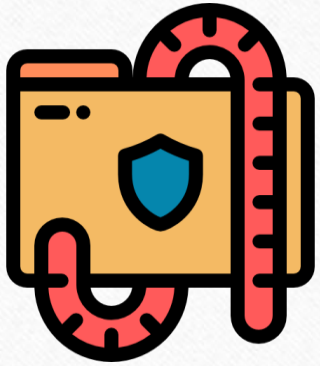
การใช้ดิจิทัลเพื่อความมั่นคงปลดภัย

มิติการเรียนรู้ รู้เท่าทันและใช้เทคโนโลยีเป็น (Digital Literacy)

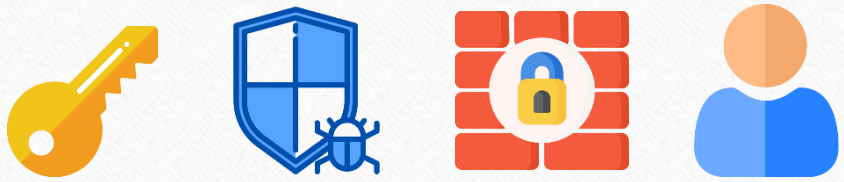
ภัยคุกคาม (Threat)

- Hacker
- Cracker
- Virus
- Worms
- Spam Mail
- Malware
- Trojan Horse



การป้องกันภัยคุกคาม (Threat Protection)

- **รหัสผ่าน (Password)** ใช้ตัวอักษร ตัวเลข ร่วมกัน ไม่ง่ายต่อการคาดเดา ควรเปลี่ยนรหัสผ่านอยู่เสมอ ไม่บอกรหัสผ่านกับผู้อื่น
- **ไฟร์วอล (Firewall)** ระบบรักษาความปลอดภัยของระบบเครือข่าย ไม่ให้ถูกโจมตีจากผู้ไม่หวังดีหรือการสื่อสารที่ไม่ได้รับอนุญาต ซึ่งมีทั้งซอฟแวร์ (Software) และฮาร์ดแวร์ (Hardware) สามารถกำหนดสิทธิ์ในการเข้า และออกได้
- **ซอฟต์แวร์ป้องกันไวรัส (Anti-Virus Software)** ควรมีการอัพเดทฐานข้อมูลไวรัสอยู่เสมอ
- **ผู้ใช้งาน (User)** ควรมีนโยบายการใช้คอมพิวเตอร์อินเทอร์เน็ตที่เหมาะสม ไม่เข้าเว็บไซต์ที่ไม่เหมาะสม และหมั่นสำรองข้อมูลอย่างสม่ำเสมอ



การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน (Authentication) คืออะไร?

- การพิสูจน์ตัวตนเป็นการปกป้องความมั่นคงปลอดภัยของระบบและข้อมูลภายในองค์กร เพื่อไม่ให้เกิดการถูกคุกคามโดยผู้ไม่ประสงค์ดีหรือจากโปรแกรมบางประเภทได้เพิ่มมากขึ้นและอาจนำมาซึ่งความเสียหายอย่างมากต่อองค์กร ดังนั้นถ้าภายในระบบมีการควบคุมความปลอดภัยที่ดีจะช่วยลดโอกาสเสี่ยงต่อการถูกคุกคามได้

การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน แบ่งออกเป็น 2 ขั้นตอน

- การระบุตัวตน (Identification) คือ ขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใครเช่น ชื่อผู้ใช้ (username)
- การพิสูจน์ตัวตน (Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริงเช่น รหัสผ่าน (Password)

กลไกของการพิสูจน์ตัวตน (Authentication mechanisms) แบ่งออกเป็น 3 คุณลักษณะ

- Possession factor เช่น กุญแจหรือเครดิตการ์ด เป็นต้น
- Knowledge factor เช่น รหัสผ่าน (passwords) หรือการใช้พิน (PINs) เป็นต้น
- Biometric factor เช่น ลายนิ้วมือ รูปแบบเรตินา (retinal patterns) หรือใช้รูปแบบเสียง (voice patterns) เป็นต้น

การพิสูจน์ตัวตน (Authentication)

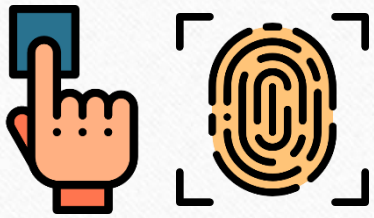
ลักษณะของการควบคุมความมั่นคงปลอดภัย (Security Controls)

- การพิสูจน์ตัวตน (Authentication) คือ ผู้เข้าใช้ระบบต้องถูกยอมรับจากระบบว่าสามารถเข้าสู่ระบบได้
- การกำหนดสิทธิ์ (Authorization) คือข้อจำกัดของบุคคลที่เข้ามาในระบบ ว่าบุคคลคนนั้นสามารถทำอะไรกับระบบได้บ้าง
- การบันทึกการใช้งาน (Accountability) คือ การบันทึกรายละเอียดของการใช้ระบบและรวมถึงข้อมูลต่างๆที่ผู้ใช้กระทำลงไปในระบบ

การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตนด้วย Biometric

- แบบที่ตรวจสอบจากลักษณะทางกายภาพ ดูจากของอวัยวะของร่างกายอย่างเช่น ลายนิ้วมือ ม่านตา เรตินา รวมทั้งหน้าตาและลายมือด้วย
- การตรวจสอบจากพฤติกรรม ดูจากรูปแบบการกดคีย์บอร์ด ลายเซ็น และเสียง



ลักษณะการทำงาน

- ตัวเซ็นเซอร์จะอ่านข้อมูลดิจิตอลเกี่ยวกับ Biometric เข้ามา จากนั้นจะได้รับการประมวลผล ดึงเอาคุณลักษณะพิเศษที่ไม่เหมือนกันของแต่ละคนออกมา จากนั้นจะสร้างเทมเพลต ซึ่งเป็นการสังเคราะห์ข้อมูลชิ้นใหม่ เพื่อใช้แทนข้อมูลที่อ่านได้จากเซ็นเซอร์ จากนั้นการพิสูจน์ตนก็จะเปรียบเทียบเทมเพลตที่สร้างขึ้นมาใหม่นี้กับไฟล์ที่มีอยู่ ถ้าเหมือนก็จะอนุญาตแต่ถ้าไม่เหมือนก็จะทำการปฏิเสธ

การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Authentication by Passwords)

- รหัสผ่าน นิยมใช้กันแพร่หลาย รหัสผ่านควรจำกัดให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นที่ทราบ การตั้งรหัสผ่านที่ง่ายเกินไป และวิทยาการและความรู้ที่ก้าวหน้าทำให้รหัสผ่านอาจจะถูกขโมยโดยระหว่างการสื่อสารผ่านเครือข่ายได้

การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตนโดยใช้ PIN (Authentication by PIN)

- PIN (Personal Identification Number) เป็นรหัสลับส่วนบุคคลที่ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบ ซึ่ง PIN ใช้อย่างแพร่หลาย โดยเฉพาะการทำธุรกรรมทางด้านธนาคาร เนื่องจาก PIN จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่น ฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะ และถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น

การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว (One-Time Password : OTP)

- One-Time Password (OTP) ถูกพัฒนาขึ้นเพื่อหลีกเลี่ยงปัญหาที่เกิดจากการใช้รหัสผ่านเพียงตัวเดียวซ้ำๆกัน
- One-Time Password (OTP) จะทำให้ระบบมีความปลอดภัยมากขึ้น เพราะรหัสผ่านจะถูกเปลี่ยนทุกครั้งก่อนที่ผู้ใช้จะเข้าสู่ระบบ

การทำงานของ OTP

- เมื่อผู้ใช้ต้องการจะเข้าใช้ระบบ ผู้ใช้จะทำการร้องขอไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์จะส่ง challenge string กลับมาให้ผู้ใช้ จากนั้นผู้ใช้จะนำ challenge string และรหัสลับที่มีอยู่กับตัวของผู้ใช้นำไปเข้าแฮชฟังก์ชันแล้วออกมาเป็นค่า response ผู้ใช้ก็จะส่งค่านั้นกลับไปยังเซิร์ฟเวอร์ เซิร์ฟเวอร์จะทำการตรวจสอบค่าที่ผู้ใช้ส่งมาเปรียบเทียบกับค่าที่เซิร์ฟเวอร์เองคำนวณได้ โดยเซิร์ฟเวอร์ก็ใช้วิธีการคำนวณเดียวกันกับผู้ใช้ เมื่อได้ค่าที่ตรงกันเซิร์ฟเวอร์ก็จะยอมรับให้ผู้ใช้เข้าสู่ระบบ

การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้ Public-key

- Public key เกิดจากหลักคณิตศาสตร์ที่เรียกว่า ฟังก์ชั่นทางเดียว (One way function) เป็นการกำหนดให้เลขตัวจากการคำนวณ เป็น Public key และ Private Key การเข้ารหัสโดยใช้กุญแจสาธารณะประกอบไปด้วยกุญแจ 2 ชนิด ที่ต้องใช้คู่กันเสมอในการเข้ารหัสและถอดรหัส

- public key เป็นกุญแจที่ผู้สร้างจะส่งออกไปให้ผู้ใช้อื่นๆ ทราบหรือเปิดเผยได้
- private key เป็นกุญแจที่ผู้สร้างจะเก็บไว้ โดยไม่เปิดเผยให้คนอื่นรู้

การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตนโดยการใช้ลายเซ็นต์ดิจิตัล (Digital Signature)

- Digital Signature เป็นสิ่งที่แสดงยืนยันตัวบุคคล (เจ้าของ email) และ email (ข้อความใน email) ว่า email นั้นได้ถูกส่งมาจากผู้ส่ง คนนั้นจริงๆ และข้อความไม่ได้ถูกเปลี่ยนแปลงและแก้ไข

- ลายเซ็นต์ดิจิทัลนอกจากจะสามารถ ระบุตัวบุคคล และ เป็นกลไกการป้องกันการปฏิเสธความรับผิดชอบแล้ว ยังสามารถป้องกันข้อมูลที่ส่งไปไม่ให้ถูกแก้ไข หรือ หากถูกแก้ไขไปจากเดิมก็สามารถล่วงรู้ได้ กระบวนการสร้างและลงลายเซ็นต์ดิจิทัล