บทที่ 3

การวิเคราะห์และออกแบบระบบ

ระบบบรหัสผ่านแบบใช้ครั้งเดียวของคุณพิษณุ ถูกพัฒนาขึ้นเพื่อเสริมประสิทธิภาพให้กับระบบการใช้รหัสผ่านในการพิสูจน์ตัวจริงของผู้เข้าใช้ระบบ แต่ยังมีข้อจำกัดบางส่วนที่ควรได้รับการแก้ไข ดังนี้

1. ระบบไม่ครอบคลุมผู้ใช้เซิร์ฟเวอร์หลายเครื่อง
2. วิธีการตรวจสอบและบำรุงรักษารหัสผ่านยังไม่ปลอดภัยเพียงพอ
3. ระบบไม่ปลอดภัยจากการสื่อสารข้อมูล
4. ไม่สะดวกต่อกลุ่มผู้ใช้ที่ต้องใช้ชื่อลงบันทึกเข้าใช้เดียวกัน
5. ใช้ได้กับส่วนขอใช้บริการเฉพาะที่เป็นระบบปฏิบัติการยูนิกซ์

เพื่อขยายให้ระบบสามารถรองรับความหลากหลายในการใช้งาน และรองรับพัฒนาการของระบบบรหัสผ่านแบบใช้ครั้งเดียวในอนาคต การแก้ไขข้อจำกัดและการปรับปรุงเพิ่มเติมจำเป็นต้องมีการเปลี่ยนแปลงบางส่วนจากระบบเดิมของคุณพิษณุ ดังนี้

1. ขยายระบบให้ครอบคลุมผู้ใช้เซิร์ฟเวอร์หลายเครื่อง
2. เพิ่มทางเลือกในการตรวจสอบและบำรุงรักษารหัสผ่าน
3. เพิ่มทางเลือกในการเข้ารหัสข้อมูลที่ใช้สื่อสาร
4. แสดงหมายเลขลำดับของรหัสผ่านปัจจุบัน
5. เพิ่มรุ่นควบคุม (version control)
6. ข้อมูลที่เกี่ยวข้อง
7. การศึกษาความเป็นไปได้ทางการพัฒนาส่วนขอใช้บริการบนระบบปฏิบัติการเน็ตแวร์และวินโดวส์เอ็นที

ข้อจำกัดของระบบเดิม

1. ระบบไม่ครอบคลุมผู้ใช้เซิร์ฟเวอร์หลายเครื่อง

จากผลสรุปการวิจัยของคุณพิษณุ บทที่ 7 ข้อ 2 “ผู้ใช้มีสิทธิเข้าใช้เซิร์ฟเวอร์ได้หลายเครื่อง ถ้าทุกเครื่องมีชื่อขอเข้าใช้ระบบเป็นชื่อเดียวกันจะสามารถขอเข้าใช้ระบบจากทุก ๆ เซิร์ฟเวอร์โดยใช้รหัสผ่านชุดเดียวกัน” สรุปได้ว่าชื่อลงบันทึกเข้าใช้ที่อยู่บนเซิร์ฟเวอร์ต่าง ๆ ถูกระบบเห็นเป็นเพียง

หนึ่งเซ็ต เพราะฉะนั้นชื่อลงบันทึกเข้าใช้ชื่อเดียวกันซึ่งอยู่ต่างเซิร์ฟเวอร์ ระบบจะเห็นเป็นชื่อลงบันทึกเข้าใช้เดียวกัน สามารถเขียนแสดงลักษณะของความสัมพันธ์ระหว่างผู้ใช้กับชื่อลงบันทึกเข้าใช้บนเซิร์ฟเวอร์ และชื่อบัญชีผู้ใช้บนเครื่องให้บริการรหัสผ่านแบบใช้ครั้งเดียวได้ดังนี้

หมายเหตุ

UL : ความสัมพันธ์ระหว่างผู้ใช้กับชื่อลงบันทึกเข้าใช้

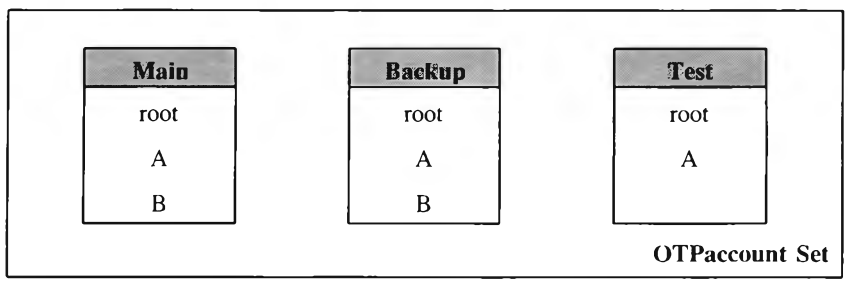
LA : ความสัมพันธ์ระหว่างชื่อลงบันทึกเข้าใช้กับชื่อบัญชีผู้ใช้

รูปที่ 3.1 ความสัมพันธ์ของส่วนที่เกี่ยวข้องในระบบของคุณพิษณุ

จากรูปแสดงให้เห็นว่า ผู้ใช้แต่ละคนสามารถมีได้หลายชื่อลงบันทึกเข้าใช้หรือกลุ่มของผู้ใช้อาจใช้ชื่อลงบันทึกเข้าใช้เดียวกัน โดยที่ชื่อลงบันทึกเข้าใช้ชื่อเหมือนกันต้องใช้รหัสผ่านชุดเดียวกัน และชื่อลงบันทึกเข้าใช้ที่ใช้ชื่อต่างกันต้องใช้รหัสผ่านต่างชุดกัน โดยไม่สนใจว่าชื่อลงบันทึกเข้าใช้เหล่านั้นอยู่บนเซิร์ฟเวอร์เครื่องใด

