บทที่ 3

การออกแบบระบบ

3.1 หลักการทำงานของระบบ

จากการทำงานของระบบบรหัสผ่านแบบใช้ครั้งเดียวของนายพิษณุ เกริกอำไพสุรกิจ เป็นการแก้ปัญหาระบบรหัสผ่าน (password) ของระบบปฏิบัติการยูนิกซ์ ซึ่งพบว่าอาจถูกลักลอบใช้โดยการค้นหารหัสผ่านด้วยวิธีต่างๆ[1] เช่น

- การลองใส่รหัสผ่านจนกระทั่งพบรหัสที่ถูก
- การคาดเดารหัสผ่านจากสิ่งที่เกี่ยวข้องกับผู้ใช้ เช่น ชื่อ-สกุล ที่อยู่ เลขประจำตัวนักศึกษา เป็นต้น
- การคาดเดารหัสผ่านจากคำศัพท์ในพจนานุกรม หรือกลุ่มคำที่เป็นที่รู้จักแพร่หลาย

การนำเอาระบบรหัสผ่านแบบใช้ครั้งเดียวมาใช้แทนระบบรหัสผ่านแบบเดิมของยูนิกซ์สามารถแก้ปัญหาดังกล่าวได้แต่ยังคงมีปัญหาบางประการที่ยังไม่ได้ถูกแก้ไข เช่น

- การดักฟัง (eavesdropping) รหัสผ่านบนเครือข่าย
- การขโมยแฟ้มรหัสผ่าน
- การปลอมตัวเป็นผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว

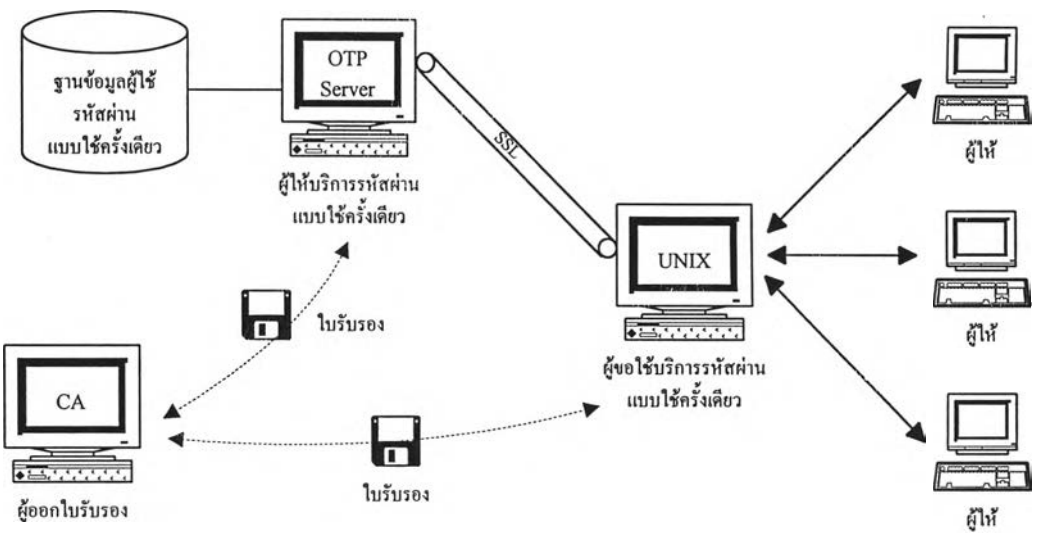
ดังนั้นจึงมีการออกแบบระบบรหัสผ่านแบบใช้ครั้งเดียวใหม่เพื่อแก้ปัญหาดังกล่าวดังนี้

- ให้มีช่องทางสื่อสารแบบเข้ารหัสที่ใช้เทคนิคการเข้ารหัสแบบลับเฉพาะเพื่อแก้ปัญหาการดักฟัง
- เพิ่มให้มีการพิสูจน์ตัวจริงโดยใช้เทคนิคการเข้ารหัสแบบสาธารณะเพื่อป้องกันการปลอมตัวเป็นผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว
- ใช้ระบบจัดการฐานข้อมูลแบบเชิงสัมพันธ์ในการเก็บข้อมูลบัญชีผู้ใช้ เครื่องที่อยู่ในความดูแลและข้อมูลรหัส ซึ่งทำให้สามารถควบคุมการเข้าถึง (access control) ข้อมูลที่มีความสำคัญได้ในระดับหนึ่ง

- ปิดกั้นการเข้าถึงเครื่องให้บริการผ่านเครือข่ายที่ไม่จำเป็น คงไว้แต่เพียงบริการรหัสผ่านแบบใช้ครั้งเดียวเท่านั้น

3.2 องค์ประกอบของระบบ

ประกอบด้วย 3 ส่วน ดังแสดงในรูปที่ 3.1 คือ



รูปที่ 3.1 แสดงระบบให้บริการรหัสผ่านแบบใช้ครั้งเดียวที่เสริมความปลอดภัยด้วยชั้นโพรโทคอลเอสเอสแอล

3.2.1 ผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว

คือ เครื่องพีซีที่ทำหน้าที่ตรวจสอบรหัสผ่านแบบใช้ครั้งเดียวผ่านช่องทางสื่อสารแบบเข้ารหัสที่มีการพิสูจน์ตัวจริงและบำรุงรักษาฐานข้อมูลของระบบรหัสผ่านแบบใช้ครั้งเดียว

3.2.2 ผู้ขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว

คือเครื่องยูนิกซ์ที่มีการปรับปรุงโปรแกรมล็อกอินให้มีการทำงานได้ทั้งแบบใช้รหัสผ่านแบบยูนิกซ์และใช้รหัสผ่านแบบใช้ครั้งเดียว โดยการตรวจสอบประเภทของผู้ใช้จากแฟ้มข้อมูล "/etc passwd "

3.2.3 ผู้ออกใบรับรอง (Certification Authorities)

ทำหน้าที่ออกใบรับรอง (Certificate) ของทั้งผู้ให้บริการและของตนเอง เพื่อใช้ในการพิสูจน์ตัวจริง

3.3 ลำดับการทำงานของระบบ (workflow)

ขั้นตอนการทำงานของระบบรหัสผ่านแบบใช้ครั้งเดียวสามารถแบ่งได้ 4 ขั้นตอน ดังแสดงในรูปที่ 3.2 คือ

3.3.1 ขั้นตอนการขอใบรับรอง

เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นผู้ให้บริการและผู้ขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว (ในที่นี้หมายถึง เครื่องแม่ข่ายยูนิกซ์) จะต้องขอใบรับรอง (certificate) จากผู้ออกใบรับรอง (Certification Authorities)

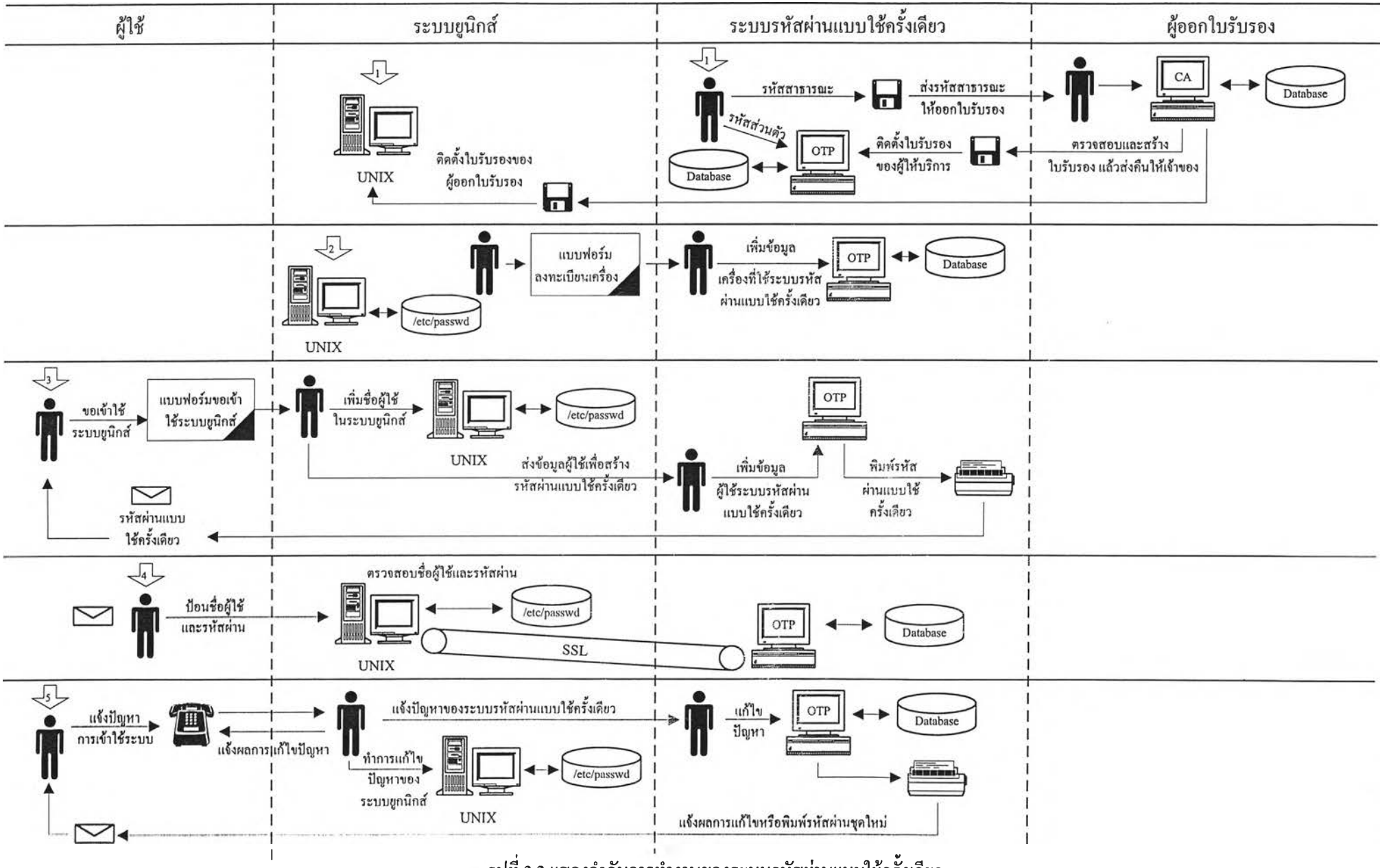
3.3.1.1 ผู้ให้บริการทำการสร้างคีย์สาธารณะและคีย์ส่วนตัวขึ้นหนึ่งชุดโดยโปรแกรมสร้างคีย์

3.3.1.2 ผู้ให้บริการนำคีย์สาธารณะไปขอออกใบรับรองจากผู้ออกใบรับรอง

3.3.1.3 ผู้ให้บริการนำใบรับรองของตนเองและของผู้ออกใบรับรองมาติดตั้งลงบนเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นผู้ให้บริการ

3.3.1.4 ผู้ขอใช้บริการระบบรหัสผ่านแบบใช้ครั้งเดียวขอใบรับรองของผู้ออกใบรับรองมาติดตั้งลงบนเครื่องคอมพิวเตอร์ที่เป็นผู้ขอใช้บริการ

หลังจากที่ทำการติดตั้งใบรับรองเป็นที่เรียบร้อยแล้วผู้ให้บริการจะสามารถพิสูจน์ตัวจริงต่อผู้ขอใช้บริการได้



รูปที่ 3.2 แสดงลำดับการทำงานของระบบรหัสผ่านแบบใช้ครั้งเดียว

3.3.2 ผู้ขอใช้บริการรหัสผ่านขอลงทะเบียนชื่อเครื่อง ชื่อโดเมน และหมายเลขไอพีต่อผู้ให้บริการ เพื่อเข้าอยู่ในขอบเขตการดูแล (region) ของผู้ให้บริการ

