บทที่ 1

บทนำ

1.1 ความสำคัญและที่มาของหัวข้อวิจัย

การปกป้องความปลอดภัยของโปรแกรมประยุกต์เป็นสิ่งสำคัญในปัจจุบัน เนื่องจากมูลค่าของโปรแกรมประยุกต์ได้รับความสนใจจากผู้ใช้งานทั่วไป รวมไปถึงผู้บุกรุกที่พยายามเข้ามาเจาะในระบบ ความเสียหายทางธุรกิจและองค์กรที่เกิดจากการคุกคามของผู้ไม่ประสงค์ดี ถูกให้ความสำคัญมากขึ้นตามลำดับ หากภายในโปรแกรมประยุกต์มีระบบควบคุมความปลอดภัยที่ดีจะช่วยลดโอกาสเสี่ยงต่อการถูกคุกคามได้ การพิสูจน์ตัวตนเป็นขั้นตอนพื้นฐานที่สำคัญของการควบคุมความปลอดภัย ในการใช้งานโปรแกรมประยุกต์ โดยทั่วไปการแสดงสิทธิ์ด้วยบัญชีผู้ใช้และรหัสผ่าน ถูกนำมาใช้งานกันอย่างกว้างขวางเพื่อรักษาสิทธิ์การใช้โปแกรมเหล่านั้น

ในบางระบบที่ต้องการความปลอดภัยสูง ๆ เช่น ระบบการเงิน การพิสูจน์ตัวตนโดยการนำบัญชีผู้ใช้ซึ่งประกอบด้วยบัญชีผู้ใช้และรหัสผ่านมาใช้งาน เพื่อพิสูจน์ตัวตนยังไม่เพียงพอต่อความปลอดภัย เนื่องจากบัญชีผู้ใช้และรหัสผ่าน ผู้บุกรุกสามารถทราบได้ หรือหากผู้ใช้ใช้อย่างไม่ระมัดระวัง ขณะที่ล็อกออนอาจมีผู้บุกรุกดักจับรหัสผ่านและเอาไปใช้งานได้ ดังนั้นจึงพัฒนากุญแจอิเล็กทรอนิกส์ ขึ้นมาใช้งาน ระบบนี้นอกจากผู้ใช้ต้องใส่บัญชีผู้ใช้และรหัสผ่านแล้วยังต้องมีฮาร์ดแวร์ ซึ่งเปรียบเสมือนกุญแจ เมื่อผู้ใช้งานล็อกออนระบบจะตรวจสอบบัญชีผู้ใช้รหัสผ่านและกุญแจอิเล็กทรอนิกส์เพื่อเข้าถึงข้อมูล ซึ่งลักษณะของกุญแจดอกนี้คือ ไม่สามารถทำซ้ำขึ้นมาใหม่ได้ ข้อมูลในการตรวจสอบสิทธิ์เปลี่ยนแปลงอยู่เสมอและระบบจะตรวจสอบกุญแจดอกนี้เป็นระยะ ๆ เพื่อให้แน่ใจถึงความปลอดภัยมากที่สุด

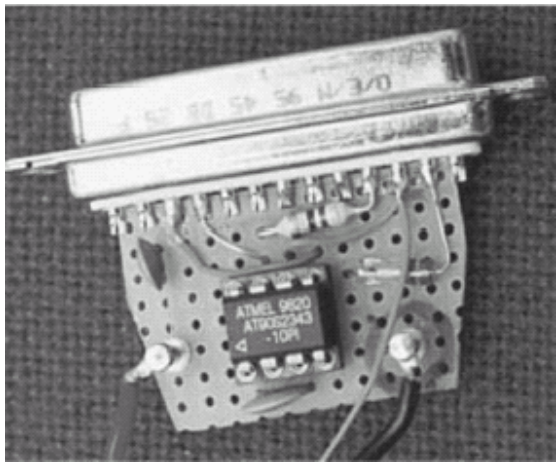
อนึ่งในภาวะปัจจุบันการคัดลอกหรือการทำสำเนาโปรแกรมเพื่อนำโปรแกรมเหล่านี้ไปใช้โดยละเมิดลิขสิทธิ์มีให้เห็นกันทั่วไป นำไปสู่ความสูญเสียเชิงธุรกิจดังนั้น กุญแจอิเล็กทรอนิกส์จึงเป็นทางเลือกอีกวิธีหนึ่งในการจัดการผู้ใช้ เหมาะสำหรับผู้ที่ต้องการพัฒนาโปรแกรมนำไปประยุกต์ใช้ต่อไปในอนาคต