ตัวอย่าง

หน่วยงานแห่งหนึ่งใช้ระบบคอมพิวเตอร์เพื่อสนับสนุนการปฏิบัติงานตลอด 24 ชั่วโมง จึงจำเป็นต้องมีระบบสำรองเพื่อลดข้อผิดพลาดที่อาจเกิดขึ้นเช่น เครื่องสำรองในกรณีที่เครื่องหลักมีปัญหา โดยให้พนักงาน 2 คนคือ นาย ก. และ นาย ข. สลับกันทำหน้าที่ดูแลระบบ เพื่อทำให้ระบบสมบูรณ์ยิ่งขึ้น การพัฒนาหรือทดสอบระบบซึ่งเป็นส่วนที่นาย ก. ต้องรับผิดชอบจะทำที่เครื่องทดสอบก่อนทำการติดตั้งจริงบนเครื่องหลักและเครื่องสำรอง ทั้งนี้เพื่อทำให้ระบบสามารถตรวจสอบได้ ระบบถูกปรับปรุงเพื่อป้องกันไม่ให้ผู้ใดสามารถใช้ชื่อลงบันทึกเข้าใช้ของ root เข้าสู่ระบบได้โดยตรง ต้องเข้าผ่านจากชื่อลงบันทึกเข้าใช้ที่กำลังเข้าใช้เท่านั้น สามารถแสดงเครื่องเซิร์ฟเวอร์และชื่อลงบันทึกเข้าใช้ที่เกี่ยวข้องได้ดังรูป



รูปที่ 3.2 แสดงประกอบตัวอย่างชื่อลงบันทึกเข้าใช้บนแต่ละเซิร์ฟเวอร์

จากรูป สามารถแสดงชื่อลงบันทึกเข้าใช้ในรูปแบบของเซ็ตได้ดังนี้

Main = {root, A, B}

Backup = {root, A, B}

Test = {root, A}

เพราะฉะนั้น OTPaccount Set = Main U Backup U Test = {root, A, B}

เพื่อเพิ่มความปลอดภัยให้กับระบบซึ่งพิสูจน์ตัวจริงของผู้เข้าใช้ด้วยรหัสผ่าน ระบบของคุณพิษณุจึงถูกนำมาใช้ สามารถสร้างชื่อลงบันทึกเข้าใช้ของผู้ใช้ในระบบบนส่วนขอใช้บริการสอดคล้องกับชื่อบัญชีผู้ใช้บนส่วนให้บริการได้ดังตาราง

User	**Main**	**Backup**	**Test**	**OTPaccount**
นาย ก.	A	A	A	OtpA
นาย ก.	-	-	root	-
นาย ข.	B	B	-	OtpB
นาย ก., นาย ข.	Root	Root	-	Otproot

ตารางที่ 3.1 แสดงชื่อลงบันทึกเข้าใช้และชื่อบัญชีผู้ใช้ในระบบของคุณพิษณุ

ผลลัพธ์ได้จากตาราง กรณีที่ระบบไม่สนใจเซิร์ฟเวอร์ คือ

1) ชื่อลงบันทึกเข้าใช้ A บนเซิร์ฟเวอร์ต่าง ๆ ใช้รหัสผ่านชุดเดียวกันได้
2) root ของเครื่องหลักและเครื่องสำรองสามารถถูกใช้โดยนาย ก. และ นาย ข.โดยใช้รหัสผ่านชุดเดียวกันได้
3) นาย ก. ไม่สามารถกำหนดให้ชื่อลงบันทึกเข้าใช้ชื่อ root บนเครื่องทดสอบ ให้ใช้รหัสผ่านต่างจากเครื่องหลักและเครื่องสำรองได้
4) นาย ก. ไม่สามารถกำหนดให้ชื่อลงบันทึกเข้าใช้ชื่อ root บนเครื่องทดสอบใช้รหัสผ่านชุดเดียวกันกับชื่อลงบันทึกเข้าใช้ชื่อ A ได้

เนื่องจากระบบของคุณพิษณุไม่สนใจเซิร์ฟเวอร์ จึงเป็นเหตุให้ส่วนให้บริการรหัสผ่านไม่สามารถแยกความแตกต่างของชื่อลงบันทึกเข้าใช้ที่อยู่ต่างกันเซิร์ฟเวอร์ได้ ทำให้ระบบมีข้อจำกัดดังนี้

1) ไม่สามารถมีชื่อลงบันทึกเข้าใช้ชื่อเดียวกันบนต่างเซิร์ฟเวอร์ ใช้รหัสผ่านต่างชุดกันได้
2) ไม่สามารถมีชื่อลงบันทึกเข้าใช้ชื่อต่างกันใช้รหัสผ่านชุดเดียวกันได้

2. วิธีการตรวจสอบและบำรุงรักษารหัสผ่านยังไม่ปลอดภัยเพียงพอ

จากการศึกษางานวิจัยของคุณพิษณุพบว่า ระบบยังมีปัญหาในส่วนของการตรวจสอบและบำรุงรักษารหัสผ่าน ดังนี้

1) การสร้างรหัสผ่านยังคงใช้วิธีสุ่มจากตัวเลขและตัวอักษรภาษาอังกฤษ ทำให้คาดเดารหัสผ่านได้ง่าย
2) การตรวจสอบรหัสผ่านจะใช้วิธีการเปรียบเทียบข้อความซึ่งสามารถปลอมแปลงได้ง่าย
3) รหัสผ่านที่ได้รับการสร้างทั้งหมดจะถูกจัดเก็บไว้บนเครื่องให้บริการโดยไม่มีการเข้ารหัส ทำให้สิ้นเปลืองเนื้อที่และไม่ปลอดภัยถ้าแฟ้มรหัสผ่านถูกขโมย

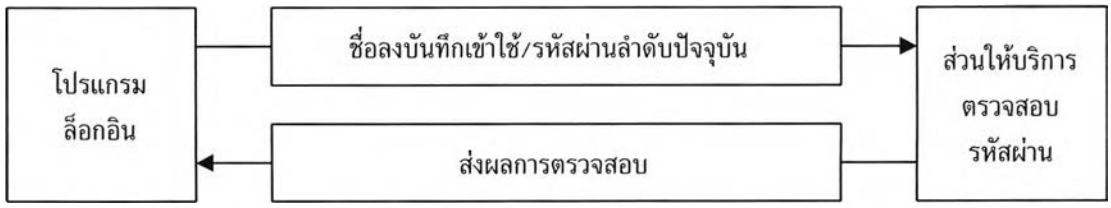
3. ระบบไม่ปลอดภัยจากการสื่อสารข้อมูล

ระบบของคุณพิษณุประกอบด้วยส่วนขอใช้และส่วนให้บริการรหัสผ่านซึ่งอยู่ต่างเครื่องกัน ทำให้การตรวจสอบรหัสผ่านของผู้ใช้ในแต่ละครั้งต้องมีการสื่อสารระหว่างเครื่องทั้งสองผ่านระบบเครือข่าย อีกทั้งลักษณะข้อมูลที่ใช้สื่อสารไม่มีการเข้ารหัส จึงเป็นสาเหตุที่ทำให้เกิดปัญหาที่ตามมา คือ

