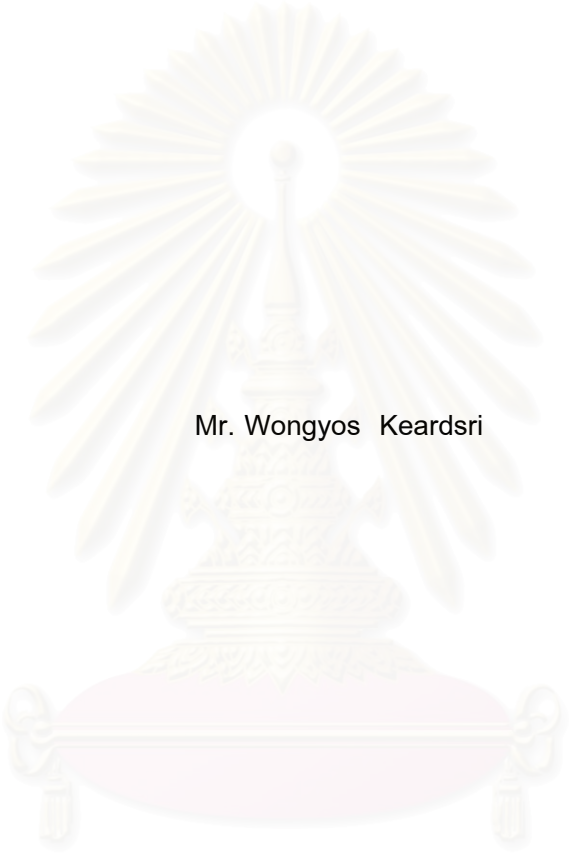
แบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว

นายวงศ์ยศ เกิดศรี

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2551

AN IP ADDRESS ANONYMIZATION SCHEME BASED ON PRIVACY LEVELS

Mr. Wongyos Keardsri



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 2008

หัวข้อวิทยานิพนธ์	แบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว
โดย	นายวงศ์ยศ เกิดศรี
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	อาจารย์ ดร.ยรรยง เต็งอำนวย
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	ดร.ภาสกร ประถมบุตร

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

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

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(อาจารย์ จารุมาดร ปิ่นทอง)

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

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม
(ดร.ภาสกร ประถมบุตร)

..... กรรมการภายนอกมหาวิทยาลัย
(ดร.โกเมน พิบูลย์โรจน์)

วงศ์ยศ เกิดศรี : แบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว. (AN IP ADDRESS ANONYMIZATION SCHEME BASED ON PRIVACY LEVELS) อ.ที่ปรึกษาวิทยานิพนธ์หลัก : อ.ดร.ยรรยง เต็งอำนวย, อ.ที่ปรึกษาวิทยานิพนธ์ร่วม : ดร.ภาสกร ประถมบุตร, 116 หน้า.

