การพิสูจน์ตัวตนแบบ 2 เงื่อนไข บน Windows
โดยใช้ Flash Drive และ รหัสผ่าน

TWO-FACTOR AUTHENTICATION ON WINDOWS
BY USING FLASH DRIVE AND PASSWORD

นายวสันต์ หลวงเรื่อง รหัส 49361782

นายเอกพงศ์ ทิงาเครือ รหัส 49362635

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร

ปีการศึกษา 2552

ใบรับรองโครงงานวิศวกรรม

หัวข้อโครงงาน การพิสูจน์ตัวตนแบบ 2 เงื่อนไข บน Windows โดยใช้ Flash Drive และ รหัสผ่าน

ผู้ดำเนินโครงงาน นายวสันต์ หลวงเรื่อง รหัส 49361782

นายเอกพงศ์ ทิงาเครือ รหัส 49362635

อาจารย์ที่ปรึกษา อาจารย์ภาณุพงศ์ สอนคม

สาขาวิชา วิศวกรรมคอมพิวเตอร์

ภาควิชา วิศวกรรมไฟฟ้าและคอมพิวเตอร์

ปีการศึกษา 2552

.....

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร อนุมัติให้โครงงานฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะกรรมการสอบโครงงานวิศวกรรม

.....ประธานกรรมการ

(อาจารย์ภาณุพงศ์ สอนคม)

.....กรรมการ

(อาจารย์เศรษฐา ตั้งค้าวานิช)

.....กรรมการ

(ดร.สุรเดช จิตประไพกุลศาล)

หัวข้อโครงงาน	การพิสูจน์ตัวตนแบบ 2 เงื่อนไข บน Windows โดยใช้ Flash Drive และ รหัสผ่าน
ผู้ดำเนินโครงงาน	นายวสันต์ หลวงเรื่อง รหัส 49361782
	นายเอกพงศ์ ทิงาเครือ รหัส 49362635
อาจารย์ที่ปรึกษา	อาจารย์ภาณุพงศ์ สอนคม
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์
ปีการศึกษา	2552

.....

บทคัดย่อ

โครงงานนี้เป็นการพัฒนาการพิสูจน์ตัวตนแบบ 2 เงื่อนไข บน Windows โดยใช้ Flash Drive และ รหัสผ่าน เพื่อจำกัดสิทธิ์การใช้งานคอมพิวเตอร์และเพิ่มความปลอดภัยให้กับข้อมูลจึงได้พัฒนาโปรแกรมเข้าสู่ระบบปฏิบัติการ Windows โดยต้องเสียบ Flash drive ตัวที่กำหนด และใส่รหัสผ่าน ซึ่งทำหน้าที่เป็นตัวกลางระหว่างผู้ใช้กับระบบปฏิบัติการ Windows โปรแกรมนี้ใช้ Microsoft Visual Basic 2008 ในการพัฒนา ผลที่ได้จากการทำโครงงานนี้ คือ ได้โปรแกรมที่ใช้เข้าสู่ระบบปฏิบัติการ Windows โดยต้องเสียบ Flash drive ตัวที่กำหนด และใส่รหัสผ่าน ซึ่งสามารถป้องกันการเจาะระบบและจำกัดสิทธิ์การเข้าใช้ระบบปฏิบัติการ Windows ของบุคคลได้

Project Title	Two-Factor Authentication on Windows by Using Flash Drive and Password		
Name	Mr.Wasan	Luangruang	ID. 49361782
	Mr.Ekapong	Thingakrua	ID. 49362635
Project Advisor	Mr.Panupong	Sornkhom	
Major	Computer Engineering		
Department	Electrical and Computer Engineering		
Academic Year	2009		

.....

ABSTRACT

This project is developing Two-Factor Authentication on Windows by Using Flash Drive and Password to restrict the right of the computer case and increase the Security to the data. Has developed the program into the Windows operating system to plug the Flash drive and set password. Which act as intermediaries between users with Windows operating systems, Microsoft Visual Basic 2008 development program. The result of this project is a program that has access to the Windows operating system to plug the Flash drive and set password. That can prevent and limit penetration of the privileges of the Windows operating system personally.

กิตติกรรมประกาศ

โครงงานวิศวกรรมคอมพิวเตอร์สำเร็จได้ด้วยดีเนื่องด้วยความอนุเคราะห์จากอาจารย์ที่ปรึกษาโครงงาน คือ อาจารย์ ภาณุพงศ์ สอนคม ผู้ซึ่งกรุณาให้ความรู้คำแนะนำและเอาใจใส่เป็นอย่างดีระหว่างการดำเนินโครงงาน อีกทั้งยังตรวจสอบข้อบกพร่องต่างๆ จนโครงงานนี้เสร็จสมบูรณ์ คณะผู้จัดทำจึงขอขอบพระคุณเป็นอย่างสูงไว้ ณ ที่ นี้

ขอขอบคุณ ดร.สุรเดช จิตประไพกุลศาล และ อาจารย์เศรษฐา ตั้งค้าวานิช ที่กรุณามารับเป็นกรรมการตรวจสอบโครงงานและให้คำแนะนำ ตรวจสอบแก้ไขโครงงานให้สมบูรณ์ยิ่งขึ้น

ในโอกาสนี้ทางคณะผู้จัดทำโครงงานจึงขอขอบคุณทุกๆท่านที่มีส่วนร่วมช่วยทำให้โครงงานนี้ประสบความสำเร็จด้วยดี

คณะผู้จัดทำ

วสันต์ หลวงเรื่อง

เอกพงศ์ ทิงาเครือ

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญรูป

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของโครงงาน

การรักษาความปลอดภัยของระบบปฏิบัติการถือเป็นเรื่องที่มีความสำคัญเป็นอย่างยิ่ง เพราะจะเป็นการป้องกันข้อมูลในส่วนที่ไม่ต้องการเปิดเผย ไม่ให้ตกไปอยู่ในมือของผู้ที่ไม่หวังดี หรือป้องกันการถูกคุกคามจากโปรแกรมบางประเภท ดังนั้นเพื่อเป็นการป้องกันปัญหาดังกล่าวจึงต้องมีการกำหนดสิทธิการเข้าใช้ การใช้ชื่อผู้ใช้และรหัสผ่าน ในปัจจุบันนี้ไม่มีความปลอดภัยเพียงพอต่อการเข้าใช้ระบบ เนื่องจากความรู้และวิทยาการที่ก้าวหน้า ทำให้เกิดผู้ที่ต้องการจะเข้ามาละเมิดระบบต่างๆมีมากขึ้น ทำให้ชื่อผู้ใช้และรหัสผ่าน อาจจะถูกลักลอบขโมยข้อมูลได้ เพราะฉะนั้นจึงควรที่จะมีการยืนยันตัวตนอย่างอื่นเข้ามาร่วมด้วย จากการศึกษาเรื่องการพิสูจน์ตัวตนโดยใช้ PIN (Authentication by PIN) พบว่า PIN (Personal Identification Number) เป็นรหัสลับส่วนบุคคลที่ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบ ซึ่ง PIN ใช้อย่างแพร่หลายโดยเฉพาะการทำธุรกรรมทางด้านธนาคาร เช่น บัตร ATM และเครดิตการ์ดต่างๆ การใช้ PIN ทำให้มีความปลอดภัยมากขึ้น เนื่องจาก PIN จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่น ฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะ และถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น

ดังนั้น ทางคณะผู้จัดทำจึงมีความสนใจที่จะจัดทำ เรื่อง การพิสูจน์ตัวตนแบบ 2 เงื่อนไขบน Windows โดยใช้ Flash Drive และรหัสผ่าน เพื่อจำกัดสิทธิ์การเข้าใช้ระบบปฏิบัติการ Windows เพราะ Flash Drive เป็นอุปกรณ์ที่แพร่หลาย สะดวกในการพกพา ราคาถูก หาได้ง่าย

1.2 วัตถุประสงค์ของโครงงาน

1.2.1 เพื่อพัฒนาโปรแกรมเข้าสู่ระบบปฏิบัติการ Windows โดยต้องเสียบ Flash Drive ตัวที่กำหนด และใส่รหัสผ่าน ซึ่งเป็นการพิสูจน์ตัวตนแบบ 2 เงื่อนไข

1.3 ขอบข่ายของโครงงาน

1.3.1 พัฒนาโปรแกรมเข้าสู่ระบบปฏิบัติการ Windows โดยต้องเสียบ Flash Drive ตัวที่กำหนด และใส่รหัสผ่าน

1.3.2 พัฒนาโปรแกรมโดยใช้หลักการของ Microsoft Visual Basic

1.3.3 จัดทำรูปแบบของโปรแกรมให้ใช้งานได้ง่าย

1.4 แผนการดำเนินงาน

	หัวข้องาน	ก.ค. 2552	ส.ค. 2552	ก.ย. 2552	ต.ค. 2552	พ.ย. 2552	ธ.ค. 2552	ม.ค. 2553
1	เสนอหัวข้อโครงงาน	←→						
2	กำหนดปัญหา		←→					
3	ศึกษาค้นคว้าเกี่ยวกับทฤษฎีที่ใช้และวิธีการการเขียนโปรแกรม			←→				
4	ออกแบบและเขียนโปรแกรม				←→	←→		
5	ทดสอบแก้ไขและปรับปรุงโปรแกรม						←→	
6	สรุปผลและจัดทำเอกสาร							←→

1.5 ผลที่คาดว่าจะได้รับ

1.5.1 พัฒนาโปรแกรมการเข้าสู่ระบบปฏิบัติการ Windows โดยต้องเสียบ Flash Drive ตัวที่กำหนดและใส่รหัสผ่าน

1.5.2 พัฒนารูปแบบของโปรแกรมให้ใช้งานได้ง่าย

1.6 งบประมาณ

ค่าหนังสือ	1,000 บาท
ค่าจัดทำเอกสาร	800 บาท
ค่าซื้อ Flash Drive	200 บาท
รวมเป็นเงินทั้งหมดทั้งสิ้น	2,000 บาท

บทที่ 2
หลักการและทฤษฎี

หลักการและทฤษฎีที่ใช้ในการพัฒนาโปรแกรมเข้าสู่ระบบปฏิบัติการ Windows โดยต้องเสียบ Flash Drive ตัวที่กำหนด และใส่รหัสผ่านนั้น ทางผู้จัดทำได้ทำการศึกษาก่อนที่จะพัฒนาโปรแกรมขึ้นมา โดยมีหลักการและทฤษฎีต่างๆ ดังนี้

2.1 นิยามความมั่นคงปลอดภัยของข้อมูล

2.2 การพิสูจน์ตัวตน (Authentication)

2.3 *Microsoft Visual Basic*

สามารถอธิบายหลักการและทฤษฎีต่างๆ ที่ใช้ในการพัฒนาโปรแกรมเข้าสู่ระบบปฏิบัติการ Windows โดยต้องเสียบ Flash Drive ตัวที่กำหนด และใส่รหัสผ่าน ได้ดังต่อไปนี้

2.1 นิยามความมั่นคงปลอดภัยของข้อมูล

จุดประสงค์หลักของความปลอดภัยทางข้อมูล คือ

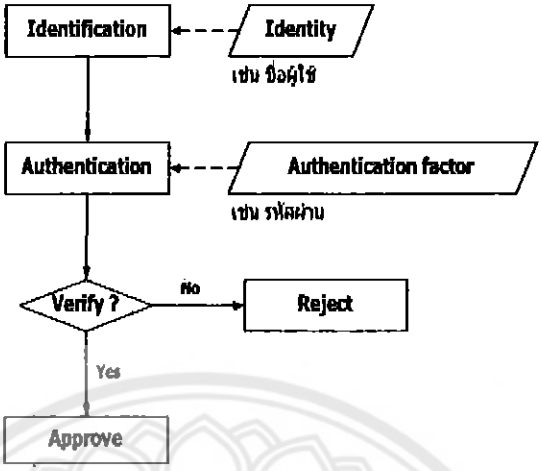
- **การรักษาความลับ (Confidentiality)** คือ การรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ และผู้มีสิทธิเท่านั้นจึงจะเข้าถึงข้อมูลนั้นได้
- **การรักษาความสมบูรณ์ (Integrity)** คือ การรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไม่ว่าจะเป็นโดย อุบัติเหตุหรือโดยเจตนา
- **ความพร้อมใช้ (Availability)** คือ การรับรองว่าข้อมูลและบริการการสื่อสารต่าง ๆ พร้อมที่จะใช้ได้ในเวลาที่ต้องการใช้งาน
- **การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation)** คือ วิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้น ทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

