การวิเคราะห์ ออกแบบ และพัฒนาระบบปูมข้อมูลจราจรทางคอมพิวเตอร์ที่มั่นคงในร้านบริการอินเทอร์เน็ต

นายพีชพล พลพงษ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2553

Analysis Design and Development of Secure Traffic Data System in Internet Cafe

Mr. Peachapol Polphong

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Computer Science

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2010

หัวข้อวิทยานิพนธ์	การวิเคราะห์ ออกแบบ และพัฒนาระบบปูมข้อมูลจราจรทางคอมพิวเตอร์ที่มั่นคงในร้านบริการอินเทอร์เน็ต
โดย	นายพีชพล พลพงษ์
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	อาจารย์ ดร.ยรรยง เต็งอำนวย

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(อาจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.เกริก ภิรมย์โสภา)

..... กรรมการภายนอกมหาวิทยาลัย
(พันตำรวจเอก.ญาณพล ยั่งยืน)

พีชพล พลพงษ์ : การวิเคราะห์ ออกแบบ และพัฒนาระบบปูมข้อมูลจราจรทางคอมพิวเตอร์ที่มั่นคงในร้านบริการอินเทอร์เน็ต. (Analysis Design and Development of Secure Traffic Data System in Internet Cafe)
อ.ที่ปรึกษาวิทยานิพนธ์หลัก : อาจารย์ ดร.ยรรยง เต็งอำนวย, 33 หน้า.

จากการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ระบบปูมข้อมูลจราจรทางคอมพิวเตอร์ถูกให้ความสำคัญมากขึ้น เนื่องจากในปัจจุบันยังไม่มีระบบที่สามารถสร้างความเชื่อมั่นให้กับทั้งผู้ให้บริการและผู้ใช้บริการอินเทอร์เน็ตในการเก็บปูมข้อมูลจราจรอย่างโปร่งใสและเป็นกลาง เพื่อไม่ให้เกิดความเคลือบแคลงใจต่อหลักฐานทางคอมพิวเตอร์ โดยเฉพาะร้านบริการอินเทอร์ที่เป็นสถานที่สาธารณะ จึงมีความจำเป็นที่จะต้องสร้างระบบที่มีความน่าเชื่อถือ ปลอดภัย และมีการลงทุนต่ำกุญแจสมมาตรเข้ารหัสข้อมูลแบบกลุ่มบนพื้นฐานของ บันทึกที่มั่นคงเพื่อการตรวจสอบ

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....
สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก .....
ปีการศึกษา 2553

5071434821 : MAJOR COMPUTER SCIENCE

KEYWORDS : SECURITY / LOG MENAGEMNET

PEACHAPOL POLPHONG : ANALYSIS DESIGN AND DEVELOPMENT OF SECURE TRAFFIC DATA SYSTEM IN INTERNET CAFE. ADVISOR : YUNYONG TENG-AMNUAY, Ph.D., 33pp.

According to an announcement of a Computer Crime Act in Thailand, computer log management system has gained attention from various stakeholders because they are not confident in security functionalities of the existing systems. The existing systems are not providing transparency and fairness to both internet users and service providers. This research aims to eliminate criticism to digital evidences. Internet café needs secured and inexpensive log management system in order to operate legally under the new law. An implementation of computationally secure and inexpensive logging method based on Secure Audit Logs had been tested in real environment at an Internet café.

Department : Computer Engineering Student's Signature .....

Field of Study : Computer Science Advisor's Signature .....

Academic Year : 2010 .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยความอนุเคราะห์อย่างดียิ่งของอาจารย์ ดร.ยรรยง เต็งอำนวย อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านได้สละเวลาให้ความรู้ ให้คำปรึกษา ตรวจสอบ ให้คำแนะนำแนวทางการวิจัย และสนับสนุนเป็นอย่างดี จนทำให้การวิจัยในครั้งนี้สำเร็จออกมาด้วยดี

ขอขอบพระคุณ อาจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์ ผู้ช่วยศาสตราจารย์ ดร.เกริก ภิรมย์โสภา และพ.ต.อ.ญาณพล ยั่งยืน กรรมการสอบวิทยานิพนธ์ ที่กรุณาเสียสละเวลา ให้คำแนะนำ ตรวจสอบ และแก้ไขวิทยานิพนธ์ฉบับนี้

ขอกราบขอบพระคุณ คุณพ่อ-คุณแม่ ที่ให้การสนับสนุนและเป็นกำลังใจที่ดีให้เสมอมา

ขอขอบคุณพี่ๆ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ที่ให้คำปรึกษาและให้การสนับสนุนเป็นอย่างดี

ท้ายที่สุด ผู้วิจัยขอขอบพระคุณเพื่อนคณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ทุกๆคน ที่คอยติดตามและให้กำลังใจ รวมถึงท่านอื่นๆ ที่มิได้กล่าวชื่อไว้ ณ ที่นี้ที่มีส่วนทำให้วิทยานิพนธ์สำเร็จได้ด้วยดี

สารบัญ

หน้า

บทคัดย่อภาษาไทย.....ง
บทคัดย่อภาษาอังกฤษ.....จ
กิตติกรรมประกาศ.....ฉ
สารบัญ.....ช
สารบัญตาราง.....ฌ
สารบัญภาพ.....ญ
บทที่ 1.....1
บทนำ.....1
1.1 ความเป็นมาและความสำคัญของปัญหา.....1
1.2 วัตถุประสงค์ของการวิจัย.....2
1.3 ขอบเขตของการวิจัย.....2
บทที่ 2.....3
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง.....3
2.1 ทฤษฎีที่เกี่ยวข้อง.....3
2.1.1 ความสมบูรณ์ของข้อมูล (Data Integrity).....3
2.1.2 รูปแบบการให้บริการอินเทอร์เน็ต.....3
2.1.3 การซ่อนตัวจากระบบปูมจราจร.....4
2.1.4 หลักการในการสืบสวนทางคอมพิวเตอร์.....5
2.2 งานวิจัยที่เกี่ยวข้อง.....7
บทที่ 3.....9
การออกแบบและวิธีดำเนินการวิจัย.....9
3.1 ความต้องการของระบบ.....9
3.2 ส่วนประกอบของระบบ.....10
3.3 ข้อมูลที่เกี่ยวข้องภายในระบบ.....12
3.4 การทำงานของระบบ.....17
บทที่ 4.....20
การทดลอง.....20

หน้า

4.1 สภาพแวดล้อมในการทดลอง 20
4.2 ระยะเวลาในการทดลอง 22
4.3 การตั้งค่าการทำงานของโปรแกรม 22
บทที่ 5 24
ผลการวิจัย 24
5.1 ผลการทดลอง 24
5.2 ผลการวิเคราะห์ 25
บทที่ 6 28
สรุปผลการวิจัยและข้อเสนอแนะ 28
6.1 สรุปผลการวิจัย 28
6.2 ข้อเสนอแนะ 29
รายการอ้างอิง 31
ประวัติผู้เขียนวิทยานิพนธ์ 33

สารบัญตาราง

หน้า

ตารางที่ 1 รายละเอียดตาราง tbl_keystore 13
ตารางที่ 2 รายละเอียดตาราง tbl_lot 13
ตารางที่ 3 รายละเอียดตาราง tbl_keystore 13
ตารางที่ 4 รายละเอียดตาราง tbl_lot 14
ตารางที่ 5 ค่าความสำคัญของแหล่งที่มาของข้อมูล (Facility) 15
ตารางที่ 6 ความสำคัญของข้อมูล (Severity) 16
ตารางที่ 7 ตัวอย่าง syslog 17
ตารางที่ 8 รายละเอียดและข้อจำกัดของเครื่องคอมพิวเตอร์ 21
ตารางที่ 9 การตั้งค่าในการทดลอง 23

สารบัญภาพ

หน้า

รูปที่ 1 ขั้นตอนการเก็บหลักฐาน 6
รูปที่ 2 ผู้เกี่ยวข้องและส่วนประกอบของระบบปูมข้อมูลจราจรทางคอมพิวเตอร์ 10
รูปที่ 3 แผนภาพระบบปูมข้อมูลจาจรทางคอมพิวเตอร์ 11
รูปที่ 4 ข้อมูลที่เครื่องแม่ข่ายภายในร้านบริการอินเทอร์เน็ต 12
รูปที่ 5 ข้อมูลที่เครื่องแม่ข่ายของภาครัฐ 14
รูปที่ 6 ขั้นตอนการทำงานของระบบปูมข้อมูลจราจรทางคอมพิวเตอร์ 17
รูปที่ 7 เครื่องคอมพิวเตอร์ในการทดลอง 20
รูปที่ 8 การทำงานของหน่วยประมวลผลแบบอนุกรมเวลา 24
รูปที่ 9 การทำงานของหน่วยประมวลผล 25
รูปที่ 10 การทำงานของฮาร์ดดิสก์ 25
รูปที่ 11 การทำงานของหน่วยความจำ 26
รูปที่ 12 การทำงานส่งข้อมูลผ่านเครือข่าย 26

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันความต้องการในการนำปูมจราจร (ปูมข้อมูลจราจรทางคอมพิวเตอร์) ไปใช้งานนั้นมีความสำคัญมากขึ้น เนื่องจากการที่ประเทศไทยได้มีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ [1] โดยเฉพาะมาตรา ๒๖ ที่กล่าวไว้ว่า ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการ ผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะราย และเฉพาะคราวก็ได้ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรี ประกาศในราชกิจจานุเบกษา ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท อีกทั้งยังมีประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร [2] ถึงข้อมูลที่ร้านบริการอินเทอร์เน็ตจำเป็นจะต้องเก็บบันทึก

ทำให้ผู้ให้บริการตามความหมายของพระราชบัญญัติดังกล่าว จำเป็นต้องเก็บปูมจราจรเป็นระยะเวลาไม่น้อยกว่าเก้าสิบวัน แต่หากปูมจราจรเหล่านั้นไม่ได้ถูกเก็บไว้อย่างมั่นคง จะทำให้ไม่สามารถนำไปใช้ประโยชน์ในชั้นศาลได้ โดยมีการกล่าวอ้างถึงที่มาของปูมจราจรว่าอาจถูกแก้ไขและความไม่น่าเชื่อถือของเครื่องที่สร้างและเก็บปูมจราจร [3]

แต่อย่างไรก็ตามหลักฐานที่เก็บมาของผู้ใช้บริการระดับ องค์กรเอกชน สถานที่ราชการและร้านบริการนั้น มีความเสี่ยงต่อการถูกแก้ไขหรือทำลาย เนื่องจากสถานที่เหล่านี้มีบุคคลที่แวะเวียนเข้ามาใช้บริการในหลากหลายวัตถุประสงค์ โดยเฉพาะอย่างยิ่งในระดับร้านบริการอินเทอร์เน็ต รวมถึงเจ้าหน้าที่ของทางการที่ประพฤติมิชอบเองด้วย

หากไม่มีระบบในการจัดการปูมจราจรที่ดี ปูมจราจรที่เกิดขึ้นนั้นอาจถูกแก้ไขปลอมแปลงและไม่สามารถนำไปใช้ประโยชน์ในชั้นศาลได้หากผู้ถูกฟ้องร้องสามารถพิสูจน์ได้ถึงความไม่น่าเชื่อถือของหลักฐาน อีกทั้งการมีระบบการจัดการปูมจราจรที่ดีนั้นยจะช่วยให้การสืบสวนทางคอมพิวเตอร์สามารถทำได้ง่ายขึ้นอีกด้วย และจากการตรวจสอบระบบการจัดการปูมจราจรแบบโอเพนซอร์ส [4] พบว่ามีการเก็บปูมจราจรอยู่ในลักษณะที่ไม่สามารถตรวจสอบได้ว่ามีการแก้ไขโดยไม่ได้รับอนุญาตหรือไม่ ทั้งที่มีงานวิจัยที่สนับสนุนระบบดังกล่าวหลายชิ้นก็ตาม [5][6][7][8] จึงมีความจำเป็นอย่างรีบด่วนที่ต้องพัฒนา เพื่อแก้ไขข้อบกพร่องนี้

1.2 วัตถุประสงค์ของการวิจัย

เพื่อวิเคราะห์ ออกแบบ และพัฒนาระบบปุ่มข้อมูลจราจรทางคอมพิวเตอร์ให้มีความมั่นคง โดยใช้ต้นทุนต่ำเพื่อใช้ในร้านบริการอินเทอร์เน็ต

1.3 ขอบเขตของการวิจัย

1. ทำการทดลองในร้านบริการอินเทอร์เน็ตซึ่งมีขนาดระหว่าง 10 – 14 เครื่อง เป็นอย่างน้อยเนื่องจากเป็นขนาดให้บริการของร้านบริการอินเทอร์เน็ตส่วนใหญ่ [9]

2. สภาพแวดล้อมที่ใช้ในการวิจัย ควรจะเป็นร้านบริการอินเทอร์เน็ตที่มีบริการหลากหลาย เช่น เกมส์ อินเทอร์เน็ต พิมพ์เอกสาร เป็นอย่างน้อยเพื่อความหลากหลายของปุมจราจรในการวิเคราะห์ข้อมูลในภายหลัง

3. เนื่องจากที่ผ่านมามีการวิจัยเกี่ยวกับความสามารถในการรักษาความปลอดภัยเป็นหลักแล้ว ดังนั้นผู้วิจัยจึงอยากนำเสนอถึงประสิทธิภาพของระบบเป็นหลัก โดยจะทดลองถึงความสามารถในการนำระบบที่สร้างขึ้นมาเพื่อใช้งานจริง

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 ความสมบูรณ์ของข้อมูล (Data Integrity)

การรักษาความสมบูรณ์ของข้อมูลนั้นมี 3 วิธีการพื้นฐาน [10] คือ การทำสำเนา (Mirroring) การสร้างภาวะคู่หรือคี่ (Parity) และโดยเฉพาะอย่างยิ่งการทำผลรวมตรวจสอบ (check sum) ซึ่งจะมีบทบาทสำคัญในการวิจัยครั้งนี้