3.3.3 ขั้นตอนการเพิ่มผู้ใช้เข้าสู่ระบบ

เป็นขั้นตอนในการเพิ่มผู้ใช้คนใหม่เข้าสู่ระบบยูนิกซ์ ซึ่งสามารถแยกประเภทผู้ใช้ได้ 2 ประเภท คือ

- ผู้ใช้ที่ใช้ระบบรหัสผ่านแบบยูนิกซ์
- ผู้ใช้ที่ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว

ดังมีขั้นตอนดังนี้

3.3.3.1 ผู้ใช้กรอกใบสมัครขอเข้าใช้บริการ

3.3.3.2 ผู้บริหารระบบยูนิกซ์พิจารณาว่าผู้ใช้ต้องการใช้รหัสผ่านประเภทใด ถ้าต้องการใช้รหัสผ่านแบบยูนิกซ์ผู้บริหารระบบสามารถเพิ่มชื่อผู้ใช้ในแฟ้ม "/etc/passwd" ตามปกติเป็นอันสิ้นสุดขั้นตอนการเพิ่ม
แต่ถ้าต้องการใช้รหัสผ่านแบบใช้ครั้งเดียวให้แก้เขตข้อมูลที่สองจากรหัสผ่านของยูนิกซ์เป็นข้อความว่า "*OPT*" แทนรหัสผ่านดังตัวอย่าง

```
postgres:!!:100:233:PostgreSQL Server:/var/lib/pgsql:/bin/bash
psycho:qO4AsB4coVaB.:501:501:Wanlop Jia:/usr/home/psycho:/bin/bash
msql:!!:300:300:mSQL Server:/usr/local/Hughes:/nosuchshell
anu:xvNavVUjhf45c:502:501:anuchart tassanaviboon:/usr/home/anu:/bin/bash
anu1:*OTP*:503:501:anuchart tassanaviboon:/usr/home/anu1:/bin/bash
```

จากนั้นส่งข้อมูลผู้ใช้ให้ผู้บริหารระบบรหัสผ่านแบบใช้ครั้งเดียวดำเนินการต่อไป

3.3.3.3 ผู้บริหารระบบรหัสผ่านแบบใช้ครั้งเดียวเพิ่มข้อมูลผู้ใช้ระบบผ่านทางโปรแกรมบำรุงรักษาระบบรหัสผ่านแบบใช้ครั้งเดียว ซึ่งโปรแกรมจะสร้างตารางข้อมูลรหัสผ่านและจัดพิมพ์รายงานรหัสผ่านเพื่อจัดส่งให้ผู้ใช้

3.3.4 ขั้นตอนการเข้าใช้ระบบยูนิกซ์

3.3.4.1 ผู้ใช้พิมพ์ชื่อผู้ใช้เมื่อได้รับข้อความพร้อมรับ (login :)

3.3.4.2 โปรแกรมล็อกอินจะตรวจสอบว่าเป็นผู้ใช้ที่ใช้รหัสผ่านแบบยูนิกซ์ หรือรหัสผ่านแบบใช้ครั้งเดียว

3.3.4.3 ผู้ใช้พิมพ์รหัสผ่านเมื่อได้รับข้อพร้อมรับ (password :) ถ้าเป็นผู้ใช้ที่ใช้รหัสผ่านแบบยูนิกซ์ ระบบยูนิกซ์จะตรวจสอบรหัสผ่านกับแฟ้ม /etc/passwd" แต่ถ้าเป็นผู้ใช้ที่ใช้รหัสผ่านแบบใช้ครั้งเดียว โปรแกรมล็อกอินจะส่งรหัสผ่านไปตรวจสอบที่ผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว

3.3.4.4 ถ้าผลการตรวจสอบรหัสผ่านถูกต้อง ระบบยูนิกซ์จะอนุญาตให้ผู้ใช้สามารถใช้งานได้ตามปกติ

3.3.5 ขั้นตอนการแจ้งปัญหาการใช้งาน

3.3.5.1 ผู้ใช้ติดต่อกับผู้บริหารยูนิกซ์ที่ผู้ใช้ต้องการใช้

3.3.5.2 ผู้บริหารยูนิกซ์ตรวจสอบปัญหา ถ้าเป็นปัญหาที่เกิดจากระบบยูนิกซ์สามารถทำการแก้ไขได้ทันที ถ้าเป็นปัญหาที่เกิดจากระบบรหัสผ่านแบบใช้ครั้งเดียว ทำการแจ้งผู้บริหารระบบรหัสผ่านแบบใช้ครั้งเดียวดำเนินแก้ไขต่อ

3.3.5.3 ผู้บริหารระบบรหัสผ่านแบบใช้ครั้งเดียวทำการแก้ไขผ่านโปรแกรมบำรุงรักษา แล้วแจ้งผลกลับให้ผู้ใช้

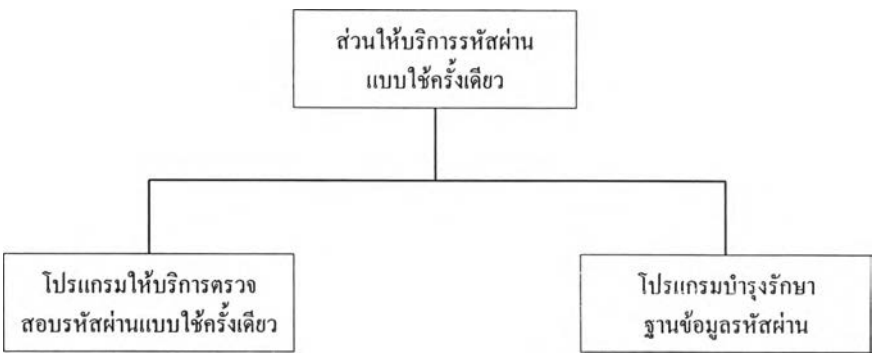
3.4 โครงสร้างและลำดับการทำงานของโปรแกรม

ระบบรหัสผ่านแบบใช้ครั้งเดียว ประกอบด้วยโปรแกรม 3 ส่วน คือ

- ส่วนให้บริการรหัสผ่านแบบใช้ครั้งเดียว
- ส่วนขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว
- ส่วนสร้างชุดคีย์สาธารณะและออกใบรับรอง

3.4.1 ส่วนให้บริการรหัสผ่านแบบใช้ครั้งเดียว

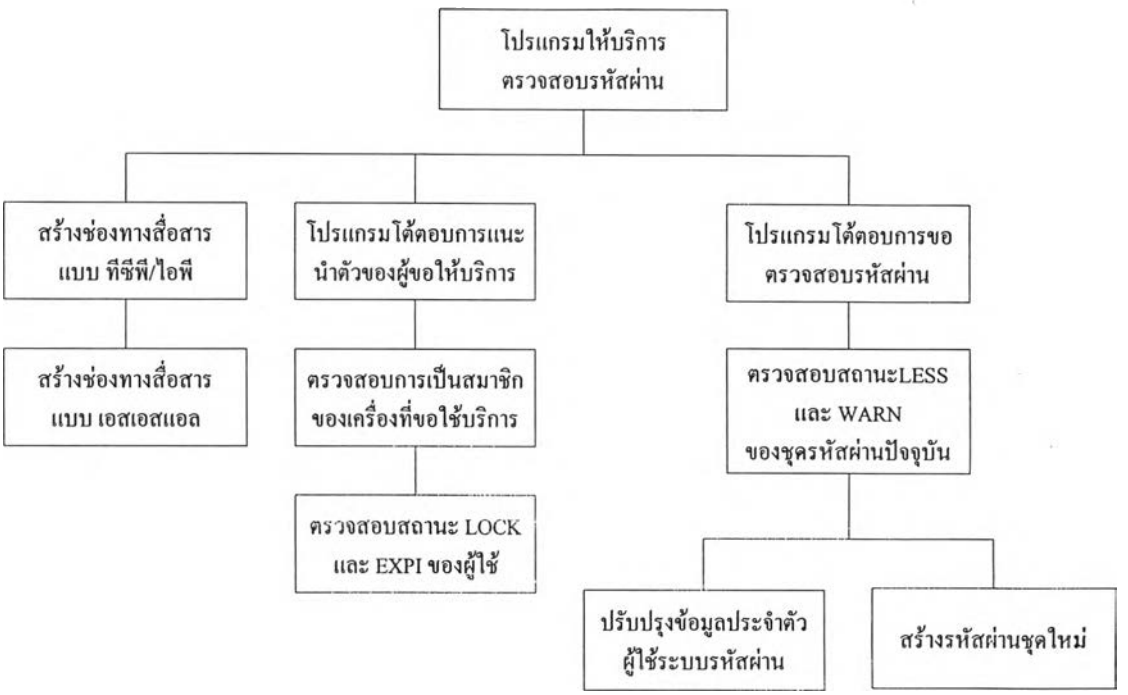
เป็นโปรแกรมที่ทำงานอยู่บนเครื่องให้บริการรหัสผ่านที่ใช้ระบบปฏิบัติการลินุกซ์ (LINUX) ประกอบด้วยโปรแกรมย่อยต่างๆ ซึ่งแสดงเป็นโครงสร้างได้ดังรูปที่ 3.3 คือ



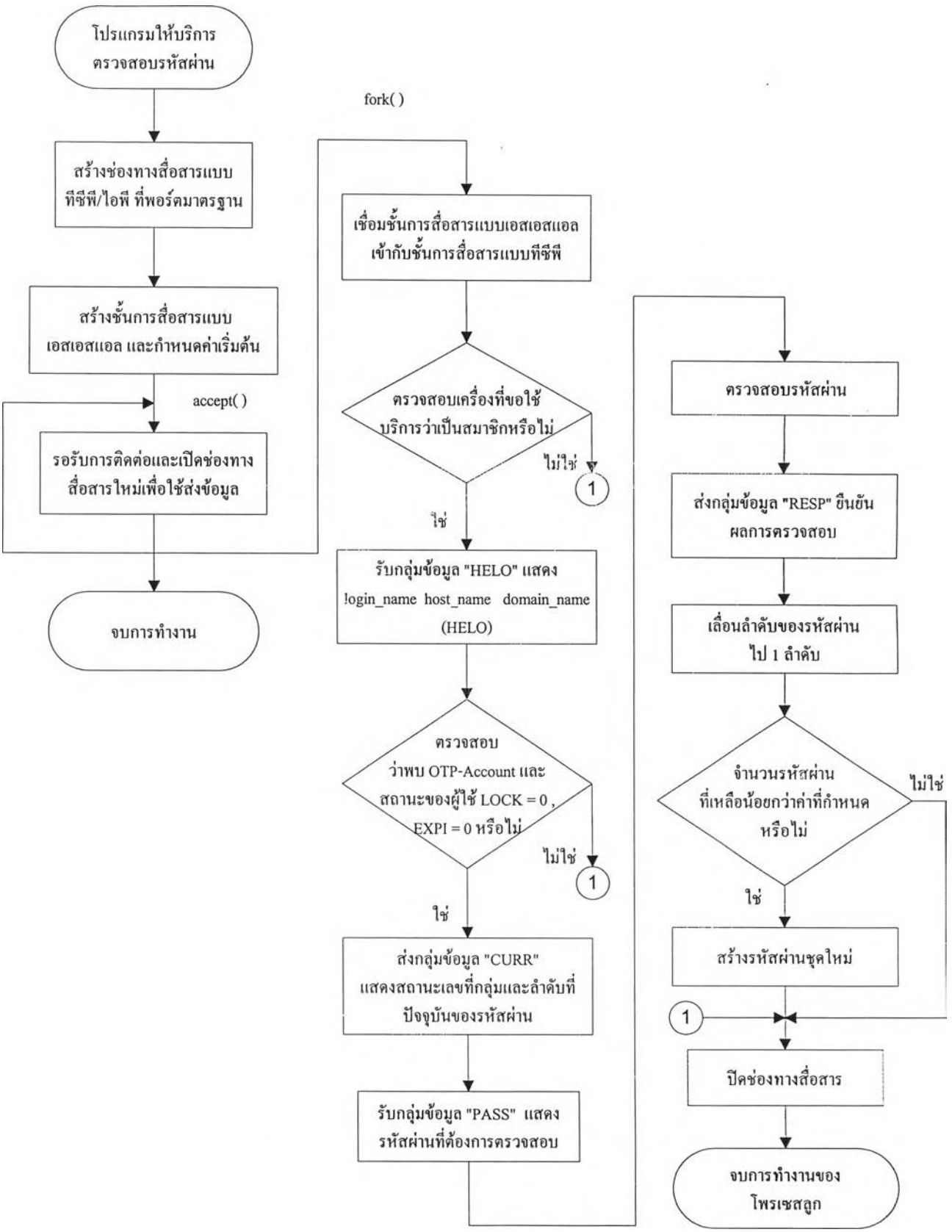
รูปที่ 3.3 โครงสร้างส่วนให้บริการรหัสผ่านแบบใช้ครั้งเดียว