2.2 การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน คือ ขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

- การระบุตัวตน (Identification) คือ ขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใคร เช่น ชื่อผู้ใช้ (Username)

- การพิสูจน์ตัวตน (Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่า เป็นบุคคลที่กล่าวอ้างจริง



รูปที่ 2.1 ขั้นตอนการพิสูจน์ตัวตน

หลักฐานที่ผู้ใช้นำมากล่าวอ้างที่เกี่ยวกับเรื่องของความปลอดภัยนั้นสามารถจำแนกได้ 2 ชนิด

- Actual identity คือ หลักฐานที่สามารถบ่งบอกได้ว่าในความเป็นจริงบุคคลที่กล่าวอ้างนั้น เป็นใคร
- Electronic identity คือ หลักฐานทางอิเล็กทรอนิกส์ซึ่งสามารถบ่งบอกข้อมูลของบุคคลนั้นได้ แต่ละบุคคลอาจมีหลักฐานทางอิเล็กทรอนิกส์ได้มากกว่า 1 หลักฐาน

2.2.1 กลไกของการพิสูจน์ตัวตน (Authentication mechanisms)

ส่วนประกอบพื้นฐานของการพิสูจน์ตัวตนสมบูรณ์แบ่งได้เป็น 3 ส่วน คือ

- การพิสูจน์ตัวตน (Authentication) คือ ส่วนที่สำคัญที่สุดเพราะเป็นขั้นตอนแรกของการเข้าใช้ระบบ ผู้เข้าใช้ระบบต้องถูกยอมรับจากระบบว่าสามารถเข้าสู่ระบบได้ การพิสูจน์ตัวตนเป็นการตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลนั้นจริง
- การกำหนดสิทธิ์ (Authorization) คือ ข้อจำกัดของบุคคลที่เข้ามาในระบบ ว่าบุคคลคนนั้นสามารถทำอะไรกับระบบได้บ้าง
- การบันทึกการใช้งาน (Accountability) คือ การบันทึกรายละเอียดของการใช้ระบบ และ รวมถึงข้อมูลต่างๆที่ผู้ใช้กระทำลงไปในระบบ เพื่อผู้ตรวจสอบจะได้ตรวจสอบได้ว่า ผู้ใช้ที่เข้ามาใช้บริการได้เปลี่ยนแปลงหรือแก้ไขข้อมูลในส่วนใดบ้าง

2.2.2 การกำหนดสิทธิ์ (Authorization)

การกำหนดสิทธิ์ คือ ขั้นตอนในการอนุญาตให้แต่ละบุคคลสามารถเข้าถึงข้อมูลหรือระบบใดได้บ้าง ก่อนอื่นต้องทราบก่อนว่าบุคคลที่กล่าวอ้างนั้นคือใคร ตามขั้นตอนการพิสูจน์ตัวตนและต้องให้แน่ใจด้วยว่าการพิสูจน์ตัวตนนั้นถูกต้อง

2.1.3 การเข้ารหัส (Encryption)

การเข้ารหัส คือ การเก็บข้อมูลให้เป็นส่วนบุคคลจากบุคคลอื่นที่ไม่ได้รับอนุญาต ส่วนประกอบ 2 ส่วนที่สำคัญที่จะช่วยทำให้ข้อมูลนั้นเป็นความลับได้ก็ คือ การกำหนดสิทธิ์และการพิสูจน์ตัวตนเพราะว่าก่อนการอนุญาตให้บุคคลที่กล่าว อ้างเข้าถึงข้อมูลหรือถอดรหัสข้อมูลนั้นต้องสามารถแน่ใจได้ว่าบุคคลที่กล่าว อ้างนั้นเป็นใครและได้รับอนุญาตให้สามารถเข้ามาดูข้อมูลได้หรือไม่ ในการเข้ารหัสนั้นวิธีการหนึ่งที่ทำได้คือการเข้ารหัสในรูปแบบของกุญแจลับ (Secret key) ซึ่งในการใช้คีย์รูปแบบนี้ต้องเฉพาะผู้ที่มีกุญแจลับนี้เท่านั้นที่สามารถ รับข้อมูลที่เข้ารหัสแล้วได้

2.4 การรักษาความสมบูรณ์ (Integrity)

การรักษาความสมบูรณ์ คือ การรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไปจากต้นฉบับ (Source) ไม่ว่าจะเป็นโดยบังเอิญหรือดัดแปลงโดยเจตนาที่อาจส่งผลเสียต่อข้อมูล การคุกคามความสมบูรณ์ของข้อมูลคือการที่บุคคลที่ไม่ได้รับอนุญาตสามารถที่จะ เข้าควบคุมการจัดการของข้อมูลได้

2.5 การตรวจสอบ (Audit)

การตรวจสอบ คือ การตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ ซึ่งสามารถใช้ในการติดตามการดำเนินการเพื่อตรวจสอบความถูกต้องและแม่นยำ ตัวอย่างเช่น การตรวจสอบบัญชีชื่อผู้ใช้ โดยผู้ตรวจบัญชี ซึ่งการตรวจสอบความถูกต้องของการดำเนินการเพื่อให้แน่ใจว่าหลักฐานทางอิเล็กทรอนิกส์นั้นได้ถูกสร้างและสั่งให้ทำงานโดยบุคคลที่ได้รับอนุญาต และในการเชื่อมต่อเหตุการณ์เข้ากับบุคคลจะต้องทำการตรวจสอบหลักฐานของบุคคล นั้นด้วย ซึ่งถือเป็นหลักการพื้นฐานของขั้นตอนการทำงานของการพิสูจน์ตัวตนด้วย

2.6 ประเภทของการพิสูจน์ตัวตน (Authentication Types)

ประเภทของการพิสูจน์ตัวตน สามารถแบ่งออกได้เป็น 3 คุณลักษณะ คือ

2.6.1 สิ่งที่คุณรู้ (Knowledge factor)

2.6.1.1 การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Authentication by Passwords)

รหัสผ่านเป็นวิธีการที่ใช้มานานและนิยมใช้กันแพร่หลาย รหัสผ่านควรจำกัดให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นที่ทราบแต่ว่าในปัจจุบันนี้ การใช้แค่รหัสผ่านไม่มีประสิทธิภาพมากพอที่จะรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ เนื่องจากการตั้งรหัสผ่านที่ง่ายเกินไป และวิทยาการและความรู้ที่ก้าวหน้าทำให้รหัสผ่านอาจจะถูกขโมยโดยระหว่างการสื่อสารผ่านเครือข่ายได้

2.6.1.2 การพิสูจน์ตัวตนโดยใช้ Password Authenticators หรือ Tokens (Authentication by Password Authenticators or Tokens)

Authenticator หรือ Token เป็นฮาร์ดแวร์พิเศษที่ใช้สร้าง "รหัสผ่านซึ่งเปลี่ยนแปลงได้ (dynamic password)" ในขณะที่กำลังเข้าสู่ระบบเครือข่าย มี 2 วิธี คือ ซิงโครนัส และ อะซิงโครนัส

การพิสูจน์ตัวตนแบบซิงโครนัส แบ่งออกเป็น 2 ประเภทตามลักษณะของการใช้งาน คือ

- การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับสถานการณ์ (Event-synchronous authentication) เมื่อผู้ใช้ต้องการที่จะเข้าสู่ระบบ ผู้ใช้จะต้องกด Token เพื่อให้ Token สร้างรหัสผ่านให้ จากนั้นผู้ใช้นำรหัสผ่านที่แสดงหลังจากกด Token ใส่ลงในฟอร์มเพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบกับเซิร์ฟเวอร์ก่อน ว่ารหัสผ่านที่ใส่มีอยู่ในเซิร์ฟเวอร์จริง จึงจะยินยอมให้ผู้ใช้เข้าสู่ระบบ
- การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับเวลา (Time-synchronous authentication) เป็นวิธีการที่สร้างรหัสผ่านโดยมีการกำหนดช่วงระยะเวลาการใช้งาน โดยปกติแล้วรหัสผ่านจะถูกเปลี่ยนทุกๆ หนึ่งนาที การสร้างรหัสผ่านจะเป็นไปอย่างต่อเนื่อง ทำให้บางครั้งรหัสผ่านที่สร้างออกมาอาจจะซ้ำกันกับรหัสผ่านตัวอื่นที่เคยสร้างมาแล้วก็ได้ เมื่อผู้ใช้ต้องการเข้าสู่ระบบก็ใส่รหัสผ่านและเวลาที่รหัสผ่านตัวนั้นถูกสร้างขึ้นมา (รหัสผ่านจะถูกสร้างขึ้นมาจาก Token) ลงในฟอร์ม เพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบเวลาและรหัสผ่านที่ผู้ใช้ใส่ลงไป กับเซิร์ฟเวอร์ว่ารหัสผ่านที่ใส่ตรงกับเวลาที่ Token สร้าง และมีอยู่ในเซิร์ฟเวอร์จริง จึงยินยอมให้ผู้ใช้เข้าสู่ระบบ

การพิสูจน์ตัวตนแบบอะซิงโครนัส หรือเรียกอีกอย่างหนึ่งว่า "challenge-response" ถูกพัฒนาขึ้น เป็นลำดับแรกๆ ของระบบการใช้ "รหัสผ่านซึ่งเปลี่ยนแปลงได้" ซึ่งถือได้ว่าเป็นการป้องกันการจู่โจมที่ปลอดภัยที่สุด เพราะเนื่องจากว่าเมื่อผู้ใช้ต้องการจะเข้าสู่ระบบ ผู้ใช้จะต้องทำ

การร้องขอไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์ก็จะส่ง challenge string มาให้ผู้ใช้ เพื่อให้ผู้ใช้ใส่ลงใน Token ที่ผู้ใช้ถืออยู่ จากนั้น Token จะทำการคำนวณรหัสผ่านออกมาให้ผู้ใช้ ผู้ใช้จึงสามารถนำรหัสผ่านนั้นใส่ลงในฟอร์มเพื่อเข้าสู่ระบบได้

การพิสูจน์ตัวตนแบบซิงโครนัสทั้งไคลเอ็นต์และเซิร์ฟเวอร์จะมีรหัสผ่านเก็บเอาไว้ แต่แบบอะซิงโครนัส ไคลเอ็นต์จะต้องติดต่อเซิร์ฟเวอร์ก่อน ก่อนจะได้รับรหัสผ่านจริง ทำให้การพิสูจน์ตัวตนแบบอะซิงโครนัสมีขั้นตอนที่ซับซ้อนกว่าแบบซิงโคนัส

ตัวอย่างของฮาร์ดแวร์พิเศษที่ใช้ในการสร้างรหัสผ่านซึ่งเปลี่ยนแปลงได้ ของการพิสูจน์ตัวตนโดยใช้ Password authenticator หรือ token

รูปที่ 2.2 ตัวอย่างของฮาร์ดแวร์พิเศษที่ใช้ในการสร้างรหัสผ่านซึ่งเปลี่ยนแปลงได้

2.6.1.3 การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว (One-Time Password: OTP)

One-Time Password ถูกพัฒนาขึ้นเพื่อหลีกเลี่ยงปัญหาที่เกิดจากการใช้รหัสผ่านเพียงตัวเดียวซ้ำๆกัน OTP จะทำให้ระบบมีความปลอดภัยมากขึ้น เพราะรหัสผ่านจะถูกเปลี่ยนทุกครั้งก่อนที่ผู้ใช้จะเข้าสู่ระบบ