โดยกระบวนการทำผลรวมตรวจสอบกับข้อมูลใดๆ นั้นมีสองขั้นตอนคือ การสร้างผลรวม และการตรวจสอบผลรวม

แฮชฟังก์ชันมีหน้าที่หลักในการสร้างผลรวมของข้อมูลที่สมบูรณ์ โดยผลรวมดังกล่าวจะถูกเก็บบันทึกไว้อย่างปลอดภัยเพื่อใช้ในการตรวจสอบในอนาคต คุณสมบัติของแฮชฟังก์ชันที่สำคัญมีอยู่สองข้อคือ แฮชฟังก์ชันที่ดีจะต้องสร้างผลลัพธ์ที่มีค่าต่างกันเสมอหากข้อมูลที่ถูกป้อนเข้าไปมีลักษณะที่ต่างกัน ถึงแม้ข้อมูลทั้งสองนั้นจะแตกต่างกันเพียงเล็กน้อยก็ตาม และผลลัพธ์ที่เกิดขึ้นนั้นจะต้องไม่สามารถถูกคำนวนกลับไปเป็นข้อมูลเดิมได้ [11]

ในส่วนของการการตรวจสอบผลรวมนั้นสามารถทำได้โดย การนำข้อมูลที่ต้องการตรวจสอบมาคำนวนผลรวมอีกครั้ง และนำผลรวมที่ได้ไปเปรียบเทียบกับผลรวมที่ได้เก็บไว้ก่อนหน้านี้ โดยข้อมูลจะสมบูรณ์ก็ต่อเมื่อผลรวมทั้งสองตรงกันและผลรวมก่อนหน้ามีความน่าเชื่อถือมากเพียงพอ

2.1.2 รูปแบบการให้บริการอินเทอร์เน็ต

รูปแบบใช้บริการอินเทอร์เน็ตผ่านร้านบริการอินเทอร์เน็ตในประเทศไทยสามารถแบ่งได้เป็นสองประเภทดังนี้

1. ร้านที่มีบริการจุดพร้อมโยง (Hotspot Wi-Fi) - ให้ใช้บริการโดยร้านเหล่านี้โดยมากไม่มีคอมพิวเตอร์ให้ใช้เพียงแต่มีบริการที่สามารถทำให้ลูกค้าเข้าถึงอินเทอร์เน็ตได้โดยลูกค้าต้องนำเครื่องคอมพิวเตอร์เข้ามาเอง ร้านแบบนี้จะมีการใช้ระบบเรเดียส (RADIUS) ซึ่งมีการบันทึกการใช้งานของผู้ใช้บริการโดยเรเดียสเซิร์ฟเวอร์ที่มีสถานที่ตั้งทางกายภาพคนละตำแหน่งกับตัวร้าน โดยมากผู้ให้บริการประเภทนี้จะเป็นผู้ให้บริการอินเทอร์เน็ตซึ่งถูกบังคับให้มีการเก็บบันทึกปูมจราจรอยู่แล้ว

2. ร้านบริการอินเทอร์เน็ต (Internet Café) – มีการให้บริการในรูปแบบที่แตกต่างกันไปโดยมากจะมีการจัดเตรียมเครื่องคอมพิวเตอร์ไว้ให้ โดยผู้ใช้บริการสามารถใช้บริการ

ได้หลากหลายรูปแบบ เช่น บริการเข้าถึงอินเทอร์เน็ต เกมส์คอมพิวเตอร์แบบออนไลน์ การพิมพ์เอกสาร ฯลฯ ร้านเหล่านี้ส่วนใหญ่มีระบบในการเชื่อมต่อสู่อินเทอร์เน็ตอย่างง่ายๆ โดยมี โมเด็ม และสวิตช์ (Switch) หรือ เราท์เตอร์ (Router) เพื่อการเชื่อมต่อเครื่องคอมพิวเตอร์ภายในร้านออกสู่อินเทอร์เน็ต และในปัจจุบันก็ได้มีการพัฒนาโปรแกรมเพื่อบริหารจัดการภายในร้านเหล่านี้ทำให้ผู้ให้บริการสามารถควบคุมการใช้งานได้ง่ายขึ้นโดยโปรแกรมเหล่านี้เช่น Ncafe MyCafeCup TrueSoft CafeSuite [12] และบางร้านก็เขียนโปรแกรมดังกล่าวขึ้นมาเอง โดยมีการเก็บบันทึกการเข้าใช้งานของผู้ใช้อยู่ด้วย แต่ไม่มีโปรแกรมใดที่เน้นถึงการเก็บบันทึกปูมจราจรที่สนับสนุนการสืบสวนทางคอมพิวเตอร์ ร้านประเภทนี้จึงเป็นร้านที่งานวิจัยนี้ให้ความสนใจ

การที่ผู้ให้บริการไม่คำนึงถึงความมั่นคงของปูมจราจรนั้น ไม่ได้แปลว่าวิธีการเก็บบันทึกปูมจราจรในปัจจุบันนั้นมีความปลอดภัยอยู่แล้ว แต่เกิดจากความซับซ้อนและต้นทุนในการดูแลรักษานั่นเอง อีกทั้งการแก้ไขปูมจราจรนั้นสามารถทำได้หลายวิธีด้วยกัน โดยเฉพาะอย่างยิ่งบนระบบปฏิบัติการวินโดวส์ ซึ่งร้านบริการอินเทอร์เน็ตนั้นนิยมใช้งานเพราะลูกค้าส่วนใหญ่ต้องการเข้ามาเพื่อเล่นเกมส์ และเกมส์เหล่านั้นโดยทั่วไปเข้าได้กับระบบปฏิบัติการวินโดวส์ได้เท่านั้น

2.1.3 การซ่อนตัวจากระบบปูมจราจร

ผู้ไม่ประสงค์ดีสามารถทำลายหลักฐาน และซ่อนตัว ได้หลายวิธี โดยวิธีที่เกี่ยวข้องกับงานวิจัยนี้คือการลบและแก้ไขปูมจราจรที่อยู่บนระบบปฏิบัติการวินโดวส์ โดยปูมจราจรบนระบบปฏิบัติการวินโดวส์นั้นถูกบันทึกเป็นตัวอักษรซึ่งไม่มีการเข้ารหัสใดๆ อยู่ในไฟล์แบบทวิภาคที่มีนามสกุล evt และสามารถเปิดอ่านได้โดยโปรแกรมเช่น Event Log Management ของทางไมโครซอฟต์เอง แต่โดยปกติแล้วไฟล์ดังกล่าวนี้จะไม่สามารถถูกแก้ไขได้ เนื่องจากตัวระบบปฏิบัติการจะทำการป้องกันไม่ให้มีการแก้ไขจากผู้บุกรุก โดยการเปิดไฟล์ค้างเอาไว้เมื่อระบบปฏิบัติการเริ่มทำงาน จนกว่าจะมีการปิดเครื่อง ถึงอย่างไรก็ตามผู้บุกรุกยังสามารถลบ หรือแก้ไขมันได้ด้วยวิธีตามตัวอย่างดังต่อไปนี้

1. ในกรณีที่ผู้บุกรุกสามารถเข้าถึงระบบได้โดยใช้สิทธิของผู้ดูแลระบบ (Administrator) ผู้บุกรุกสามารถสั่งลบข้อความในปูมจราจรทั้งหมดได้โดยใช้สิทธิ์ของผู้ดูแล เพียงแต่ระบบปฏิบัติการจะทำการบันทึกไว้ว่ามีการลบปูมจราจร ซึ่งจะทำให้ผู้ดูแลระบบสามารถทราบได้ภายหลังว่ามีการบุกรุกเกิดขึ้นจากบันทึกที่ว่ามีการลบปูมจราจร
2. ผู้บุกรุกอาจใช้วิธีถอดฮาร์ดดิส หรือปลุกเครื่องคอมพิวเตอร์เข้าระบบปฏิบัติการอื่นเพื่อข้ามผ่านการป้องกันของระบบปฏิบัติการวินโดวส์ และแก้ไขไฟล์ดังกล่าวได้โดยง่าย

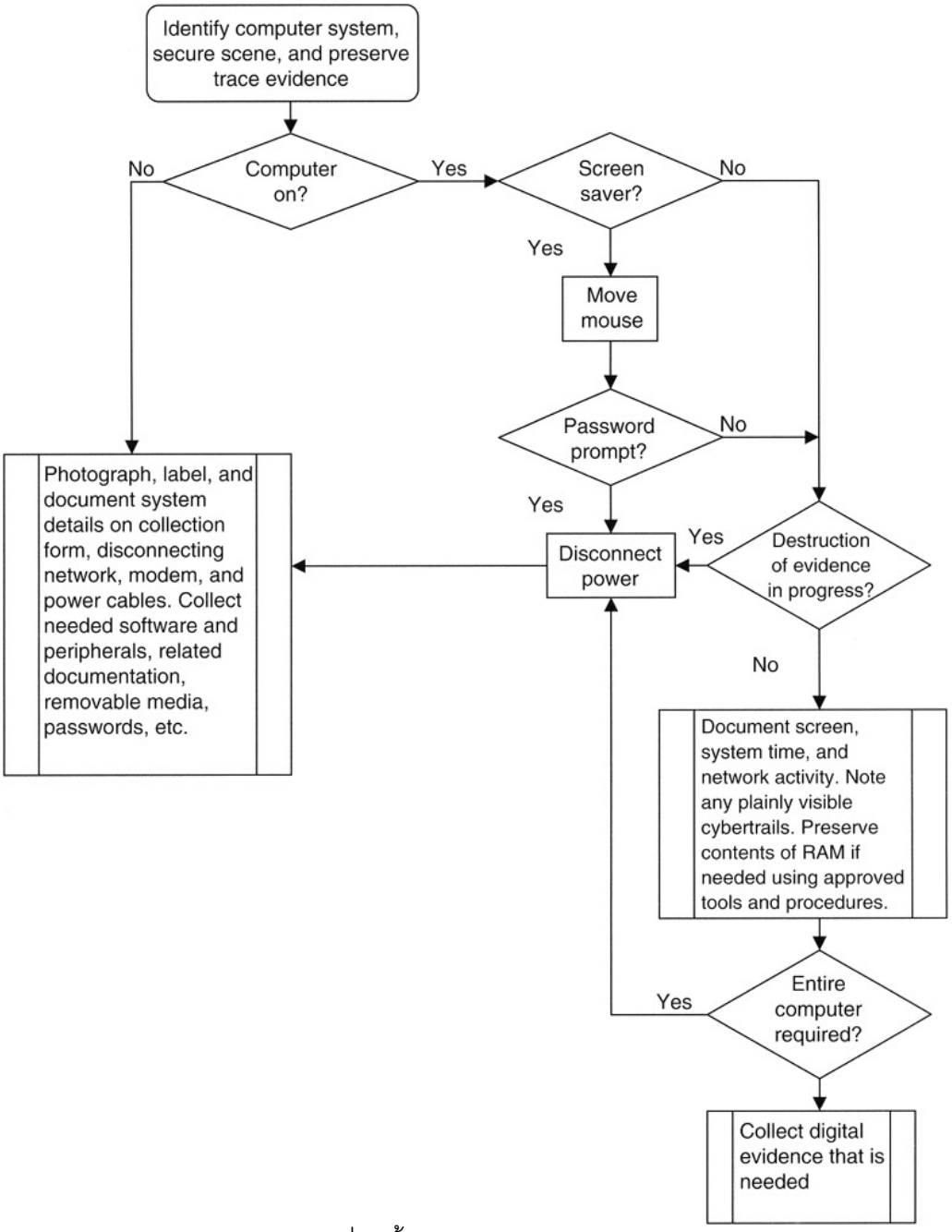
3. ผู้บุกรุกสามารถใช้โปรแกรมเพื่อลบ หรือแก้ไขปูมจราจร เช่น โปรแกรม WinZapper [13] หรือ ELsave [14]

สองวิธีหลังที่กล่าวมาจะทำให้ผู้ดูแลระบบไม่สามารถทราบได้ถึงความเปลี่ยนแปลงของปูมจราจรแม้แต่น้อย เพราะสามารถทำให้ผู้บุกรุกเลือกที่จะลบหรือแก้ไขในส่วนของร่องรอยที่ตัวเองทำไว้เพียงเท่านั้น ซึ่งยากแก่การสังเกต ในกรณีที่ผู้บุกรุกไม่ทำให้ช่องว่างของเวลาระหว่างแต่ละเหตุการณ์นั้นมีมากจนผิดสังเกต

2.1.4 หลักการในการสืบสวนทางคอมพิวเตอร์

โดยธรรมชาติของหลักฐานทางอิเล็กทรอนิกส์ (Electronic Evidence) นั้นค่อนข้างบอบบาง สามารถแก้ไข ทำให้เกิดความเสียหาย หรือทำลายได้โดยง่ายหากไม่ปฏิบัติด้วยความรอบคอบ กระบวนการในการสืบสวนทางคอมพิวเตอร์นั้นมีขั้นตอนพื้นฐานอย่างน้อย 4 ประการด้วยกัน และในแต่ละส่วนนั้นก็เพื่อแก้ไขข้อด้อยของหลักฐานทางอิเล็กทรอนิกส์ [15]

1. การเก็บรวบรวมหลักฐาน (Collection)
2. การตรวจสอบ (Examination)
3. การวิเคราะห์ (Analysis)
4. การรายงานผล (Reporting)



รูปที่ 1 ขั้นตอนการเก็บหลักฐาน

จากรูปที่ 1 ในการเก็บหลักฐานนั้น เจ้าพนักงานต้องทำตามขั้นตอนต่างๆ มากมาย เพื่อให้ได้มาซึ่งหลักฐานที่น่าเชื่อถือ [16] โดยเจ้าหน้าที่จำเป็นต้องไปถึงสถานที่ด้วยตนเอง เพื่อดำเนินการเก็บหลักฐาน และหลังจากที่ได้หลักฐานก็มีขั้นตอนในการรักษาหลักฐานเพื่อให้เกิดความมั่นคงเช่น การบรรจุหลักฐานเพื่อการขนย้าย การขนย้าย และรักษาสายโซ่แห่งการถือครองวัตถุพยาน (Chain of Custody) ที่เป็นปูมจราจร

