อัตราความผิดพลาดการจำแนกการโจมตีหลอกที่ระดับการโจมตีที่กำหนด	โจมตีหลอก	ไม่บังคับ
	PS-PD	ระยะเวลาที่ใช้ในการประมวลผลของระบบย่อยตรวจจับการโจมตีหลอก	ชีวมิติจริงแท้หรือโจมตีหลอก	ไม่บังคับ

7.2 การวัดสำหรับการประเมินผลระบบย่อยเก็บข้อมูลชีวมิติ

การวัดสมรรถนะการตรวจจับการโจมตีหลอกในขั้นตอนการรับข้อมูลตัวอย่างชีวมิติ สามารถทดสอบสมรรถนะของฮาร์ดแวร์เก็บข้อมูลชีวมิติ รวมทั้งซอฟต์แวร์ควบคุมการรับข้อมูลภายใน โดยตัวชี้วัดสมรรถนะของการทดสอบการตรวจจับการโจมตีหลอกในระบบย่อยเก็บข้อมูลชีวมิติสามารถแบ่งออกได้เป็น 3 ด้าน ได้แก่

7.2.1 การวัดการรับข้อมูล

(1) *อัตราการเก็บข้อมูลตัวอย่างชีวมิติจากการโจมตีหลอก* (attack presentation acquisition rate: APAR) หมายถึง อัตราที่ระบบย่อยเก็บข้อมูลชีวมิติสามารถเก็บข้อมูลตัวอย่างชีวมิติจากการโจมตีหลอกได้ โดยพิจารณาจากค่าคุณภาพของข้อมูลตัวอย่างชีวมิติ ซึ่งคำนวณได้จากการนำจำนวนครั้งการโจมตีหลอกที่เก็บข้อมูลตัวอย่างชีวมิติได้ หารด้วยจำนวนครั้งการโจมตีหลอกทั้งหมด

(2) *FTER* (อ้างอิงข้อกำหนด 4.6.1 อยู่ใน ขมธอ. 30 เล่ม 1 [5]) ซึ่งจะวัดและรายงานเมื่อมีการทดสอบร่วมกับกระบวนการลงทะเบียน

(3) *FTAR* (อ้างอิงข้อกำหนด 4.6.2 อยู่ใน ขมธอ. 30 เล่ม 1 [5]) ซึ่งจะวัดและรายงานเมื่อมีการทดสอบร่วมกับกระบวนการรู้จำชีวมิติ

7.2.2 การวัดการไม่ตอบสนอง

ผู้ประเมินผลต้องรายงานอัตราการไม่ตอบสนอง สำหรับระบบย่อยเก็บข้อมูลชีวมิติ โดยใช้การวัดดังต่อไปนี้

(1) *อัตราการไม่ตอบสนองต่อการโจมตีหลอก* (attack presentation non-response rate: APNRR) หมายถึง อัตราที่ระบบย่อยเก็บข้อมูลชีวมิติไม่ตอบสนอง (ใช่/ไม่ใช่) เมื่อทำการโจมตีหลอก ซึ่งคำนวณได้จากการนำจำนวนครั้งการโจมตีหลอกที่ระบบไม่ตอบสนอง หารด้วยจำนวนครั้งการโจมตีหลอกทั้งหมด

(2) อัตราการไม่ตอบสนองต่อชีวมิติจริงแท้ (bona fide presentation non-response rate: BPNRR) หมายถึง อัตราที่ระบบย่อยเก็บข้อมูลชีวมิติไม่ตอบสนอง (ใช่/ไม่ใช่) เมื่อทำการแสดงชีวมิติจริงแท้ ซึ่งคำนวณได้จากการนำจำนวนครั้งการแสดงชีวมิติจริงแท้ที่ระบบไม่ตอบสนอง หารด้วยจำนวนครั้งการแสดงชีวมิติจริงแท้ทั้งหมด

7.2.3 การวัดประสิทธิภาพ

ค่าตัวชี้วัดนิยามโดยระยะเวลาที่ใช้ในการประมวลผลของระบบย่อยเก็บข้อมูลชีวมิติ (data capture subsystem processing duration: DCS-PD) ซึ่งคำนวณเป็นช่วงเวลาเฉลี่ย และควรรายงานแยกระหว่างการโจมตีหลอกและการแสดงชีวมิติจริง โดยการคำนวณจะไม่รวมกรณีที่ระบบไม่ตอบสนอง