การทำงานของ OTP คือ เมื่อผู้ใช้ต้องการจะเข้าใช้ระบบ ผู้ใช้จะทำการร้องขอไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์จะส่ง challenge string กลับมาให้ผู้ใช้ จากนั้นผู้ใช้จะนำ challenge string และรหัสลับที่มีอยู่กับตัวของผู้ใช้นำไปเข้า Hash ฟังก์ชันแล้วออกมาเป็นค่า response ผู้ใช้ก็จะส่งค่านั้นกลับไปยังเซิร์ฟเวอร์ เซิร์ฟเวอร์จะทำการตรวจสอบค่าที่ผู้ใช้ส่งมาเปรียบเทียบกับค่าที่เซิร์ฟเวอร์เองคำนวณได้ โดยเซิร์ฟเวอร์ก็ใช้วิธีการคำนวณเดียวกันกับผู้ใช้ เมื่อได้ค่าที่ตรงกันเซิร์ฟเวอร์ก็จะยอมรับให้ผู้ใช้เข้าสู่ระบบ

2.6.1.4 การพิสูจน์ตัวตนโดยใช้การถาม - ตอบ (Zero-knowledge proofs)

เป็นวิธีการพิสูจน์ตัวตนโดยใช้การถาม - ตอบ เมื่อผู้ใช้เข้ามาในระบบแล้ว ระบบจะแน่ใจได้อย่างไรว่าผู้ใช้คนนั้น เป็นคนที่ได้รับอนุญาตให้เข้ามาใช้ระบบได้จริง การใช้ชื่อผู้ใช้และรหัสผ่าน ในปัจจุบันนี้ไม่มีความปลอดภัยเพียงพอต่อการเข้าใช้ระบบ เนื่องจากความรู้และวิทยาการที่ก้าวหน้า ทำให้เกิดผู้ที่ต้องการจะเข้ามาละเมิดระบบต่างๆมีมากขึ้น ทำให้ชื่อผู้ใช้และรหัสผ่าน อาจจะถูกลักลอบดักข้อมูลระหว่างการสื่อสารกันได้

การที่จะทำให้ระบบมั่นใจได้ว่า ผู้ที่เข้าไปในระบบผู้นั้นเป็นผู้ที่ได้รับอนุญาตจริง นั่นก็คือระบบจะใช้การถาม - ตอบ ซึ่งคำถามและคำตอบเหล่านี้ ผู้ใช้จะเป็นคนสร้างคำถามและคำตอบขึ้นมาเอง จากนั้นจะส่งให้กับเซิร์ฟเวอร์ ซึ่งคำถาม - คำตอบที่ผู้ใช้สร้างขึ้นมา ผู้ใช้เท่านั้นจะเป็นคนที่ทราบคำตอบของแต่ละคำถามที่ถูกสร้าง และเมื่อผู้ใช้คนนั้นๆเข้าสู่ระบบได้ ระบบจะถามสุ่มคำถามเหล่านั้นที่ผู้ใช้คนนั้นๆ สร้างขึ้นมา ถามผู้ใช้คนนั้นๆก่อนที่จะยอมให้เข้าใช้ระบบได้จริง การให้ใช้ระบบได้จริงจะได้รับการยินยอมก็ต่อเมื่อการตอบคำตอบที่ผู้ใช้ตอบ นั้นสัมพันธ์กับคำตอบที่มีอยู่ในเซิร์ฟเวอร์ ยกตัวอย่างเช่น นาย ก. กับ นาย ข. รู้จักกันมานานและสนิทกัน นาย ก. และ นาย ข. ย่อมมีความสนิทกันเป็นส่วนตัวเมื่อนาย ก. และนาย ข. เล่น MSN กัน ต่างฝ่ายต่างจะแน่ใจได้อย่างไรว่า คนที่ตนคุยอยู่เป็นบุคคลเดียวกันกับที่ตนรู้จัก เพราะว่านาย ก. หรือ นาย ข. อาจจะทำการเข้าระบบทิ้งไว้ หรือ อาจจะมีบุคคลอื่นสามารถดักจับหลักฐานและข้อมูลที่สามารถเข้าสู่ระบบของคนใดคนหนึ่งไว้ได้ แล้วทำการสวมรอยแทน นั่นก็คือการใช้คำถามและคำตอบที่มีเพียงนาย ก. และ นาย ข. เท่านั้นที่ทราบ

2.6.1.5 การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ(Public-key cryptography)

เป็นการรักษาความปลอดภัยของข้อมูลระหว่างการส่งข้ามเครือข่ายวิธีหนึ่งที่นิยมใช้กันอยู่ในปัจจุบัน การเข้ารหัสแบบคู่รหัสกุญแจนี้จะมีความปลอดภัยมากกว่าการเข้ารหัสข้อมูลแบบธรรมดา แต่ก็ไม่ได้หมายความว่าการเข้ารหัสแบบคู่รหัสกุญแจนี้จะเป็นวิธีที่เหมาะสมที่สุดของวิธีการเข้ารหัส ทั้งนี้ขึ้นอยู่กับประเภทงานของแต่ละองค์กรหรือบุคคลการเข้ารหัสโดยใช้กุญแจสาธารณะ ประกอบไปด้วยกุญแจ 2 ชนิด ที่ต้องใช้คู่กันเสมอในการเข้ารหัสและถอดรหัส คือ

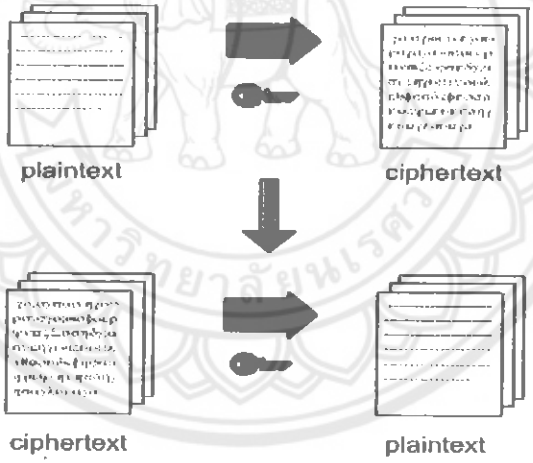
- กุญแจสาธารณะ (Public key) เป็นกุญแจที่ผู้สร้างจะส่งออกไปให้ผู้ใช้อื่นๆ ทราบหรือเปิดเผยได้
- กุญแจส่วนตัว (Private key) เป็นกุญแจที่ผู้สร้างจะเก็บไว้ โดยไม่เปิดเผยให้คนอื่นรู้

กระบวนการของการเข้ารหัสแบบคู่รหัสกุญแจ มีดังนี้

1. ผู้ใช้แต่ละคนจะสร้างคู่รหัสกุญแจของตัวเองขึ้นมา เพื่อใช้สำหรับการเข้ารหัสและการถอดรหัส
2. กุญแจสาธารณะจะถูกส่งออกไปยังผู้ใช้คนอื่นๆ แต่กุญแจส่วนตัวจะถูกเก็บที่ตนเอง
3. เมื่อจะส่งข้อมูลออกไปหาผู้ใช้คนใด ข้อมูลที่ส่งจะถูกเข้ารหัสด้วยกุญแจสาธารณะก่อนถูกส่งออกไป
4. เมื่อผู้รับได้รับข้อความแล้วจะใช้กุญแจส่วนตัวซึ่งเป็นคู่รหัสกันถอดรหัสออกมา

การเข้ารหัสโดยใช้กุญแจสาธารณะสามารถใช้ได้ทั้งในการเข้ารหัส (Encryption) และการพิสูจน์ตัวตน (Authentication)

การประยุกต์ใช้ในการเข้ารหัสข้อมูล (Encryption) เป็นการนำข้อมูลที่จะส่งไปยังผู้รับมาเข้ารหัสด้วยกุญแจสาธารณะของผู้รับ และเมื่อผู้รับได้รับข้อความนั้นแล้วจะถอดรหัสออกมาด้วยกุญแจส่วนตัว จึงจะเห็นได้ว่ามีเพียงผู้รับเท่านั้นที่จะสามารถถอดรหัสออกมาได



รูปที่ 2.3 การเข้ารหัสโดยใช้กุญแจสาธารณะ

2.6.2 สิ่งที่คุณมี (Possession factor)

2.6.2.1 การพิสูจน์ตัวตนโดยใช้ PIN (Authentication by PIN)

PIN (Personal Identification Number) เป็นรหัสลับส่วนบุคคลที่ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบ ซึ่ง PIN ใช้อย่างแพร่หลายโดยเฉพาะการทำธุรกรรมทางด้านธนาคาร เช่น บัตร ATM และเครดิตการ์ดต่างๆ การใช้ PIN ทำให้มีความปลอดภัยในการสื่อสารข้ามระบบเครือข่ายสาธารณะ

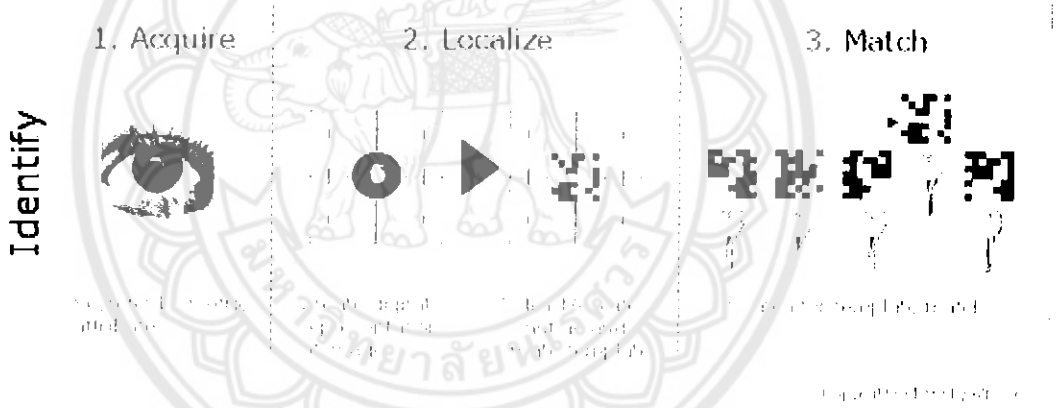
มากขึ้น เนื่องจาก PIN จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่น ฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะและถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น

2.6.3 สิ่งที่คุณเป็น (Biometric factor)

2.6.3.1 การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล (Authentication by Biometric traits)

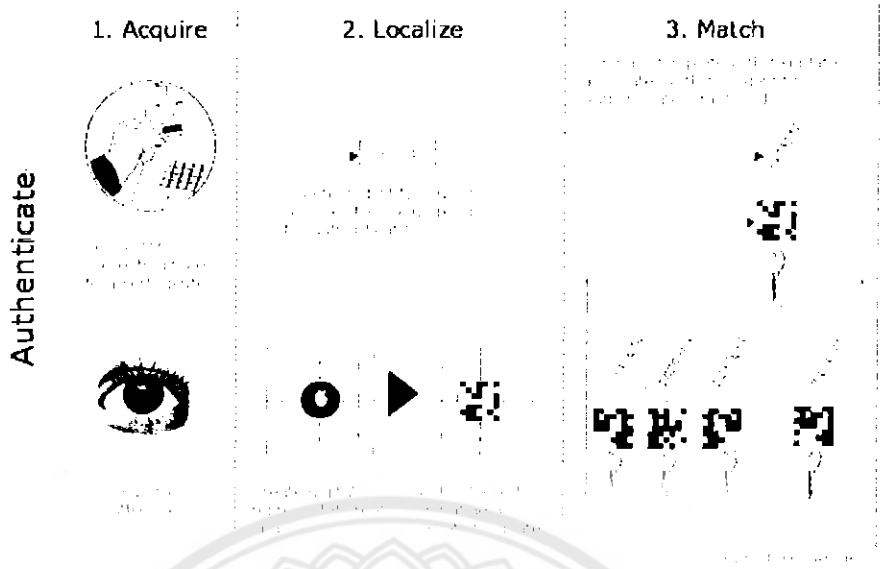
ลักษณะทางชีวภาพของแต่ละบุคคลเป็นลักษณะเฉพาะและลอกเลียนแบบกันไม่ได้ การนำมาใช้ในการพิสูจน์ตัวตนจะเพิ่มความน่าเชื่อถือได้มากขึ้น เช่น การใช้ลายนิ้วมือ เสียง ม่านตา เป็นต้น จึงมีการนำเทคโนโลยีนี้มาช่วยในการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยก่อนเข้าสู่ระบบ เช่น การใช้ควบคู่กับการใช้รหัสผ่าน