1) การลักลอบดักฟังข้อมูลเพื่อนำไปใช้ประโยชน์ในอนาคต
2) การลักลอบเปลี่ยนแปลงข้อมูลเพื่อให้ได้มาซึ่งสิทธิในการใช้ระบบ
3) การลักลอบปลอมแปลงเครื่องเพื่อให้ได้มาซึ่งสิทธิในการเข้าใช้ระบบ

4. ไม่สะดวกต่อกลุ่มผู้ใช้ที่ต้องใช้ชื่อลงบันทึกเข้าใช้เดียวกัน

การสื่อสารระหว่างส่วนขอใช้และส่วนให้บริการรหัสผ่านในระบบของคุณพิษณุเกิดขึ้นเมื่อโปรแกรมล็อกอินส่งชื่อลงบันทึกเข้าใช้พร้อมรหัสผ่าน หรือคำสั่งพิเศษไปให้ส่วนให้บริการทำการตรวจสอบและส่งผลการตรวจสอบกลับคืนมาให้โปรแกรมล็อกอินเท่านั้น ซึ่งไม่สะดวกเมื่อชื่อลงบันทึกเข้าใช้นั้นถูกใช้โดยกลุ่มของผู้ใช้ เพราะไม่มีการแสดงหมายเลขลำดับของรหัสผ่านปัจจุบันสำหรับใช้เข้าระบบให้ผู้ใช้ทราบ



รูปที่ 3.3 ขั้นตอนการสื่อสารในระบบของคุณพิษณุ

ตัวอย่าง

login : account

password : _____

จากตัวอย่างสมมุติว่า ชื่อลงบันทึกเข้าใช้ชื่อ account ถูกโดยกลุ่มผู้ใช้ในแผนกบัญชี กรณีผู้ใช้ในแผนกต้องการเข้าระบบ หลังจากพิมพ์ชื่อลงบันทึกเข้าใช้จะต้องมีการสอบถามกันในกลุ่มของผู้ใช้เพื่อให้ได้มาซึ่งลำดับของรหัสผ่านปัจจุบันก่อนพิมพ์รหัสผ่านปัจจุบันลำดับที่ถูกต้องเข้าไปได้

5. ใช้ได้กับส่วนขอใช้บริการเฉพาะที่เป็นระบบปฏิบัติการยูนิกซ์

ระบบรหัสผ่านแบบใช้ครั้งเดียวของคุณพิษณุมุ่งเน้นการทำงานทั้งส่วนให้บริการและส่วนขอใช้บริการเฉพาะในส่วนของระบบปฏิบัติการยูนิกซ์เท่านั้น

การแก้ไขข้อจำกัดและปรับปรุงเพิ่มเติม

1. ขยายระบบให้ครอบคลุมผู้ใช้เซิร์ฟเวอร์หลายเครื่อง

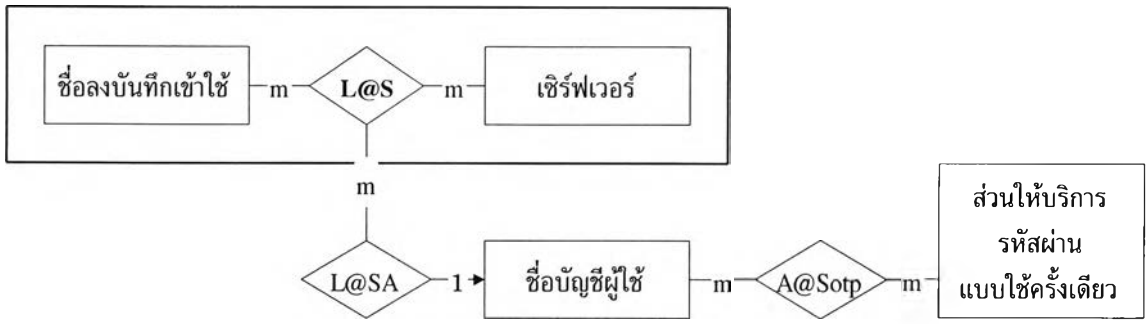
เพื่อขยายระบบให้สามารถครอบคลุมผู้ใช้เซิร์ฟเวอร์หลายเครื่องทำได้โดย ให้ความสนใจเซิร์ฟเวอร์ในระบบเพื่อใช้เป็นเงื่อนไขสำหรับแยกความแตกต่างในกรณีที่ใช้ชื่อลงบันทึกเข้าใช้ชื่อเหมือนกัน สามารถแสดงความสัมพันธ์ของระบบได้ดังรูป

หมายเหตุ

UL : ความสัมพันธ์ระหว่างผู้ใช้กับชื่อลงบันทึกเข้าใช้

L@S : ความสัมพันธ์ระหว่างชื่อลงบันทึกเข้าใช้กับเซิร์ฟเวอร์

รูปที่ 3.4 ความสัมพันธ์ระหว่างผู้ใช้ ชื่อลงบันทึกเข้าใช้ และเซิร์ฟเวอร์



หมายเหตุ

L@S : ความสัมพันธ์ระหว่างชื่อลงบันทึกเข้าใช้กับเซิร์ฟเวอร์

L@SA : ความสัมพันธ์ระหว่างชื่อลงบันทึกเข้าใช้และเซิร์ฟเวอร์กับชื่อบัญชีผู้ใช้

A@SO : ความสัมพันธ์ระหว่างชื่อบัญชีผู้ใช้กับส่วนให้บริการรหัสผ่าน

รูปที่ 3.5 ความสัมพันธ์ระหว่างชื่อลงบันทึกเข้าใช้ของแต่ละเซิร์ฟเวอร์กับชื่อบัญชีผู้ใช้