ดังนั้นประโยชน์ของการนำกุญแจอิเล็กทรอนิกส์มาประยุกต์ใช้สามารถสรุปได้ดังนี้

- เพิ่มความปลอดภัยและความน่าเชื่อถือให้กับโปรแกรมประยุกต์
- ลดความเสี่ยงและความเสียหาย เมื่อนำไปประยุกต์ใช้ในเชิงพาณิชย์
- ส่งเสริมให้มีผู้พัฒนาโปรแกรมประยุกต์มากขึ้น

1.2 การตรวจเอกสาร

1.2.1 ฮาร์ดแวร์ล็อก (Dhananjay V.Gadre, 2000) ซึ่งออกแบบมาเพื่อล็อกการใช้งานเครื่องคอมพิวเตอร์หรือป้องกันการใช้โปรแกรมที่ต้องการจำกัดสิทธิ์การใช้งาน ซึ่งลักษณะการทำงานของฮาร์แวร์ล็อกนี้จะต่อประสานกับพอร์ตอนุกรม หรือพอร์ตขนาน ดังแสดงในภาพประกอบ 1-1 ภายในอุปกรณ์จะมีไมโครคอนโทรลเลอร์เบอร์ AT90S2343 ทำหน้าที่ตรวจสอบรหัสผ่านและส่งข้อมูลกลับมายังเครื่องคอมพิวเตอร์ เมื่อเปิดเครื่องคอมพิวเตอร์หรือเปิดโปรแกรมที่ต้องการใช้งาน อุปกรณ์ภายในที่ออกแบบมานี้จะทำการตรวจสอบสิทธิ์การใช้งานโดยให้ผู้ใช้กรอกรหัสผ่าน ซึ่งเก็บไว้ในอุปกรณ์ที่ต่ออยู่กับพอร์ตอนุกรมหรือพอร์ตขนาน หากผู้ใช้ไม่ต่ออุปกรณ์ตัวนี้ไว้ที่เครื่องคอมพิวเตอร์หรือกรอกรหัสผ่านผิด เครื่องคอมพิวเตอร์ก็จะปฏิเสธการใช้งาน ทันทีทำให้ผู้ใช้งานไม่สามารถใช้งานโปรแกรมที่ต้องการได้



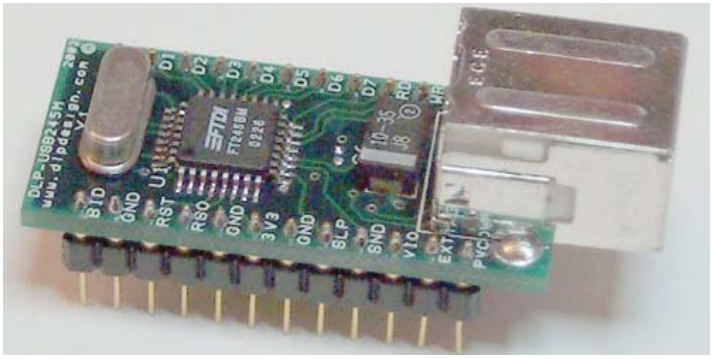
ภาพประกอบ 1-1 ลักษณะฮาร์ดแวร์ล็อกผ่านทางพอร์ตขนาน

(ที่มา:Dhananjay V.Gadre,2000)