ตัวอย่างการใช้งานของการพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพร่วมกับการใช้ token การ์ด หรือสมาร์ทการ์ด



รูปที่ 2.4 ขั้นตอนการพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพ

ในขั้นตอนของการเก็บหลักฐานทางชีวภาพ จากตัวอย่างของรูป ในขั้นแรกระบบจะทำการเก็บภาพของเรตินาจากบุคคลที่ถือ Token การ์ดหรือสมาร์ทการ์ด จากนั้นจะนำภาพเรตินาที่ได้มาแยกแยะเพื่อหาลักษณะเด่นของแต่ละบุคคลเพื่อไม่ให้ซ้ำกับบุคคลอื่น แล้วเก็บไว้เป็น template ซึ่ง template ที่ได้จะถูกบันทึกเป็นกุญแจคู่กับรหัสผ่านที่มีอยู่ใน token การ์ด หรือสมาร์ทการ์ดของแต่ละบุคคล



รูปที่ 2.5 ขั้นตอนของการตรวจสอบหลักฐานทางชีวภาพร่วมกับการใช้ Token การ์ด

ในขั้นตอนของการตรวจสอบหลักฐาน ผู้ใช้ที่ถือ Token การ์ด หรือ สมาร์ทการ์ด จะนำบัตรมาผ่านเครื่องอ่านบัตรและแสดงเรตินาให้เครื่องเก็บภาพ เมื่อเครื่องอ่านบัตร อ่านค่าเลขที่ได้จากบัตรแล้ว ก็จะนำไปหากุญแจ ซึ่งในขณะเดียวกันภาพเรตินาที่เครื่องเก็บไว้ได้ ก็จะนำไปแยกแยะเพื่อหาลักษณะเด่น แล้วเก็บค่าไว้เป็น template และนำ template ที่ได้ไปตรวจสอบกับ template ที่เก็บไว้เพื่อหากุญแจ และนำกุญแจที่ได้มาเปรียบเทียบกันว่าตรงกันหรือไม่ ถ้าตรงกันก็แสดงว่าผู้ที่ถือบัตรกับผู้ใช้เป็นคนเดียวกัน จึงอนุญาตให้เข้าสู่ระบบได้

2.3 Microsoft Visual Basic

Microsoft Visual Basic หรือที่เรียกสั้นๆ ว่า VB ซึ่งเป็นเครื่องมือที่ช่วยให้การพัฒนาซอฟต์แวร์ต่าง ๆ เป็นไปได้อย่างรวดเร็ว รวมทั้งสามารถพัฒนาซอฟต์แวร์ได้หลายอย่างด้วยกัน ตั้งแต่โปรแกรมธรรมดาทั่วไปจนถึงโปรแกรมเกี่ยวกับฐานข้อมูล หรือโปรแกรมทางอินเตอร์เน็ต เป็นต้น

สำหรับ VB เป็นเครื่องมือในการสร้างโปรแกรมบนระบบปฏิบัติการ Windows ที่ใช้งานง่าย โดยการสร้างโปรแกรมใน VB นั้น จะเป็นการเลือกเครื่องมือต่าง ๆ มาออกแบบหน้าจอของโปรแกรมที่เราจะสร้าง ซึ่งเราเรียกการเขียนโปรแกรมลักษณะนี้ว่า Visual Programming การเขียนโปรแกรมแบบนี้ เราจะไม่จำเป็นต้องเขียนคำสั่งต่าง ๆ มาก ก็สามารถสร้างโปรแกรมได้อย่างง่ายดายและรวดเร็ว

โปรแกรม Visual Basic เป็นโปรแกรมที่ได้เปลี่ยนรูปแบบการเขียนโปรแกรมใหม่ โดยมีชุดคำสั่งมาสนับสนุนการทำงาน มีเครื่องมือต่าง ๆ ที่เรียกกันว่า คอนโทรล (Controls) ไว้สำหรับช่วยในการออกแบบโปรแกรม โดยเน้นการออกแบบหน้าจอแบบกราฟฟิก หรือที่เรียกว่า Graphic User Interface (GUI) ทำให้การจัดรูปแบบหน้าจอเป็นไปได้ง่าย และในการเขียนโปรแกรมนั้นจะเขียนแบบ Event - Driven Programming คือ โปรแกรมจะทำงานก็ต่อเมื่อเหตุการณ์ (Event) เกิดขึ้น ตัวอย่างของเหตุการณ์ได้แก่ ผู้ใช้เลื่อนเมาส์ ผู้ใช้กดปุ่มบนคีย์บอร์ด ผู้ใช้กดปุ่มเมาส์ เป็นต้น เครื่องมือ หรือ คอนโทรล ต่าง ๆ ที่ Visual Basic ได้เตรียมไว้ให้ ไม่ว่าจะเป็น Form TextBox Label เป็นต้น ถือว่าเป็นวัตถุ (Object ในที่นี้ขอใช้คำว่า ออบเจ็กต์) นั่นหมายความว่า ไม่ว่าจะเป็นเครื่องมือใด ๆ ใน Visual Basic จะเป็นออบเจ็กต์ทั้งสิ้น สามารถที่จะควบคุมการทำงาน แก้ไขคุณสมบัติของออบเจ็กต์นั้นได้โดยตรง ในทุกๆ ออบเจ็กต์จะมีคุณสมบัติ (properties) และเมธอด (Methods) ประจำตัว ซึ่งในแต่ละออบเจ็กต์ อาจจะมีคุณสมบัติและเมธอดที่เหมือน หรือต่างกันก็ได้ ขึ้นอยู่กับชนิดของออบเจ็กต์

ในการพัฒนาโปรแกรมประยุกต์ด้วย Visual Basic การเขียนโค้ดจะถูกแบ่งออกเป็นส่วนๆ เรียกว่า โพรซีเดอร์ (procedure) แต่ละโพรซีเดอร์จะประกอบไปด้วย ชุดคำสั่งที่พิมพ์เข้าไปแล้ว ทำให้คอนโทรลหรือออบเจ็กต์นั้น ๆ ตอบสนองการกระทำของผู้ใช้ ซึ่งเรียกว่าการเขียนโปรแกรมเชิงวัตถุ (Object Oriented Programming-OOP) แต่ตัวภาษา Visual Basic ยังไม่ถือว่าเป็นการเขียนโปรแกรมแบบ OOP อย่างแท้จริง เนื่องจากข้อจำกัดหลายๆ อย่างที่ Visual Basic ไม่สามารถทำได้

บทที่ 3
วิธีการดำเนินการ

วิธีการพัฒนาโปรแกรมการเข้าสู่ระบบ Windows โดยต้องเสียบ Flash Drive ตัวที่กำหนดและใส่รหัสผ่าน เราจะดำเนินการพัฒนาโดยใช้โปรแกรม Microsoft Visual Studio 2008 โดยในบทนี้จะอธิบายถึงหลักการและวิธีการพัฒนาโปรแกรม

3.1 ศึกษาปัญหา

การใช้คอมพิวเตอร์ที่มีผู้ใช้หลายคนอาจมีปัญหาในด้านการรักษาความปลอดภัย ทำให้เกิดความไม่ปลอดภัยของข้อมูล ซึ่งการใช้แค่รหัสผ่านอย่างเดียวอาจจะยังไม่เพียงพอ เพราะอาจจะเกิดการที่รหัสผ่านรั่วไหล จึงได้มีแนวคิดที่จะนำ Flash Drive เข้ามามีส่วนร่วมในการยืนยันตัวตนเพื่อทำให้เกิดความปลอดภัยมากขึ้น โดยเริ่มพัฒนาดังนี้

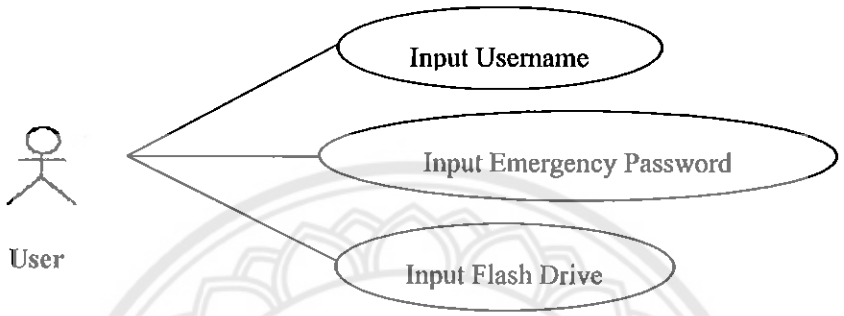
- ในตอนแรกโปรแกรมจะตรวจสอบ Flash Drive ว่ามีข้อมูลในไฟล์ที่กำหนดไว้ใน Flash Drive หรือไม่
- ภายหลังพบว่าไฟล์นั้นอาจถูก Copy ได้ จึงเปลี่ยนเป็นตรวจสอบวันที่ สร้างไฟล์และข้อมูลที่กำหนดไว้ใน Flash Drive
- ต่อมาพัฒนาเป็นโปรแกรม 2 โปรแกรมย่อย คือ โปรแกรม Create Key Flash Drive สำหรับสร้างไฟล์ที่เข้ารหัสให้กับ Flash Drive และโปรแกรม Check Flash Drive สำหรับตรวจสอบและถอดรหัสไฟล์ของ Flash Drive เพื่อง่ายในการใช้งาน

ข้อมูลที่จะเก็บไว้ในไฟล์ คือ Username ที่ Login, วันที่สร้างไฟล์, ขนาดของ Flash Drive, ชื่อของ Flash Drive, ชนิดของ Flash Drive และ ประเภท Flash Drive ซึ่งจะนำไปใช้ในโปรแกรม Check Flash Drive

3.2 การออกแบบโปรแกรม

โปรแกรมการเข้าสู่ระบบ Windows โดยต้องเสียบ Flash Drive ตัวที่กำหนด และใส่รหัสผ่าน จะประกอบด้วยโปรแกรมย่อย 2 โปรแกรม คือ โปรแกรม Create Key Flash Drive และโปรแกรม Check Flash Drive

3.2.1 Use case diagram ของโปรแกรม Create Key Flash Drive

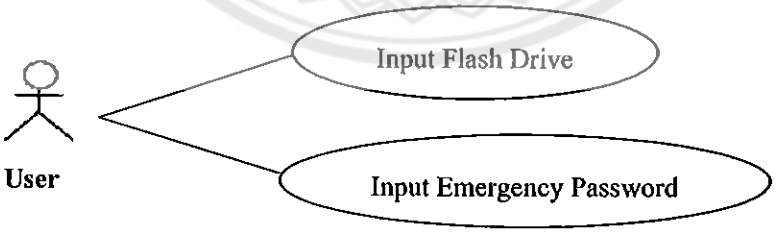


รูปที่ 3.1 Use case diagram Create Key Flash Drive

การติดต่อกับผู้ใช้ของ โปรแกรม Create Key Flash Drive มี 3 ขั้นตอนคือ

1. ผู้ใช้ใส่ Username ที่ต้องการสร้างให้กับระบบ
2. ผู้ใช้ใส่รหัสผ่านฉุกเฉิน
3. ผู้ใช้เสียบ Flash Drive