เงื่อนไขที่ระบบสามารถรองรับได้

1) ผู้ใช้ที่มีชื่อลงบันทึกเข้าใช้อยู่บนเซิร์ฟเวอร์ต่าง ๆ ที่ใช้ชื่อลงบันทึกเข้าใช้เดียวกัน สามารถใช้รหัสผ่านชุดเดียวได้
2) ผู้ใช้ที่มีชื่อลงบันทึกเข้าใช้อยู่บนเซิร์ฟเวอร์ต่าง ๆ ซึ่งอาจใช้ชื่อลงบันทึกเข้าใช้ต่างกัน สามารถใช้รหัสผ่านชุดเดียวได้
3) ชื่อลงบันทึกเข้าใช้ชื่อเดียวกันซึ่งอยู่ต่างเซิร์ฟเวอร์กัน ที่เป็นของผู้ใช้คนละคนกันให้ใช้รหัสผ่านต่างชุดกัน
4) แต่ละชื่อลงบันทึกเข้าใช้อาจถูกใช้ได้โดยผู้ใช้หลายคน

ตัวอย่าง

จากตัวอย่างที่ได้กล่าวมาในส่วนของข้อจำกัด หลังจากระบบได้รับการปรับปรุงการออกแบบความสัมพันธ์ โดยใช้ชื่อลงบันทึกเข้าใช้กับเซิร์ฟเวอร์เป็นเงื่อนไขในการกำหนดชื่อบัญชีผู้ใช้บนเครื่องให้บริการรหัสผ่าน ทำให้สามารถจัดการกับชื่อลงบันทึกเข้าใช้ได้เพิ่มขึ้นซึ่งจะเห็นได้จากตาราง

User	**Main**	**Backup**	**Test**	**OTPaccount**
นาย ก.	A	A	root	OtpA
นาย ข.	B	B	-	OtpB
นาย ก., นาย ข.	Root	-	-	OtpMroot
นาย ก., นาย ข.	-	Root	-	OtpBroot

ตารางที่ 3.2 แสดงชื่อลงบันทึกเข้าใช้แต่ละเซิร์ฟเวอร์กับชื่อบัญชีผู้ใช้

จากตารางจะเห็นว่าระบบสามารถรองรับเงื่อนไขได้เพิ่มขึ้นจากเดิมดังนี้

1) นาย ก. สามารถมีชื่อลงบันทึกเข้าใช้ root กับ A ใช้รหัสผ่านชุดเดียวกันได้
2) ชื่อลงบันทึกเข้าใช้ root บนต่างเครื่องกันสามารถใช้รหัสผ่านต่างชุดกันได้

ดังนั้น เพื่อขยายระบบรหัสผ่านแบบใช้ครั้งเดียวให้ครอบคลุมผู้ใช้เซิร์ฟเวอร์หลายเครื่องจึงต้องใช้ ชื่อเซิร์ฟเวอร์และชื่อลงบันทึกเข้าใช้เป็นข้อมูลที่ใช้สำหรับสื่อสารกับส่วนให้บริการรหัสผ่าน

ฟิลด์	รูปแบบ	รายละเอียด
Domain_Length	Short Integer	ความยาวของชื่อเซิร์ฟเวอร์
Domain_Name	String	ชื่อเซิร์ฟเวอร์ที่ขอใช้บริการรหัสผ่าน
Login_Length	Short Integer	ความยาวของชื่อลงบันทึกเข้าใช้
Login_Name	String	ชื่อลงบันทึกเข้าใช้

ตารางที่ 3.3 รูปแบบของข้อมูลที่ใช้กำหนดชื่อบัญชีผู้ใช้บนเครื่องให้บริการรหัสผ่าน

สาเหตุที่กำหนดให้รูปแบบของฟิลด์ Login_Name สามารถยืดหยุ่นได้เพราะจากการศึกษาข้อมูล รูปแบบของชื่อลงบันทึกเข้าใช้บนระบบยูนิกซ์จะประกอบด้วยตัวอักษรตั้งแต่ 2-8 ตัว แต่สำหรับระบบปฏิบัติการวินโดวส์สามารถรองรับตัวอักษรได้ถึง 20 ตัวอักษร และระบบปฏิบัติการเน็ตแวร์สามารถรองรับได้ถึง 47 ตัวอักษร ซึ่งโดยทั่วไปไม่นิยมใช้ชื่อลงบันทึกเข้าใช้ยาวมาก ดังนั้นจึงถือว่าการออกแบบรูปแบบลักษณะนี้ประหยัดกว่า

2. เพิ่มทางเลือกในการตรวจสอบและบำรุงรักษารหัสผ่าน

เพื่อเพิ่มความปลอดภัยให้กับระบบในส่วนของการตรวจสอบและบำรุงรักษารหัสผ่าน อาจนำอัลกอริทึมมาตรฐานที่สามารถแก้ปัญหาเหล่านี้มาใช้ในการพัฒนาระบบ เช่น MD2 MD4 MD5 และ SHS เป็นต้น

ดังนั้น รูปแบบของกลุ่มข้อมูลที่ใช้ในการสื่อสารควรมีส่วนที่ใช้สำหรับระบุอัลกอริทึมที่ใช้เพื่อทำให้ส่วนขอใช้และส่วนให้บริการสามารถเข้าใจตรงกัน ซึ่งจะมีประโยชน์อย่างมากในกรณีที่ส่วนให้บริการสามารถรองรับอัลกอริทึมได้หลากหลาย แต่การระบุอัลกอริทึมในกลุ่มข้อมูลที่ใช้สื่อสารไม่ควรสื่อความหมายอย่างชัดเจน เพราะอาจเป็นข้อมูลที่ผู้ลักลอบดักฟังข้อมูลสามารถนำไปใช้เป็นจุดเริ่มต้นในการลักลอบเข้าสู่ระบบได้