ข้อดีของระบบนี้	ข้อด้อยของระบบนี้
• ออกแบบได้ง่าย • ต้นทุนต่ำ	• เจาะระบบ (Hack) ได้ง่ายเนื่องจากระบบไม่ซับซ้อน • ขณะใช้งานค่อนข้างยุ่งยากเนื่องจากพอร์ตขนานอยู่ด้านหลังของคอมพิวเตอร์ • ขณะที่ใช้งาน หากต้องการพิมพ์งานผ่านพอร์ตขนาน จะไม่สามารถทำได้เนื่องจากพอร์ตขนานของคอมพิวเตอร์ถูกใช้ไปแล้ว • แนวทางในการพัฒนาคอมพิวเตอร์ในอนาคตจะไม่มีพอร์ตอนุกรมหรือพอร์ตขนาน เนื่องจากผู้ผลิตจะนิยมใช้พอร์ต USB มากขึ้น

1.2.2 FTDI โมดูล (http://www.FTID.com) ลักษณะของ FTDI เป็นโมดูลสำเร็จรูปที่ออกแบบมา เพื่ออำนวยความสะดวกให้คอมพิวเตอร์ติดต่อกับอุปกรณ์ภายนอกโดยผ่านพอร์ต USB เช่นกรณีที่เครื่องคอมพิวเตอร์ไม่มีพอร์ตอนุกรม สามารถใช้ FTDI ในการส่งข้อมูลออกทางพอร์ต USB แล้วข้อมูลก็จะถูกแปลงให้อยู่ในรูปแบบของพอร์ตอนุกรม ได้ทำให้สามารถใช้พอร์ตอนุกรม โดยผ่าน พอร์ต USB ได้ซึ่งลักษณะของโมดูลจะเป็นดังภาพประกอบ 1-2

หากต้องการใช้โมดูลนี้ ซึ่งประกอบด้วยชิปที่ใช้ในการต่อประสานกับคอมพิวเตอร์และสามารถต่อกับหน่วยความจำภายนอก เพื่อเก็บค่ารหัสประจำตัวและรหัสลับต่าง ๆ ไว้ภายในมาใช้ทำเป็นกุญแจอิเล็กทรอนิกส์สามารถทำได้ แต่ไม่เหมาะสมที่จะมาใช้ในงานนี้ เนื่องจากไม่สามารถเก็บรหัส ประจำตัวและรหัสลับต่าง ๆ ที่ต้องการเก็บได้อย่างปลอดภัย เนื่องจากหากเก็บค่าต่าง ๆที่เป็นข้อมูลลับไว้ในหน่วยความจำภายนอกแล้ว หากมีผู้ที่ต้องการทราบว่า ภายในหน่วยความจำมีอะไรเก็บอยู่ก็สามารถอ่านหน่วยความจำนี้ได้



ภาพประกอบ 1-2 FDI Module FT245BM

ที่มา (http://www.FTID.com)

ข้อดีของระบบนี้	ข้อด้อยของระบบนี้
• นำมาพัฒนาต่อได้ง่ายเนื่องจากเป็นอุปกรณ์สำเร็จรูปที่พร้อมใช้งาน	• ระบบไม่ค่อยปลอดภัยเนื่องจากต้องต่อหน่วยความจำภายนอกเพิ่มเข้าไป

1.2.3 USB ฮาร์ดล็อก (http://www.rainbow.com) เป็นผลิตภัณฑ์สำเร็จรูปที่มีจำหน่ายในท้องตลาดได้แก่ i-Key, Rainbow เป็นต้น ซึ่งออกแบบมาเพื่อใช้เป็นฮาร์ดล็อกโดยภายในอุปกรณ์จะประกอบด้วยไมโครคอนโทรลเลอร์และชิปต่อประสานพอร์ต USB ซึ่งคล้ายกับการทำงานของกุญแจอิเล็กทรอนิกส์ดังภาพประกอบ 1-3