3.2.2 Use case diagram ของโปรแกรม Check Flash Drive



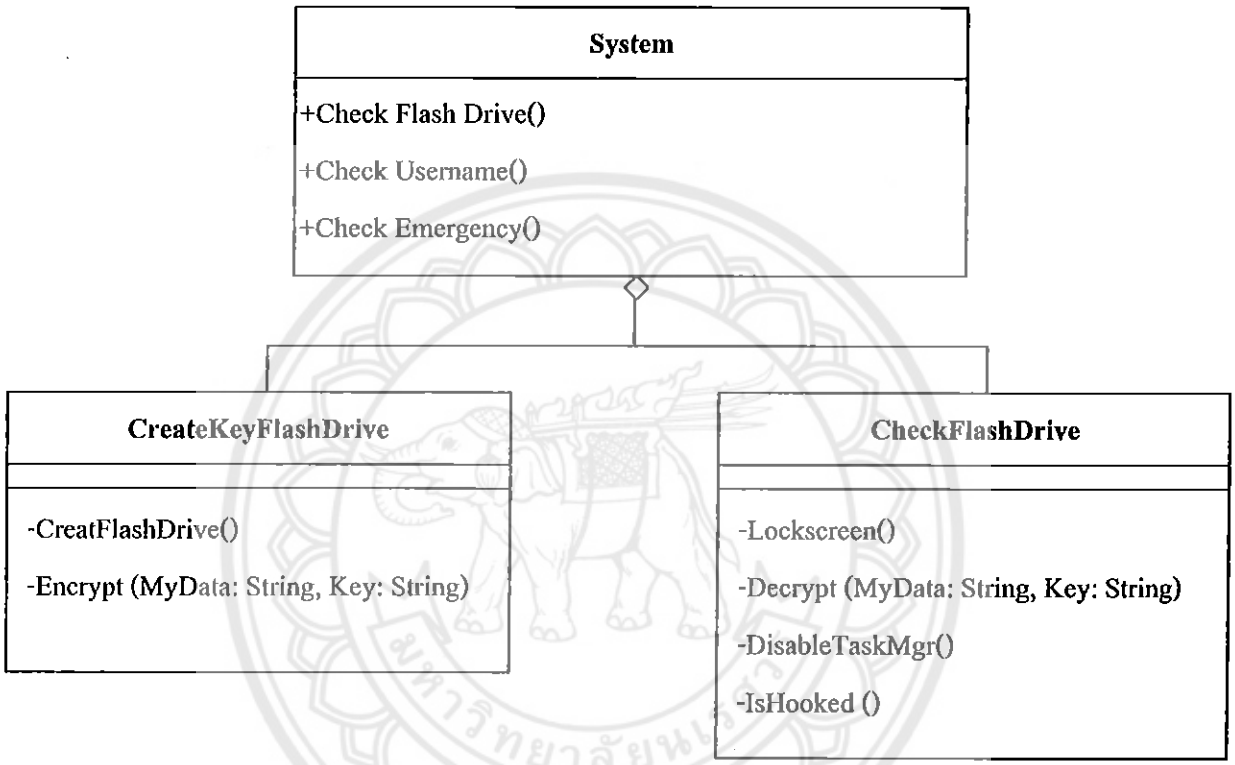
รูปที่ 3.2 Use case diagram Check Flash Drive

การติดต่อกับผู้ใช้ของโปรแกรม Check Flash Drive มี 2 ขั้นตอนคือ

1. ผู้ใช้เสียบ Flash Drive
2. ผู้ใช้ใส่รหัสผ่านฉุกเฉิน กรณีลืม Flash Drive

3.2.3 Class Diagram

จาก Use Case Diagram เราได้นำ Use Case มาวิเคราะห์เป็นรูปแบบของ Class และนำมาสร้างเป็นแผนภาพ Class Diagram ดังรูปที่ 3.3



รูปที่ 3.3 Class Diagram

- **Class System**

  เป็น Class หลักของโปรแกรม ประกอบไปด้วยฟังก์ชั่นต่างๆ ดังนี้

  - Check Flash Drive() เป็นฟังก์ชั่นที่ใช้ในการตรวจสอบว่ามีการเสียบ Flash Drive หรือไม่
  - Check Username() เป็นฟังก์ชั่นที่ใช้ในการตรวจสอบว่ามีการใส่ Username ให้กับระบบแล้วหรือไม่
  - Check Emergency( )เป็นฟังก์ชั่นที่ใช้ในการตรวจสอบว่ามีการใส่รหัสผ่านฉุกเฉินให้กับระบบแล้วหรือไม่

- **Class CreateKeyFlashDrive**

  เป็น Class ที่ใช้สร้างไฟล์ให้กับ Flash Drive และติดตั้งโปรแกรม ประกอบไปด้วยฟังก์ชั่นต่างๆ ดังนี้

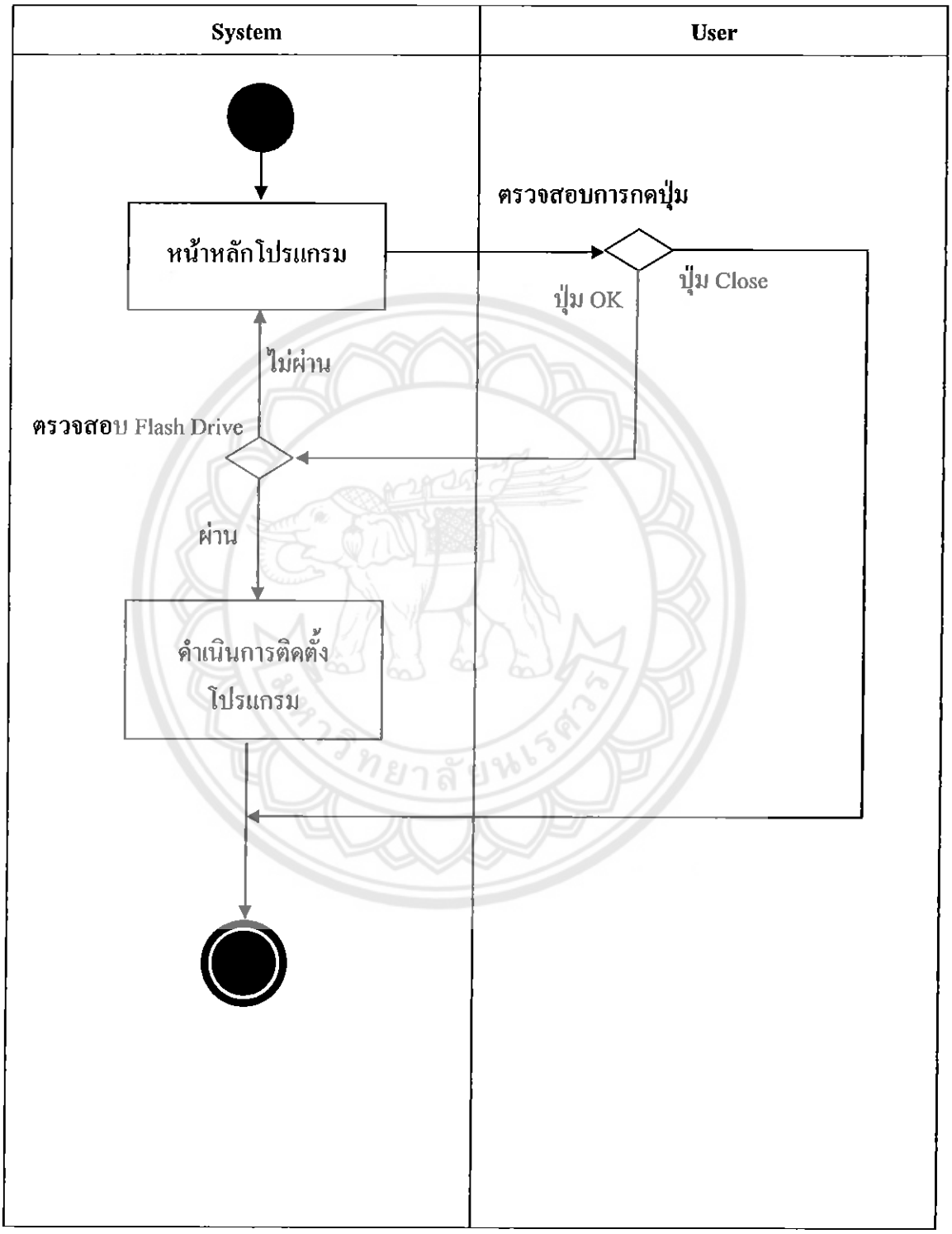
  - CreatFlashDrive() เป็นฟังก์ชั่นที่ใช้ในการสร้างไฟล์ที่ถูกเข้ารหัสให้กับ Flash Drive และติดตั้งโปรแกรมลงไปในระบบปฏิบัติการ
  - Encrypt (MyData: String, Key: String) เป็นฟังก์ชั่นในการเข้ารหัสแบบ XOR

- **Class CheckFlashDrive**

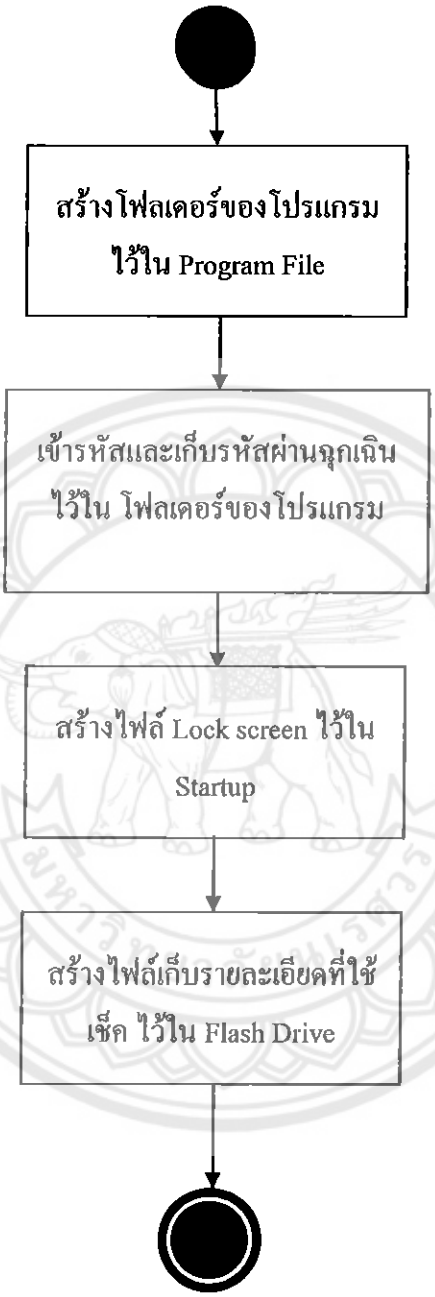
  เป็น Class ที่ใช้ตรวจสอบไฟล์ใน Flash Drive ประกอบไปด้วยฟังก์ชั่นต่างๆ ดังนี้

  - Lockscreen() เป็นฟังก์ชั่นที่ใช้ในการตรวจสอบไฟล์ที่ถูกเข้ารหัสและถอดรหัส
  - Decrypt (MyData: String, Key: String) เป็นฟังก์ชั่นที่ใช้ในการถอดรหัสแบบ XOR
  - DisableTaskMgr()() เป็นฟังก์ชั่นที่ใช้ในการ ไม่ให้ Task Manager ทำงานได้
  - IsHooked () เป็นฟังก์ชั่นที่ใช้ในการล็อคการกดปุ่มบน Keyboard