ก่อนที่เจ้าหน้าที่จะสามารถนำหลักฐานอย่างเช่น ฮาร์ดดิสก์ฮาร์ดดิสก์ไปใช้นั้น เจ้าหน้าที่ต้องสร้างสำเนาขึ้นมาหนึ่งชุด และเก็บหลักฐานตัวจริงไว้ในหีบห่อที่มีตราประทับเพื่อป้องกันไม่ให้

ผู้ใดมาแกะออกได้โดยไม่ทิ้งร่องรอย และเจ้าหน้าที่ต้องสร้างสำเนาขึ้นมาอีกอย่างน้อยหนึ่งชุดจากสำเนาชุดแรกเพื่อนำมาเปิดอ่าน หรือค้นหาร่องรอยของอาชญากรรมทางคอมพิวเตอร์ต่อไป

กระบวนการมากมายเหล่านี้ก็เพื่อให้หลักฐานสามารถนำไปใช้ได้ในชั้นศาล โดยหลักฐานนั้นต้องสามารถพิสูจน์ได้ว่าเป็นตัวจริง และไม่มีการแก้ไขเกิดขึ้นกับตัวหลักฐาน ซึ่งโดยปกติแล้วสามารถพิสูจน์ได้ด้วยการหาผลรวมตรวจสอบ (Checksum) ระหว่างฮาร์ดดิสก์ที่ได้จากที่เกิดเหตุและสำเนาที่สร้างขึ้น

ระบบปูมข้อมูลจราจรทางคอมพิวเตอร์ที่มั่นคงสามารถช่วยลดความซับซ้อน และความผิดพลาดในการเก็บวัตถุพยานทางคอมพิวเตอร์ เพราะระบบที่นำเสนอนี้สามารถยืนยันความบริสุทธิ์ของปูมข้อมูลจราจรได้ทุกเมื่อโดยที่เจ้าหน้าที่ของทางภาครัฐไม่จำเป็นที่จะต้องเข้าถึงวัตถุพยานทางคอมพิวเตอร์ทางกายภาพ ซึ่งการการเข้าถึงวัตถุพยานทางกายภาพของเจ้าหน้าที่ได้สร้างความเคลือบแคลงใจอยู่ตลอดเวลาตามสื่อหนังสือพิมพ์ และโทรทัศน์

2.2 งานวิจัยที่เกี่ยวข้อง

งานวิจัยในด้านการบันทึกข้อมูลโดยไม่ให้มีการแก้ไขนั้นได้มีการพัฒนามานานแล้ว เช่น การเขียนข้อมูลลงบนสื่อที่ถูกแก้ไขได้ยากอย่างกระดาษ หรือ ซีดี แต่การทำงานนั้นไม่เหมาะสมที่จะนำมาใช้งานในปัจจุบันเนื่องจากปริมาณของปูมจราจรเพิ่มขึ้นอย่างรวดเร็ว เกินกว่าจะสามารถเขียนลงบนสื่อประเภทดังกล่าวได้ทัน การวิจัยของ เบลเล และ ยี [6] เป็นงานวิจัยแรกซึ่งถูกตีพิมพ์อย่างแพร่หลายถึงวิธีการเก็บบันทึกข้อมูลไปข้างหน้าโดยรักษาบูรณภาพของมันไว้ หรือ เชนียร์ และ เคลซี่ [5] ที่ตีพิมพ์งานวิจัยเกี่ยวกับวิธีการบันทึกข้อมูลเหตุการณ์เพื่อสนับสนุนการสืบสวนทางด้านคอมพิวเตอร์ ในลักษณะของระบบแบบกระจาย และงานวิจัยทั้งสองนี้ได้มีการอ้างถึงและนำมาพัฒนาโดยนักวิจัยอีกหลายท่าน [17]

ล็อกคริพท์ (Logcrypt) โดย ฮอลต์ [7] เป็นอีกระบบหนึ่งที่พัฒนาบนพื้นฐานของ เชนียร์ และ เคลซี่ โดยเปลี่ยนจากการใช้กุญแจลับ ไปเป็นกุญแจสาธารณะ และเน้นถึงการทำงานบนระบบที่บันทึกข้อมูลเหตุการณ์ที่เกิดขึ้นพร้อมๆ กันเป็นจำนวนมากอย่างมีประสิทธิภาพ โดยการรวมข้อมูลเหตุการณ์ที่เกิดขึ้นภายใต้ระยะเวลาที่กำหนดไว้ เพื่อทำการเข้ารหัสและเก็บบันทึกในคราวเดียวภายใต้ระยะเวลา T โดย T เป็นเวลาที่ผู้บุกรุกจำเป็นต้องใช้ในการเข้าควบคุมเครื่องคอมพิวเตอร์ ซึ่งหลักการนี้ทำให้ไม่จำเป็นต้องเข้ารหัสทุกเหตุการณ์ที่เกิดขึ้นทำให้เครื่องคอมพิวเตอร์ทำงานน้อยลง

อย่างไรก็ตามงานวิจัยเหล่านี้ต่างมีจุดประสงค์เดียวกันคือ ระบบการทำงานนั้นต้องสามารถต่อต้านการแก้ไขข้อมูลที่ได้ถูกบันทึกไว้แล้วก่อนที่ผู้บุกรุกจะสามารถเข้าควบคุมเครื่องคอมพิวเตอร์ และสามารถควบคุมการเข้าถึงข้อมูลของบุคคลภายนอก ทั้งหมดนี้เพื่อรักษาคุณค่าของหลักฐาน และช่วยเหลือเจ้าหน้าที่ผู้สืบสวนในการเก็บรักษาและตรวจสอบหลักฐานนั้นเอง แต่

ยังมีงานวิจัยอีกบางส่วนที่จำเป็นต้องนำมาประกอบเพื่อให้สถาปัตยกรรมนี้มีความสมบูรณ์มากขึ้นเมื่อถูกนำไปใช้งาน

งานวิจัยของ วอเตอร์ บาลเฟนซ์ เดอร์พี และ เสม็ทเทอร์ [8] นั้นทำให้ข้อมูลเหตุการณ์ที่ถูกบันทึกไว้สามารถนำมาค้นหาได้โดยง่าย โดยระบบจะเปิดเผยให้ผู้ที่ต้องการค้นหาข้อมูลเหตุการณ์เฉพาะในส่วนที่จำเป็นเท่านั้น ซึ่งมีส่วนสำคัญในการช่วยเหลือผู้วิเคราะห์ข้อมูลอย่างมาก และสามารถลดข้อบกพร่องในงานวิจัยของ เซนียร์ และ เคลซี่ ที่ ฮอลต์ กล่าวว่าไม่มีความปลอดภัยเนื่องจากผู้ที่ทำการพิสูจน์หลักฐานสามารถสร้างข้อมูลเหตุการณ์ปลอมขึ้นมาใหม่ได้ เพราะเขาจำเป็นต้องล่วงรู้ถึงกุญแจสำหรับถอดรหัสเพื่อพิสูจน์หลักฐาน ซึ่งเป็นข้อจำกัดของการเข้ารหัสโดยกุญแจลับ

ในบทนี้ได้กล่าวถึงทฤษฎีและงานวิจัยที่มีส่วนช่วยในการแก้ไขปัญหาความไม่ปลอดภัยของข้อมูลที่ร้านบริการอินเทอร์เน็ต รวมถึงรูปแบบของร้านบริการอินเทอร์เน็ตที่ใช้ในการทดลอง ในบทต่อไปจะกล่าวถึงการออกแบบและวิธีดำเนินการวิจัย

บทที่ 3
การออกแบบและวิธีดำเนินการวิจัย

หลังการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เมื่อปี พ.ศ. 2550 ได้มีความพยายามมากมายที่จะผลักดันให้เกิดกระบวนการในการเก็บรักษาปูมข้อมูลจราจรของผู้ให้บริการอินเทอร์เน็ต ระบบปูมข้อมูลจราจรนี้จึงเกิดขึ้นเพื่อเป็นแนวทางในการเก็บรักษาข้อมูลอย่างมั่นคง

3.1 ความต้องการของระบบ

ความต้องการของระบบแบ่งเป็นสองส่วนคือ ส่วนของผู้ให้บริการร้านอินเทอร์เน็ต และฝ่ายความมั่นคง

ความต้องการจากผู้ให้บริการร้านอินเทอร์เน็ต

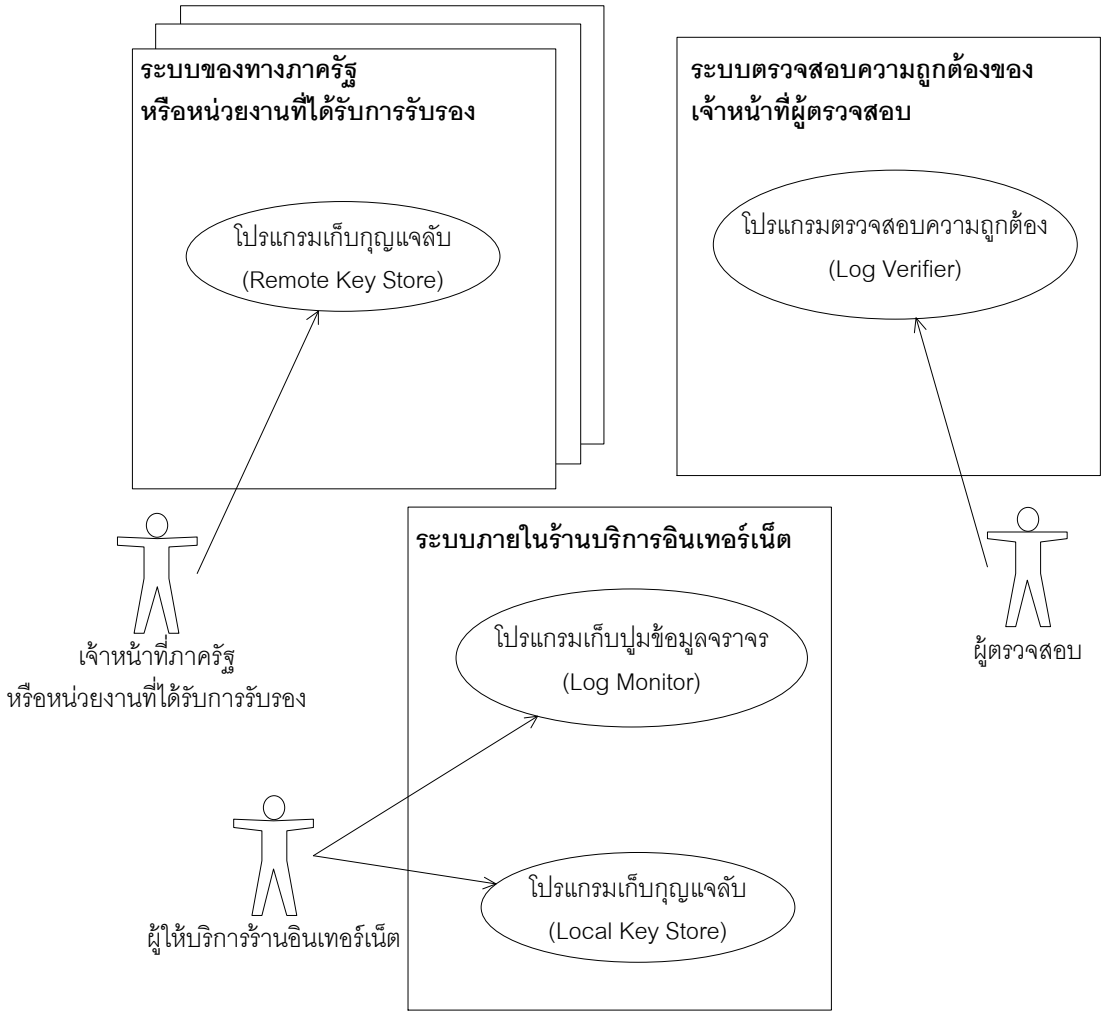
1. ไม่ก่อให้เกิดผลกระทบต่อประสิทธิภาพของระบบเครือข่ายและเครื่องคอมพิวเตอร์ภายในร้านบริการอินเทอร์เน็ต
2. มีระบบสมาชิก
3. รองรับการบันทึกข้อมูลการเข้าใช้งานของผู้ใช้บริการที่ไม่ใช่สมาชิก
4. สามารถคำนวนระยะการใช้งานเพื่อคำนวนค่าใช้จ่ายให้กับลูกค้า และออกใบเสร็จได้
5. มีค่าใช้จ่ายในการบำรุงรักษาต่ำ

ความต้องการจากฝ่ายที่ต้องการความมั่นคงของข้อมูลจราจรเพื่อสนับสนุนการการสืบสวนทางคอมพิวเตอร์

1. เก็บข้อมูลที่สามารถระบุตัวบุคคล เวลาของการเข้าใช้และเลิกใช้บริการ หมายเลขเครื่องที่ใช้ IP Address (Internet Protocol Address) [2]
2. เก็บรักษาปูมข้อมูลจราจรทางคอมพิวเตอร์ด้วยวิธีการที่มั่นคงปลอดภัยตาม ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการในข้อ 8
3. มีการตรวจสอบอุปกรณ์และระบบต้นทางว่าเป็นอุปกรณ์ที่ได้รับอนุญาตแล้ว
4. ต้องมีการป้องกันการเข้าถึงข้อมูลที่ส่งผ่านระบบเครือข่ายโดยไม่ได้รับอนุญาต
5. มีการแสดงข้อผิดพลาดอย่างชัดเจนในกรณีที่การจัดเก็บไม่สมบูรณ์
6. มีการสร้างบัญชีผู้ใช้งาน เพื่อไม่ให้เกิดการซ้ำซ้อนในการใช้งาน และสามารถพิสูจน์ตัวตนได้ก่อนการเข้าใช้งาน
7. มีการจำกัดการเข้าถึงระบบแบบลำดับชั้น เพื่อให้สามารถจำกัดสิทธิ์ในการเข้าถึงส่วนต่างๆ ของระบบได้อย่างมีประสิทธิภาพ