7.2.4 สรุป

การรายงานสมรรถนะการตรวจจับการโจมตีหลอกของระบบย่อยเก็บข้อมูลชีวมิติ ต้องรายงานข้อมูลต่าง ๆ ในตารางที่ 2

ตารางที่ 2 รายละเอียดสมรรถนะการตรวจจับการโจมตีหลอกของระบบย่อยเก็บข้อมูลชีวมิติ

ระบบย่อย	ตัวชี้วัด		ชนิดชีวมิติที่แสดง	การรายงาน
ระบบย่อยเก็บข้อมูลชีวมิติ	APAR	อัตราการเก็บข้อมูลตัวอย่างชีวมิติจากการโจมตีหลอก	โจมตีหลอก	บังคับ
	FTER	อัตราความผิดพลาดจากการลงทะเบียนชีวมิติ (อ้างอิงข้อกำหนด 4.6.1 ใน ขมธอ. 30-2565 [5])	ชีวมิติจริงแท้	บังคับเมื่อมีการทดสอบร่วมกับกระบวนการลงทะเบียน
	FTAR	อัตราความผิดพลาดจากการเก็บข้อมูลตัวอย่างชีวมิติ (อ้างอิงข้อกำหนด 4.6.2 ใน ขมธอ. 30-2565 [5])	ชีวมิติจริงแท้	บังคับเมื่อมีการทดสอบร่วมกับกระบวนการรู้จำชีวมิติ
	APNRR	อัตราการไม่ตอบสนองต่อการโจมตีหลอก	โจมตีหลอก	บังคับ
	BPNRR	อัตราการไม่ตอบสนองต่อชีวมิติจริงแท้	ชีวมิติจริงแท้	บังคับ
	DCS-PD	ระยะเวลาที่ใช้ในการประมวลผลของระบบย่อยเก็บข้อมูลชีวมิติ	ชีวมิติจริงแท้หรือโจมตีหลอก	ไม่บังคับ

7.3 การวัดสำหรับการประเมินผลระบบเต็ม

การทดสอบแบบเต็มระบบเป็นการทดสอบระบบครบวงจร (end-to-end) เต็มรูปแบบ โดยจะวิเคราะห์รวมตั้งแต่ ระบบย่อยเก็บข้อมูลชีวมิติ ส่วนการตรวจจับการโจมตีหลอก และเพิ่มในส่วนขั้นตอนการเปรียบเทียบชีวมิติ (comparison subsystem) โดยอาจมีการแยกวิเคราะห์เพื่อตรวจสอบได้ ดังนี้

(1) การตรวจสอบแบบที่ 1 จะมีการตรวจจับครอบคลุมใน (1) ระบบย่อยเก็บข้อมูลชีวมิติ (2) ระบบย่อยตรวจจับการโจมตีหลอก และ (3) ระบบย่อยการเปรียบเทียบชีวมิติ

(2) การตรวจสอบแบบที่ 2 จะมีการตรวจจับครอบคลุมใน (1) ระบบย่อยเก็บข้อมูลชีวมิติ และ (2) ระบบย่อยการเปรียบเทียบชีวมิติ

(3) การตรวจสอบแบบที่ 3 จะมีการตรวจจับครอบคลุมใน (1) ระบบย่อยตรวจจับการโจมตีหลอก และ (2) ระบบย่อยการเปรียบเทียบชีวมิติ

(4) การตรวจสอบแบบที่ 4 จะมีการตรวจจับเพียงในระบบย่อยการเปรียบเทียบชีวมิติ

7.3.1 ตัววัดความแม่นยำ

ตัวชี้วัดสมรรถนะด้านความแม่นยำในการรู้จำ โดยจะแบ่งตามลักษณะการทำงานของระบบได้แก่ การพิสูจน์ยืนยันชีวมิติและการระบุชีวมิติ