3.2.4 Activity diagram ของ โปรแกรม Create Key Flash Drive

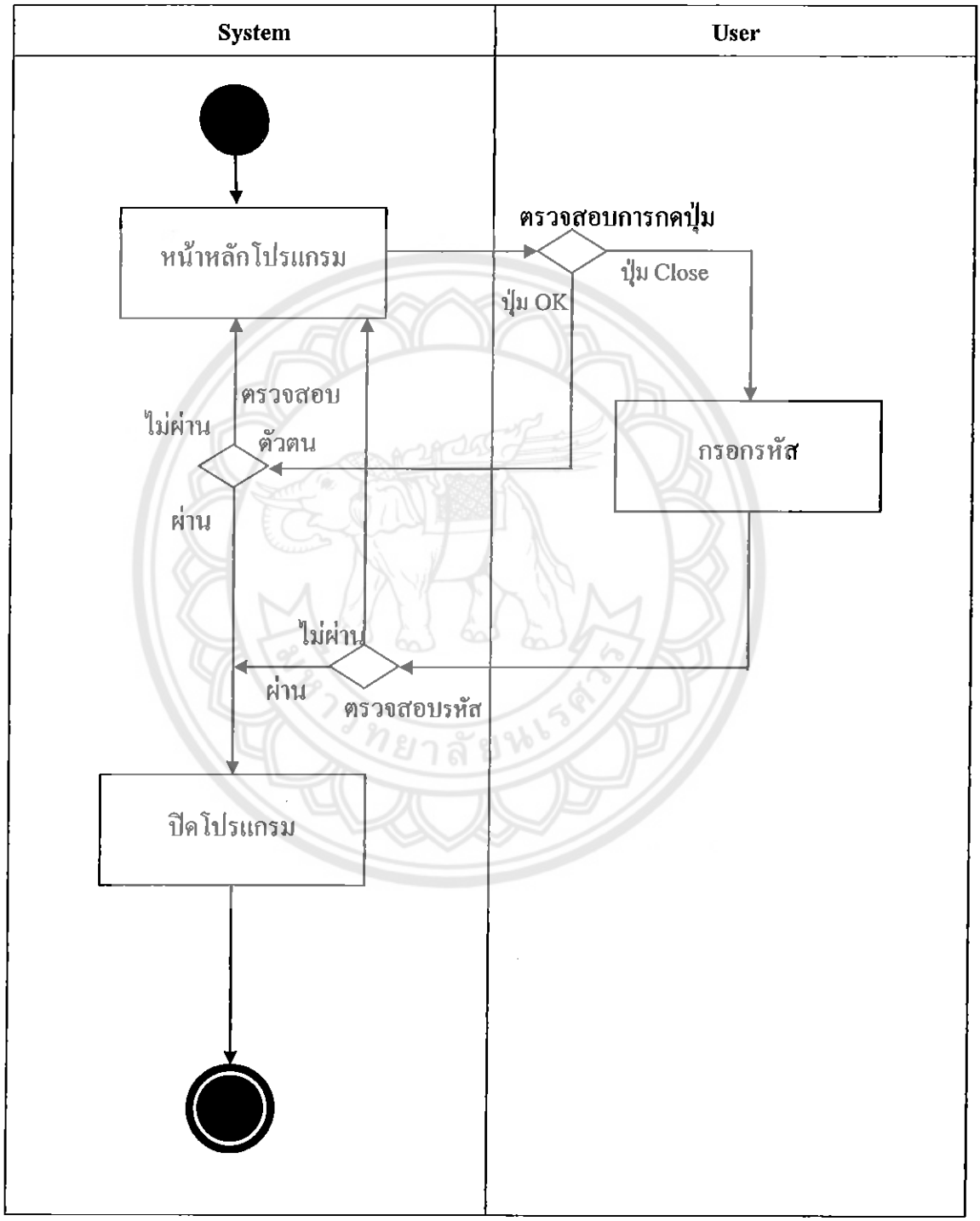


รูปที่ 3.4 Activity diagram Create Key Flash Drive

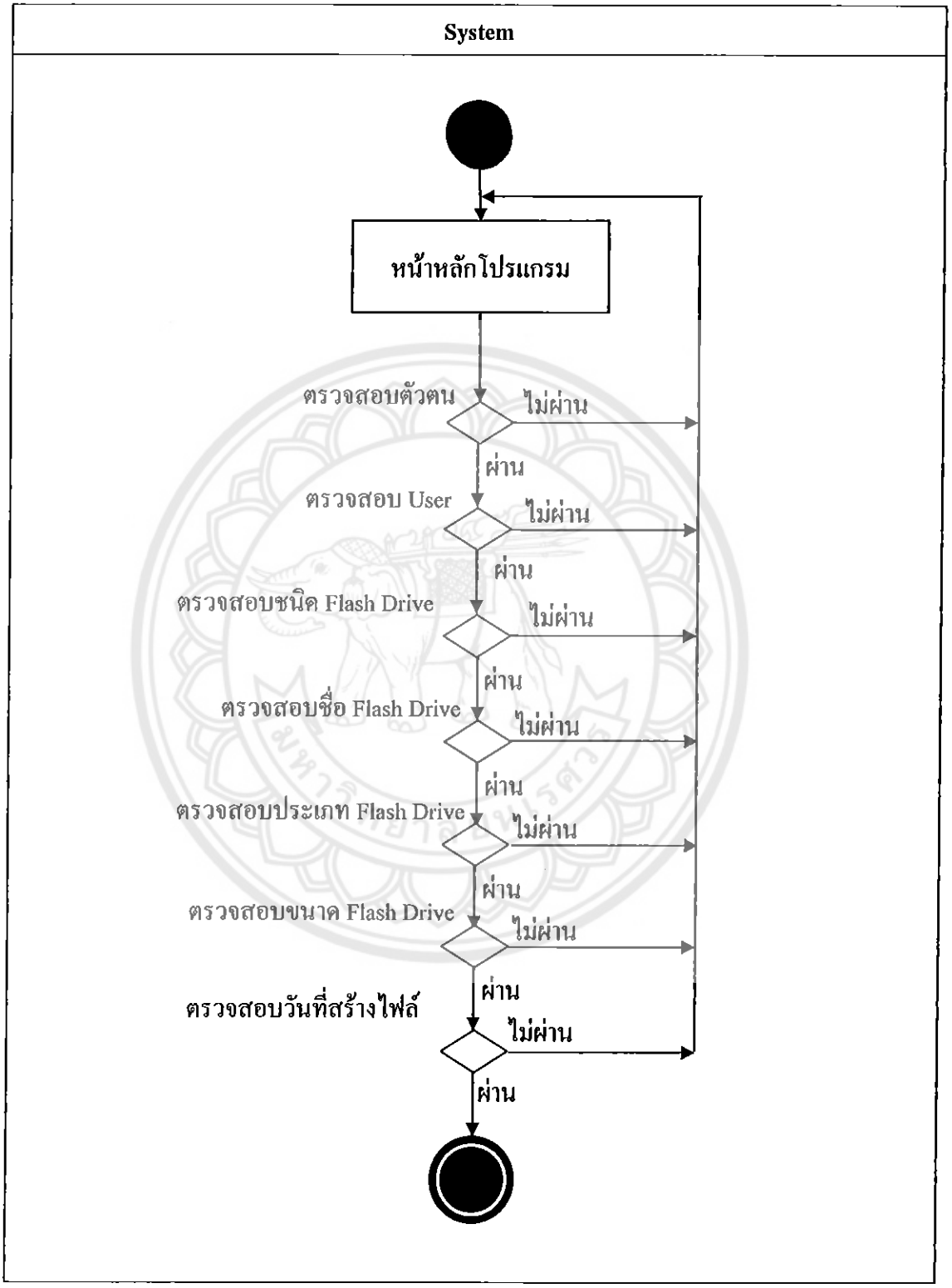


รูปที่ 3.5 Activity diagram Create Key Flash Drive (ต่อ)

3.2.5 Activity diagram ของ โปรแกรม Check Flash Drive



รูปที่ 3.6 Activity diagram Check Flash Drive



รูปที่ 3.7 Activity diagram Check Flash Drive (ต่อ)

บทที่ 4

ผลการทดลอง

เมื่อพัฒนาโปรแกรมเข้าสู่ระบบปฏิบัติการ Windows โดยต้องเสียบ Flash Drive ตัวที่กำหนด และใส่รหัสผ่าน เสร็จสมบูรณ์ ผู้จัดทำจะทำการทดสอบ ว่าเป็นไปตามเงื่อนไขที่กำหนดไว้หรือไม่ คือ การพิสูจน์ตัวตนแบบ 2 เงื่อนไข ดังนี้

4.1 การพิสูจน์ตัวตนเงื่อนไขที่ 1 ใช้รหัสผ่าน

4.2 การพิสูจน์ตัวตนเงื่อนไขที่ 2 ใช้ Flash Drive

จะอธิบายการทดลองต่างๆ ดังนี้

4.1 การพิสูจน์ตัวตนเงื่อนไขที่ 1 ใช้รหัสผ่าน

เป็นการสร้าง User Account จากระบบปฏิบัติการ Windows ที่มีอยู่แล้ว ซึ่งใช้ในการพิสูจน์ตัวตนเงื่อนไขที่ 1 คือ รหัสผ่าน

รูปที่ 4.1 การ Login เข้าสู่ Windows โดยใช้ รหัสผ่าน

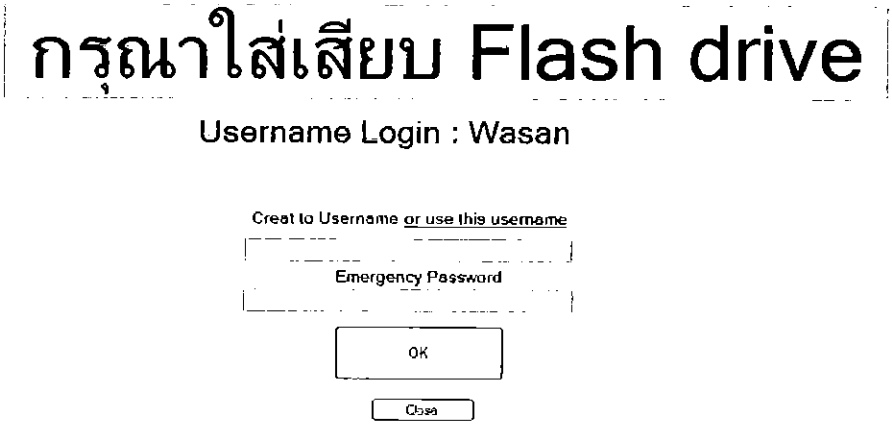
4.2 การพิสูจน์ตัวตนเงื่อนไขที่ 2 ใช้ Flash Drive

เป็นการพัฒนาโปรแกรมขึ้นมาเพื่อใช้ในการสร้างและตรวจสอบ Flash Drive ว่าเป็นตัวที่กำหนดไว้หรือไม่

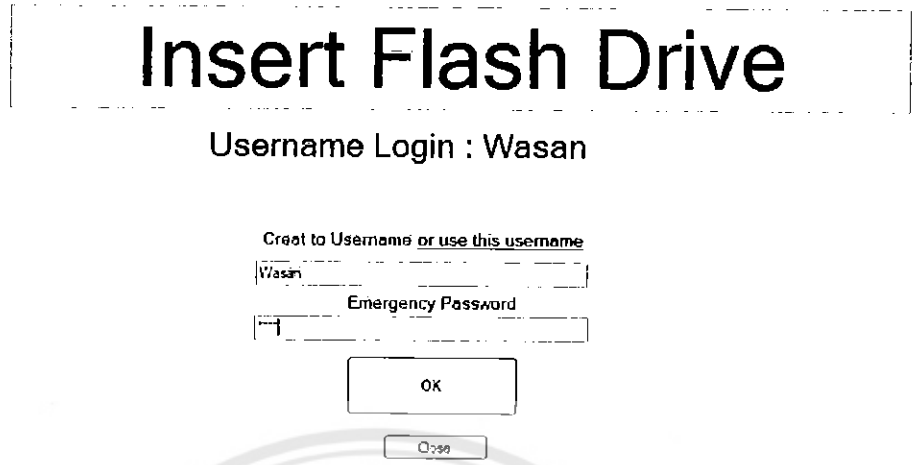
4.2.1 การทดลองใช้งานโปรแกรม Create Key Flash Drive

โปรแกรมนี้เป็นการสร้างไฟล์ให้กับ Flash Drive ต้องใส่ Flash Drive ที่ต้องการสร้างไฟล์มีรูปร่างหน้าตา ดังในรูปที่ 4.2 จะประกอบไปด้วยการใส่ชื่อ Username และการใส่รหัสผ่านฉุกเฉิน ดังในรูปที่ 4.4 แต่ถ้าไม่ได้เสียบ Flash Drive จะเป็นดังในรูปที่ 4.3 เมื่อทำการสร้างเสร็จสมบูรณ์จะเป็นดังในรูปที่ 4.5