ปัจจุบันการปิดบังหมายเลขไอพีเป็นวิธีการหนึ่งที่สำคัญสำหรับการวิเคราะห์เครือข่ายและการวิจัยเครือข่าย โดยขั้นตอนการปิดบังของหมายเลขไอพีคือการเปลี่ยนรูปหมายเลขไอพีดั้งเดิมให้เป็นหมายเลขไอพีนิรนาม ทั้งนี้เพื่อต้องการรักษาความลับของข้อมูลส่วนบุคคลของผู้ใช้ในเครือข่ายไม่ให้ถูกล่วงละเมิดความเป็นส่วนตัวได้ กระบวนการปิดบังหมายเลขไอพีที่มีชื่อเสียงได้แก่ ทีซีพีดีไพรว์ คริปโตแพน การเข้าถึงแบบหลายชั้น และทีเอสเอ แต่กระบวนการเหล่านี้ยังใช้งานได้ไม่เหมาะสมกับหน้าที่งานของการวิเคราะห์เครือข่ายที่แท้จริง และปิดบังทั้ง 32 บิตของหมายเลขไอพีอย่างไม่จำเป็น ในความเป็นจริงแล้วสามารถปิดบังเพียงบางบิตหรือบางส่วนที่จำเป็นของหมายเลขไอพีได้ตามความเหมาะสมและตามระดับความเป็นส่วนตัวที่แตกต่างกันได้ งานวิจัยเรื่องนี้จึงได้นำเสนอระดับความเป็นส่วนตัว 5 ระดับเพื่อใช้ในกระบวนการปิดบังหมายเลขไอพีอันได้แก่ ระดับที่ไม่มีการปิดบัง ระดับการปิดบังส่วน n บิตซ้าย ระดับการปิดบังส่วน n บิตขวา ระดับการปิดบังทั้ง 32 บิต และระดับการปิดบังทั้ง 32 บิตแบบสุ่ม งานวิจัยได้ประยุกต์ใช้ระดับความเป็นส่วนตัวเหล่านี้กับวิธีการปิดบังที่คงไว้ซึ่งกลุ่มเครือข่ายโดยเลือกใช้วิธีคริปโตแพน นอกจากนี้งานวิจัยเรื่องนี้ยังได้นำเสนอปัจจัยการปิดบัง 3 ปัจจัยเพื่อใช้สำหรับพิจารณาเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุดในการปิดบังหมายเลขไอพี ได้แก่ โครงสร้างต้นไม้ของความเป็นส่วนตัว รายการวิเคราะห์เครือข่าย และกฎหมายคอมพิวเตอร์ ซึ่งปัจจัยการปิดบังทั้ง 3 ปัจจัยถูกผนวกเข้าด้วยกันโดยใช้วิธีการแบบกฎ หลักการทั้งหมดนี้ได้มาซึ่งแบบแผนการปิดบังหมายเลขไอพีใหม่บนพื้นฐานของระดับความเป็นส่วนตัว ซึ่งเหมาะสำหรับการใช้งานตามหน้าที่การวิเคราะห์เครือข่ายต่างๆ อย่างเหมาะสม และเป็นประโยชน์สำหรับองค์กรใดองค์กรหนึ่งที่ต้องการแลกเปลี่ยนข้อมูลระหว่างกัน ทั้งยังเหมาะสำหรับการสูบจับแพ็คเก็ตขนาดมหาศาล

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก .....

ปีการศึกษา 2551 ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์ร่วม .....

4970541621 : MAJOR COMPUTER SCIENCE
KEYWORDS : IP ADDRESS ANONYMIZATION / PRIVACY / PRIVACY LEVELS / NETWORK ANALYSIS / PACKET SNIFFER

WONGYOS KEARDSRI : AN IP ADDRESS ANONYMIZATION SCHEME BASED ON PRIVACY LEVELS. ADVISOR : YUNYONG TENG-AMNUAY, Ph.D., CO-ADVISOR : PASSAKON PRATHOMBUTR, Ph.D., 116 pp.

Nowadays, an IP address anonymization is an important technique for network analysis and Internet research. The method of anonymization is the changing of original IP address to anonymized IP address to keep the private information of users in network and to prevent suitable a disclosure and violation of user privacy. The well-known anonymization techniques are TCPdpriv, Crypto-PAn, Multiple Access Level, and TSA; however, they are unsuitable for network analysis functions. The current techniques anonymize all 32 bits of IP address unnecessarily. In fact, we can anonymize the necessary bits or parts of IP address for different privacy levels. In this research, we propose 5 privacy levels for anonymization scheme as follows; non-anonymization, n-left anonymization, n-right anonymization, full anonymization, and randomly full anonymization. We apply these privacy levels to prefix-preserving IP address anonymization, the technique which can preserve network relationship among the same network group from original IP addresses, specifically to Crypto-PAn. Moreover, we present 3 anonymization factors used in considering and selecting appropriate privacy level. The 3 anonymization factors are as follows; privacy tree structures, network analysis functions, and computer law. We combine these factors by using rule-based method. Our anonymization scheme is applicable to an administrator who analyzes packet data in different functions. The scheme benefits any organizations in exchanging network data, and also appropriates for heavy-duty packet tracers and sniffers.

Department : Computer Engineering Student's Signature : W. Keardsri
Field of Study : Computer Science Advisor's Signature : Yunyong
Academic Year : 2008 Co-Advisor's Signature : Passakon

กิตติกรรมประกาศ

เป็นระยะเวลา 3 ปีเต็มที่ผู้วิจัยได้เพียรพยายาม ศึกษาค้นคว้า และทำวิจัยอย่างมุ่งมั่นจนวิทยานิพนธ์เรื่องนี้สำเร็จลุล่วงไปด้วยดี ซึ่งมีผู้ที่มีพระคุณและบุคคลมากมายที่คอยช่วยเหลือ คอยเป็นกำลังใจ และมอบสิ่งที่ดีเสมอมา ผู้วิจัยขอขอบพระคุณดังต่อไปนี้