ฟิลด์	รูปแบบ	รายละเอียด
Algorithm	Short Integer	ชนิดของอัลกอริทึม

ตารางที่ 3.4 รูปแบบของข้อมูลที่ใช้เพื่อระบุชนิดของอัลกอริทึม

ตัวอย่าง

0 ระบบการให้บริการรหัสผ่านแบบใช้ครั้งเดียวของคุณพิษณุ

1 MD2

2 MD4

3 MD5

4 SHS

รูปแบบข้อมูลที่เลือกใช้เป็นชนิดตัวเลข จึงมั่นใจได้ว่าสามารถรองรับความหลากหลายของอัลกอริทึมใหม่ ๆ เท่าที่มีอยู่ในปัจจุบันและอนาคตได้เพียงพอ

3. เพิ่มทางเลือกในการเข้ารหัสข้อมูลที่ใช้สื่อสาร

การเพิ่มความปลอดภัยให้กับข้อมูลที่ใช้สื่อสารสามารถทำได้โดยนำวิธีการเข้ารหัสข้อมูลมาใช้ เพราะข้อมูลที่ได้รับการเข้ารหัสเมื่อถูกขโมยไปได้จะต้องได้รับการถอดรหัสจากวิธีการและคีย์ที่ถูกต้องเท่านั้นจึงสามารถนำข้อมูลไปใช้ประโยชน์ได้ ซึ่งการทำเช่นนั้นต้องใช้เวลานานมากพอควร และเมื่อเพิ่มการเข้ารหัสให้กับระบบรหัสผ่านแบบใช้ครั้งเดียวยิ่งทำให้ความปลอดภัยของระบบรหัสผ่านแบบใช้ครั้งเดียวที่ใช้ในระบบเครือข่ายมีความสมบูรณ์มากยิ่งขึ้น นอกจากนั้นการเข้ารหัสยังสามารถใช้สำหรับตรวจสอบความถูกต้องของข้อมูลเพื่อป้องกันการลักลอบเปลี่ยนแปลงข้อมูลและพิสูจน์ตัวจริงของเครื่องที่ส่งข้อมูลได้ด้วย

เช่นเดียวกันกับการตรวจสอบและการบำรุงรักษารหัสผ่าน รูปแบบของกลุ่มข้อมูลที่ใช้ในการสื่อสารควรมีการกำหนดชนิดของการเข้ารหัสข้อมูลไว้เป็นทางเลือก สำหรับการขอใช้บริการที่ต้องระวังเรื่องความปลอดภัยที่แตกต่างกัน ตามสถานการณ์และสภาวะแวดล้อมที่ใช้

ฟิลด์	รูปแบบ	รายละเอียด
Cryptograph	Short Integer	ชนิดของการเข้ารหัส

ตารางที่ 3.5 รูปแบบของข้อมูลที่ใช้เพื่อระบุชนิดของการเข้ารหัส

ตัวอย่าง

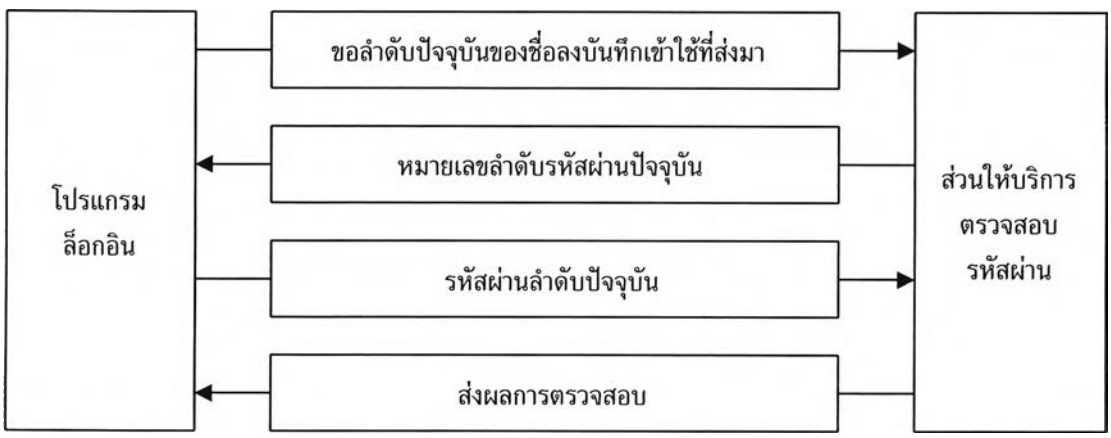
0 ไม่มีการเข้ารหัสข้อมูล

1 DES

2 IDEA

4. แสดงหมายเลขลำดับของรหัสผ่านปัจจุบัน

การแสดงหมายเลขลำดับของรหัสผ่านปัจจุบันให้ผู้ใช้ทราบหลังจากพิมพ์ชื่อลงบันทึกเข้าใช้ เป็นการอำนวยความสะดวกในการทำงานให้กับผู้ใช้เพื่อลดความยุ่งยากในการตรวจสอบลำดับของรหัสผ่านปัจจุบัน โดยเฉพาะอย่างยิ่งกลุ่มของผู้ใช้ในกรณีที่ใช้ชื่อลงบันทึกเข้าใช้เดียวกัน แต่การทำเช่นนี้ต้องทำการเปลี่ยนแปลงขั้นตอนของการสื่อสาร ซึ่งสามารถแสดงให้เห็น ดังรูป



รูปที่ 3.6 ขั้นตอนการสื่อสารในระบบของคุณพิษณุที่ได้รับการปรับปรุง

ตัวอย่าง

login : jkit

otp 77

password : _____

เพราะฉะนั้น รูปแบบของกลุ่มข้อมูลที่ใช้ในการสื่อสารจึงควรมีส่วนที่ใช้บอกประเภทของคำร้องขอและการตอบกลับของกลุ่มข้อมูลที่ใช้ในการสื่อสารในแต่ละครั้ง

ฟิลด์	รูปแบบ	รายละเอียด
Request_Reply	Short Integer	ประเภทของคำร้องขอและการตอบกลับ