รูปที่ 4.2 โปรแกรม Create Key Flash Drive



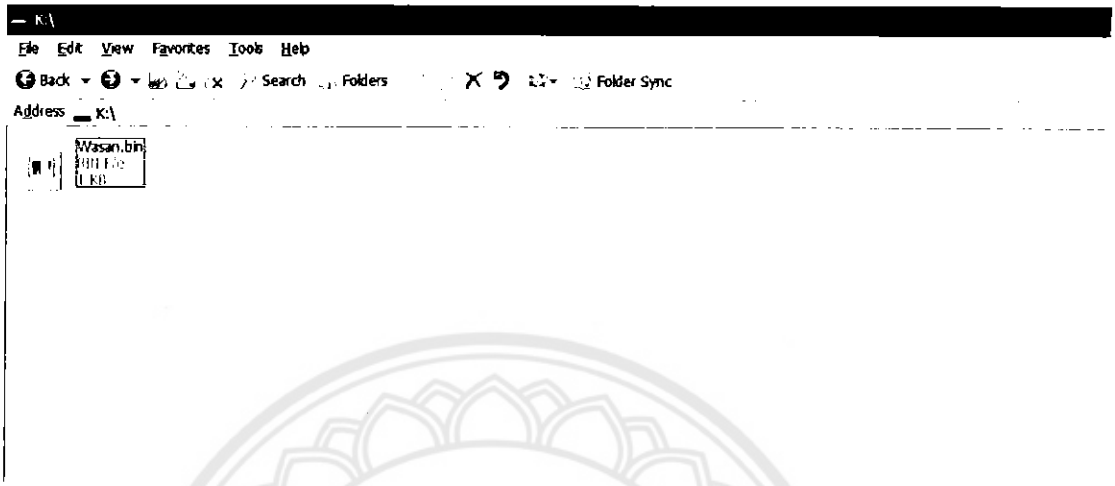
รูปที่ 4.3 โปรแกรม Create Key Flash Drive ขณะไม่ใส่ Flash Drive



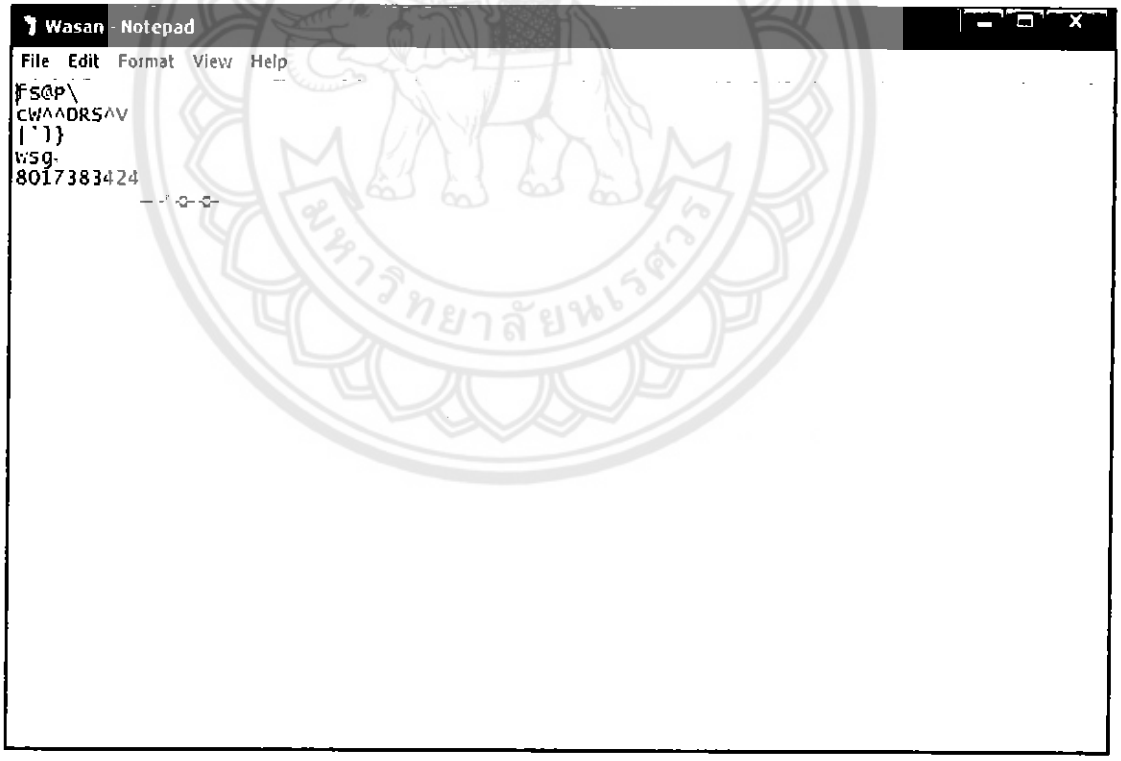
รูปที่ 4.4 โปรแกรม Create Key Flash Drive ขณะใส่ Username และ ใส่รหัสฉุกเฉิน

รูปที่ 4.5 โปรแกรม Create Key Flash Drive เสร็จสมบูรณ์

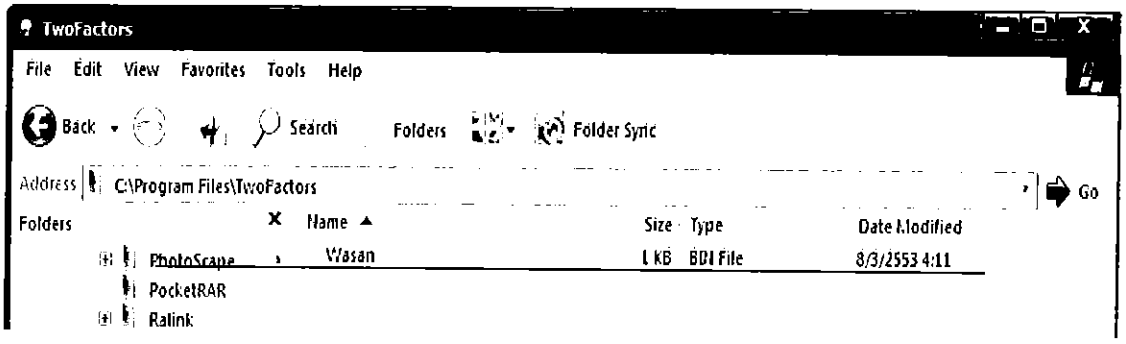
เมื่อโปรแกรมเสร็จสมบูรณ์ จะได้ไฟล์ .bin ออกมา ดังในรูปที่ 4.6 คือ ไฟล์ชื่อ Wasan.bin เก็บไว้ใน Flash Drive ซึ่งจะเป็นไฟล์ที่มีการเข้ารหัสเอาไว้ดังในรูที่ 4.7 และยังสร้างไฟล์ข้อมูลรหัสผ่านฉุกเฉินไว้ใน Program file ดังในรูปที่ 4.8 ซึ่งเป็นไฟล์ที่การเข้ารหัสไว้เหมือนกัน



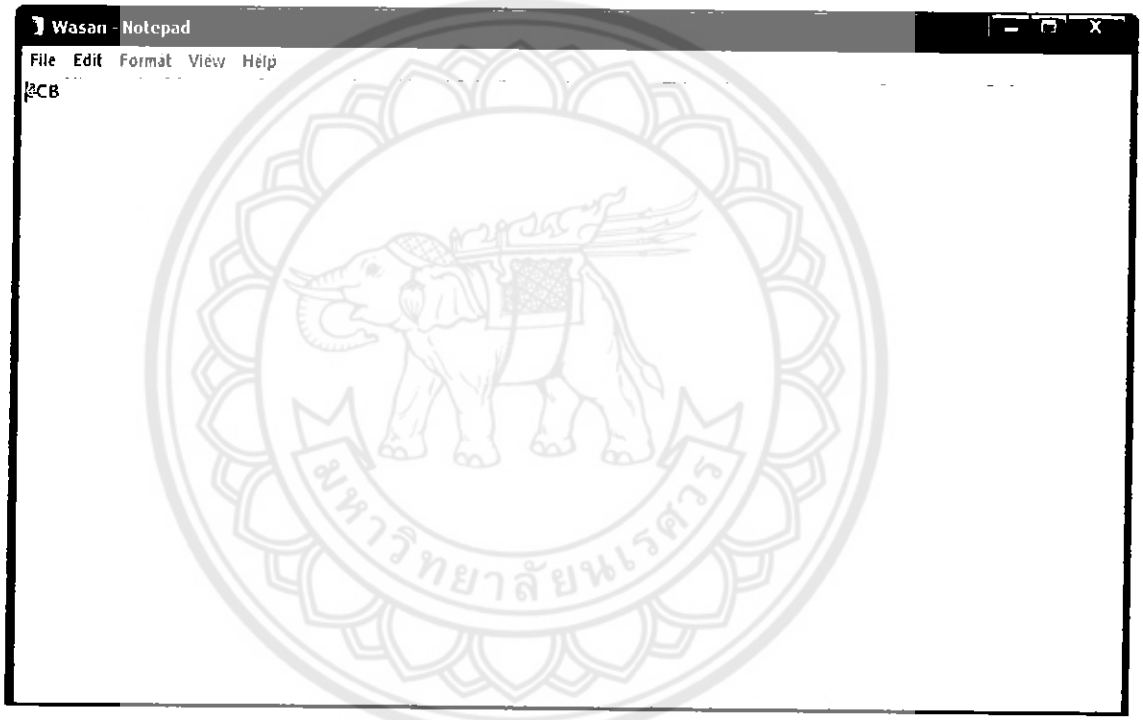
รูปที่ 4.6 ไฟล์ที่สร้างเสร็จใน Flash Drive



รูปที่ 4.7 ไฟล์ข้อมูลที่ถูกเข้ารหัส



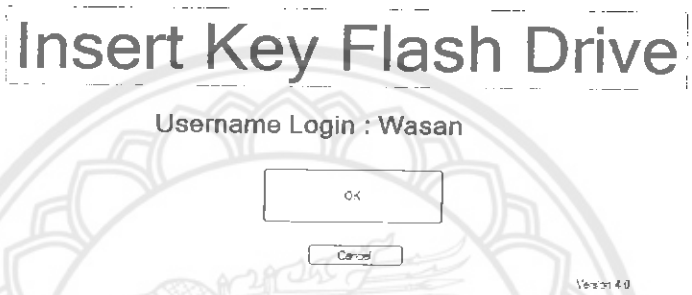
รูปที่ 4.8 ไฟล์ข้อมูลรหัสผ่านฉุกเฉินที่สร้างเสร็จใน Program file



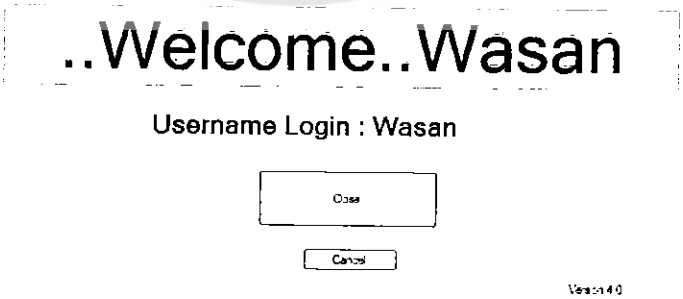
รูปที่ 4.9 ไฟล์ข้อมูลรหัสผ่านฉุกเฉินที่ถูกเข้ารหัส

4.2.2 การทดลองใช้งานโปรแกรม Check Flash Drive

โปรแกรมนี้จะขึ้นมาบนหน้าจอโดยอัตโนมัติเมื่อ เราใช้งานโปรแกรม Create Key Flash Drive ไปแล้ว เมื่อเริ่มระบบใหม่ก็จะมีรูปแบบหน้าตา ดังในรูปที่ 4.10 ขึ้นมา โปรแกรมนี้ใช้ในการตรวจสอบไฟล์ใน Flash Drive เมื่อเสียบ Flash Drive ที่ถูกต้องโปรแกรมจะออกจากโปรแกรมเข้าสู่ระบบปฏิบัติการ Windows ได้ ดังในรูปที่ 4.11