ภาพประกอบ 1-3 ลักษณะของฮาร์ดล็อก

(ที่มา http://www.rainbow.com)

ลักษณะภาพประกอบ 1-3 เป็นผลิตภัณฑ์ที่มีขายในท้องตลาด แต่ไม่เคยเปิดเผยข้อมูลทางด้านเทคนิคมาก่อนว่ามีกระบวนการทำงานอย่างไร

ข้อดีของระบบนี้	ข้อด้อยของระบบนี้
• มีความปลอดภัยสูง และใช้งานได้ง่าย	• ต้องนำเข้าเทคโนโลยี • ต้นทุนสูง

1.2.4 Montgomery reduction with even modulus (Departmet of Electrical and Computer Engineering ,Oregon State university USA ,1994) เป็นงานวิจัยที่รับรองโดย RSA Data Security ,Inc.,Redwood City ,California กล่าวถึงการลดทอนเลขยกกำลัง $C = m^e \bmod n$ ซึ่งเป็นสมการการเข้ารหัสลับแบบ RSA โดยใช้การคูณแบบมอดุลาร์ (modular multiplication) และอัลกอริทึมเลขชี้กำลัง (exponentiation algorithms) บนพื้นฐานการลดทอนของวิธีการทวินิยม (Binary method) ช่วยให้ อัลกอริทึมการลดทอนแบบ Montgomery สามารถใช้ได้มีประสิทธิภาพได้ทั้งกรณีที่ n เป็นเลขคู่และเลขคี่

งานวิจัยนี้มีหลักการทำงานที่คล้ายกับ USB ฮาร์ดล็อกซึ่งแสดงในภาพประกอบ 1-3 กล่าวคือเมื่อโปรแกรมประยุกต์ที่เราต้องการจำกัดสิทธิ์ถูกผู้ใช้เรียกใช้งาน ระบบจะมีการตรวจสอบว่ามี กุญแจอิเล็กทรอนิกส์ต่ออยู่กับเครื่องคอมพิวเตอร์หรือไม่ หากต่ออยู่กับระบบ ระบบจะส่งข้อมูลไปตรวจสอบว่าใช่ กุญแจอิเล็กทรอนิกส์ของระบบหรือไม่ จากนั้นจะทำการส่งข้อมูลที่เข้ารหัสแบบ RSA ไปสอบถาม กุญแจอิเล็กทรอนิกส์และหาก กุญแจอิเล็กทรอนิกส์ตอบกลับมายังระบบได้อย่างถูกต้อง ระบบจึงจะยอมให้ใช้โปรแกรมประยุกต์ที่ผู้ใช้ต้องการใช้งานได้ ในระหว่างที่มีการแลกเปลี่ยนข้อมูลเพื่อการตรวจสอบ กุญแจอิเล็กทรอนิกส์นี้ ข้อมูลจะถูกเข้ารหัส ตลอดช่วงการ

สื่อสาร นั้นหมายความว่าข้อมูลที่ถูกส่งออกไป จะเปลี่ยนแปลงทุกครั้งที่มีการเข้าใช้งานและหลังจากนั้นเมื่อผู้ใช้ ใช้งานโปรแกรมไปในระยะเวลาหนึ่ง โปรแกรมก็จะตรวจสอบ กุญแจอิเล็กทรอนิกส์อีกครั้ง ซึ่งการตรวจสอบนี้จะตรวจสอบเป็นระยะ ๆ เพื่อให้แน่ใจว่าผู้ใช้ เป็นผู้ใช้งานโปรแกรมจริงที่ได้รับสิทธิ์ และหากว่าผู้ใช้งานนำ กุญแจอิเล็กทรอนิกส์ออกจากเครื่องคอมพิวเตอร์โปรแกรมก็จะปฏิเสธการใช้งานทันที ทั้งนี้ขึ้นอยู่กับการนำระบบนี้ไปประยุกต์ใช้งาน