ตารางที่ 3.6 รูปแบบของข้อมูลที่ใช้เพื่อบอกประเภทของคำร้องขอและการตอบกลับ

ตัวอย่างข้อมูลที่ใช้ในการสื่อสาร

ข้อมูล	ส่ง/รับ	เหตุการณ์ที่เกี่ยวข้อง
10	L/P	เมื่อต้องการทราบหมายเลขลำดับของรหัสผ่านปัจจุบัน
11	P/L	การตอบกลับหมายเลขลำดับของรหัสผ่านปัจจุบัน
1	L/P	เมื่อต้องการตรวจสอบรหัสผ่าน
2	P/L	ผลของการตรวจสอบรหัสผ่านกลับสู่โปรแกรมล็อกอิน
4	L/P	เมื่อต้องการสร้างรหัสผ่านชุดใหม่
5	L/P	เมื่อต้องการเลื่อนไปใช้รหัสผ่านตัวแรกในคอลัมน์ถัดไป
6	L/P	เมื่อต้องการเลื่อนไปใช้รหัสผ่านตัวแรกในแฟ้มรหัสผ่านชุดถัดไป
9	P/L	1. ผลของการสร้างรหัสผ่านชุดใหม่ 2. ผลของการเลื่อนไปใช้รหัสผ่านตัวแรกในคอลัมน์ถัดไป 3. ผลของการเลื่อนไปใช้รหัสผ่านตัวแรกในแฟ้มรหัสผ่านชุดถัดไป
99	P/L	เมื่อมีความผิดพลาดในการทำงาน

หมายเหตุ

L/P : โปรแกรมล็อกอินส่งความต้องการให้กับส่วนให้บริการรหัสผ่าน

P/L : โปรแกรมล็อกอินรับผลการทำงานจากส่วนให้บริการรหัสผ่าน

ปัญหาที่เกิดขึ้นจากขั้นตอนที่เพิ่มขึ้นเพื่ออำนวยความสะดวกให้กับผู้ใช้คือ ถ้ากลุ่มของผู้ใช้ต้องการเข้าใช้ระบบพร้อมกันโดยใช้ชื่อลงบันทึกเข้าใช้เดียวกัน หลังจากพิมพ์ชื่อลงบันทึกเข้าใช้ระบบจะแสดงหมายเลขลำดับเดียวกันของรหัสผ่านให้ผู้ใช้พิมพ์รหัสผ่าน ผู้ใช้คนแรกที่พิมพ์รหัสผ่านถูกต้องเท่านั้นที่สามารถเข้าสู่ระบบได้ เพราะลำดับของรหัสผ่านที่เก็บไว้ที่ส่วนให้บริการจะเปลี่ยนไป ทำให้ผู้ใช้อื่นที่พิมพ์รหัสเดียวกันแต่ช้ากว่าไม่สามารถเข้าสู่ระบบได้ ปัญหานี้สามารถแก้ไขได้ด้วยการห้ามไม่ให้มีการใช้ชื่อลงบันทึกเข้าใช้เดียวกันเข้าใช้ระบบได้พร้อมกัน โดยการกำหนดให้ส่วนให้บริการทำการหน่วงเวลาไว้จนกว่าจะรู้ผลของการเข้าสู่ระบบของผู้ใช้คนแรกจึงจะแสดงหมายเลขลำดับรหัสผ่านปัจจุบันให้ผู้ใช้ลำดับถัดไปทราบ

5. เพิ่มรุ่นควบคุม

จากข้อมูลที่ผ่านมาทำให้คาดเดาได้ว่าหลังจากระบบได้รับการปรับปรุง จะสามารถรองรับเงื่อนไขและมีทางเลือกที่หลากหลาย จึงสมควรอย่างยิ่งที่ควรมีการเจรจาระหว่างส่วนขอใช้และส่วนให้บริการเพื่อให้เข้าใจตรงกันเกี่ยวกับขั้นตอนและความสามารถในการตอบสนองความต้องการ ก่อนดำเนินการขั้นตอนต่อไป

ฟิลด์	รูปแบบ	รายละเอียด
Version	Integer	รุ่นควบคุม

ตารางที่ 3.7 รูปแบบของข้อมูลที่ใช้เพื่อบอกรุ่นควบคุม

ตัวอย่าง

000 รุ่นของคุณพิษณุ
100 รุ่นของคุณพิษณุที่ได้รับการปรับปรุงในส่วนของขั้นตอนในการสื่อสาร
101 ปรับปรุงจากรุ่น 100 โดยเพิ่มส่วนของการเข้ารหัสข้อมูลชนิด DES ให้เป็นทางเลือก

จากข้อมูลตัวอย่าง แสดงให้เห็นว่าตัวเลข 2 หลักสุดท้ายจะถูกใช้เพื่อระบุถึงการเปลี่ยนแปลงเพียงเล็กน้อย เช่น เพิ่มส่วนของการเข้ารหัสชนิด DES ให้ระบบเดิม ตรงกันข้ามกับตัวเลขลำดับก่อนหน้าจะถูกใช้เมื่อมีการเปลี่ยนแปลงมากพอสมควร เช่น เปลี่ยนแปลงขั้นตอนการสื่อสาร ดังนั้นในกรณีที่ทั้งสองฝ่ายใช้รุ่นที่หมายเลขลำดับก่อน 2 หลักสุดท้ายเหมือนกัน ส่วนให้บริการซึ่งใช้รุ่นที่มากกว่าจะสามารถรองรับส่วนขอใช้บริการที่ใช้รุ่นน้อยกว่าได้เสมอ แต่สำหรับรุ่นที่มีหมายเลขลำดับก่อน 2 หลักสุดท้ายต่างกัน ส่วนให้บริการซึ่งใช้รุ่นที่มากกว่าจะรองรับรุ่นน้อยกว่าได้หรือไม่ขึ้นอยู่กับวัตถุประสงค์ในการพัฒนา

6. ข้อมูลที่เกี่ยวข้อง

ข้อมูลที่เกี่ยวข้องจะต้องสอดคล้องกับรุ่นควบคุม ชนิดของอัลกอริทึม ชนิดของการเข้ารหัส และข้อมูลที่ใช้บอกประเภทของคำร้องขอและการตอบกลับ ขนาดของข้อมูลของการสื่อสารในแต่ละครั้งจึงไม่สามารถระบุได้แน่นอน ขึ้นอยู่กับปัจจัยดังกล่าว เพื่อกำหนดขนาดให้ฟิลด์ของข้อมูลที่เกี่ยวข้องให้สามารถรองรับข้อมูลได้อย่างมีประสิทธิภาพควรทำให้ขนาดที่ใช้รองรับข้อมูลสามารถยืดหยุ่นได้ โดยเพิ่มฟิลด์ตัวเลขสำหรับใช้ระบุขนาดของข้อมูลให้กับรูปแบบของกลุ่มข้อมูล