3.4.1.1 โปรแกรมให้บริการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว

ทำหน้าที่รับรหัสผ่านจากผู้ขอใช้บริการมาทำการตรวจสอบและส่งผลตรวจสอบกลับไปยังผู้ขอใช้บริการแทนการตรวจสอบรหัสผ่านที่แฟ้ม "/etc/passwd" โพรเซสนี้จะทำงานในลักษณะเป็นการประมวลผลส่วนหลัง (background process) ที่มีการส่งผ่านข้อมูลไปยังผู้ขอใช้บริการผ่านทางช่องทางสื่อสารแบบเข้ารหัสและมีการพิสูจน์ตัวจริง โดยมีโครงสร้างของโปรแกรมดังแสดงในรูปที่ 3.4 และมีลำดับการทำงานของโปรแกรม ดังแสดงในรูปที่ 3.5



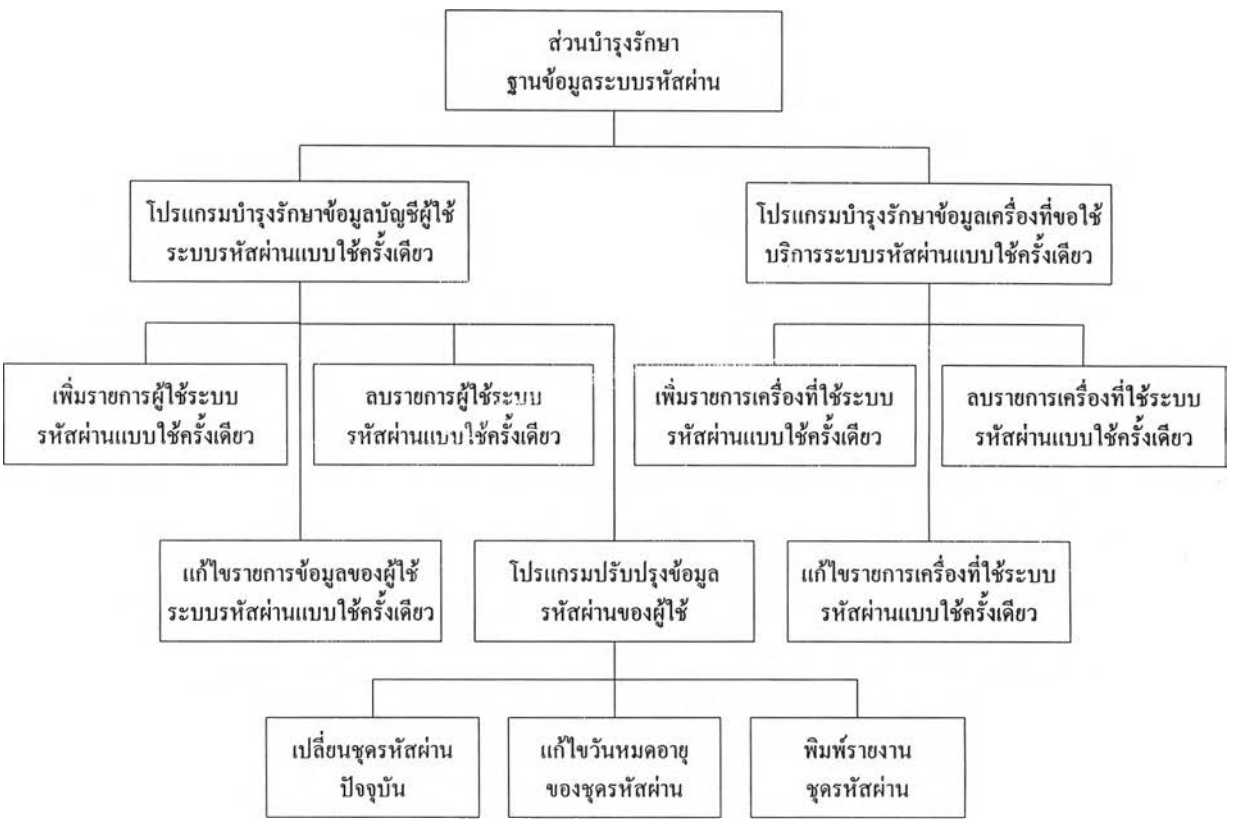
รูปที่ 3.4 โครงสร้างของโปรแกรมให้บริการตรวจสอบรหัสผ่าน



รูปที่ 3.5 ผังงานแสดงการทำงานของโปรแกรมให้บริการตรวจสอบรหัสผ่าน

3.4.1.2 โปรแกรมบำรุงรักษาฐานข้อมูลระบบรหัสผ่านแบบใช้ครั้งเดียว

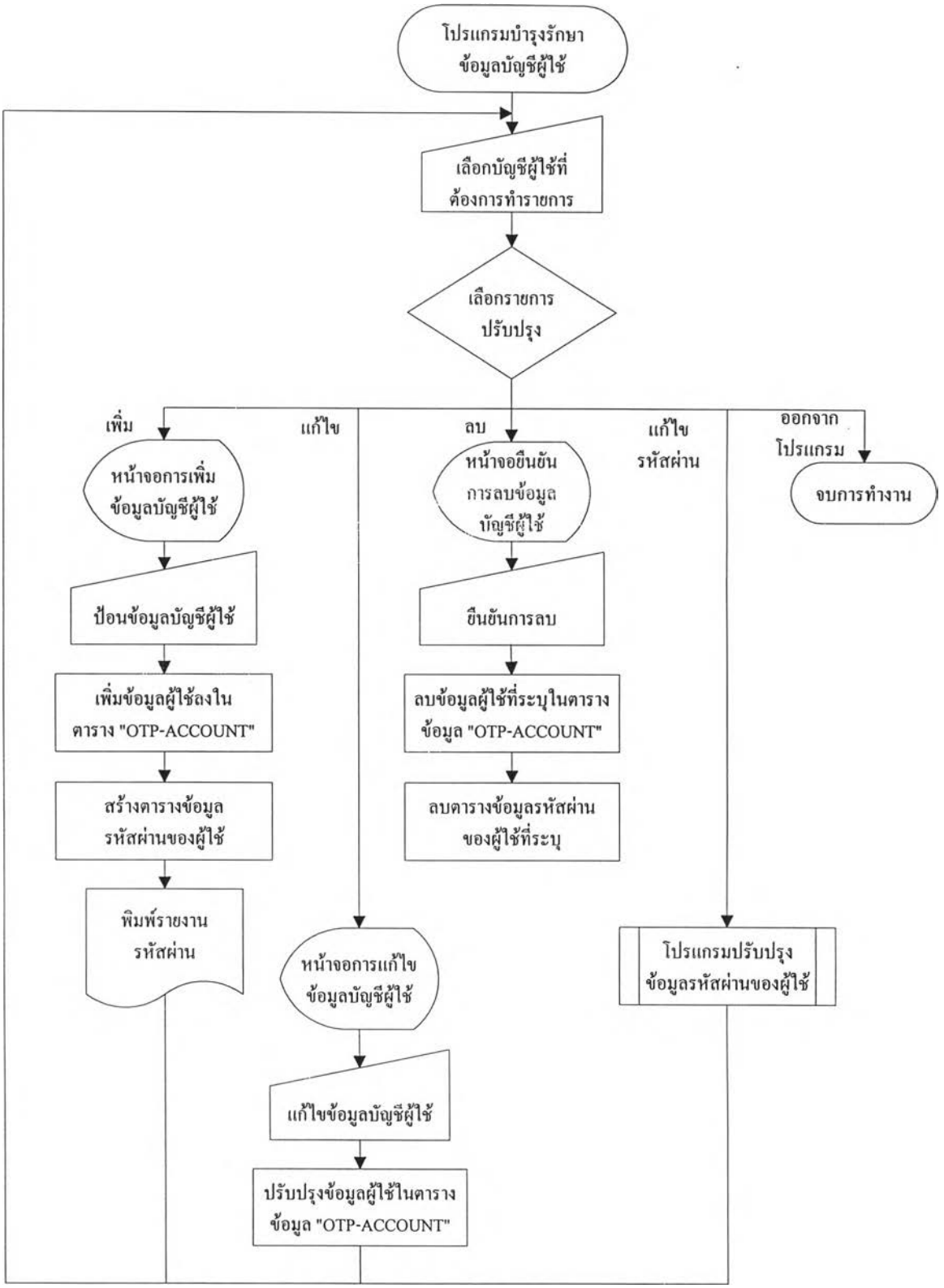
ทำหน้าที่ในการบำรุงรักษาฐานข้อมูลที่ใช้ในระบบ ได้แก่ ฐานข้อมูลบัญชีผู้ใช้ ฐานข้อมูลเครื่องขอใช้บริการ และฐานข้อมูลรหัสผ่าน โดยมีโครงสร้างของโปรแกรมดังรูปที่ 3.6 และมีความสามารถดังนี้



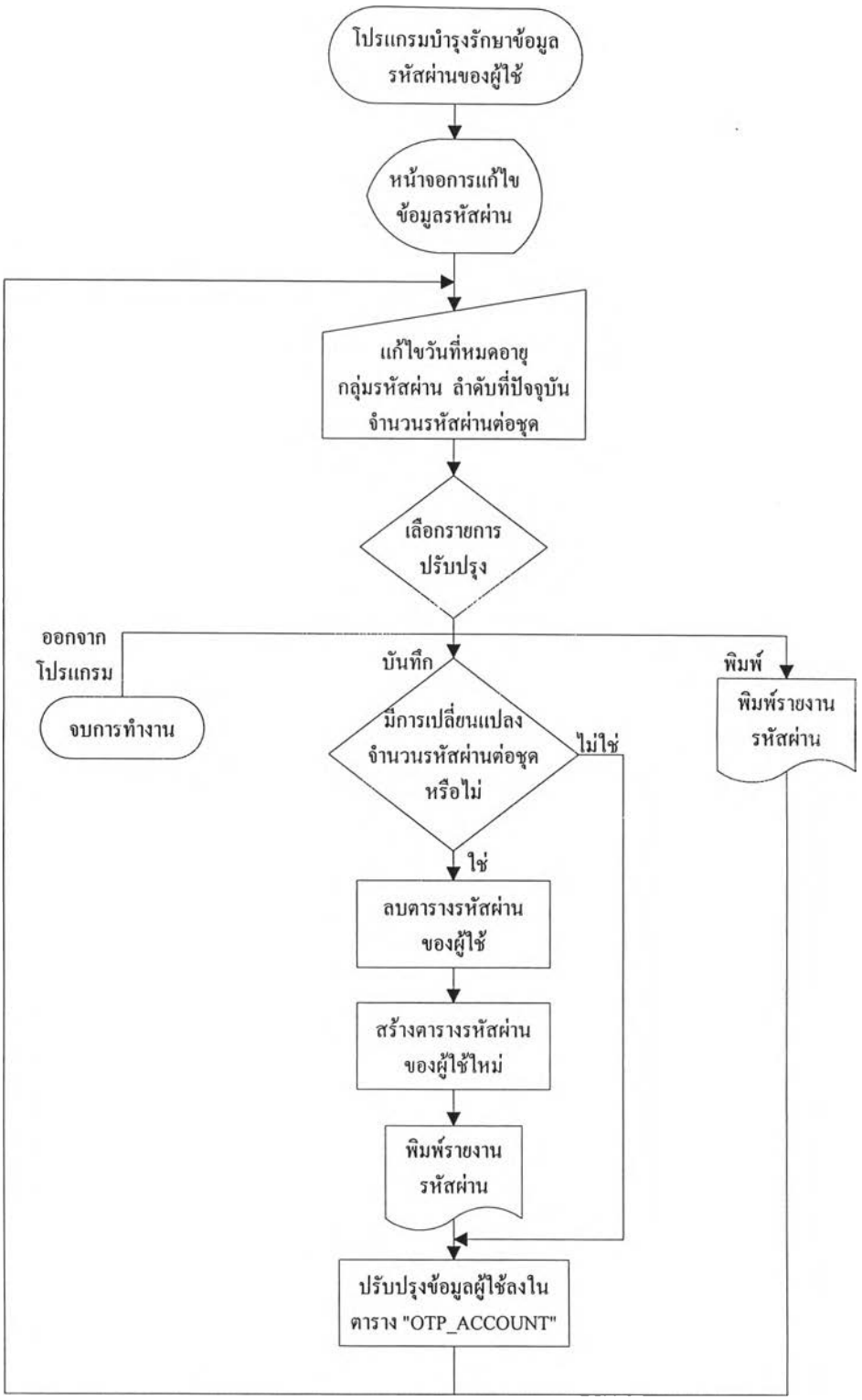
รูปที่ 3.6 โครงสร้างโปรแกรมบำรุงรักษาฐานข้อมูลระบบรหัสผ่าน