จากความต้องการของทั้งสองกลุ่มนั้นประเด็นหลักในการออกแบบระบบคือความสามารถในการเก็บปูมข้อมูลจราจรทางคอมพิวเตอร์ของร้านบริการอินเตทอร์เน็ตตามหลักเกณฑ์ด้วยต้นทุน และค่าบำรุงรักษาต่ำ ในส่วนของการออกแบบและพัฒนา ระบบสมาชิก การออกใบเสร็จและการสร้างบัญชีผู้ใช้งานนั้น ยังไม่สามารถพัฒนาได้เนื่องจากอาจจะก่อให้เกิดความเสียหายต่อธุรกิจ เพราะในทางปฏิบัตินั้นพบว่าลูกค้าสามารถเข้าใช้เครื่องคอมพิวเตอร์ได้โดยไม่ต้องมีการลงชื่อหรือตรวจบัตรประชาชนแต่อย่างใด

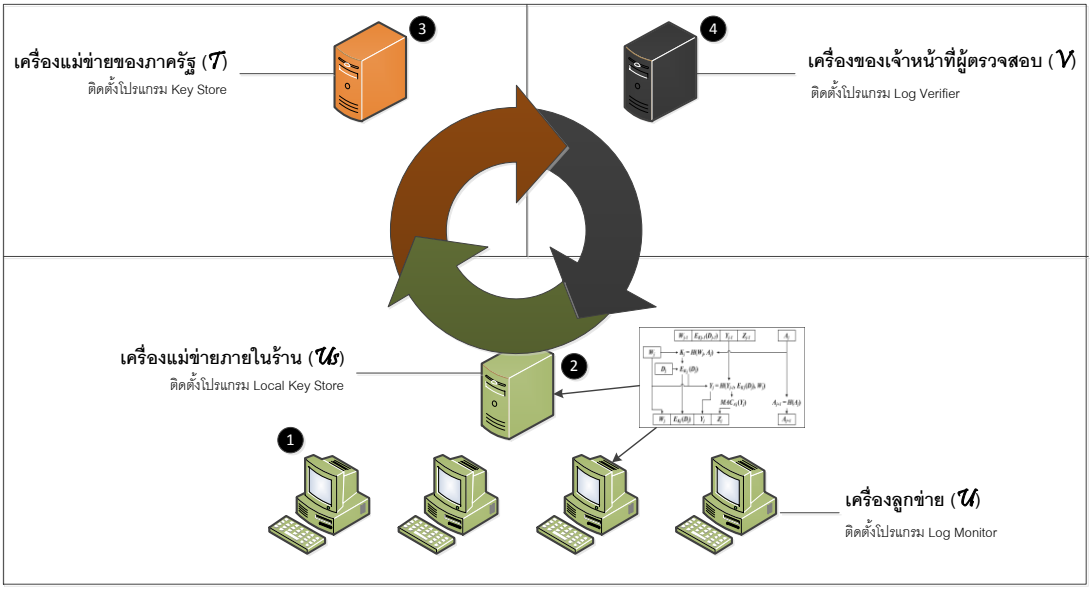
3.2 ส่วนประกอบของระบบ



รูปที่ 2 ผู้เกี่ยวข้องและส่วนประกอบของระบบปูมข้อมูลจราจรทางคอมพิวเตอร์

ผู้เกี่ยวข้องภายในระบบตามรูปที่ 2 มีดังนี้

1. ผู้ให้บริการร้านอินเทอร์เน็ต (ผู้ให้บริการ)
2. เจ้าหน้าที่ภาครัฐ หรือหน่วยงานที่ได้รับการรับรอง (เจ้าหน้าที่)
3. ผู้ตรวจสอบ (ผู้ตรวจสอบ)



รูปที่ 3 แผนภาพระบบปูมข้อมูลจาจรทางคอมพิวเตอร์

โปรแกรมและระบบที่เกี่ยวข้องกับระบบปูมข้อมูลจราจรทางคอมพิวเตอร์ ดังรูปที่ 3 มีดังต่อไปนี้

1. ระบบภายในร้านบริการอินเทอร์เน็ต
   1.1. Log Monitor – ทำหน้าที่บันทึกการใช้งานอินเทอร์เน็ตของผู้ใช้บริการให้เป็นไปตามหลักเกณฑ์การเก็บรักษาปูมข้อมูลจราจรทางคอมพิวเตอร์ซึ่งประกาศโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โปรแกรม Log Monitor จะถูกติดตั้งไว้ยังเครื่องลูกข่ายที่ให้บริการแก่ลูกค้าภายในร้านบริการอินเทอร์เน็ต
   1.2. Local Key Store – ทำหน้าที่เก็บปูมข้อมูลจราจรจากการใช้งานของผู้ใช้บริการร้านอินเทอร์เน็ต และเก็บรักษากุญแจลับจากเครื่องลูกข่ายทั้งหมดภายในร้านโดยใช้หลักการเดียวกันกับการเก็บปูมข้อมูลจราจรของเครื่องลูกข่ายในการเข้ารหัสกุญแจลับดังกล่าว โดยกุญแจลับที่ Local Key Store สร้างขึ้นจะถูกส่งไปเก็บที่เครื่องแม่ข่ายของภาครัฐอีกทอดหนึ่งโปรแกรม Local Key Store จะถูกติดตั้งไว้ยังเครื่องแม่ข่ายภายในร้านบริการอินเทอร์เน็ต
2. ระบบของทางภาครัฐ หรือหน่วยงานที่ได้รับการรับรอง
   Key Store – ทำหน้าที่เก็บรักษากุญแจลับจากเครื่องแม่ข่ายภายในร้านบริการอินเทอร์เน็ต โปรแกรม Key Store จะถูกติดตั้งไว้ยังเครื่องแม่ข่ายของทางภาครัฐ ในในทางปฏิบัติระบบนี้ควรมีมากกว่า 1 ระบบเพราะเป็นการป้องกันในกรณีที่ระบบใดระบบหนึ่งถูกโจมตี หรือได้รับความเสียหาย
3. ระบบตรวจสอบความถูกต้อง
   Log Verifier – ถูกใช้งานโดยผู้ตรวจสอบที่เป็นกลาง โดยผู้ตรวจสอบต้องทำการติดต่อขอกุญแจลับจากทางภาครัฐหรือหน่วยงานที่ได้รับการรับรองในข้อ 2 และนำ

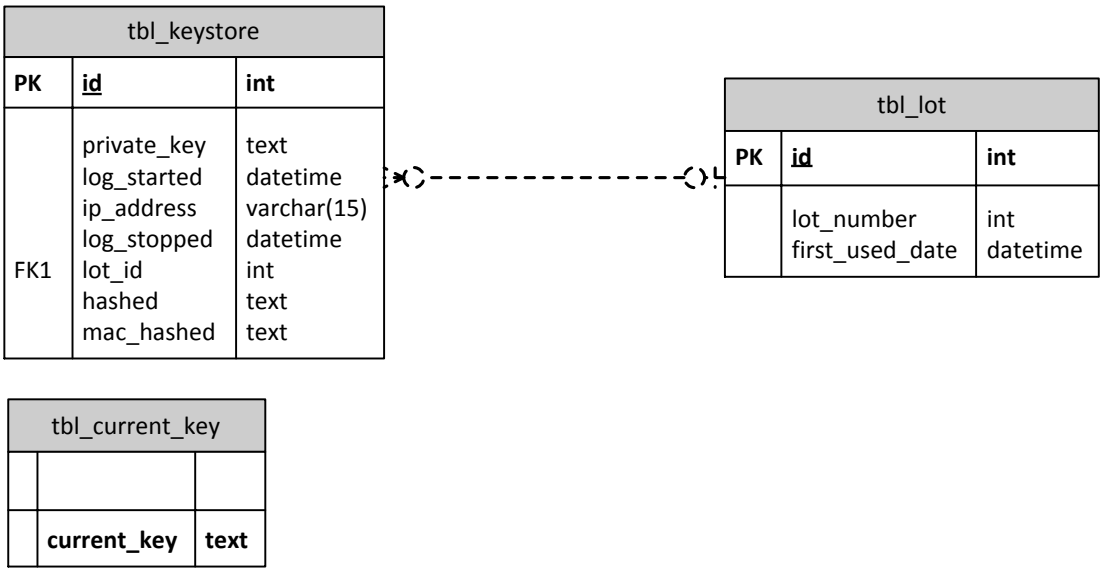
กุญแจลับดังกล่าวมาตรวจสอบความสมบูรณ์ของปูมข้อมูลที่ถูกเก็บไว้โดยผู้ให้บริการ โปรแกรมจะถูกติดตั้งไว้ยังเครื่องคอมพิวเตอร์ของเจ้าหน้าที่ผู้ตรวจสอบ

3.3 ข้อมูลที่เกี่ยวข้องภายในระบบ

ถึงแม้ข้อมูลที่ที่เกี่ยวข้องภายในระบบจะถูกแสดงด้วยแผนภาพแสดงความสัมพันธ์ระหว่างข้อมูล (Entity Relationship Diagram) และในการทดลองนั้นข้อมูลจะถูกเก็บอยู่ในฐานข้อมูล แต่ไม่ได้หมายความว่าในการนำไปใช้งานจริงนั้นข้อมูลทั้งหมดจำเป็นจะต้องถูกเก็บอยู่ในฐานข้อมูลเสมอไป ยกตัวอย่างเช่นตาราง tbl_current_key ซึ่งมีข้อมูล current_key เก็บอยู่ภายใน ข้อมูลนี้มีความสำคัญมาก หากมีผู้ไม่ประสงค์ดีขโมยไปจะสามารถสร้างปูมข้อมูลจราจรเท็จขึ้นมาได้โดยที่ Log Verifier จะให้ผลตรวจสอบที่เป็นจริง แต่ในทางปฏิบัติสามารถแก้ปัญหาได้ด้วยการเข้ารหัสฐานข้อมูล หรือเข้ารหัสข้อมูลดังกล่าวเก็บไว้ในหน่วยความจำ

ข้อมูลที่เครื่องแม่ข่ายภายในร้าน

เครื่องแม่ข่ายภายในร้านมีหน้าที่เก็บปูมข้อมูลจราจรในรูปแบบของไฟล์โดยไม่มีการแก้ไขเปลี่ยนแปลง และกุญแจลับจากเครื่องลูกข่ายภายในร้านจะถูกบันทึกไว้ในฐานข้อมูลเพื่อง่ายแก่การค้นหา



รูปที่ 4 ข้อมูลที่เครื่องแม่ข่ายภายในร้านบริการอินเทอร์เน็ต

ตารางที่ 1 รายละเอียดตาราง tbl_keystore

ชื่อสดมภ์	ประเภทของข้อมูล	รายละเอียด
id	int	หมายเลขรหัสลับ
private_key	text	รหัสลับที่เข้ารหัสแล้ว
log_started	datetime	วันและเวลาที่เครื่องลูกข่ายส่งรหัสเข้ามา
ip_address	varchar(15)	หมายเลข IP Address ของเครื่องลูกข่าย
log_stopped	datetime	วันและเวลาที่เครื่องลูกข่ายเก็บปุ่มข้อมูลจราจรด้วยรหัสดังกล่าวเสร็จสมบูรณ์
lot_id	int	รหัสชุดของปุ่มจราจร
hashed	text	แฮชข้อมูลในตารางทั้งหมดเพื่อยืนยันความถูกต้องภายหลัง
mac_hashed	text	เข้ารหัสข้อมูลในตารางอีกครั้งหนึ่งเพื่อป้องกันการแก้ไข

ตารางที่ 2 รายละเอียดตาราง tbl_lot

ชื่อสดมภ์	ประเภทของข้อมูล	รายละเอียด
id	int	หมายเลขรหัสชุดของปุ่มข้อมูลจราจร
lot_number	int	รหัสชุดของปุ่มข้อมูลจราจร
first_used_date	datetime	วันและเวลาที่เริ่มใช้งาน

ตารางที่ 3 รายละเอียดตาราง tbl_keystore

ชื่อสดมภ์	ประเภทของข้อมูล	รายละเอียด
current_key	text	กุญแจลับที่ใช้งานในการเข้ารหัสจากเครื่องลูกข่าย

ข้อมูลที่เครื่องแม่ข่ายของภาครัฐ

เครื่องแม่ข่ายของทางภาครัฐมีหน้าที่จัดเก็บกุญแจลับที่ถูกส่งมาจากร้านบริการอินเทอร์เน็ต และเนื่องจากเครื่องแม่ข่ายของทางภาครัฐถูกสันนิษฐานว่ามีความปลอดภัยสูง กุญแจลับที่ถูกจัดเก็บในฐานข้อมูลจึงไม่มีการเข้ารหัสแต่อย่างใด

tbl_keystore		
PK	**id**	**int**
	private_key received_datetime ip_address	text datetime varchar(15)

รูปที่ 5 ข้อมูลที่เครื่องแม่ข่ายของภาครัฐ

ตารางที่ 4 รายละเอียดตาราง tbl_lot

ชื่อสดมภ์	ประเภทของข้อมูล	รายละเอียด
id	int	หมายเลขรหัสชุดของปูมจราจร
private_key	text	รหัสชุดของปูมจราจร
received_datetime	datetime	วันและเวลาที่เริ่มใช้งาน
ip_address	varchar(15)	หมายเลข IP Address ของเครื่องแม่ขายที่ร้านบริการอินเทอร์เน็ต

ปูมข้อมูลจราจรนั้นจะถูกจัดเก็บในรูปแบบ syslog [18] เนื่องจากมีความแพร่หลายมากกว่า Windows Event Log ซึ่งเป็นลิขสิทธิ์ของบริษัทไมโครซอฟแต่เพียงผู้เดียว โดยจะมีการเก็บข้อมูลดังนี้

1. ส่วน PRI – สำหรับกำหนดลำดับความสำคัญของข้อมูลที่ถูกบันทึก สามารถคำนวนได้จากค่าความสำคัญของข้อมูลสองค่าด้วยกันคือ ความสำคัญของแหล่งที่มาของข้อมูล (Facility) และ ความสำคัญของข้อมูล (Severity) โดยการคำนวนระดับความสำคัญนั้นสามารถทำได้โดยการนำค่าจากตารางที่ 5 และ 6 มาคำนวนตามสูตรการคำนวนต่อไปนี้