7.3.1.1 การประเมินผลระบบพิสูจน์ยืนยันตัวตน

สำหรับระบบยืนยันตัวตน สำหรับแต่ละ PAIS อย่างน้อยควรจะรายงานอย่างใดอย่างหนึ่ง เช่น อัตราการยอมรับการโจมตีหลอกแบบปลอมตัวตน (IAPAR) และจำนวนตัวอย่างที่ใช้ในการคำนวณอัตราต่างๆ หรืออัตราการปฏิเสธจากการโจมตีหลอกแบบปกปิดตัวตน (CAPRR) และจำนวนตัวอย่างที่ใช้ในการคำนวณอัตราต่างๆ ดังต่อไปนี้

(1) อัตราการยอมรับการโจมตีหลอกแบบปลอมตัวตน (impostor attack presentation accept rate: IAPAR) หมายถึง อัตราส่วนของการโจมตีหลอกแบบปลอมตัวตนที่สามารถเข้าระบบได้โดยที่ไม่ใช่เจ้าของชีวมิติ หรือ อัตราที่คะแนนเปรียบเทียบจากการโจมตีหลอกมีค่ามากกว่าค่าเทรชโฮลด์ โดยจะรายงานแยกตามประเภทเครื่องมือการโจมตีหลอก PAIS ซึ่งคำนวณได้จากสมการ (4)

$$IAPAR(T) = \frac{1}{N_P}\sum_{i=1}^{N_P} H(v_i - T) \qquad (4)$$

โดยที่

T คือ ค่าเทรชโฮลด์

N_P คือ จำนวนการโจมตีหลอกทั้งหมดของเครื่องมือแต่ละชนิดที่ใช้ในการทดสอบ

$H(x)$ คือ ฟังก์ชันขั้นบันไดหนึ่งหน่วย โดย $H(0) = 1$ และ v คือคะแนนเปรียบเทียบของการโจมตีหลอก

(2) อัตราการยอมรับการโจมตีหลอกแบบปลอมตัวตนที่ระดับการโจมตีที่กำหนด (impostor attack presentation accept rate at the given attack potential: $IAPAR_{AP}$) หมายถึง อัตราการยอมรับการ

โจมตีหลอกแบบปลอมตัวตนสูงที่สุดจากเครื่องมือการโจมตีหลอกทุกประเภทของระดับการโจมตีที่กำหนดและระดับการโจมตีที่ต่ำกว่าทั้งหมด ซึ่งคำนวณได้จากสมการ (5)

$$IAPAR_{AP} = \max_{P \in A_{AP}} (IAPAR_P) \quad (5)$$

โดยที่

A_{AP} คือ เซ็ตย่อยของ PAIS ที่มีศักยภาพในการโจมตีเทียบเท่าหรือต่ำกว่า x หรือ ประเภทเครื่องมือการโจมตีหลอกทั้งหมดของระดับการโจมตีที่กำหนดและระดับการโจมตีที่ต่ำกว่าทั้งหมด

P คือ PAIS

(3) อัตราการปฏิเสธจากการโจมตีหลอกแบบปกปิดตัวตน (concealer attack presentation reject rate: CAPRR) หมายถึง อัตราการปฏิเสธการเข้าระบบที่เกิดจากการโจมตีหลอกแบบปกปิดตัวตน เช่น ผู้ก่อการร้ายทำการศัลยกรรมใบหน้าแล้วระบบไม่สามารถรู้จำได้ว่าเป็นผู้ก่อการร้าย ซึ่งคำนวณได้จากการนำจำนวนครั้งการโจมตีหลอกแบบปกปิดตัวตนที่ระบบปฏิเสธการเข้าระบบหรือไม่สามารถรู้จำได้ว่าเป็นบุคคลที่ลงทะเบียนในระบบ หารด้วยจำนวนครั้งการโจมตีหลอกแบบปกปิดตัวตนทั้งหมด

7.3.1.2 การประเมินผลระบบระบุตัวตนผลบวก

สำหรับระบบระบุตัวตนผลบวก สำหรับแต่ละการโจมตีด้วยแต่ละ PAIS จะต้องรายงานอัตราการยอมรับการโจมตีหลอกแบบปลอมตัวตน (IAPAR) และจำนวนตัวอย่างที่ใช้ในการคำนวณอัตราต่างๆ