- เพิ่ม แก้ไข และลบ รายการในฐานข้อมูลบัญชีผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว
- แก้ไขข้อมูลเกี่ยวกับรหัสผ่าน เช่น วันที่หมดอายุ จำนวนรหัสผ่านต่อชุด กลุ่มรหัสผ่าน และลำดับที่ปัจจุบันของรหัสผ่าน
- เพิ่ม แก้ไข และลบ รายการในฐานข้อมูลเครื่องขอใช้บริการ

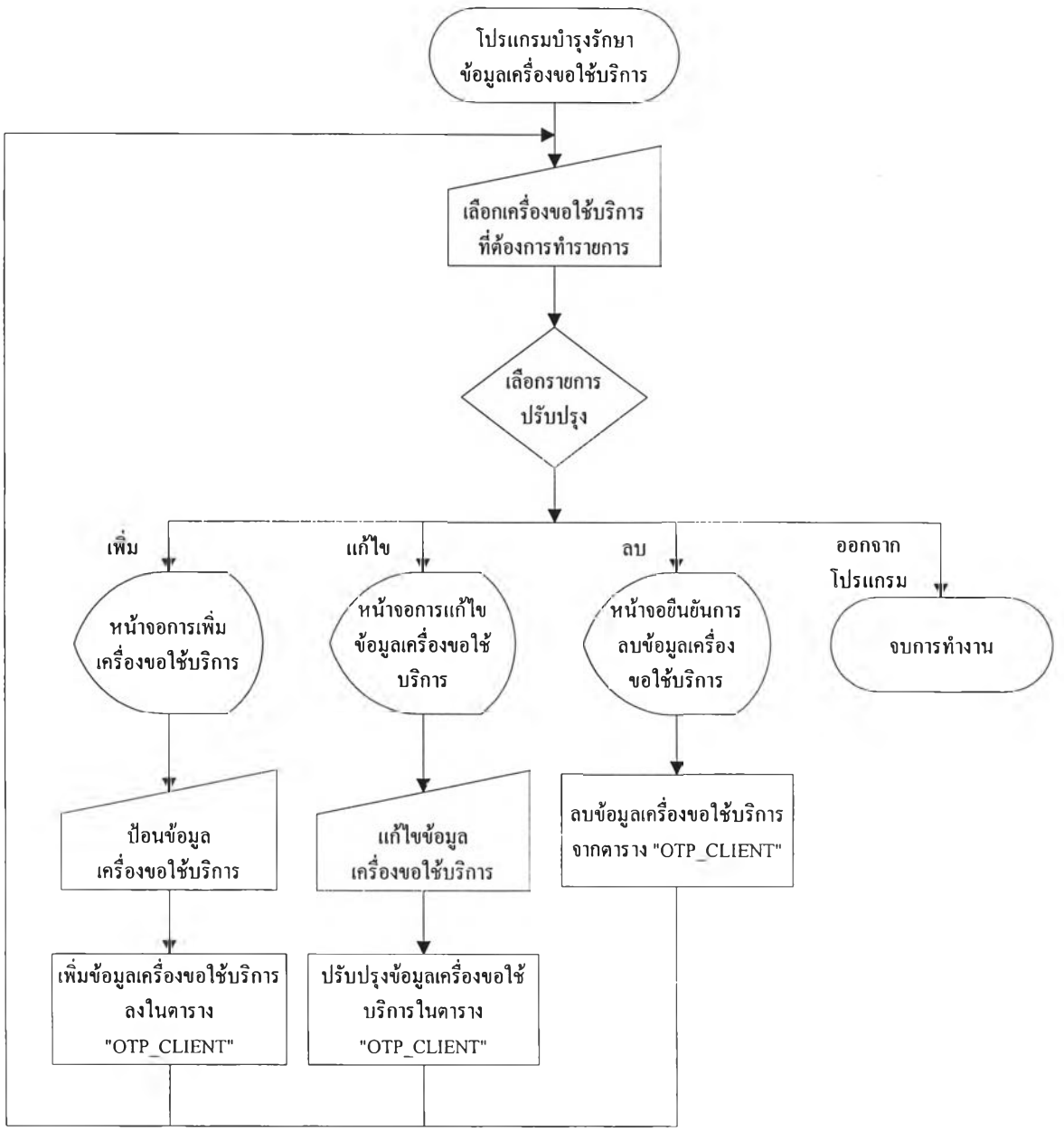
การทำงานของโปรแกรมทั้งหมดถูกแสดงในรูปที่ 3.7, 3.8 และ 3.9



รูปที่ 3.7 ผังงานแสดงการทำงานของโปรแกรมปรับปรุงข้อมูลบัญชีผู้ใช้



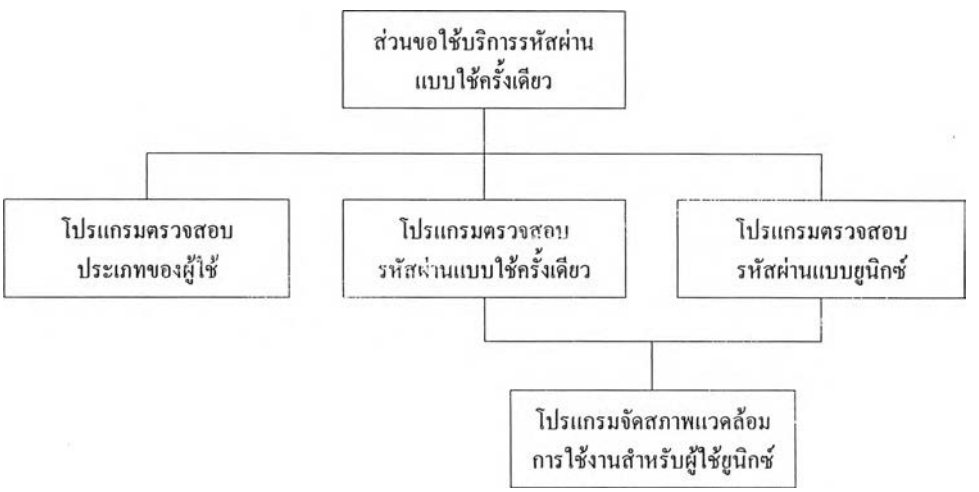
รูปที่ 3.8 ผังแสดงการทำงานของโปรแกรมปรับปรุงข้อมูลรหัสผ่านของผู้ใช้



รูปที่ 3.9 ผังงานแสดงการทำงานของโปรแกรมปรับปรุงข้อมูลเครื่องขอใช้บริการ

3.4.2 ส่วนขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว

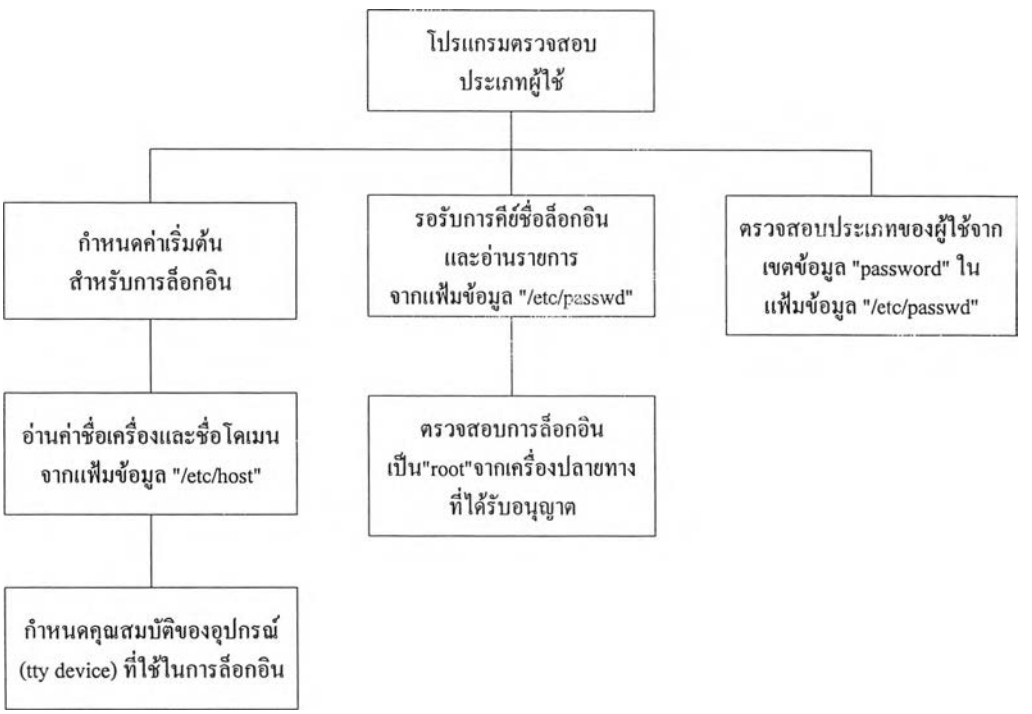
เป็นโปรแกรมที่ทำงานอยู่บนเครื่องยูนิกซ์ที่ขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว ทำหน้าที่ในการรับการคีย์ชื่อล็อกอิน (login name) และรหัสผ่าน (password) ซึ่งในที่นี้สามารถเป็นได้ทั้งรหัสผ่านและยูนิกซ์และรหัสผ่านแบบใช้ครั้งเดียว โดยขึ้นกับประเภทของผู้ใช้ ประกอบด้วยโปรแกรมย่อย ดังแสดงในรูปที่ 3.10 คือ