PRI = (ความสำคัญของแหล่งที่มาของข้อมูล * 8) + ความสำคัญของข้อมูล

ค่าที่ได้จะถูกนำมาใส่ไว้ระหว่างเครื่องหมาย < และ > เพื่อสร้างข้อความในส่วน PRI

ตารางที่ 5 ค่าความสำคัญของแหล่งที่มาของข้อมูล (Facility)

ค่าความสำคัญ	**แหล่งที่มาของข้อมูล** (Facility)
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages (note 1)
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon (note 2)
10	security/authorization messages (note 1)
11	FTP daemon
12	NTP subsystem
13	log audit (note 1)
14	log alert (note 1)
15	clock daemon (note 2)
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

ตารางที่ 6 ความสำคัญของข้อมูล (Severity)

ค่าความสำคัญ	**ความสำคัญของข้อมูล** (Severity)
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

2. ส่วน HEADER – ระบุถึงเวลาของเหตุการณ์ และชื่อเครื่องหรือ IP Address ของเครื่องนั้นๆ โดยเวลาของเหตุการณ์จะถูกบันทึกด้วยรูปแบบ Mmm dd hh:mm:ss ซึ่งสามารถอธิบายได้ดังนี้

   2.1 Mmm – คือตัวย่อของเดือนในภาษาอังกฤษ Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov และ Dec

   2.2 dd – วันที่ ระบุโดยใช้ตัวเลขสองหลัก ตั้งแต่ 00 ถึง 31

   2.3 hh – ชั่วโมง ระบุโดยใช้ตัวเลขสองหลัก ตั้งแต่ 00 ถึง 23

   2.4 mm – นาที ระบุโดยใช้ตัวเลขสองหลัก ตั้แต่ 00 ถึง 59

   2.5 ss – วินาที ระบุโดยใช้ตัวเลขสองหลัก ตั้งแต่ 00 ถึง 59

   หลังจากระบุวันที่แล้วให้เว้นช่องว่างหนึ่งตัวอักษรและตามด้วยชื่อเครื่องหรือ IP Address

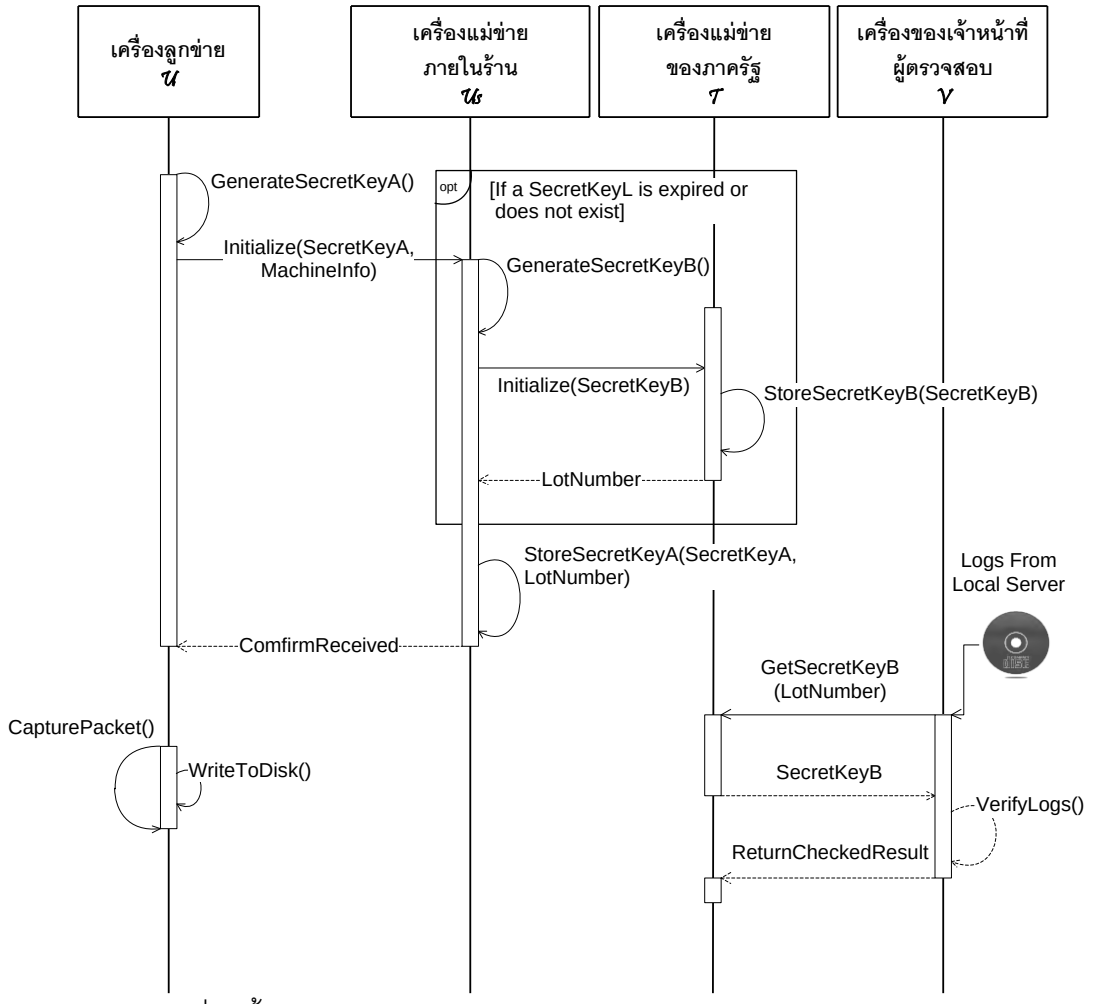
3. ส่วน MSG – ซึ่งมีข้อมูลของโปรแกรมที่ก่อให้เกิดเหตุการนั้นๆ และคำอธิบายเพิ่มเติม โดยระบบจะทำการจัดเก็บ IP Address ของเครื่องปลายทางเพิ่มเติม เพื่อให้เป็นไปตามพระราชบัญญัติฯ ข้อมูลในส่วนนี้ไม่มีรูปแบบที่ตายตัวหรือข้อบังคับใดต่างจากข้อมูลในส่วนอื่น ดังตัวอย่างในตารางที่ 7

ตารางที่ 7 ตัวอย่าง syslog

ลำดับ	ตัวอย่าง
1.	<34>Oct 11 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8
2.	<0>Oct 22 10:52:12 scapegoat 1990 Oct 22 10:52:01 TZ-6 scapegoat.dmz.example.org 10.1.2.3 sched[0]: That's All Folks!
3.	<165>Aug 24 05:34:00 CST 1987 mymachine myproc[10]: %% It's time to make the do-nuts. %% Ingredients: Mix=OK, Jelly=OK # Devices: Mixer=OK, Jelly_Injector=OK, Frier=OK # Transport: Conveyer1=OK, Conveyer2=OK # %%

3.4 การทำงานของระบบ

หลังจากการติดตั้งโปรแกรมที่มีทั้งหมดลงตามเครื่องต่างๆ แล้วการทำงานของระบบปูมข้อมูลจราจรทางคอมพิวเตอร์สามารถอธิบายตามรูปที่ 6 ได้ดังนี้



รูปที่ 6 ขั้นตอนการทำงานของระบบปูมข้อมูลจราจรทางคอมพิวเตอร์

การทำงานที่เครื่องลูกข่าย

1. Log Monitor ทำการสร้างกุญแจลับ A สำหรับการเข้ารหัสปูมข้อมูลจราจรที่เกิดขึ้น โดยกุญแจลับ A จะถูกส่งไปเก็บยังเครื่องแม่ข่ายภายในร้านพร้อมกับ IP Address ของเครื่องลูกข่ายเครื่องนั้น และเมื่อเครื่องแม่ข่ายภายในร้านยืนยันการรับกุญแจลับ A แล้ว Log Monitor จะทำการแฮชกุญแจลับ A โดยผลที่ได้คือ A2 = HASH(A) และทำลายกุญแจลับ A ทิ้งทันทีก่อนนำ A2 ไปเข้ารหัสปูมข้อมูลแรกเริ่ม
2. เมื่อทำการเข้ารหัสปูมข้อมูลแรกเริ่มเสร็จสิ้นแล้ว Log Monitor จะทำการแฮชกุญแจลับ A2 ทันที ผลที่ได้คือ A3 = HASH(A2) โดย A3 จะถูกนำไปใช้เข้ารหัสปูมข้อมูลจราจรต่อไป

   กระบวนการลูกโซ่แฮช [19] (HASH Chain) นี้จะถูกทำซ้ำไปเรื่อยๆ จน Log Monitor สิ้นสุดการทำงาน และปูมข้อมูลสุดท้ายที่บันทึกจะมีข้อความระบุไว้เพื่อให้ง่ายต่อการวิเคราะห์ข้อมูลในภายหลัง โดยผู้วิเคราะห์สามารถระบุได้ว่าการบันทึกปูมข้อมูลจราจรบนไฟล์เสร็จสิ้นอย่างสมบูรณ์หรือไม่
3. ในการบันทึกปูมข้อมูลจราจรลงบนไฟล์นั้น Log Monitor จะทำการปิดไฟล์ และสร้างไฟล์ใหม่เมื่อไฟล์มีขนาดตามค่าที่ระบุไว้

การทำงานที่เครื่องแม่ข่ายภายในร้าน

4. เมื่อเครื่องแม่ข่ายภายในร้านได้รับกุญแจลับ A มาแล้ว Local Key Store จะทำการเข้ารหัสกุญแจลับดังกล่าวโดยการสร้างกุญแจลับ B ขึ้น ในกรณีที่ยังไม่มีกุญแจลับ B หรือกุญแจลับ B หมดอายุ
5. เมื่อได้กุญแจลับ B แล้ว กุญแจลับ B จะถูกส่งไปเก็บไว้ยังเครื่องของภาครัฐ และรอผลการยืนยันการบันทึกพร้อมหมายเลขชุดของปูมข้อมูลจราจร
6. Local Key Store จะบันทึกกุญแจลับ A ควบคู่ไปกับหมายเลขชุดของปูมข้อมูลจราจร เพื่อสามารถระบุได้ว่าไฟล์ของปูมข้อมูลจราจรนั้นๆ ควรใช้กุญแจลับชุดใดในการถอดรหัส

การทำงานที่เครื่องของภาครัฐ

7. เครื่องของภาครัฐไม่มีหน้าที่ใดๆ นอกเหนือจากการบันทึกกุญแจลับ B และส่งคืนหมายเลขชุดของปูมข้อมูลจราจร เพื่อให้เป็นไปตามจุดประสงค์ที่ต้องการให้เครื่องของภาครัฐทำงานให้น้อยที่สุด เพราะหากถูกนำไปใช้งานจริง เครื่องของภาครัฐต้องทำหน้าที่บันทึกข้อมูลจำนวนมากจากร้านบริการอินเทอร์เน็ตทั่วประเทศ

การทำงานที่เครื่องของผู้ตรวจสอบ

8. เมื่อมีความต้องการในการตรวจสอบจากทางภาครัฐ เจ้าหน้าที่ที่ทำหน้าที่เก็บหลักฐานสามารถขอรหัสรับจากภาครัฐ และนำไปตรวจสอบความถูกต้องที่ร้านบริการอินเทอร์เน็ต โดยมีขั้นขั้นตอนในการตรวจสอบความถูกต้องมีดังนี้ โปรแกรม Log Versifier ได้รับกุญแจลับ B แล้ว โปรแกรมจะเข้าไปทำการถอดรหัสหากุญแจลับ A ที่เหมาะสมจากเครื่องแม่ข่ายภายในร้านบริการอินเทอร์เน็ตเพื่อถอดรหัสปูมข้อมูลจราจรอีกทอดหนึ่ง โปรแกรมสามารถระบุได้ว่าปูมข้อมูลจราจรทางคอมพิวเตอร์ถูกแก้ไขหรือไม่โดยการทดลองถอดรหัสปูมข้อมูล หากสามารถถอดรหัสได้โดยกุญแจลับ A ที่ถูกเข้ารหัสไว้ก่อนหน้าก็สามารถสรุปได้ว่าปูมข้อมูลนั้นไม่มีการแก้ไขเกิดขึ้น

ในบทนี้ได้กล่าวถึงรายละเอียดในการออกแบบระบบปูมข้อมูลจราจรที่มั่นคงในร้านบริการอินเทอร์เน็ต รวมถึงการทำงานของระบบที่เครื่องลูกข่าย เครื่องแม่ข่ายภานในร้าน และเครื่องของทางภาครัฐโดยละเอียด ส่วนในบทถัดไปจะกล่าวถึงการทดลอง และสภาพแวดล้อมในการทดลอง

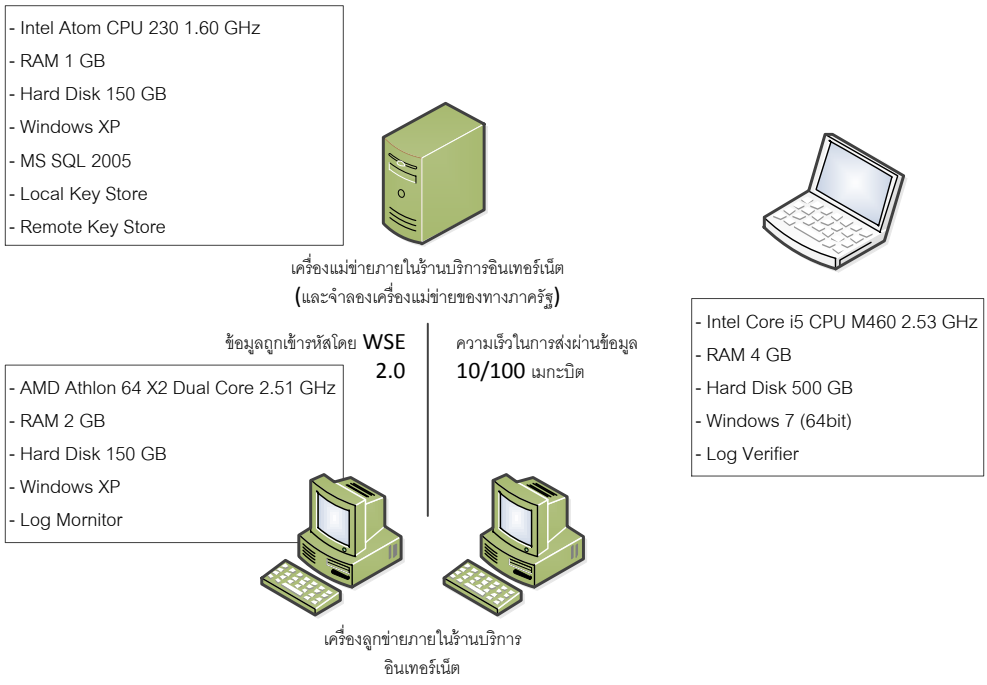
บทที่ 4
การทดลอง

หลังจากการออกแบบและพัฒนาระบบปูมข้อมูลจราจรที่มั่นคงถูกทดลองในร้านบริการอินเทอร์เน็ตที่มีผู้ใช้บริการตลอด 24 ชั่วโมงภายใต้ข้อสันนิษฐานว่าไม่ความพยายามในการบุกรุกระบบจากผู้ใช้บริการ การทดลองมีจุดประสงค์เพื่อพิสูจน์ผลกระทบจากการติดตั้งระบบปูมข้อมูลจราจรที่มั่นคงในเครื่องคอมพิวเตอร์ที่มีการใช้งานปกติจากผู้ใช้บริการ