7.3.1.3 การประเมินผลระบบระบุตัวตนผลลบ

สำหรับระบบยืนยันตัวตน สำหรับแต่ละ PAIS อย่างน้อยควรจะรายงานอย่างใดอย่างหนึ่ง เช่น IAPAR และจำนวนตัวอย่างที่ใช้ในการคำนวณอัตราต่างๆ หรือ CAPRR และจำนวนตัวอย่างที่ใช้ในการคำนวณอัตราต่างๆ ดังต่อไปนี้

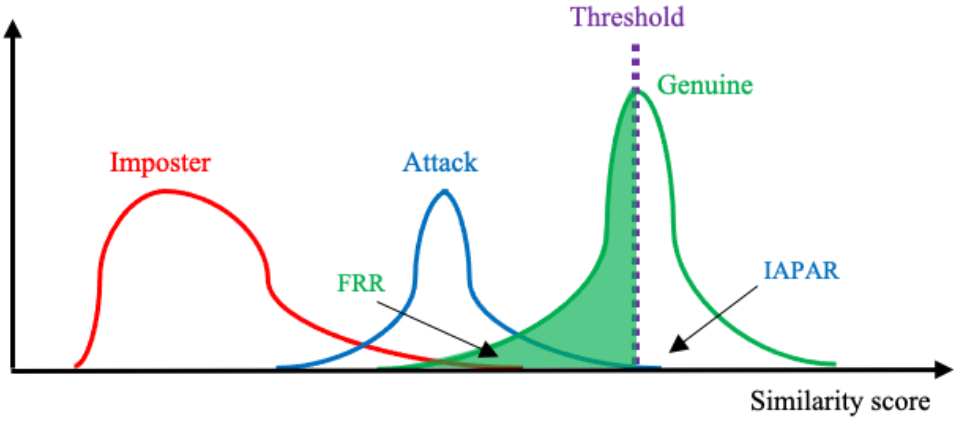
สำหรับระบบระบุตัวตนผลลบ สำหรับแต่ละการโจมตีด้วยแต่ละ PAIS จะต้องรายงานอัตราการไม่ระบุตัวตนจากการโจมตีหลอกแบบปกปิดตัวตน (CAPNIR) และจำนวนตัวอย่างที่ใช้ในการคำนวณอัตราต่างๆ

7.3.2 ตัววัดประสิทธิภาพ

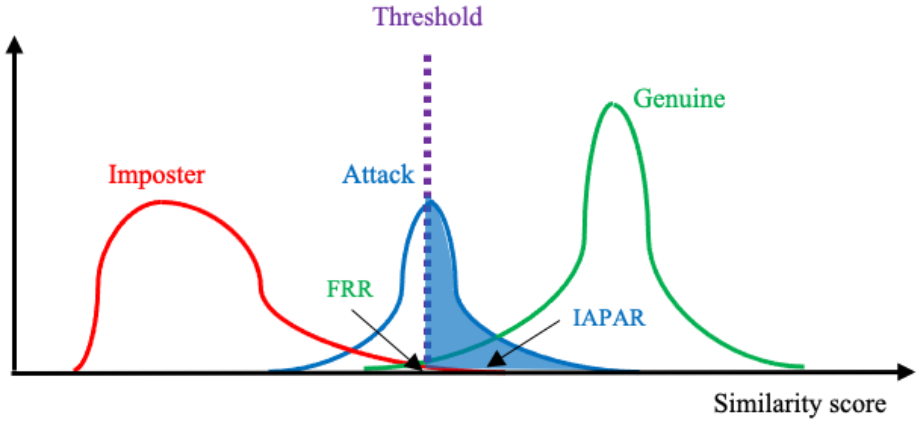
ค่าตัวชี้วัดนิยามโดยระยะเวลาที่ใช้ในการประมวลผลแบบเต็มระบบ (full-system processing duration: FS-PD) ซึ่งจะวัดเป็นระยะเวลารวมทั้งระบบ ซึ่งระยะเวลาที่ใช้สำหรับการทดสอบโจมตีหลอกอาจแตกต่างกับการทดสอบด้วยชีวมิติจริง ดังนั้นการวัด FS-PD จะใช้เพื่อพิจารณาความเปลี่ยนแปลงของระยะเวลาที่ใช้ในการประมวลผลของกลไกการตรวจจับการโจมตีหลอก รวมถึงควรรายงาน FS-PD แบบเปิดใช้และไม่เปิดใช้กลไกการตรวจจับการโจมตีหลอกด้วย