ฟิลด์	รูปแบบ	รายละเอียด
Data_Length	Short Integer	ขนาดของข้อมูลที่เกี่ยวข้อง
Data	String	ข้อมูลที่เกี่ยวข้อง

ตารางที่ 3.8 รูปแบบของข้อมูลที่ใช้รองรับข้อมูลที่สอดคล้องกับวัตถุประสงค์

ตัวอย่าง

###	หมายเลขลำดับของรหัสผ่านปัจจุบัน
******	รหัสผ่านปัจจุบัน
Ok	รหัสผ่านถูกต้อง
Message	ข้อความต่าง ๆ
Error	ข้อผิดพลาดต่าง ๆ

สำหรับฟิลด์ที่ใช้ส่งเวลาที่สร้างกลุ่มข้อมูล (Time_Val) ยังคงรูปแบบเดิมเพื่อนำมาใช้สำหรับจัดการในส่วนของการยึด (lock) ชื่อบัญชีผู้ใช้ เพื่อป้องกันปัญหาที่อาจเกิดขึ้นในกรณีที่กลุ่มผู้ใช้ต้องการเข้าระบบพร้อมกันโดยใช้ชื่อลงบันทึกเดียวกัน

7. การศึกษาความเป็นไปได้ทางการพัฒนาส่วนขอใช้บริการบนระบบปฏิบัติการเน็ตแวร์และวินโดวส์เอ็นที

7.1 ระบบปฏิบัติการเน็ตแวร์

เนื่องจากไม่สามารถหาโปรแกรมต้นฉบับของโปรแกรมล็อกอินได้เหมือนกับระบบยูนิกซ์ วิธีการหนึ่งที่สามารถทำได้เพื่อพัฒนาระบบรหัสผ่านแบบใช้ครั้งเดียวก็คือ การสร้างส่วนที่ทำหน้าที่เสมือนเป็นหน้ากากขึ้นมาครอบโปรแกรมล็อกอินของระบบ ซึ่งมีวิธีการและขั้นตอนการทำงานดังนี้

วิธีการจัดการ

1) กำหนดให้ชื่อลงบันทึกเข้าใช้ระบบรหัสผ่านให้สามารถเข้าสู่ระบบปฏิบัติการได้โดยไม่ต้องใช้รหัสผ่านในการตรวจสอบ หรือใช้รหัสผ่านที่ไม่มีการเปลี่ยนแปลง

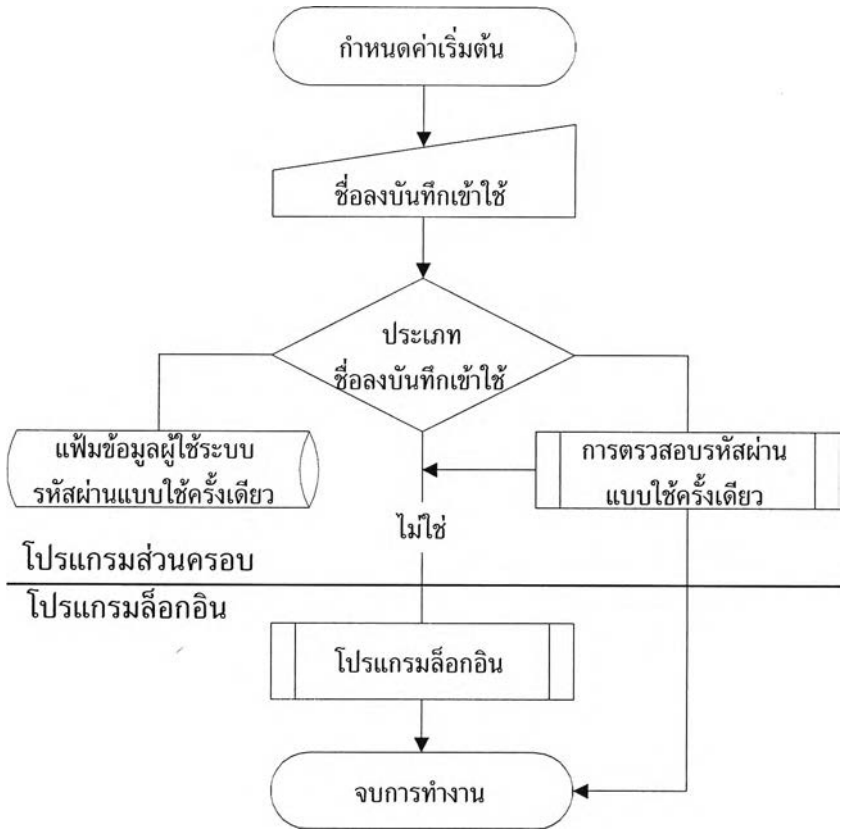
2) สร้างแฟ้มข้อมูลสำหรับเก็บชื่อลงบันทึกเข้าใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว

3) ซ่อนโปรแกรมล็อกอินของระบบเพื่อไม่ให้ผู้ใช้ทราบ เช่น การเปลี่ยนชื่อโปรแกรม

4) พัฒนาโปรแกรมขึ้นมาเป็นหน้ากากโปรแกรมล็อกอินของระบบ ให้มีรูปแบบการทำงานเหมือนกับโปรแกรมล็อกอิน

รูปแบบของคำสั่งโปรแกรมล็อกอินของระบบปฏิบัติการเน็ตแวร์ รุ่น 3.12

LOGIN [/option...] [fileserver[name]] [scriptparameters]