4.1 สภาพแวดล้อมในการทดลอง

ดังที่กล่าวไปแล้วข้างต้นว่าร้านบริการอินเทอร์เน็ตที่ใช้ในการทดลองควรมีขนาดไม่ต่ำกว่า 10 - 14 เครื่อง และร้านบริการอินเทอร์เน็ตที่เราใช้ในการทดลองนั้นมีขนาด 38 ที่นั่ง แต่สามารถทำการทดลองได้จากเครื่องคอมพิวเตอร์จำนวนเพียง 2 เครื่องเท่านั้นเพราะมีความกังวลจากเจ้าของกิจการว่าอาจจะก่อให้เกิดผลกระทบต่อการดำเนินธุรกิจของร้านบริการอินเทอร์เน็ตดังกล่าวในแง่ความปลอดภัย เนื่องจากทางร้านจำเป็นที่ต้องปิดโปรแกรมป้องกันการเปลี่ยนแปลงข้อมูลบนฮาร์ดดิสก์เพื่อให้โปรแกรมสามารถบันทึกปูมข้อมูลจราจรลงบนฮาร์ดดิสก์ได้

เครื่องคอมพิวเตอร์ที่ใช้ในการทดลองมีทั้งหมด 3 เครื่องดังรูปที่ 7 โดยจัดให้เครื่องแม่ข่ายภายในร้านและเครื่องแม่ข่ายของทางภาครัฐทำงานอยู่บนเครื่องคอมพิวเตอร์เดียวกัน เพราะไม่มีความจำเป็นต้องทดสอบความสามารถในการส่งผ่านข้อมูลระหว่างกัน เนื่องจากการที่มีเครื่องแม่ข่ายภายในร้านเพียงเครื่องเดียว โดยเครื่องคอมพิวเตอร์ทั้งหมดมีความสามารถตามตารางที่ 8



รูปที่ 7 เครื่องคอมพิวเตอร์ในการทดลอง

ตารางที่ 8 รายละเอียดและข้อจำกัดของเครื่องคอมพิวเตอร์

คอมพิวเตอร์	**โปรแกรมที่ถูกติดตั้ง**	**รายละเอียด และข้อจำกัด**
เครื่องที่ลูกข่าย จำนวน 2 เครื่อง	Log Monitor	- ติดตั้งระบบปฏิบัติการวินโดวส์เอ็กพี - หน่วยประมวลผล AMD Athlon 64 X2 Dual Core Processor 4800+ ความเร็ว 2.51 กิกะเฮิรตซ์ - แรมขนาด 2 กิกะไบต์ - ฮาร์ดดิสก์ความจุ 150 กิกะไบต์ - ความเร็วในการรับส่งข้อมูลในเครือข่าย10/100 เมกะบิตต่อวินาที
เครื่องแม่ข่ายภายในร้านและเครื่องแม่ข่ายของทางภาครัฐ จำนวน 1 เครื่อง	Local Key Store และ Remote Key Store	- ติดตั้งระบบปฏิบัติการวินโดวส์เอ็กพี - ติดตั้งระบบจัดการฐานข้อมูลไมโครซอฟต์เอสคิวแอล 2005 - หน่วยประมวลผล Intel Atom CPU 230 ความเร็ว 1.60 กิกะเฮิรตซ์ - แรมขนาด 1 กิกะไบต์ - ฮาร์ดดิสก์ความจุ 150 กิกะไบต์ - ความเร็วในการรับส่งข้อมูลในเครือข่าย10/100 เมกะบิตต่อวินาที
เครื่องสำหรับผู้ตรวจสอบ จำนวน 1เครื่อง	Log Verifier	- ติดตั้งระบบปฏิบัติการวินโดวส์เซเว่น (64 บิต) - หน่วยประมวลผล Intel Core i5 CPU M460 ความเร็ว 2.53 กิกะเฮิรตซ์ - แรมขนาด 4 กิกะไบต์ - ฮาร์ดดิสก์ความจุ 500 กิกะไบต์ - ความเร็วในการรับส่งข้อมูลในเครือข่าย10/100/1000 เมกะบิตต่อวินาที

หลังจากทำการติดตั้งโปรแกรมตามตารางที่ 8 แล้ว โปรแกรม Windows Performance Logs and Alerts ได้รับการตั้งค่าให้เก็บข้อมูลการทำงานของคอมพิวเตอร์ สาเหตที่ใช้โปรแกรมนี้เก็บข้อมูลการทำงานของระบบนั้นเพื่อเป็นการรบกวนสภาพแวดล้อมเดิมของเครื่องลูกข่ายให้น้อยที่สุด และเนื่องจากจุดประสงค์หลักในการทดลองคือความสามารถในการให้บริการหลังจากติดตั้งโปรแกรม โดยมีการเก็บข้อมูลต่างๆ ดังนี้ การทำงานของหน่วยประมวลผล การทำงานของฮาร์ดดิสก์ การทำงานของหน่วยความจำ และการทำงานของอุปกรณ์เชื่อมต่อในเครือข่าย (Network Interface Card)

4.2 ระยะเวลาในการทดลอง

ระยะเวลาในการเก็บข้อมูลคือ 2 สัปดาห์ โดยในสัปดาห์แรกเป็นการเก็บข้อมูลการทำงานของเครื่องคอมพิวเตอร์ลูกข่ายทั้งสองเครื่องในขณะที่ติดตั้งโปรแกรม Log Monitor และสัปดาห์ที่สองเป็นการเก็บข้อมูลการทำงานของคอมพิวเตอร์ทั้งสองเครื่องในขณะที่ไม่มีโปรแกรม Log Monitor อยู่ ถึงอย่างไรก็ตามข้อมูลที่ถูกใช้ในการวิเคราะห์ผลนั้นเป็นข้อมูลในวันศุกร์ วันเสาร์ และวันอาทิตย์จากทั้งสองสัปดาห์ เนื่องจากว่าทั้งสามวันนี้เป็นวันที่ลูกค้าเข้าใช้บริการจนเต็มความจุของร้าน และมีผลให้เครื่องทั้งสองถูกใช้งานในระยะเวลาชั่วโมงที่ค่อนข้างใกล้เคียงกันมากกว่าในวันอื่นๆ ที่ลูกค้าสามารถเลือกใช้บริการจากเครื่องคอมพิวเตอร์เครื่องใดก็ได้ ซึ่งอาจมีผลให้เครื่องที่ใช้ในการทดลองไม่ถูกใช้งานเลยก็เป็นได้

4.3 การตั้งค่าการทำงานของโปรแกรม

โปรแกรม Log Monitor และ Local Key Store ถูกออกแบบมาให้สามารถตั้งค่าการทำงานได้ตามตารางที่ 9 เนื่องจากการตั้งค่าบางอย่างอาจมีผลต่อการทดลอง

ตารางที่ 9 การตั้งค่าในการทดลอง

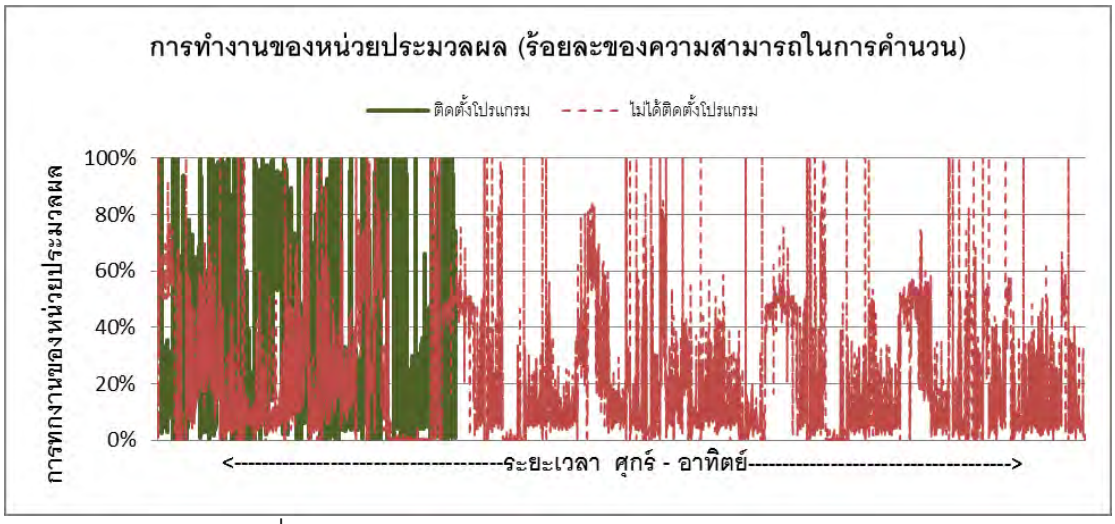
โปรแกรม	**ค่าต่าง ๆ และการตั้งค่า**	**คำอธิบาย**
Log Monitor	WriteInterval_Second = 30 วินาที	เพื่อไม่ให้เป็นการรบกวนการทำงานของฮาร์ดดิสก์ Log Monitor จะเก็บข้อมูลไว้ในหน่วยความจำเป็นระยะเวลาตามค่าที่ตั้งไว้ หลังจากครบกำหนดโปรแกรมจะทำการบันทึกข้อมูลลงฮาร์ดดิสก์
	TCPTimeOut and UDPTimeOut = 30 วินาที	เนื่องจากโปรแกรม Log Monitor ถูกออกแบบให้เก็บปูมข้อมูลจราจร ในขณะที่มีการเริ่มต้นการสื่อสารกับเครื่องปลายทาง และขณะสิ้นสุดการสื่อสาร ดังนั้น TCPTimeOut และค่า UDPTimeOut จึงใช้เพื่อระบุการสิ้นสุดการสื่อสารเมื่อไม่มีการติดต่อระหว่างกันเกินกว่าเวลาที่กำหนด
	FileSizeMB = 1 เมกะไบต์	FileSizeMB ระบุขนาดของไฟล์ที่เก็บปูมข้อมูลจราจร การตั้งค่าเท่ากับ 1 เมกะไบต์ช่วยให้ผู้วิเคราะห์สามารถทำงานได้สะดวกขึ้น เนื่องจากไฟล์ที่มีขนาดใหญ่เกินไปจะไม่สามารถเปิดใช้งานได้กับโปรแกรมแก้ไขข้อความทั่วไป เช่น โปรแกรม notepad ที่ถูกติดตั้งมาพร้อมกับระบบปฏิบัติการวินโดวส์รุ่นเก่านั้นไม่สามารถเปิดไฟล์ที่มีขนาดใหญ่เกินกว่า 45 กิโลไบต์ หรือแม้ใน ในระบบปฏิบัติการวิโดวส์เอ็กพีจะระบุว่าสามารถเปิดไฟล์ได้ถึง 32 เมกะไบต์ แต่ในทางปฏิบัติก็เริ่มมีปัญหากับไฟล์ที่มีขนาดเล็กกว่านั้นมาก เป็นต้น
Local Server	GetNewKeyFromRemoteServer_MIN = 1 ชั่วโมง	ค่านี้เป็นค่าที่ภาครัฐเป็นผู้กำหนดว่า Local Server ควรส่งรหัสลับใหม่เข้ามาเก็บเมื่อใด โดยยิ่งค่านี้มีความถี่มากเท่าไหร่จะยิ่งทำให้โอกาสที่ปูมข้อมูลจราจรที่ถูกบันทึกแล้วมีโอกาสที่จะถูกแก้ไขได้มีน้อยลงมากเท่านั้น

บทที่ 5
ผลการวิจัย

จากการทดลองระบบปูมข้อมูลจราจรที่ร้านบริการอินเทอร์เน็ตเป็นระยะเวลา 2 สัปดาห์ ข้อมูลในระหว่างวันศุกร์ ถึงวันอาทิตย์ของแต่ละสัปดาห์ถูกนำมาวิเคราะห์ผลการทดลองดังนี้