7.3.3 สมรรถนะการประเมินผลระบบเต็มโดยทั่วไป

ในการทดสอบแบบเต็มระบบสำหรับการพิสูจน์ยืนยันชีวมิติ ค่าเทรชโฮลด์ที่ทำให้อัตราการยอมรับจากการโจมตีหลอกต่ำสุด อาจจะไม่ใช่ตัวบ่งบอกสมรรถนะการรู้จำสูงสุด ตัวอย่างเช่น ในรูปที่ 3 (ก) มีการกำหนดค่าเทรชโฮลด์ที่ทำให้ IAPAR มีค่าเท่ากับ 0% อาจทำให้ FRR มีสูงถึง 65% และในทางกลับกันในรูปที่ 3 (ข) ถ้าลดค่าเทรชโฮลด์ลงจะทำให้ค่า FRR ลดลงเหลือ 1% แต่ค่า IAPAR สูงขึ้นถึง 41%



(ก)



(ข)

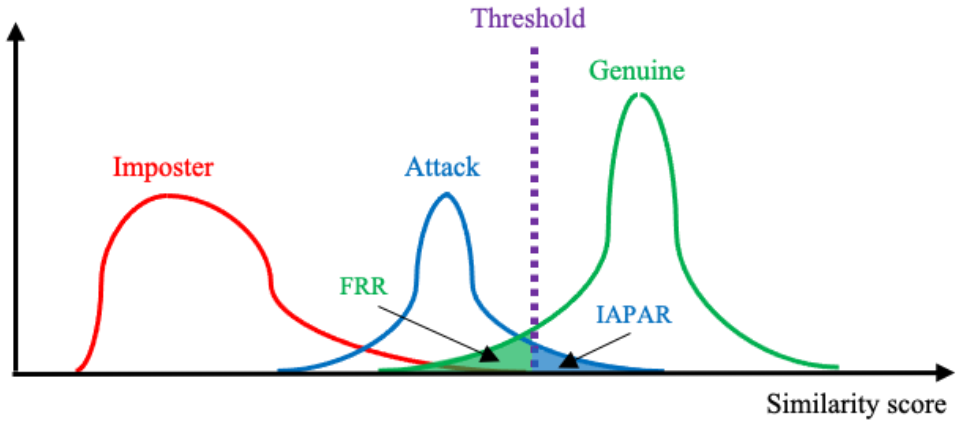
รูปที่ 3 ตัวอย่างผลกระทบต่อ IAPAR จากการปรับค่าเทรชโฮลด์คะแนนเปรียบเทียบ

ดังนั้น การรายงานผลการทดสอบต้องมีการรายงาน อัตราการยอมรับการโจมตีหลอกแบบปลอมตัวตนสัมพัทธ์ (relative impostor attack presentation accept rate: RIAPAR) เพื่อให้การวิเคราะห์สมรรถนะโดยรวมทั้งระบบการรู้จำและการป้องกันการโจมตีหลอกเป็นไปอย่างมีประสิทธิภาพ โดยอัตรา RIAPAR สามารถคำนวณได้จากสมการที่ (6)

$$RIAPAR(T) = IAPAR(T) + FRR(T) \quad (6)$$

รูปที่ 4 แสดงตัวอย่างการกำหนดค่าเทรชโฮลด์ที่ทำให้ RIAPAR มีค่าต่ำสุด ซึ่งหมายถึงผลรวมระหว่างค่า FRR และค่า IAPAR มีค่าต่ำสุดและทำให้สมรรถนะการรู้จำที่มีระบบป้องกันการโจมตีหลอกมีสมรรถนะสูงสุด