รูปที่ 3.7 ขั้นตอนการทำงานของการระบบรหัสผ่านแบบใช้ครั้งเดียวบนระบบเน็ตแวร์

ขั้นตอนการทำงาน

1) กำหนดค่าเริ่มต้นของระบบ
2) ผู้ใช้พิมพ์ชื่อลงบันทึกเข้าใช้ระบบ
3) โปรแกรมที่พัฒนาทำการตรวจสอบชื่อลงบันทึกเข้าใช้เทียบกับแฟ้มข้อมูลผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว
4) ผลการตรวจสอบ
   4.1) ถ้าชื่อลงบันทึกเข้าใช้เป็นของระบบเน็ตแวร์โปรแกรมจะเรียกโปรแกรมล็อกอินของระบบพร้อมทั้งผ่านกลุ่มของพารามิเตอร์ให้ดำเนินการต่อไป
   4.2) ถ้าชื่อลงบันทึกเข้าใช้เป็นของระบบรหัสผ่านแบบใช้ครั้งเดียว ชื่อลงบันทึกเข้าใช้นั้นจะถูกส่งให้ส่วนบริการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว
      4.2.1) ผลการตรวจสอบถูกต้องโปรแกรมจะผ่านกลุ่มของพารามิเตอร์ รวมทั้งรหัสผ่านที่ไม่เปลี่ยนแปลงของชื่อลงบันทึกเข้าใช้ในกรณีที่กำหนดให้ชื่อลงบันทึกเข้าใช้ต้องมีรหัสผ่าน ให้โปรแกรมล็อกอินของระบบ
      4.2.2) รหัสผ่านไม่ถูกต้องโปรแกรมจะสิ้นสุด

7.2 ระบบปฏิบัติการวินโดวส์เอ็นที

ปัญหาเนื่องจากไม่สามารถหาโปรแกรมต้นแบบมาศึกษายังคงเกิดขึ้นกับระบบปฏิบัติการวินโดวส์เอ็นทีเหมือนกับระบบปฏิบัติการเน็ตแวร์ และส่วนที่จัดการในการพิสูจน์ตัวจริงของผู้ใช้โดยใช้รหัสผ่านในภาวะกราฟฟิก (graphic mode) ไม่เหมือนกับระบบยูนิกซ์หรือของเน็ตแวร์ที่สามารถแยกเป็นแฟ้มเพื่อให้เรียกใช้ได้ทันที เพราะส่วนล็อกอินเข้าสู่ระบบจะรวมเป็นส่วนเดียวกันกับระบบปฏิบัติการ ซึ่งมีการจัดการที่ยุ่งยากซับซ้อนไม่สามารถแทรกโปรแกรมเข้าไปแก้ไขได้โดยตรง

อย่างไรก็ตาม การเข้าใช้งานระบบยังคงสามารถทำได้โดยผ่านส่วนต่อประสานรายงานคำสั่ง (command-line interface) ซึ่งในส่วนนี้มีความเป็นไปได้ที่จะพัฒนาโปรแกรมขึ้นมาครอบโปรแกรมล็อกอินเข้าสู่ระบบเหมือนกับระบบปฏิบัติการเน็ตแวร์

รูปแบบคำสั่งโปรแกรมล็อกอินของระบบปฏิบัติการวินโดวส์เอ็นที รุ่น 3.5 และ 4.0 ผ่านส่วนต่อประสานรายงานคำสั่ง

NET LOGON [user [password | ?]] [/DOMAIN:name] [/YES] [/SAVEPW:NO]

รูปแบบของกลุ่มข้อมูลที่ใช้ในการติดต่อสื่อสาร

จากข้อมูลที่กล่าวมาแล้วข้างต้น สามารถสรุปรูปแบบของกลุ่มข้อมูลให้รองรับพัฒนาการของระบบรหัสผ่านแบบใช้ครั้งเดียวเพื่อนำมาใช้ในการสื่อสารระหว่างส่วนขอใช้และส่วนให้บริการ ได้ดังตาราง

ฟิลด์	รูปแบบ	รายละเอียด
Version	Integer	รุ่นควบคุม
Time_Val	Char[10]	เวลาที่สร้างกลุ่มข้อมูลนี้
Domain_Length	Short Integer	ความยาวของชื่อเซิร์ฟเวอร์
Domain_Name	String	ชื่อเซิร์ฟเวอร์ที่ขอใช้บริการ
Login_Length	Short Integer	ความยาวของชื่อลงบันทึกเข้าใช้
Login_Name	String	ชื่อลงบันทึกเข้าใช้
Algorithm	Short Integer	ชนิดของอัลกอริทึม
Cryptograph	Short Integer	ชนิดของการเข้ารหัส
Request_Reply	Short Integer	ประเภทของคำร้องขอและการตอบกลับ
Data_Length	Short Integer	ความยาวของข้อมูลที่เกี่ยวข้อง
Data	String	ข้อมูลที่เกี่ยวข้อง

ตารางที่ 3.9 รูปแบบของกลุ่มข้อมูลที่ใช้ในการติดต่อสื่อสารที่ได้รับการปรับปรุง

สรุปผลการวิเคราะห์และออกแบบระบบ

จากการปรับปรุงรูปแบบของกลุ่มข้อมูลที่ใช้ในการสื่อสารระหว่างส่วนขอใช้และส่วนให้บริการ สามารถแก้ไขข้อจำกัดและการขยายประสิทธิภาพให้กับระบบเดิม ได้ดังตารางต่อไปนี้

ข้อจำกัดของระบบเดิม	หลังจากได้รับการปรับปรุง
1 ไม่ครอบคลุมผู้ใช้เซิร์ฟเวอร์หลายเครื่อง	1 ครอบคลุมผู้ใช้เซิร์ฟเวอร์หลายเครื่อง
2 วิธีการตรวจสอบและบำรุงรักษารหัสผ่านยังไม่ปลอดภัยเพียงพอ	2 เพิ่มทางเลือกในการตรวจสอบและบำรุงรักษารหัสผ่าน
3 ไม่ปลอดภัยจากการสื่อสารข้อมูล	3 เพิ่มทางเลือกในการเข้ารหัสข้อมูล
4 ไม่สะดวกต่อกลุ่มผู้ใช้ที่ต้องใช้ชื่อลงบันทึกเข้าใช้เดียวกัน	4 แสดงหมายเลขลำดับของรหัสผ่านปัจจุบันให้ผู้ใช้ทราบ
	5 เพิ่มรุ่นควบคุม

ตารางที่ 3.10 แสดงการเปรียบเทียบระบบก่อนและหลังปรับปรุง