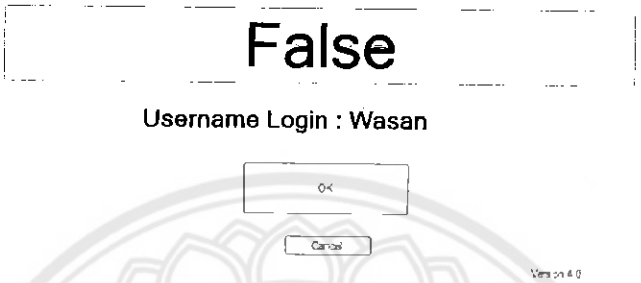


รูปที่ 4.10 โปรแกรม Check Flash Drive

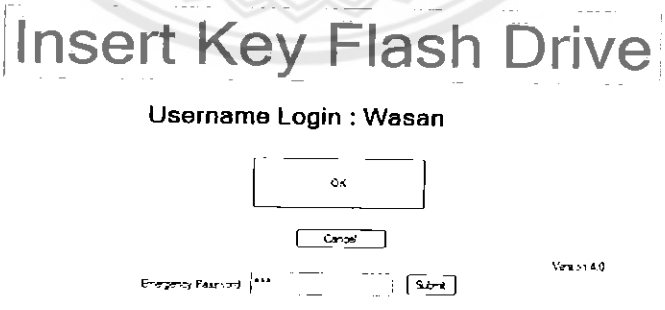


รูปที่ 4.11 โปรแกรม Check Flash Drive เมื่อเสียบ Flash Drive ที่ถูกต้อง

แต่ถ้าเสียบ Flash Drive ตัวอื่นที่ไม่ใช่ตัวที่กำหนด โปรแกรมจะล็อคหน้าจอ ออกจากระบบไม่ได้ ดังในรูปที่ 4.12 ในกรณีลืม Flash Drive ให้ใส่รหัสผ่านฉุกเฉินก็จะออกจากโปรแกรมได้ ดังในรูปที่ 4.13



รูปที่ 4.12 โปรแกรม Check Flash Drive เมื่อเสียบ Flash Drive ตัวอื่น



รูปที่ 4.13 โปรแกรม Check Flash Drive ใส่รหัสฉุกเฉิน

บทที่ 5
สรุปผลและวิเคราะห์ผล

โครงงานนี้พัฒนาเพื่อผู้ใช้งานคอมพิวเตอร์ในการจำกัดสิทธิ์การเข้าใช้งานคอมพิวเตอร์ และเพื่อเพิ่มความปลอดภัยให้กับระบบปฏิบัติการ โดยต้องมี Flash Drive ตัวที่กำหนด และรหัสผ่าน เป็นการพิสูจน์ตัวตนแบบ 2 เงื่อนไข ในบทนี้ เป็นการสรุปผลการดำเนินงานโครงการ ปัญหาและอุปสรรค และข้อเสนอแนะเพื่อเป็นแนวทางในการพัฒนาของผู้ที่สนใจต่อไป โครงงานถูกพัฒนาด้วยโปรแกรม Microsoft Visual Basic 2008

5.1 ผลการทดลอง

การทดลองได้เริ่มจากการพัฒนาโปรแกรมเข้าสู่ระบบปฏิบัติการ Windows โดยต้องเสียบ Flash Drive ตัวที่กำหนด และใส่รหัสผ่าน ซึ่งจะประกอบด้วยโปรแกรมย่อย 2 โปรแกรม คือ โปรแกรม Create Key Flash Drive และโปรแกรม Check Flash Drive โปรแกรมนี้จะใช้ในการสร้างและตรวจสอบไฟล์ที่ประกอบด้วยข้อมูล Username ที่ Login เข้า Windows, วันที่สร้างไฟล์, ขนาดของ Flash Drive, ชื่อของ Flash Drive, ชนิดของ Flash Drive, ประเภทของ Flash Drive ที่มีการเข้ารหัสไว้แล้ว ในการทดลองนี้ใช้ชื่อไฟล์ (Wasan.bin) ซึ่งนำมาใช้ในการอ้างอิงเพื่อตรวจสอบการเข้าสู่ระบบปฏิบัติการ

การทดลองใส่รหัสผ่านให้กับ User Account จากระบบปฏิบัติการ Windows ที่มีอยู่แล้ว สามารถทำได้ และผ่าน

การทดลองโดยใช้ไฟล์ (Wasan.bin) ที่บรรจุอยู่ใน Flash Drive ตัวที่กำหนด โปรแกรมจะสามารถตรวจสอบและถอดรหัสได้ทำให้สามารถเข้าสู่ระบบปฏิบัติการได้พร้อมขึ้นข้อความ Welcome

การทดลองเสียบ Flash Drive ตัวที่ไม่มีไฟล์ ที่กำหนดจะไม่สามารถเข้าสู่ระบบปฏิบัติการได้ พร้อมขึ้นข้อความ False

การทดลองคัดลอก (Wasan.bin) ไปไว้ใน Flash Drive ตัวอื่น ผลปรากฏว่าโปรแกรมไม่สามารถทำงานได้เนื่องจากข้อมูลต่างๆ ไม่ตรงตาม Flash Drive ตัวที่กำหนด

การทดลองแก้ไขข้อมูลในไฟล์ (Wasan.bin) ผลปรากฏว่าโปรแกรมไม่สามารถทำงานได้ เนื่องจากข้อมูลภายในไฟล์ (Wasan.bin) ไม่ตรงตามที่กำหนด

การทดลองใส่รหัสผ่านฉุกเฉิน กรณีลืม Flash Drive สามารถเข้าสู่ระบบปฏิบัติการได้

การทดลอง Log off เปลี่ยน User แล้วเสียบ Flash Drive ที่ไม่ได้สร้างไฟล์ให้กับ User นี้ ปรากฏว่า ไม่สามารถเข้าระบบได้

กล่าวโดยสรุป โปรแกรมเข้าสู่ระบบปฏิบัติการ Windows โดยต้องเสียบ Flash Drive ตัวที่กำหนด และใส่รหัสผ่าน สามารถจำกัดสิทธิ์การเข้าใช้ได้อย่างมีประสิทธิภาพ มีความปลอดภัยและสามารถใช้งานได้ง่าย

5.2 สรุปผลการทดลอง

1. จากผลการทดลองใส่รหัสผ่านของ User Account จากระบบปฏิบัติการ Windows ที่มีอยู่แล้ว สามารถผ่านไปได้ ซึ่งเป็นการพิสูจน์ตัวตนเงื่อนไขที่ 1

2. จากผลการทดลองเมื่อทำการ สร้างไฟล์ให้กับ Flash Drive ตัวที่ต้องการ โดยโปรแกรม Create Key Flash Drive สามารถทำได้อย่างสะดวกและรวดเร็ว ถูกต้องตามที่กำหนดเอาไว้ และสามารถเข้ารหัสไฟล์ได้

3. จากผลการทดลองตรวจสอบ Flash Drive ตัวที่กำหนด โดยโปรแกรม Check Flash Drive สามารถตรวจสอบผ่านได้อย่างถูกต้องเข้าสู่ระบบปฏิบัติการ Windows ได้ คือ สามารถถอดรหัสไฟล์ได้ถูกต้อง ซึ่งเป็นการพิสูจน์ตัวตนเงื่อนไขที่ 2 แต่เมื่อนำ Flash Drive ตัวอื่นที่ไม่ได้สร้างไฟล์โดยโปรแกรม Create Key Flash Drive จะไม่สามารถเข้าสู่ระบบปฏิบัติการ Windows ได้ เพราะไม่มีไฟล์ที่เข้ารหัสไว้

4. จากผลการทดสอบโปรแกรมปรากฏว่าเป็นไปตามเงื่อนไขที่กำหนดได้จริง

5.3 ปัญหาและแนวทางแก้ไข

1. ผู้พัฒนาไม่มีความรู้เกี่ยวกับการใช้งาน Microsoft Visual Basic 2008 มากนัก จึงต้องใช้เวลาในการศึกษาพอสมควร

2. การพัฒนาโปรแกรมทั้ง 2 ต้องมีการเข้ารหัสและถอนรหัส จึงใช้เวลาในการพัฒนามากพอสมควร เนื่องจากมีความซับซ้อน

3. การพัฒนาโปรแกรมมีปัญหาด้านรูปแบบของวันที่ เช่น บางเครื่องเป็น วัน เดือน ปี แต่บางเครื่องเป็น ปี เดือน วัน ทำให้ต้องใช้เวลาในการจัดรูปแบบ

5.4 ข้อเสนอแนะ

1. ก่อนการดำเนินงาน ควรศึกษาข้อมูลให้เข้าใจมากที่สุด เพื่อลดข้อผิดพลาดในการทำงาน
2. เพิ่มเงื่อนไขที่ใช้ในการตรวจสอบให้มากขึ้น เพื่อให้เกิดความปลอดภัยมากขึ้น
3. พัฒนาให้โปรแกรมใช้ในระบบปฏิบัติการ Windows ได้ทุกเวอร์ชัน
4. ควรทำเป็น Windows Service เพื่อให้เป็นระบบมากขึ้น
5. ทำให้ไฟล์ที่สร้างใน Flash Drive ไม่สามารถแก้ไขได้ มองไม่เห็น และไม่สามารถลบได้

เอกสารอ้างอิง

[1] กิตินันท์ พลสวัสดิ์. **เริ่มต้น Visual Basic 2008 ฉบับโปรแกรมเมอร์. พิมพ์ครั้งที่ 1. นนทบุรี :** สำนักพิมพ์ไอดีซี. 2552.

[2] สิริพร จิตต์เจริญธรรม. "ความรู้เบื้องต้นเกี่ยวกับ การพิสูจน์ตัวตน" [Online]. Available: http://www.thaicert.org/paper/authen/authentication_guide.php2547.

ภาคผนวก

นิยามคำศัพท์

Authentication (การพิสูจน์ตัวตน) คือ ขั้นตอนการยืนยันความถูกต้องของหลักฐาน ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

Authorization (การกำหนดสิทธิ์) คือ ข้อจำกัดของบุคคลที่เข้ามาในระบบ ว่าบุคคลคนนั้นสามารถทำอะไรกับระบบได้บ้าง

Accountability (การบันทึกการใช้งาน) คือ การบันทึกรายละเอียดของการใช้ระบบ

Identification (การระบุตัวตน) คือ ขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใคร

Encryption (การเข้ารหัส) คือ การเก็บข้อมูลให้เป็นส่วนบุคคลจากบุคคลอื่นที่ไม่ได้รับอนุญาต

Integrity (การรักษาความสมบูรณ์) คือ การรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไปจากต้นฉบับ

Audit (การตรวจสอบ) คือ การตรวจสอบหลักฐานทางอิเล็กทรอนิกส์

Authentication by Passwords (การพิสูจน์ตัวตนโดยใช้รหัสผ่าน)

Authentication by Tokens (การพิสูจน์ตัวตนโดยใช้ Tokens)

One-Time Password (การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว)

Zero-knowledge proofs (การพิสูจน์ตัวตนโดยใช้การถาม - ตอบ)

Public-key cryptography (การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ)

Authentication by PIN (การพิสูจน์ตัวตนโดยใช้ PIN)

Authentication by Biometric traits (การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล)

ประวัติผู้เขียนโครงงาน

ชื่อ นายวสันต์ หลวงเรื่อง

ภูมิลำเนา 39/1 ม.6 ต.หาดล้า อ.ท่าปลา จ.อุตรดิตถ์

ประวัติการศึกษา

- จบระดับมัธยมศึกษาจากโรงเรียนท่าปลาประชาอุทิศ
- ปัจจุบันกำลังศึกษาในระดับปริญญาตรีชั้นปีที่ 4

สาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

มหาวิทยาลัยนเรศวร

E-mail: wasan_fc@hotmail.com

ชื่อ นายเอกพงศ์ ทิงาเครือ

ภูมิลำเนา 276/5 ม.11 ต.ทุ่งเสลี่ยม อ.ทุ่งเสลี่ยม จ.สุโขทัย

ประวัติการศึกษา

- จบระดับมัธยมศึกษาจากโรงเรียนทุ่งเสลี่ยมชนูปถัมภ์
- ปัจจุบันกำลังศึกษาในระดับปริญญาตรีชั้นปีที่ 4

สาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

มหาวิทยาลัยนเรศวร

E-mail: eak_zuza@hotmail.com