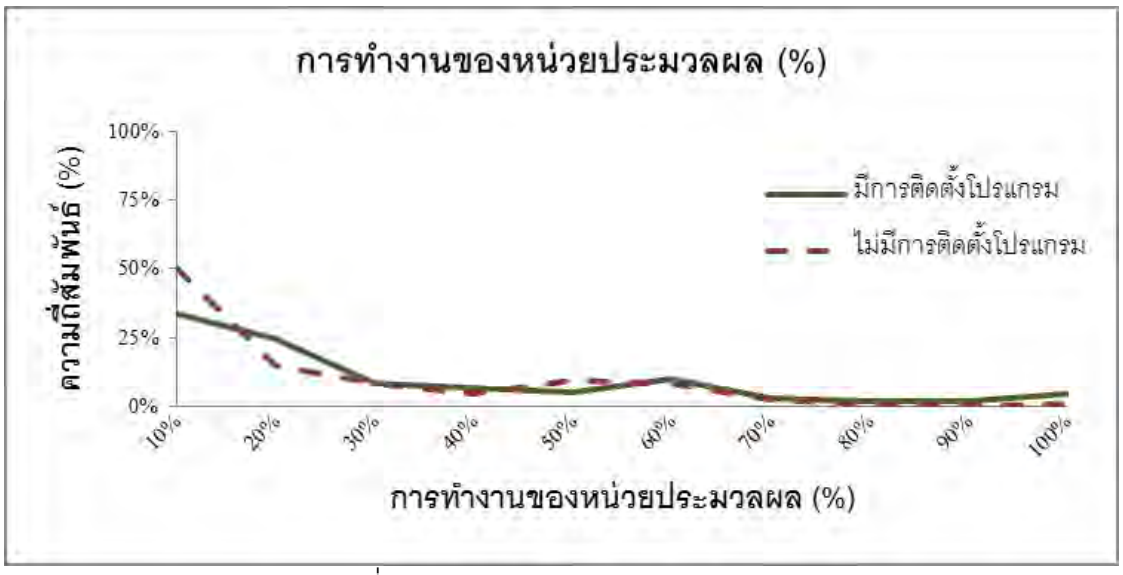
5.1 ผลการทดลอง

ข้อมูลที่เก็บได้จาก Windows Performance Logs and Alert เป็นแบบอนุกรมเวลา ซึ่งเป็นการยากที่จะเปรียบเทียบให้เห็นถึงความแตกต่างที่เกิดขึ้นจากการเก็บตัวอย่างทั้งสองอาทิตย์ ดังตัวอย่างในรูปที่ 8

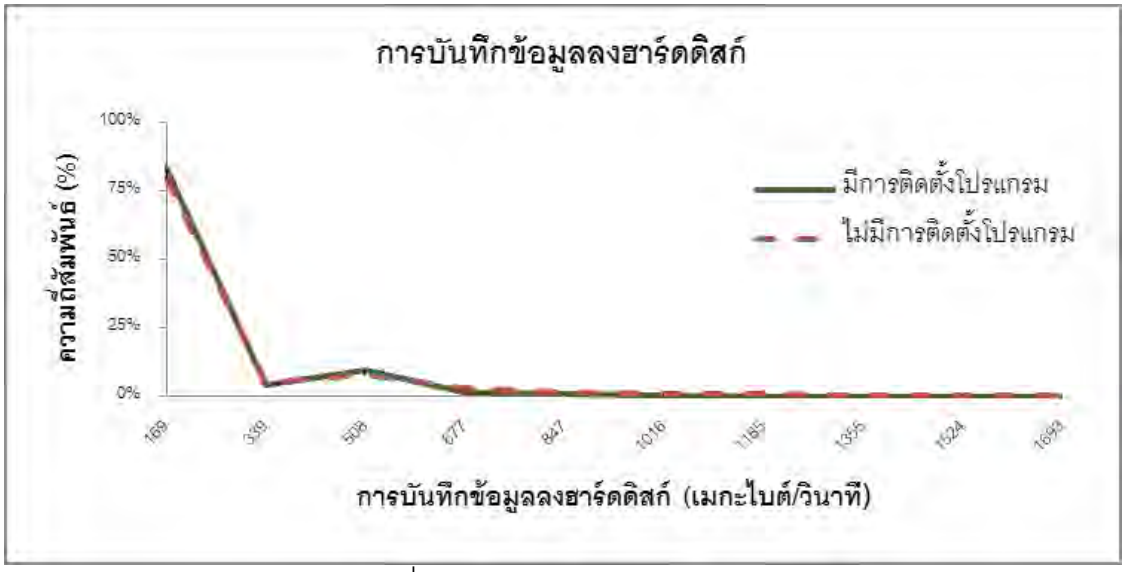


รูปที่ 8 การทำงานของหน่วยประมวลผลแบบอนุกรมเวลา

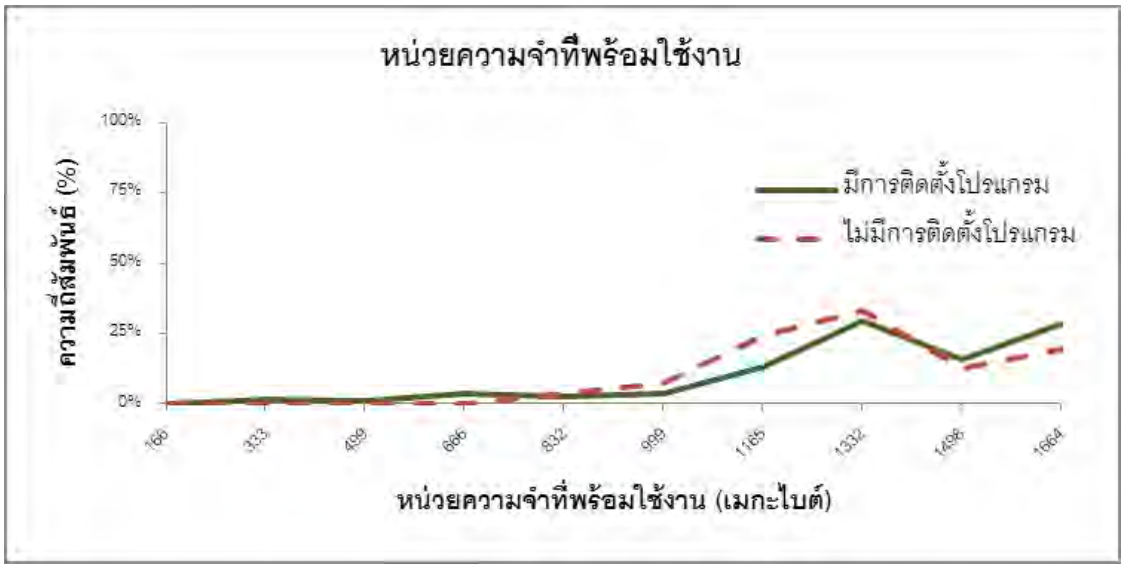
ดังนั้นข้อมูลจึงถูกแปลงให้อยู่ในรูปแบบความถี่สัมพันธ์ แต่ในบางครั้งเครื่องคอมพิวเตอร์อาจถูกเปิดทิ้งไว้เฉยๆ โดยไม่ได้ทำงาน หรืออาจมีการใช้งานโปรแกรมเช่น โปรแกรมตรวจจับไวรัส หรือการทำงานผิดพลาดของบางโปรแกรม ซึ่งเหตุการณ์เหล่านี้ใช้งานทรัพยากรของเครื่องคอมพิวเตอร์มากผิดปกติ และอาจส่งผลให้การวิเคราะห์ข้อมูลผิดพลาด ดังนั้นจึงมีการตัดข้อมูลออก ร้อยละห้าจากทั้งส่วนที่คอมพิวเตอร์ไม่มีการทำงาน และส่วนที่คอมพิวเตอร์มีการทำงานมากผิดปกติ [20] โดยรูปที่ 9 ถึงรูปที่ 12 แสดงผลการเก็บตัวอย่างจากวันที่ 28 ถึง 30 มกราคม 2554 ในขณะที่ติดตั้งโปรแกรม Log Monitor และจากวันที่ 15 ถึง 17 กุมภาพันธ์ 2554 ในขณะที่ไม่มีการติดตั้งโปรแกรมใดๆ ปูมข้อมูลจราจรที่ถูกบันทึกได้ตลอดระยะเวลา 2 สัปดาห์มีขนาด 177 เมกะไบต์



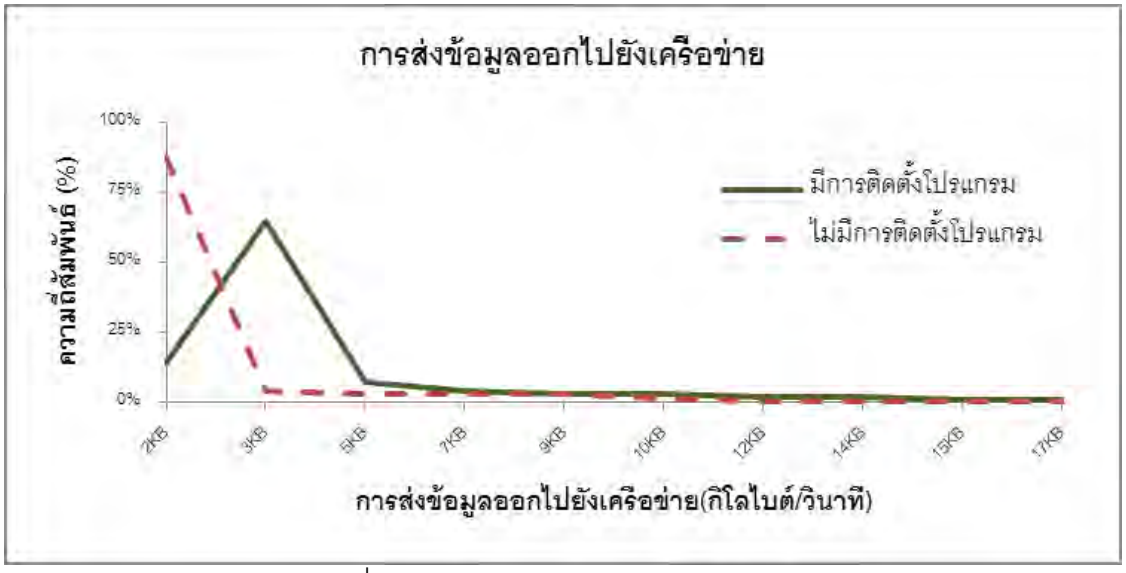
รูปที่ 9 การทำงานของหน่วยประมวลผล



รูปที่ 10 การทำงานของฮาร์ดดิสก์



รูปที่ 11 การทำงานของหน่วยความจำ



รูปที่ 12 การทำงานส่งข้อมูลผ่านเครือข่าย

5.2 ผลการวิเคราะห์

จากรูปที่ 9 จะเห็นได้ว่าขณะที่มีและไม่มี Log Monitor นั้นการทำงานของหน่วยประมวลผลแทบไม่มีความแตกต่างกัน โดยเฉพาะอย่างยิ่งในช่วงที่หน่วยประมวลผลทำงานอยู่ในระดับร้อยละ 10 ของความสามารถที่มีนั้น กราฟแสดงผลให้เห็นว่าเครื่องคอมพิวเตอร์ในขณะที่ไม่มีโปรแกรมติดตั้งอยู่ทำงานหนักกว่าในขณะที่ไม่มีโปรแกรมติดตั้ง ซึ่งจริงๆ แล้วควรออกมาใน

ทิศทางตรงกันข้าม โดยสามารถสรุปได้ว่าเมื่อติดตั้งโปรแกรมแล้วเครื่องคอมพิวเตอร์สามารถประมวลผลได้อย่างเป็นปกติ และการทำงานหนักหรือเบาของหน่วยประมวลผลนั้นน่าจะมีผลมาจากปัจจัยอื่น

กราฟในรูปที่ 10 ถึงรูปที่ 12 ล้วนแล้วแต่แสดงผลไปในทิศทางเดียวกันคือผลการเปรียบเทียบไม่สามารถบ่งบอกได้ถึงผลกระทบจากการติดตั้งโปรแกรมแต่อย่างใด ซึ่งอาจเป็นเพราะการตั้งค่าการทำงานของโปรแกรมตามตารางที่ 8 ที่อาจมากหรือน้อยเกินไปจนไม่ส่งผลให้ที่เป็นรูปธรรม ถึงแม้ในทางกลับกันก็สามารถสรุปได้เช่นกันว่าโปรแกรมสามารถทำงานได้โดยไม่ส่งกระทบต่อการทำงานของเครื่องคอมพิวเตอร์ซึ่งเป็นจุดสำคัญที่การทดลองนี้ต้องการพิสูจน์ทราบ

เพื่อให้ทราบถึงที่มาของประสิทธิภาพในการทำงาน จึงมีความจำเป็นต้องทำการทดลองเพิ่มเติม โดยการทดลองบันทึกปูมข้อมูลจราจรที่เกิดขึ้นจากการดาวน์โหลดข้อมูล 147.71 เมกะไบต์ ในกรณีที่ไม่มีประกาศจากกระทรวงเทคโนโลยีสารสนเทศเกี่ยวข้องกับการเก็บปูมข้อมูลจราจรทางคอมพิวเตอร์ ระบบปูมข้อมูลจราจรอาจต้องทำการเก็บข้อมูลเป็นจำนวนกลุ่มข้อมูล (packet) ทั้งหมด 181,705 กลุ่มข้อมูล แต่ระบบปูมข้อมูลจราจรที่นำเสนอมีการเก็บข้อมูลเพียง 2 กลุ่มข้อมูลเท่านั้น คือ กลุ่มแรกเมื่อเครื่องต้นทางและปลายทางเริ่มการติดต่อ และกลุ่มที่สองเมื่อเครื่องต้นทางและปลายทางหยุดการติดต่อนานเกินกว่าค่า TCPTimeOut ที่ระบุไว้ แต่เนื่องจากการดาวน์โหลดเป็นกิจกรรมที่มีความต่อเนื่องจึงส่งผลให้ระบบที่นำเสนอบันทึกปูมข้อมูลจราจรน้อยมากกว่าระบบทั่วไป ซึ่งหากการใช้งานเปลี่ยนแปลงรูปแบบไป เช่น เล่นเกมส์ออนไลน์ การค้นดูข้อมูลบนอินเทอร์เน็ต หรือการสื่อสารผ่านสังคมออนไลน์ อาจส่งผมให้ความแตกต่างระหว่างระบบทั่วไป และระบบที่นำเสนอมีน้อยลงเนื่องจากความหลากหลายของเครื่อปลายทางที่มากขึ้นและธรรมชาติของการใช้งานที่ไม่มีความต่อเนื่องเท่ากับการดาวน์โหลดข้อมูล