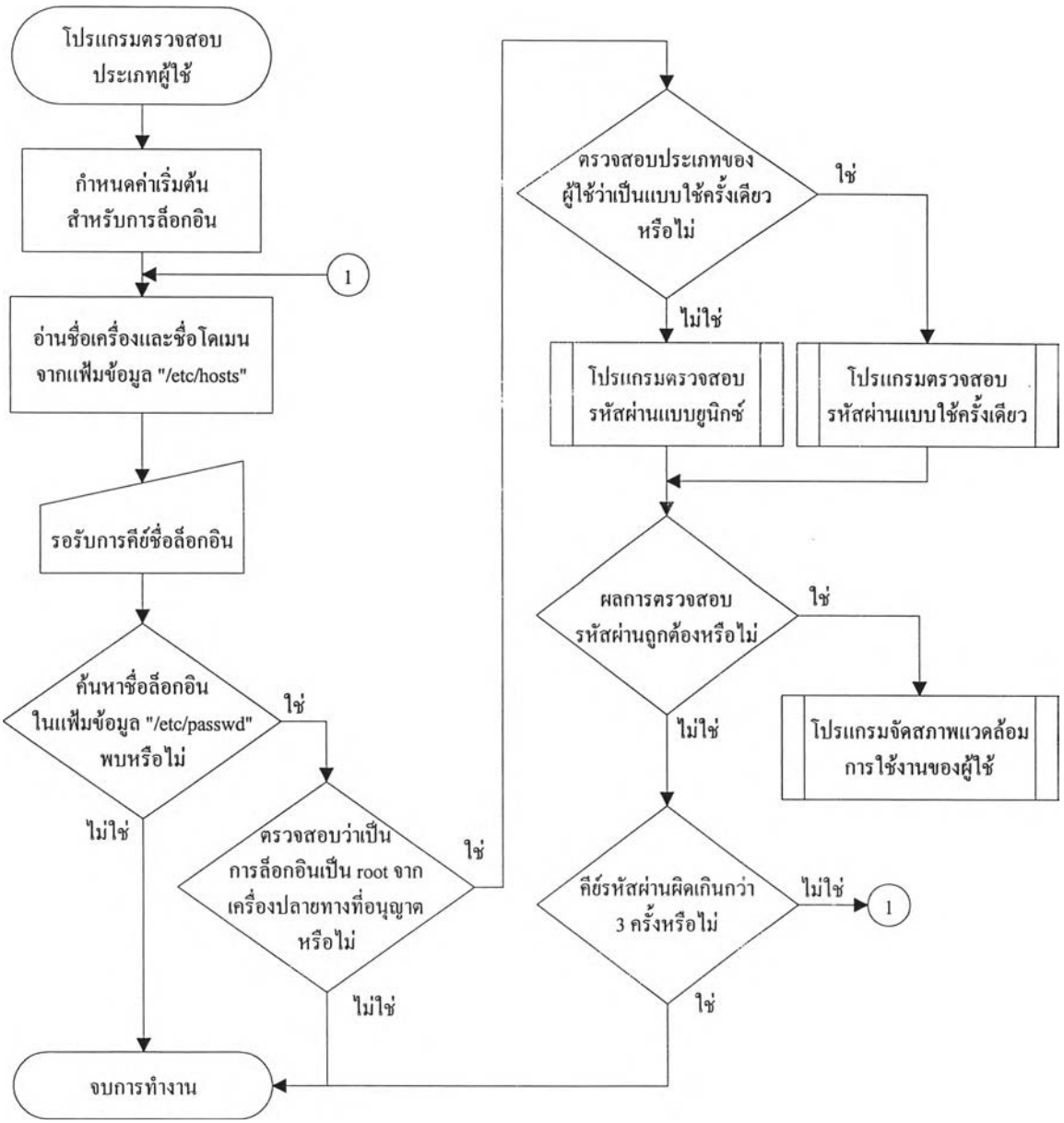
รูปที่ 3.10 โครงสร้างส่วนขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว

3.4.2.1 โปรแกรมตรวจสอบประเภทของผู้ใช้

เป็นโปรแกรมที่ทำหน้าที่แทนโปรแกรมล็อกอินปกติของยูนิกซ์ในการรับชื่อล็อกอินมาทำการตรวจสอบว่า ผู้ใช้จัดอยู่ในประเภทที่ใช้รหัสผ่านแบบยูนิกซ์หรือรหัสผ่านแบบใช้ครั้งเดียว โดยตรวจสอบจากแฟ้มข้อมูล "/etc/passwd" ถ้าเขตข้อมูลรหัสผ่านมีค่าเป็น "*OTP*" แสดงว่าเป็นผู้ใช้ประเภทใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว ดังมีโครงสร้างของโปรแกรมในรูปที่ 3.11 และมีการทำงานของโปรแกรมดังแสดงในรูปที่ 3.12



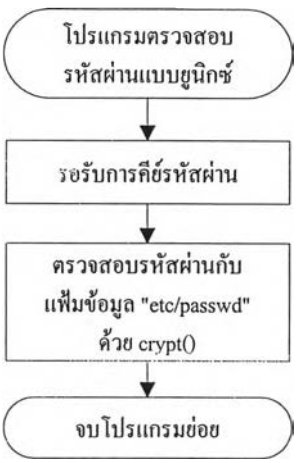
รูปที่ 3.11 โครงสร้างโปรแกรมตรวจสอบประเภทของผู้ใช้



รูปที่ 3.12 ผังงานแสดงการทำงานของโปรแกรมตรวจสอบประเภทของผู้ใช้

3.4.2.2 โปรแกรมตรวจสอบรหัสผ่านแบบยูนิกซ์

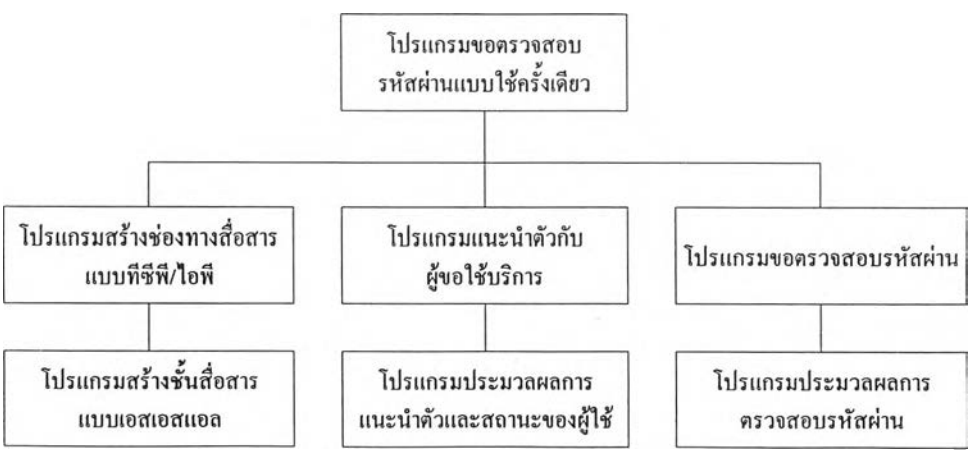
ทำหน้าที่ตรวจสอบความถูกต้องของรหัสผ่านกับแฟ้ม “etc/passwd” ถ้ารหัสผ่านถูกต้องจะกำหนดสภาพแวดล้อมและอนุญาตให้ผู้ใช้เข้าใช้งานได้



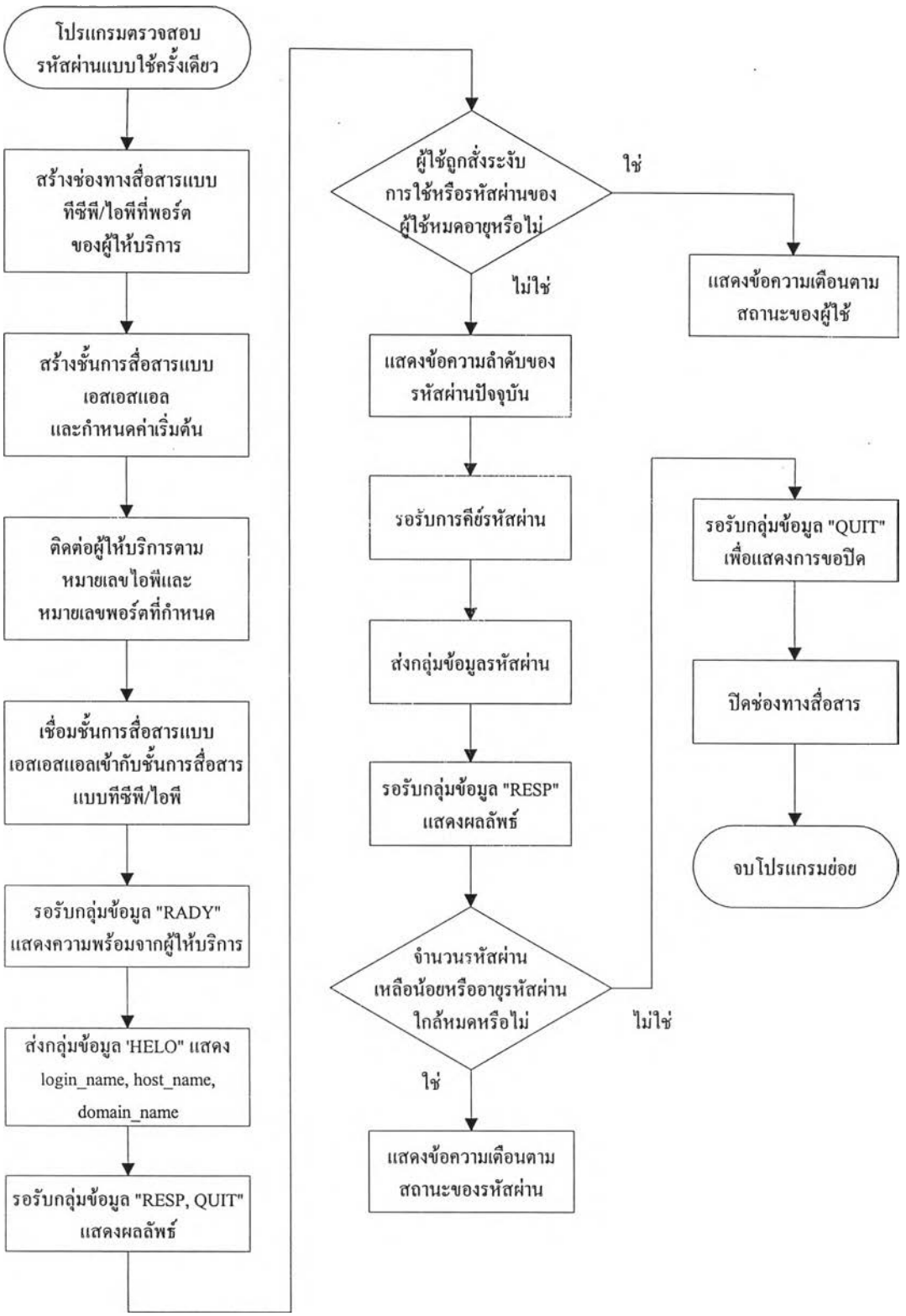
รูปที่ 3.13 ผังงานแสดงการทำงานของโปรแกรมตรวจสอบรหัสผ่านแบบยูนิกซ์

3.4.2.3 โปรแกรมตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว

ทำหน้าที่พิสูจน์ตัวจริงเครื่องให้บริการและสร้างช่องทางสื่อสารแบบเข้ารหัส จากนั้นส่งรหัสผ่านผ่านช่องทางสื่อสารแบบเข้ารหัสไปตรวจสอบ ถ้าผลการตรวจสอบถูกต้องจะกำหนดสภาพแวดล้อมและอนุญาตให้ผู้ใช้เข้าใช้งานได้ มีโครงสร้างของโปรแกรมดังแสดงในรูปที่ 3.14 และมีลำดับการทำงานของโปรแกรมดังแสดงในรูปที่ 3.15



รูปที่ 3.14 โครงสร้างโปรแกรมตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว



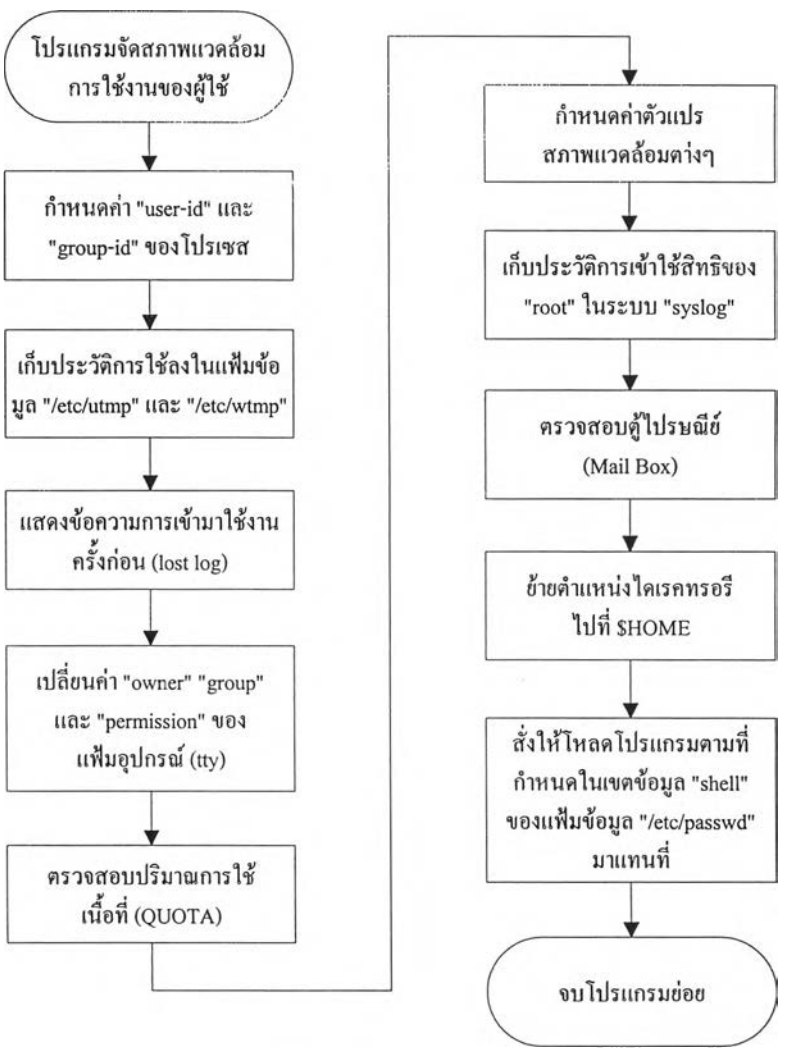
รูปที่ 3.15 ผังงานแสดงการทำงานของโปรแกรมตรวจสอบ
รหัสผ่านแบบใช้ครั้งเดียว

3.4.2.4 โปรแกรมจัดสภาพแวดล้อมการใช้งานสำหรับผู้ใช้ยูนิกซ์

ทำหน้าที่ในการกำหนดและจัดสภาพแวดล้อมของผู้ใช้ยูนิกซ์ตามที่ถูกกำหนดอยู่ในแฟ้มข้อมูล "/etc/passwd" ของยูนิกซ์ ได้แก่

- หมายเลขผู้ใช้ (user ID)
- หมายเลขกลุ่มผู้ใช้ (group ID)
- ไดเรกทรอรีของผู้ใช้ (home directory)
- โปรแกรมที่ถูกเรียกใช้ (shell program)

มีลำดับการทำงานของโปรแกรมดังแสดงในรูปที่ 3.16



รูปที่ 3.16 ผังงานแสดงการทำงานของโปรแกรมจัดสภาพแวดล้อมการใช้งานสำหรับผู้ใช้ยูนิกซ์

3.5 ลำดับการทำงานของโพรโทคอล

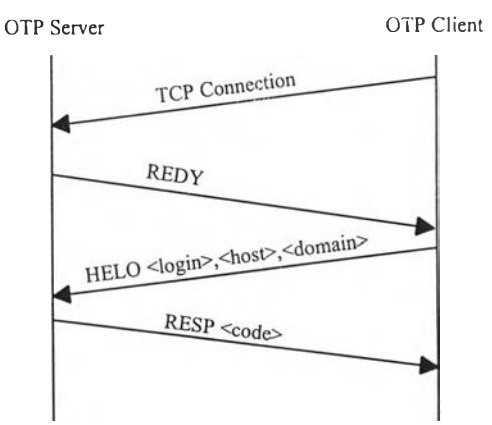
เนื่องจากมีความจำเป็นต้องแลกเปลี่ยนข้อมูลระหว่างผู้ให้บริการหัสผ่านแบบใช้ครั้งเดียว และผู้ขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว เพื่อการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว จึงมีความจำเป็นที่จะต้องกำหนดลำดับชั้นการแลกเปลี่ยนข้อมูลของชั้นสื่อสารประยุกต์ (application layer) ขึ้นเพื่อรองรับการทำงานดังกล่าว โพรโทคอลที่กำหนดสามารถแบ่งการทำงานออกได้เป็น 3 ระยะ คือ

3.5.1 ระยะการแนะนำตัว

ระยะนี้เป็นการแนะนำตัวของผู้ขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียวต่อผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียวโดยมีลำดับการทำงานดังแสดงในรูปที่ 3.17 เพื่อเป็นการตรวจสอบสถานะของผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว ผลการตรวจสอบจะผ่านเมื่อ

- เครื่องที่ขอใช้บริการอยู่ในความดูแลของผู้ให้บริการ
- พบชื่อผู้ใช้ในฐานข้อมูลรหัสผ่านแบบใช้ครั้งเดียว
- ผู้ใช้ไม่ถูกสั่งยกเลิกการใช้งาน
- บัญชีผู้ใช้ยังไม่หมดอายุการใช้งาน

ถ้าผลการตรวจสอบไม่ผ่านผู้ให้บริการรหัสจะขอปิดการติดต่อทันที

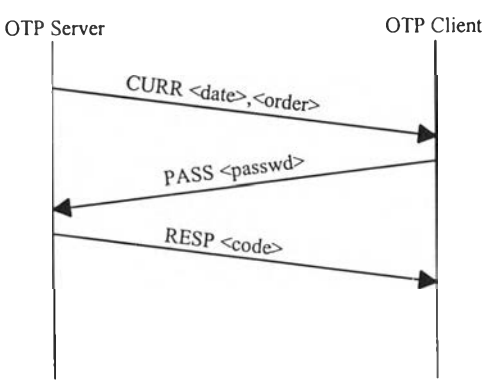


รูปที่ 3.17 แสดงลำดับการทำงานในระยะแนะนำตัว

- เมื่อผู้ขอใช้บริการทำการติดต่อใช้บริการ โดยการขอเปิดช่องทางสื่อสาร ทีซีพี ผู้ให้บริการจะทำการตรวจสอบหมายเลขไอพีของเครื่องที่ขอใช้บริการกับฐานข้อมูลของเครื่องที่อยู่ในความดูแลของผู้ให้บริการ ถ้าหมายเลขไอพีไม่อยู่ในฐานข้อมูล ผู้ให้บริการจะขอปิดการติดต่อทันทีด้วยกลุ่มข้อมูล "QUIT <code>"
- ถ้าหมายเลขไอพีอยู่ในฐานข้อมูลผู้ให้บริการจะส่งกลุ่มข้อมูล "REDY" แสดงความพร้อมให้ผู้ขอใช้บริการเข้าใช้บริการได้
- ผู้ขอใช้บริการแนะนำตัวโดยการส่งกลุ่มข้อมูล "HELO <login name>, <host name>, <domain name>" เพื่อให้ผู้ให้บริการนำ ชื่อล็อกอิน ชื่อเครื่อง และชื่อโดเมน ไปตรวจสอบกับฐานข้อมูลบัญชีผู้ใช้รหัสผ่านแบบใช้ครั้งเดียว
- ถ้าพบ ผู้ให้บริการส่งผลการตรวจสอบกลับด้วยกลุ่มข้อมูล "RESP <code>" ซึ่งมีรหัสแสดงผลการตรวจสอบบัญชีผู้ใช้รหัสผ่านแบบใช้ครั้งเดียว ดังมีความหมายต่างๆ ตามตำแหน่งบิทของเลขฐานสอง ดังแสดงในรูปที่ 3.22
- ถ้าไม่พบ ผู้ให้บริการจะขอปิดการติดต่อด้วยกลุ่มข้อมูล "QUIT <code>"

3.5.2 ระยะการขอตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว

ระยะนี้จะเป็นการทำงานหลังจากที่การแนะนำตัวประสพความสำเร็จ จึงทำการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียวของผู้ใช้ โดยมีลำดับการทำงานดังแสดงในรูปที่ 3.18



รูปที่ 3.18 แสดงลำดับการทำงานในระยะตรวจสอบรหัสผ่าน

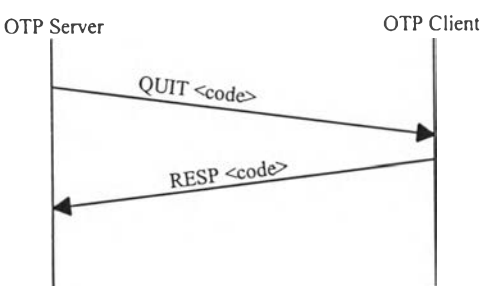
- ผู้ให้บริการส่งกลุ่มข้อมูล “CURR <date>,<order>” เพื่อส่งวันที่สร้างและลำดับของกลุ่มรหัสผ่านแบบใช้ครั้งเดียวที่ใช้อยู่ เพื่อให้ผู้ใช้สามารถดีย์รหัสผ่านตามวันที่สร้างและลำดับที่ถูกต้อง
- ผู้ขอใช้บริการส่งกลุ่มข้อมูล “PASS <password>” เพื่อส่งรหัสผ่านที่ผู้ใช้ดีย์ให้ผู้ให้บริการนำรหัสผ่านที่ได้รับไปตรวจสอบกับรหัสผ่านที่เก็บในฐานข้อมูลรหัสผ่านแบบใช้ครั้งเดียว
- ผู้ให้บริการส่งกลุ่มข้อมูล “RESP <code>” เพื่อแสดงผลการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว รูปแบบของรหัสแสดงดังรูปที่ 3.22 ถ้าผลการตวจสอบรหัสผ่านถูก บิท “PASS” มีค่าเป็น 1 ถ้าผิด บิท “PASS” มีค่าเป็น 0

3.5.3 ระยะขอปิดการติดต่อ

ระยะนี้เป็นการขอปิดการติดต่อสื่อสารเนื่องจากเหตุการณ์ต่างๆ ดังนี้

- ผลการตรวจสอบเครื่องที่ขอใช้บริการรหัสผ่านพบว่าเครื่องดังกล่าวไม่ได้เป็นสมาชิกที่อยู่ในความดูแลของผู้ให้บริการ
- ผลการตรวจสอบสถานะผู้ใช้รหัสผ่านแบบใช้ครั้งเดียวในบัญชีผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียวไม่ผ่าน เช่น ถูกระงับการใช้ รหัสผ่านหมดอายุ หรือไม่พบในบัญชีผู้ใช้
- การสิ้นสุดการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว
- การเกิดข้อผิดพลาดขึ้นระหว่างการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว

โดยมีลำดับการทำงานดังแสดงในรูปที่ 3.19

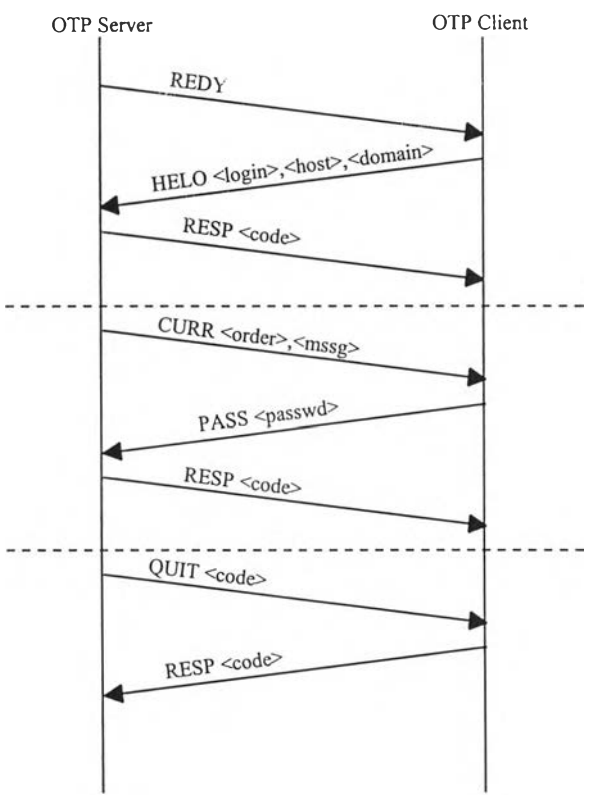


รูปที่ 3.19 แสดงลำดับการทำงานในระยะปิดการติดต่อ

- ผู้ให้บริการจะขอปิดการติดต่อโดยการส่งกลุ่มข้อมูล “QUIT <code>” พร้อมรหัสแสดงเหตุผลการขอปิดการติดต่อ ดังแสดงในรูปที่ 3.22
- เครื่องขอใช้บริการส่งกลุ่มข้อมูล “RESP <code>” พร้อมรหัสแสดงว่าพร้อมปิด (CONF = 1) รูปแบบของรหัสแสดงดังรูปที่ 3.22

ในบางกรณีที่เกิดข้อผิดพลาดขึ้นในการติดต่อสื่อสาร ทั้งฝั่งผู้ให้บริการและผู้ขอใช้บริการ สามารถขอปิดการติดต่อสื่อสารได้โดยมีขั้นตอนเหมือนกัน

เมื่อนำลำดับการทำงานของโพรโทคอลทั้ง 3 ระยะมาประกอบกัน จะได้ขั้นตอนการทำงานทั้งหมดของโพรโทคอลที่ใช้ในการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว ตั้งแต่ต้นจนสิ้นสุดการทำงาน ดังแสดงในรูปที่ 3.20



รูปที่ 3.20 แสดงลำดับการทำงานของโพรโทคอลชั้นการสื่อสารประยุกต์เพื่อการบริการรหัสผ่านแบบใช้ครั้งเดียว

3.6 รูปแบบของกลุ่มข้อมูล (message format)

กลุ่มข้อมูลที่ใช้ในโพรโทคอล ประกอบด้วย 3 เขตข้อมูล ดังแสดงในรูปที่ 3.21

รูปที่ 3.21 รูปแบบของกลุ่มข้อมูล

3.6.1 เขตข้อมูล TYPE

เป็นเขตข้อมูลที่ใช้ระบุประเภทของกลุ่มข้อมูล ประกอบด้วยตัวอักษร 4 ตัว โดยมีชนิดต่างๆ ดังแสดงในตารางที่ 3.1

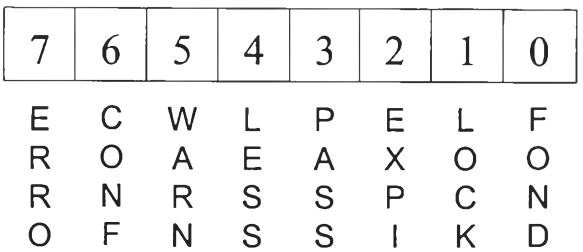
ชื่อประเภท	รายละเอียดการใช้
REDY	แสดงความพร้อมของผู้ให้บริการที่จะรับการติดต่อ
HELO	แนะนำตัวผู้ขอใช้บริการ โดยการส่งบัญชีผู้ใช้รหัสผ่านแบบใช้ครั้งเดียว (OTP account)
CURR	แสดงวันที่สร้างและลำดับของรหัสผ่านแบบใช้ครั้งเดียวของผู้ใช้ที่ระบุในกลุ่มข้อมูล “HELO”
PASS	ส่งรหัสผ่านแบบใช้ครั้งเดียวที่ต้องการตรวจสอบ
QUIT	ขอปิดการติดต่อ
RESP	แสดงผลการทำงานของคำสั่งในกลุ่มข้อมูลคำสั่ง ได้แก่ HELO PASS QUIT เป็นต้น

ตารางที่ 3.1 รายละเอียดประเภทต่างๆ ของกลุ่มข้อมูล

3.6.2 เขตข้อมูลข้อมูล (DATA)

เป็นเขตข้อมูลที่ใช้ส่งข้อมูลหรือผลลัพธ์ตามชนิดของกลุ่มข้อมูลที่ระบุไว้ในเขตข้อมูล “TYPE” รูปแบบรหัสของผลลัพธ์การทำงานและชื่อบิทถูกกำหนด

ตามตำแหน่งของบิทดังแสดงรูปที่ 3.22 ความหมายของแต่ละบิทมีรายละเอียดดังตารางที่ 3.2



รูปที่ 3.22 รูปแบบรหัสแสดงผลลัพธ์การทำงาน

ชื่อบิท	ความหมาย
FOUND	ค้นหาบัญชีผู้ใช้รหัสผ่านแบบใช้ครั้งเดียว (OTP account) ถ้าพบกำหนดให้เป็น 1 ถ้าไม่พบกำหนดให้เป็น 0
LOCK	ผู้ใช้รหัสผ่านแบบใช้ครั้งเดียวถูกระงับการใช้ กำหนดให้เป็น 1
EXPI	รหัสผ่านแบบใช้ครั้งเดียวของผู้ใช้หมดอายุการใช้ กำหนดให้เป็น 1
PASS	รหัสผ่านที่ส่งมาตรวจสอบถูกต้องกำหนดให้เป็น 1 ถ้าผิดกำหนดให้เป็น 0
LESS	จำนวนรหัสผ่านแบบใช้ครั้งเดียวเหลือน้อยกว่าจำนวนขั้นต่ำที่กำหนดให้เป็น 1
WARN	รหัสผ่านแบบใช้ครั้งเดียวของผู้ใช้เหลืออายุการใช้งานน้อยกว่าจุดเตือน กำหนดให้เป็น 1
CONF	ยืนยันคำร้องขอให้เริ่มทำงานได้ มีค่าเป็น 1
ERRO	เกิดข้อผิดพลาดขึ้น มีค่าเป็น 1

ตารางที่ 3.2 ความหมายของบิทต่างๆ ในรหัสแสดงผลลัพธ์

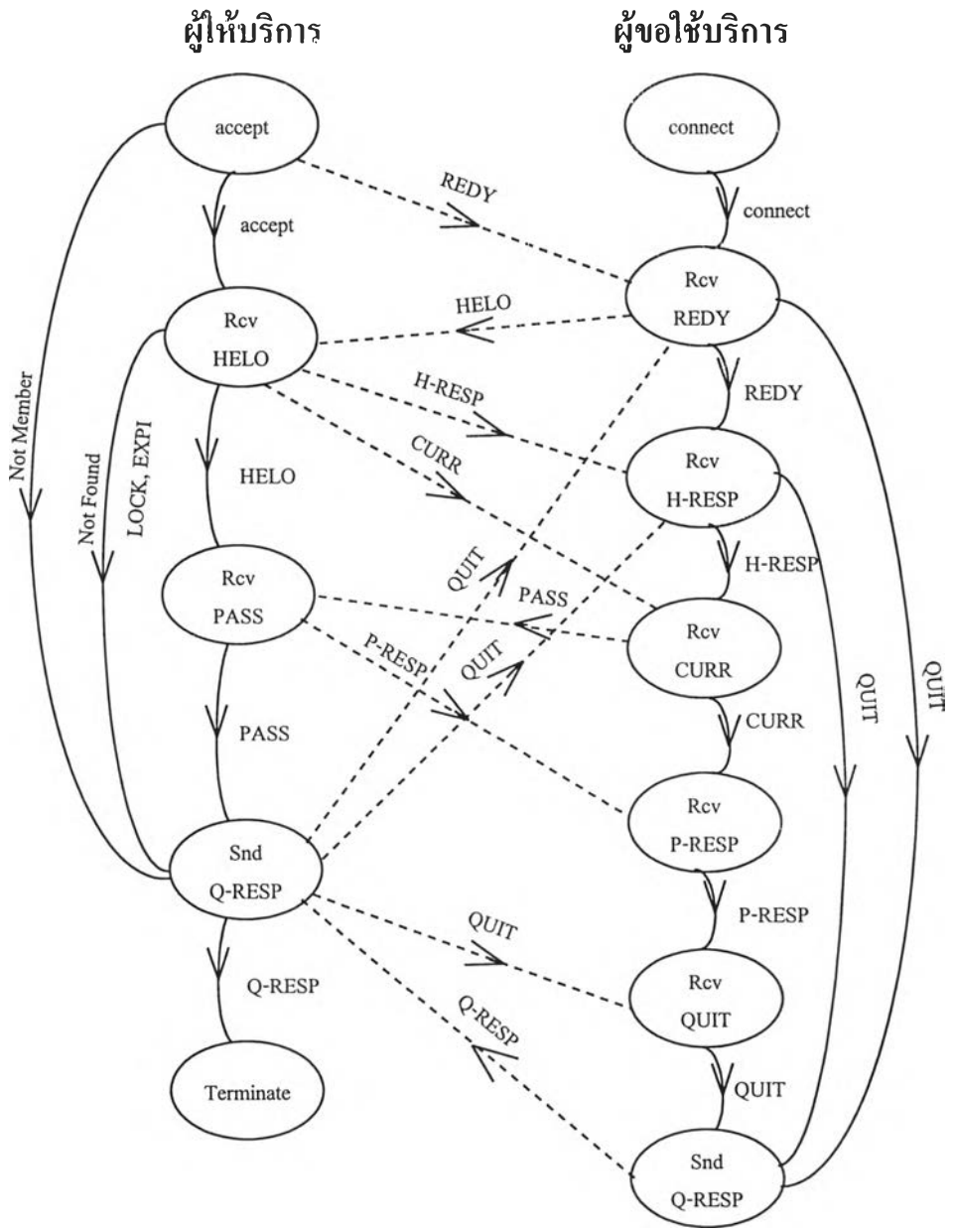
3.6.3 เขตข้อมูลปิดท้าย (FLAG)

เป็นเขตข้อมูลที่ใช้บอกจุดสิ้นสุดของกลุ่มข้อมูล

3.7 สถานะการทำงานของระบบ

เนื่องจากสถาปัตยกรรมที่เป็นระบบรับ-ให้บริการ (client-server) ทำให้การทำงานของโปรแกรมสามารถเขียนเป็นผังแสดงสถานะ (state diagram) ได้ดังรูปที่ 3.23

จากผังแสดงสถานะจะเห็นว่า ผู้ให้บริการและผู้ขอใช้บริการเปรียบเสมือนมีผังสถานะการทำงานที่อิสระต่อกัน ซึ่งทำงานประสานเวลากัน (synchronous) โดยมีกลุ่มข้อมูล (message) ของโพรโทคอลทำหน้าที่ในการประสานเวลาการทำงานของผู้ให้บริการกับผู้ขอใช้บริการเข้าหากัน



รูปที่ 3.23 ผังสถานะการทำงานของผู้ให้บริการและผู้ขอใช้บริการ

3.8 โครงสร้างฐานข้อมูลของระบบ

ระบบรหัสผ่านแบบใช้ครั้งเดียวจะมีฐานข้อมูลของระบบเก็บอยู่ที่ผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว ฐานข้อมูลที่ใช้เป็นฐานข้อมูลเชิงสัมพันธ์ (relational database) ที่สามารถสืบค้นได้ด้วยคำสั่ง เอสคิวแอล (SQL) ของระบบจัดการฐานข้อมูล (database management system) ชื่อ "mSQL" ฐานข้อมูลประกอบด้วย ตารางข้อมูล (table) หลัก 3 ตาราง คือ

3.8.1 ตารางข้อมูลบัญชีผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว "OTP_ACCOUNT"