การทดสอบการป้องกันการโจมตีหลอกในระบบการระบุชีวมิติแบ่งออกเป็น 2 กรณี ได้แก่



รูปที่ 4 ตัวอย่างการปรับค่าเทรชโฮลด์ที่สามารถเพิ่มสมรรถนะ RIAPAR

ตัวชี้วัดสมรรถนะด้านความแม่นยำในการรู้จำสำหรับการทดสอบระบบการระบุชีวมิติ

(1) การทดสอบการระบุชีวมิติเชิงบวก คือ การระบุชีวมิติที่ค้นหาด้วยชีวมิติของบุคคลที่ไม่ได้ลงทะเบียนในฐานข้อมูล เช่น ผู้โจมตีไม่ได้ลงทะเบียนในฐานข้อมูลแต่พยายามปลอมชีวมิติเป็นบุคคลในฐานข้อมูล โดยผลลัพธ์รายการบุคคลที่ระบบตอบกลับมาจะใช้ในการบ่งชี้สมรรถนะ ซึ่งการทดสอบการป้องกันการโจมตีหลอกด้วยการปลอมแปลงประเภทต่าง ๆ (PAIS) จะมีรูปแบบการรายงานดังนี้

- ค่าตัวชี้วัดที่ 1 นิยามโดยอัตราการระบุชีวมิติสำเร็จจากการโจมตีหลอกแบบปลอมตัวตน (impostor attack presentation identification rate: IAPIR) หมายถึง อัตราที่ผลลัพธ์รายการบุคคลที่ระบบตอบกลับมามีรายการบุคคลเป้าหมายที่ผู้โจมตีสวมตัวตน ซึ่งคำนวณได้จากการนำจำนวนครั้งการโจมตีหลอกแบบปลอมตัวตนที่ผลลัพธ์รายการบุคคลที่ระบบตอบกลับมามีรายการบุคคลเป้าหมาย หารด้วยจำนวนครั้งการโจมตีหลอกแบบปลอมตัวตนทั้งหมด
- ค่าตัวชี้วัดที่ 2 นิยามโดย FPIR (อ้างอิงข้อกำหนด 6.4.1 อยู่ใน ขมธอ. 30 เล่ม 1 [5]) รวมถึงข้อมูลต่าง ๆ ที่เกี่ยวข้อง เช่น จำนวนบุคคลในฐานข้อมูล

(2) การทดสอบการระบุชีวมิติเชิงลบ คือ การระบุชีวมิติที่ค้นหาด้วยชีวมิติของบุคคลที่ลงทะเบียนในฐานข้อมูล เช่น ผู้โจมตีลงทะเบียนในฐานข้อมูลแต่พยายามปลอมชีวมิติเป็นบุคคลที่ไม่ได้ลงทะเบียนฐานข้อมูล โดยผลลัพธ์รายการบุคคลที่ระบบตอบกลับมาจะใช้ในการบ่งชี้สมรรถนะ ซึ่งการทดสอบการป้องกันการโจมตีหลอกด้วยการปลอมแปลงประเภทต่าง ๆ (PAIS) จะมีรูปแบบการรายงานดังนี้

- ค่าตัวชี้วัดที่ 1 นิยามโดยอัตราการระบุชีวมิติไม่สำเร็จจากการโจมตีหลอกแบบปกปิดตัวตน (concealer attack presentation non-identification rate: CAPNIR) ซึ่งหมายถึง อัตราที่ผลลัพธ์รายการบุคคลที่ระบบตอบกลับมาไม่มีรายการบุคคลของผู้โจมตี ซึ่งคำนวณได้จากการนำจำนวนครั้งการโจมตีหลอกแบบปกปิดตัวตนที่ผลลัพธ์รายการบุคคลที่ระบบตอบกลับมาไม่มีรายการบุคคลของผู้โจมตี หารด้วยจำนวนครั้งการโจมตีหลอกแบบปกปิดตัวตนทั้งหมด
- ค่าตัวชี้วัดที่ 2 นิยามโดย FNIR (อ้างอิงข้อกำหนด 6.4.1 อยู่ใน ขมธอ. 30 เล่ม 1 [5]) รวมถึงข้อมูลต่าง ๆ ที่เกี่ยวข้อง เช่น จำนวนบุคคลในฐานข้อมูล

7.3.4 สรุป

การรายงานสมรรถนะการตรวจจับการโจมตีหลอกของการทดสอบแบบเต็มระบบต้องรายงานข้อมูลต่าง ๆ ในตารางที่ 3