บทที่ 6
สรุปผลการวิจัยและข้อเสนอแนะ

ถึงแม้ผลการทดลองจะออกมาเป็นที่น่าพอใจ แต่หากวิเคราะห์ถึงปัญหาในการนำไปใช้งานจริงในสภาพแวดล้อมที่ไม่สามารถกำหนดการใช้งานของผู้ใช้งานได้ ระบบปูมข้อมูลจราจรก็ยังมีข้อที่ต้องขบคิดเพื่อหาทางแก้ไขต่อไปในอนาคต โดยสามารถสรุปผลการวิจัยและข้อเสนอแนะได้ดังนี้

6.1 สรุปผลการวิจัย

จากการทดลองสามารถสรุปได้ว่าโปรแกรมทั้งหมดที่ติดตั้งลงในระบบของร้านบริการอินเทอร์เน็ตสามารถทำงานได้ตลอด 24 ชั่วโมงโดยไม่มีการขัดข้อง อีกทั้งร้านบริการอินเทอร์เน็ตยังสามารถให้บริการแก่ลูกค้าในหลากหลายรูปแบบ ทั้งบริการการเข้าถึงอินเทอร์เน็ต พิมพ์เอกสาร รวมไปถึงบริการเกมส์ทั้งออนไลน์และออฟไลน์ได้โดยไม่มีปัญหารบกวนแต่อย่างใด โดยเฉพาะในส่วนบริการเกมส์ ซึ่งเป็นส่วนที่มีความจำเป็นที่ต้องใช้ความสามารถในการประมวลผลค่อนข้างมาก ก็ยังไม่ได้รับผลกระทบจากโปรแกรมที่ติดตั้งลงไปแม้แต่น้อย

หน่วยความจำที่สามารถใช้งานได้ การบันทึกข้อมูลลงฮาร์ดดิสก์ หรือการส่งข้อมูลบนเครือข่ายซึ่งอาจถูกรบกวนจากโปรแกรมที่ติดตั้งลงไป ยังสามารถใช้งานได้ตามปกติ และตามที่ได้กล่าวไปแล้วว่าผลลัพธ์ที่ดีนี้อาจเกิดจากการตั้งค่าต่างๆ ของโปรแกรมที่อาจมากหรือน้อยจนเกินไป แต่ถึงอย่างไรก็ตามผลการทดลองได้พิสูจน์ออกมาให้เห็นแล้วว่าโปรแกรมที่ติดตั้งลงไปนั้นไม่ก่อให้เกิดการรบกวนต่อระบบใดๆ ภายในร้านบริการอินเทอร์เน็ต

ทั้งนี้จากการสัมภาษณ์เจ้าของกิจการและพนักงานดูแลร้าน พบว่าการติดตั้งโปรแกรมเป็นไปด้วยความราบรื่น? และไม่ได้รับการร้องเรียนจากลูกค้าที่ใช้งานเครื่องที่ทำการทดลองแต่อย่างใด อีกทั้งลูกค้าที่นั่งใช้งานเครื่องคอมพิวเตอร์ทั้งสองเครื่องอยู่เป็นประจำก็ยังคงใช้งานอยู่ ณ ตำแหน่งเดิม

ในส่วนของปูมข้อมูลจราจรที่ใช้เนื้อที่ประมาณ 117 เมกะไบต์จากการเก็บตัวอย่างเป็นเวลา 2 สัปดาห์ ซึ่งหากนำไปใช้งานจริงทางร้านต้องเก็บข้อมูลเป็นระยะเวลา 90 วันตามกฎหมาย ซึ่งทางร้านต้องเตรียมที่เก็บข้อมูลที่มีขนาดไม่ต่ำกว่า 600 กิกะไบต์

เสียงตอบรับจากทางร้านในประเด็นนี้ออกมาในเชิงบวก โดยเจ้าของกิจการให้เหตุผลว่าราคาฮาร์ดดิสก์ในปัจจุบันนั้นถูกมาก โดยทางร้านเองสามารถซื้อฮาร์ดดิสก์ขนาด 1 เทระไบต์ได้ 2 ถึง 3 ลูกโดยไม่มีปัญหาอะไร ซึ่งน่าจะเพียงพอต่อความต้องการของระบบในจุดนี้

6.2 ข้อเสนอแนะ

ถึงแม้การทดลองแสดงผลลัพธ์ในทิศทางที่ดี อย่างไรก็ตามระบบปูมข้อมูลจราจรที่มั่นคงยังมีความต้องการในการพัฒนาในอีกหลายแง่มุมดังนี้

1. ข้อควรปรับปรุงที่ได้รับการเสนอแนะจากทางเจ้าของกิจการคือ โปรแกรมควรสามารถทำงานกับโปรแกรมควบคุมการทำงาน (NCafé) ที่ทางทางร้านใช้งานอยู่ในขณะนี้ได้ ซึ่งโปรแกรมดังกล่าวจะลบการเปลี่ยนแปลงใดๆ ที่เกิดขึ้นบนฮาร์ดดิสก์ทุกครั้งที่เครื่องเปิดขึ้นมาใหม่ ส่งผลให้ต้องมีการปรับปรุงให้ไฟล์ที่มีปูมข้อมูลจราจรต้องถูกส่งไปเก็บยังเครื่องแม่ข่ายภายในร้านก่อนที่จะปิดเครื่องทุกครั้ง
2. การป้องกันการโจมตีแบบ Denial of Service (DoS) ที่สามารถก่อกวนการทำงานของของแม่ข่ายของทางภาครัฐ และเครื่องแม่ข่ายของร้านบริการอินเทอร์เน็ตให้ไม่สามารถรับกุญแจลับเพื่อมาเก็บบันทึกได้ ซึ่งอาจแก้ไขได้โดยการเพิ่มเครื่องคอมพิวเตอร์แม่ข่ายในการจัดเก็บกุญแจรับ หรือติดไฟร์วอลล์เพื่อป้องกันการโจมตีดังกล่าว
3. แฮชฟังก์ชันที่นำมาใช้ในการทดลองไรอนาคตควรถูกแทนที่ด้วย SHA-256 หรือ SHA-512 ซึ่งได้รับการยอมรับในปัจุบัน เนื่องจาก SHA-1 แฮชฟังชั่นในการทดลองนี้กำลังจะไม่เป็นที่ยอมรับในการใช้งาน [21]
4. นอกเหนือจากการส่งกุญแจลับไปเก็บยังเครื่องคอมพิวเตอร์ที่มีความปลอดภัยสูงแล้ว ควรมีการส่งข้อมูลอื่นร่วมด้วยเช่น ค่าจากแฮชฟังก์ชันไฟล์ที่สิ้นสุดการบันทึกปูมข้อมูลจราจรทางคอมพิวเตอร์ เพื่อการยืนยันในภายหลังว่าไฟล์นั้นไม่ได้ถูกแก้ไข ถึงแม้กุญแจลับจะถูกขโมยไปเพื่อสร้างปูมข้อมูลจราจรเท็จขึ้นมาแทนที่ของเดิม
5. มีความเป็นไปได้ที่เครื่องลูกข่ายไม่ส่ง หรือไม่บันทึกปูมข้อมูลจราจรไปยังเครื่องแม่ข่าย ซึ่งในงานวิจัยในอนาคตควรเปลี่ยนแปลงกระบวนการในการดักจับการใช้งานอินเทอร์เน็ตและบันทึกปูมข้อมูลจราจรจากเครื่องลูกข่ายไปที่เครื่องแม่ข่ายแทน เพื่อเพิ่มความมั่นคงให้แก่ระบบ
6. ควรเพิ่มจำนวนร้านบริการอินเทอร์เน็ตในการทดลอง และแยกเครื่องแม่ข่ายของร้านบริการอินเทอร์เน็ตออกจากเครื่องแม่ขายของทางภาครัฐ รวมถึงการจัดวางเครื่องแม่ขายของทางภาครัฐภายนอกเครือข่ายของร้านบริการอินเทอร์เน็ต เพื่อเพิ่มความน่าเชื่อถือให้แก่ผลการทดลอง
7. ในระหว่างที่โปรแกรม Log Monitor รอเพื่อเข้ารหัสเหตุการณ์ ระยะเวลาในการรอนี้ก่อให้เกิดช่องโหว่ เนื่องจากกุญแจลับที่ใช้กับเหตการณ์ก่อนหน้าถูกเก็บอยู่ในหน่วยความจำและอาจถูกขโมยไปเพื่อการปลอมแปลงปูมข้อมูลจราจรถึงแม้ว่าจะมีการ

แฮชกุญแจลับดังกล่าวแล้วก็ตาม ดังนั้นระบบควรที่จะร่นระยะเวลาในการรอให้สั้นที่สุดเท่าที่จะเป็นไปได้

ในการทดลองไฟล์ขนาด 1 เมกะไบต์สามารถบันทึกปูมข้อมูลจราจรทางอินเทอร์เน็ตได้นานประมาณ 1 ชั่วโมงก่อนที่ระบบจะทำการสร้างกุญแจลับและส่งไฟล์ดังกล่าวไปเก็บอย่างปลอดภัยที่เครื่องแม่ข่ายภายในร้านบริการอินเทอร์เน็ต ดังนั้นผู้บุกรุกจึงมีระยะเวลาในการทดลองหากุญแจลับนาน 1 ชั่วโมงเช่นเดียวกัน ค่ากำหนดของขนาดไฟล์ที่ใหญ่เกินไปจึงมีส่วนทำให้ความปลอดภัยลดลง ดังนั้นจึงไม่ควรตั้งค่ากำหนดขนาดของไฟล์ให้ใหญ่จนเกินไป ในการวิจัยในอนาคตนั้นค่ากำหนดตัวนี้ควรจะเปลี่ยนเป็นระยะเวลาที่ไฟล์จะอยู่ที่เครื่องลูกข่ายแทน เพื่อให้ไฟล์ถูกส่งไปเก็บยังเครื่องแม่ข่ายที่ที่มีความปลอดภัยสูงกว่าโดยเร็วที่สุด

8. ระบบควรมีการระบุตัวตนของผู้ใช้บริการที่หลากหลาย เพื่อป้องกันการปลอมแปลงตัวบุคคลในการใช้บริการที่ร้านบริการอินเทอร์เน็ต เช่น การมีชื่อผู้ใช้และรหัสผ่านให้ผู้ใช้งานแต่ละคน ควบคู่กับบัตรสมาชิกหรือการถ่ายภาพในรูปแบบเดียวกับด่านตรวจคนเข้าเมืองของสนามบินในหลายประเทศรวมทั้งประเทศไทย

รายการอ้างอิง

[1] “พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550,” ราชกิจจานุเบกษา 124 ตอนที่ 27 ก (18 มิถุนายน 2550)

[2] “ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550,” ราชกิจจานุเบกษา 124 ตอนพิเศษ 102 ง (23 สิงหาคม 2550)

[3] Schweitzer, D. Incident Response Computer Forensics Toolkit. Canada: Wiley Publishing, Inc., 2003.

[4] National Institute of Standards and Technology. Guide to Computer Security Log Management. U.S. Department of Commerce. (September 2006): C-3 – C-6

[5] Schneier, B. and Kelsey, J. Secure audit logs to support computer forensics(ACM, 1999) Transactions on Information and System Security, Transactions on Information and System Security (TISSEC), 2, 2, 1999.

[6] Bellare, M. and Yee, B. Forward Integrity for Secure Audit Logs, Technical Report, Computer Science and Engineering Department. University of California at San Diego, 1997.

[7] Hold, J. Logcrypt: Forward Security and Public Verification for Secure Audit Logs. ACM International Conference Proceeding Series, 167 2006: 203 – 211.

[8] Waters, B., Balfanz D., Durfee, Glenn., and Smetters D. Building an Encrypted and Searchable. In The 11th Annual Network and Distributed System Security Symposium, 2004.

[9] หนังสือพิมพ์ฐานเศรษฐกิจ. ธุรกิจร้านอินเทอร์เน็ต...ขวัญใจวัยรุ่น [ออนไลน์]. 2552. แหล่งที่มา: http://www.thannews.th.com/detialnews.php?id=M2624031&issue=2403 [2552 มีนาคม].

[10] Sivathanu, G., Wright, C., and Zadok, E. Ensuring data integrity in storage: techniques and applications. Stony Brook University, Tech. Rep. FSL-04-04, 2004.

[11] Mitchell, C., Rush, D., and Walker, M. A Remark on Hash Functions for Message Authentication. ACM Computers and Security, 8, (February 1989).

[12] สัมภาษณ์ ธนัท บุญวิสิฐกุล, เจ้าของกิจการร้านอินเทอร์เน็ต, 1 กุมภาพันธ์ 2553.

[13] Vidstrom, A. The Toolbox[Online]. 2011. Available from: http://ntsecurity.nu/toolbox[2009, May]

[14] Lauritsen, J. Elsave[Online]. 2011. Available from: http://www.ibt.ku.dk/jesper/elsave[1999, July]

[15] Technical Working Group for Electronic Crime Scene Investigation. Electronic Crime Scene Investigation: A Guide for First Responders. U.S. Department of Justice. (2001): 2.

[16] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 2nd ed. Great Britain: Academic Press, 2004.

[17] ACM Digital Library. Secure audit logs to support computer forensics[Online]. 2011. Available from: http://portal.acm.org/citation.cfm?id=317089[2011, April]

[18] C. Lonvick. The BSD syslog Protocol[Online]. 2011. Available from: http://www.ietf.org/rfc/rfc3164.txt[2001 August]

[19] Goyal, P. How to Re-initialize a Hash Chain. IACR Eprint archive, 2004.

[20] Field, A. Discovering Statistics Using SPSS. 3rd Edition. SAGE Publications, London, 2009.

[21] National Institute of Standards and Technology. Secure Hashing[Online]. 2011. Available from: http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html[2011, April]

ประวัติผู้เขียนวิทยานิพนธ์

นายพีชพล พลพงษ์ เกิดวันที่ 20 กุมภาพันธุ์ พ.ศ. 2525 กรุงเทพมหานคร สำเร็จการศึกษาระดับปริญญาวิทยาศาสตร์บัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ จากมหาวิทยาลัยเว็บสเตอร์ประเทศออสเตรีย ในปีการศึกษา 2547 หลังจากนั้นได้เข้ามาศึกษาต่อในหลักสูตรวิทยาศาสตร์มหาบัณฑิต สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2550