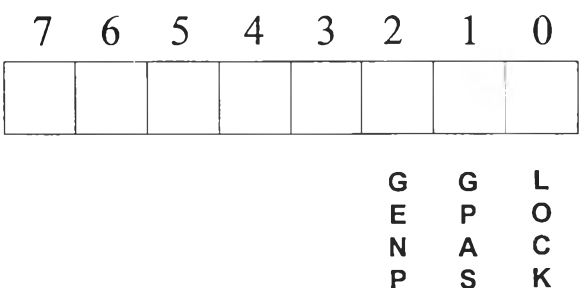
เป็นตารางข้อมูลที่ใช้เก็บข้อมูลของผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว ประกอบด้วยเขตข้อมูลต่างๆ ดังแสดงในตารางที่ 3.3

เขตข้อมูล	รูปแบบ	รายละเอียด
login_name	Char[8]	ชื่อผู้ใช้ของระบบยูนิกซ์
host_name	Char[10]	ชื่อเครื่องที่ขอใช้รหัสผ่านแบบใช้ครั้งเดียว
domain_name	Char[20]	ชื่อโดเมนของเครื่องที่ขอใช้รหัสผ่านแบบใช้ครั้งเดียว
first_name	Char[50]	ชื่อของผู้ใช้
last_name	Char[80]	ชื่อสกุลของผู้ใช้
address	Char[80]	ที่อยู่ของผู้ใช้
city	Char[20]	จังหวัด
country	Char[20]	ประเทศ
zip_code	Char[10]	รหัสไปรษณีย์
tel_number	Char[20]	หมายเลขโทรศัพท์
e_mail	Char[50]	ที่อยู่ของจดหมายอิเล็กทรอนิกส์
create_date_0	Date	วันที่สร้างรหัสผ่านแบบใช้ครั้งเดียวชุดที่0
create_date_1	Date	วันที่สร้างรหัสผ่านแบบใช้ครั้งเดียวชุดที่1
expire_date	Date	วันหมดอายุของบัญชีผู้ใช้รหัสผ่าน

ตารางที่ 3.3 ตารางข้อมูลผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว

เขตข้อมูล	รูปแบบ	รายละเอียด
cur_passwd	Int	ตำแหน่งของรหัสผ่านปัจจุบัน
total_passwd	Int	จำนวนรหัสผ่านในแต่ละชุดรหัสผ่าน
flag	Int	รหัสเลขฐานสองที่ใช้บอกสถานะ ดังนี้ - การถูกสั่งระงับการใช้ - ชุดรหัสผ่านที่ใช้ (0, 1) - การสร้างชุดรหัสผ่านใหม่ โดยมีรายละเอียดดังรูปที่ 3.24

ตารางที่ 3.3 ตารางข้อมูลผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว



LOCK = 1 ผู้ใช้ถูกสั่งระงับการใช้งาน

GPAS = 0, 1 ชุดของรหัสผ่านที่ใช้ในปัจจุบัน

GENP = 1 มีการสร้างรหัสผ่านชุดใหม่เรียบร้อยแล้ว

รูปที่ 3.24 รูปแบบรหัสของเขตข้อมูล FLAG

ตารางข้อมูลบัญชีผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว มีเขตข้อมูลหลัก (primary key) 3 เขตข้อมูลคือ

- เขตข้อมูล login_name
- เขตข้อมูล host_name
- เขตข้อมูล domain_name

เขตข้อมูลทั้ง 3 เมื่อรวมกันจะเท่ากับเป็นการระบุผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว (OTP-account) 1 รายการ (record) นอกจากนี้เขตข้อมูล “host_name” และเขตข้อมูล “domain_name” ยังสามารถมีค่าเป็น ALL ซึ่งหมายถึงทุกๆ เครื่องและทุกๆ โดเมนตามลำดับ

ดังนั้นการสร้างรายการของผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียวจึงสามารถมีการระบุขอบเขตได้ 3 วิธี คือ

3.8.1.1 ระบุผู้ใช้ต่อหนึ่งเครื่อง “<login> + <host> + <domain>”

เป็นการระบุถึงผู้ใช้บนเครื่องๆ หนึ่ง ภายใต้โดเมนที่ระบุเท่านั้น เช่น <userA> + <pioneer> + <cp.eng.chula.ac.th> หมายถึง ผู้ใช้ที่มีชื่อล็อกอินเป็น userA บนเครื่องชื่อ “pioneer” ภายใต้โดนเมน “cp.eng.chula.ac.th” เท่านั้น

3.8.1.2 ระบุผู้ใช้ต่อหนึ่งโดเมน “<login> + ALL + <domain>”

เป็นการระบุผู้ใช้สำหรับทุกๆ เครื่อง ภายใต้โดเมนที่กำหนด เช่น <userA> + ALL + <cp.eng.chula.ac.th> หมายถึง ผู้ใช้ที่มีชื่อล็อกอิน “userA” บนเครื่องใดๆ ภายใต้โดเมน “cp.eng.chula.ac.th”

3.8.1.3 ระบุผู้ใช้ต่อหนึ่งระบบ “<login> + ALL + ALL”

เป็นการระบุผู้ใช้สำหรับทุกๆ เครื่องในระบบ เช่น <userA> + ALL + ALL หมายถึง ผู้ใช้ที่มีชื่อ “userA” บนเครื่องใดๆ ภายในระบบ ซึ่งในที่นี้จะหมายถึง เครื่องที่มีรายการอยู่ในตารางข้อมูลที่ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว

3.8.2 ตารางข้อมูลรหัสผ่านแบบใช้ครั้งเดียว “OTP_PASSWORD”

เป็นตารางข้อมูลที่ใช้เก็บรหัสผ่านแบบใช้ครั้งเดียวของผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว โดยผู้ใช้ระบบรหัสผ่านแต่ละรายการจะมีตารางข้อมูลรหัสผ่าน 1 ชุด โดยอาศัยบัญชีผู้ใช้รหัสผ่านแบบใช้ครั้งเดียว “<login_name>_<host_name_<domain_name>” เป็นชื่อของตารางข้อมูลรหัสผ่าน รายละเอียดของเขตข้อมูลในตารางข้อมูลรหัสผ่านแสดงในตารางที่ 3.4

เขตข้อมูล	รูปแบบ	รายละเอียด
ord	Int	ลำดับที่ของรหัสผ่าน
password	char[8]	รหัสผ่านแบบใช้ครั้งเดียว

ตารางที่ 3.4 ตารางข้อมูลรหัสผ่านแบบใช้ครั้งเดียว

3.8.3 ตารางข้อมูลเครื่องที่ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว "OTP_CLIENT"

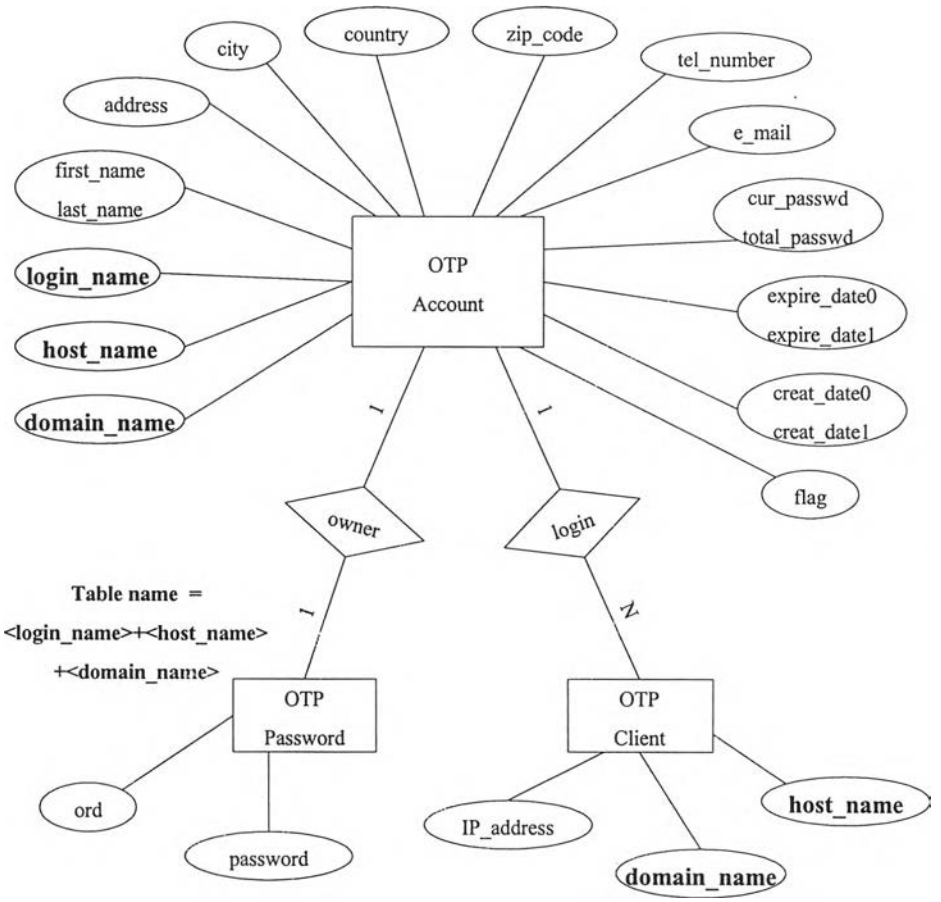
เป็นตารางข้อมูลที่ใช้เก็บข้อมูลของเครื่องผู้ขอใช้บริการทุกเครื่องที่อยู่ในขอบเขตการดูแล (region) ของผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว (server) ประกอบด้วยเขตข้อมูลต่างๆ ดังแสดงในตารางที่ 3.5

เขตข้อมูล	รูปแบบ	รายละเอียด
host_name	Char[10]	ชื่อเครื่องที่ขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว
domain_name	char[20]	ชื่อโดเมนของเครื่องที่ขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว
ip_address	Char[15]	หมายเลขไอพีของเครื่องที่ขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว

ตารางที่ 3.5 ตารางข้อมูลเครื่องที่ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว

3.8.4 ความสัมพันธ์ของตารางข้อมูล

ความสัมพันธ์ของตารางข้อมูลทั้งสาม สามารถแสดงได้ด้วยแผนผังแสดงความสัมพันธ์ของเอนทิตี (entity relation diagram) ดังแสดงในรูปที่ 3.25 ประกอบด้วย



รูปที่ 3.25 แผนผังแสดงความสัมพันธ์ของเอนทิตี

3.8.4.1 ความสัมพันธ์ระหว่างบัญชีผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว "OTP_ACCOUNT" กับเครื่องที่ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว "OTP_CLIENT" เป็นแบบหนึ่งต่อกลุ่ม (one-to-many) เป็นผลให้ผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียวสามารถล็อกอินได้บนเครื่องหลายๆ เครื่อง โดยใช้ชุดรหัสผ่านเพียงชุดเดียว

3.8.4.2 ความสัมพันธ์ระหว่างผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว "OTP_ACCOUNT" กับชุดรหัสผ่านแบบใช้ครั้งเดียว "OTP_PASSWORD" เป็นแบบหนึ่งต่อหนึ่ง (one-to-one) โดยอาศัยการตั้งชื่อตารางข้อมูลรหัสผ่านตามเขตข้อมูลหลัก (primary key) ของตารางข้อมูลบัญชีผู้ใช้ระบบรหัสผ่านเป็นตัวเชื่อมความสัมพันธ์ระหว่างตารางข้อมูลทั้งสอง

ส่วนสาเหตุที่ต้องแยกตารางข้อมูลรหัสผ่านออกจากตารางข้อมูลผู้ใช้ เนื่องจากจำนวนเขตข้อมูลของรหัสผ่านมีค่าไม่คงที่ โดยมีค่าตามจำนวนรหัสผ่านต่อชุดที่ผู้บริหารระบบกำหนดให้กับผู้ใช้ (ค่าของเขตข้อมูล “total_passwd” ใช้กำหนดจำนวนรหัสผ่านต่อชุด)