1.3 วัตถุประสงค์ของโครงการวิจัย

1.3.1 เพื่อศึกษาการติดต่อกับพอร์ต USB

1.3.2 เพื่อสร้างชุดอุปกรณ์รักษาความปลอดภัยผ่านทางพอร์ต USB

1.3.3 เพื่อศึกษาการเข้ารหัสบนไมโครคอนโทรลเลอร์

1.3.4 เพื่อพัฒนาความรู้ด้านระบบรักษาความปลอดภัยขึ้นใช้เอง ซึ่งช่วยลดการนำเข้าเทคโนโลยีจากต่างประเทศ

1.4 ขั้นตอนของการทำวิจัย

1.4.1 ทำการตรวจสอบและศึกษาการทำงานของระบบที่มีใช้อยู่ในปัจจุบัน เพื่อเป็นแนวทางในการออกแบบกุญแจอิเล็กทรอนิกส์ พร้อมทั้งวางแผนการออกแบบกุญแจอิเล็กทรอนิกส์

1.4.2 ศึกษาการทำงานของ USB และอุปกรณ์อิเล็กทรอนิกส์ที่รองรับการทำงาน USB พร้อมทั้งเขียนโปรแกรมติดต่อกับพอร์ต USB

1.4.3 ออกแบบโพรโทคอนรับส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์และนำโพรโทคอนที่ออกแบบเขียนโปรแกรมแลกเปลี่ยนข้อมูลผ่านทางพอร์ต USB และพอร์ตขนาน

1.4.4 ศึกษาการเข้ารหัสแบบ RSA พร้อมเขียนโปรแกรมตามทฤษฎี

1.4.5 ศึกษาการลดทอนแบบ Montgomery และทฤษฎีจำนวน พร้อมทั้งเขียนโปรแกรมตามทฤษฎีเหล่านี้ ๆ

1.4.6 สร้างกุญแจอิเล็กทรอนิกส์ด้วยไมโครคอนโทรลเลอร์พร้อมทดสอบการทำงานระบบจริง

1.5 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

1.5.1 พัฒนาความรู้ความเข้าใจในการเขียนโปรแกรมติดต่อกับพอร์ต USB

1.5.2 พัฒนาความรู้ด้านไมโครคอนโทรลเลอร์

1.5.3 ช่วยให้ระบบงานที่ต้องการความปลอดภัยสูงเช่น งานการเงิน มีความปลอดภัยมากขึ้น

1.5.4 ลดการนำเข้าเทคโนโลยีจากต่างประเทศ

1.5.5 พัฒนาอุปกรณ์ที่มีจำหน่ายในท้องตลาดมาใช้ประโยชน์ให้มากขึ้น นอกเหนือการใช้งานอยู่ในปัจจุบัน

1.5.6 พัฒนาเทคโนโลยีด้านความปลอดภัยขึ้นใช้เอง และนำไปสู่การพัฒนาเพื่อธุรกิจในอนาคต

1.6 สรุปท้ายบท

เนื้อหาโดยภาพรวมของบทนี้ได้กล่าวถึงที่มาของปัญหา ในการกำจัดสิทธิ์การใช้งานโปรแกรมโดยใช้ กุญแจอิเล็กทรอนิกส์เข้ามาเพิ่มความปลอดภัยให้กับโปรแกรมให้มากขึ้น เนื้อหาที่จะกล่าวต่อไปในบทที่ 2 เป็นหลักการพื้นฐานในการติดต่อสื่อสารกับพอร์ต USB การเข้ารหัสลับแบบ RSA และอัลกอริทึมการลดทอนแบบ Montgomery ซึ่งจะนำไปสู่การออกแบบและสร้าง กุญแจอิเล็กทรอนิกส์ในบทที่ 3 และการทดสอบการใช้งานในบทที่ 4 และบทที่ 5 เป็นสรุปผลการทดสอบรวมถึงปัญหาและข้อเสนอแนะต่าง ๆ