ตารางที่ 3 รายละเอียดสมรรถนะการตรวจจับการโจมตีหลอกของการทดสอบแบบเต็มระบบ

ระบบย่อย	ตัวชี้วัด		ชนิดชีวมิติที่แสดง	การรายงาน
ส่วนการเปรียบเทียบชีวมิติแบบพิสูจน์ยืนยันชีวมิติ	FAR/FRR	อัตราการยอมรับผิดพลาดและอัตราการปฏิเสธผิดพลาด (อ้างอิงข้อกำหนด 5.4.2 ใน ขมธอ. 30-2565 [5])	ชีวมิติจริง	บังคับ
	IAPAR	อัตราการยอมรับการโจมตีหลอกแบบปลอมตัวตน	โจมตีหลอก	บังคับ
	RIAPAR	อัตราการยอมรับการโจมตีหลอกแบบปลอมตัวตนสัมพัทธ์	ชีวมิติจริงและโจมตีหลอก	บังคับ
	CAPRR	อัตราการปฏิเสธจากการโจมตีหลอกแบบปกปิดตัวตน	โจมตีหลอก	บังคับ
	$IAPAR_{AP}$	อัตราการยอมรับการโจมตีหลอกแบบปลอมตัวตนที่ระดับการโจมตีที่กำหนด	โจมตีหลอก	ไม่บังคับ
	FS-PD	ระยะเวลาที่ใช้ในการประมวลผลแบบเต็มระบบ	ชีวมิติจริงหรือโจมตีหลอก	ไม่บังคับ
ส่วนการเปรียบเทียบชีวมิติแบบระบุชีวมิติเชิงบวก	FPIR	อัตราความผิดพลาดเชิงบวกจากการระบุชีวมิติผิด (อ้างอิงข้อกำหนด 6.4.1 ใน ขมธอ. 30-2565 [5])	ชีวมิติจริง	บังคับ
	IAPIR	อัตราการระบุชีวมิติสำเร็จจากการโจมตีหลอกแบบปลอมตัวตน	โจมตีหลอก	บังคับ
	FS-PD	ระยะเวลาที่ใช้ในการประมวลผลแบบเต็มระบบ	ชีวมิติจริงหรือโจมตีหลอก	ไม่บังคับ
ส่วนการเปรียบเทียบชีวมิติแบบระบุชีวมิติเชิงลบ	FNIR	อัตราความผิดพลาดเชิงลบจากการระบุชีวมิติผิด (อ้างอิงข้อกำหนด 6.4.1 ใน ขมธอ. 30-2565 [5])	ชีวมิติจริง	บังคับ
	CAPNIR	อัตราการระบุชีวมิติไม่สำเร็จจากการโจมตีหลอกแบบปกปิดตัวตน	โจมตีหลอก	บังคับ
	FS-PD	ระยะเวลาที่ใช้ในการประมวลผลแบบเต็มระบบ	ชีวมิติจริงหรือโจมตีหลอก	ไม่บังคับ

บรรณานุกรม

[1] ขมธอ. 29 เล่ม 1-2565 ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม 1: การใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน

[2] ขมธอ. 29 เล่ม 2-2565 ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม 2: การใช้งานเทคโนโลยีการรู้จำใบหน้าสำหรับการพิสูจน์และยืนยันตัวตน

[3] ขมธอ. 29 เล่ม 3-2565 ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม 3: การใช้งานเทคโนโลยีการรู้จำลายนิ้วมือสำหรับการพิสูจน์และยืนยันตัวตน

[4] ขมธอ. 29 เล่ม 4-2565 ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม 4: การใช้งานเทคโนโลยีการรู้จำลายม่านตาสำหรับการพิสูจน์และยืนยันตัวตน

[5] ขมธอ. 30-2565 ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทดสอบสมรรถนะการทำงานเทคโนโลยีชีวมิติ

[6] International Organization for Standardization, “ISO/IEC 19795-1:2021, Information technology — Biometric performance testing and reporting — Part 1: Principles and framework”, May 2021.

[7] International Organization for Standardization, “ISO/IEC 30107-1:2023, Information technology — Biometric presentation attack detection — Part 1: Framework”, August 2023.

[8] International Organization for Standardization, “ISO/IEC 30107-3:2023, Information technology — Biometric presentation attack detection — Part 3: Testing and reporting”, January 2023.