บุคคลสองท่านแรกที่ผู้วิจัยขอขอบพระคุณเป็นอย่างยิ่งคือ อาจารย์ ดร.ยรรยง เต็งอำนวย อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก ซึ่งท่านคอยให้คำปรึกษา ให้ความช่วยเหลือ และแนะนำสิ่งที่เป็นประโยชน์ต่อการทำวิทยานิพนธ์เสมอมา ทั้งยังถ่ายทอดประสบการณ์การทำวิจัยที่ท่านมีมายาวนานได้อย่างเชี่ยวชาญยิ่ง อีกท่านหนึ่งคือ ดร.ภาสกร ประถมบุตร อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม ซึ่งท่านคอยเติมเต็มความรู้ และคอยติดตามความก้าวหน้าในการทำวิทยานิพนธ์อยู่ตลอดเวลา ทั้งยังอำนวยความสะดวกในการให้คำปรึกษาและการทำวิจัย ณ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC)

ลำดับต่อมาผู้วิจัยขอขอบพระคุณ อาจารย์ จารุมาตร ปิ่นทอง ประธานสอบวิทยานิพนธ์ และ ดร.โกเมน พิบูลย์โรจน์ กรรมการสอบวิทยานิพนธ์ ที่ได้กรุณาให้คำแนะนำและชี้แนะแนวทางที่เป็นประโยชน์ต่อการทำวิทยานิพนธ์ในครั้งนี้

ลำดับต่อมาผู้วิจัยขอขอบพระคุณทุนสถาบันบัณฑิตวิทยาศาสตร์และเทคโนโลยีไทย (Thailand Graduate Institute of Science and Technology : TGIST) ภายใต้การดูแลของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) เลขที่ทุน TGIST 01-50-076 เลขที่ผู้รับทุน TG-44-09-50-076M ที่ได้ให้เงินสนับสนุนการทำวิทยานิพนธ์ในทุกๆ ส่วน ทั้งค่าเล่าเรียน ค่าใช้จ่ายประจำเดือน ค่าทำวิจัย และค่าการนำเสนอผลงานวิจัย ทำให้ผู้วิจัยมีพลังในการสร้างสรรค์ผลงานเพื่อให้ได้มาซึ่งวิทยานิพนธ์ที่สมบูรณ์ที่สุด

นอกจากนี้ผู้วิจัยขอขอบพระคุณบุคคลต่างๆ ดังต่อไปนี้ อาจารย์ ดร.ลัดดา ปรีชาวีรกุล จากมหาวิทยาลัยสงขลานครินทร์ ที่คอยให้คำปรึกษาและให้ความห่วงใยเสมอมา ดร.วสันต์ ภัทรอธิคม จาก สวทช. ในการช่วยเหลือเรื่องการสมัครทุนวิจัย คณาจารย์ภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย ที่ประสิทธิ์ประสาทความรู้อันมีค่ายิ่ง สมาชิกห้องปฏิบัติการวิศวกรรมระบบสารสนเทศ (ISEL) ที่สร้างความสนุกสนานในการทำงาน และเพื่อนร่วมรุ่นสาขาวิทยาศาสตร์คอมพิวเตอร์ (CS36) ที่คอยห่วงใยซึ่งกันและกันเสมอมา

สุดท้ายนี้ผู้วิจัยขอขอบพระคุณสมาชิกในครอบครัวทุกคนได้แก่ คุณพ่อ คุณแม่ คุณป้า และน้องชายทั้งสองคน ที่ได้ให้ความรัก กำลังใจ และสร้างแรงบันดาลใจให้เกิดพลังความมุ่งมั่นต่อการทำวิทยานิพนธ์ และในวันข้างหน้าผู้วิจัยหวังเป็นอย่างยิ่งว่าจะได้นำเอาความรู้และประสบการณ์ที่ได้รับมาทั้งหมดนี้กลับไปพัฒนาบ้านเกิดอย่างภาคภูมิใจในสักวันหนึ่ง

สารบัญ

หน้า

หน้า

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันการวิเคราะห์และจัดการเครือข่ายมีความจำเป็นอย่างยิ่งในการดูแลและควบคุมระบบเครือข่ายให้สามารถทำงานได้อย่างปกติ มีความถูกต้อง และมีประสิทธิภาพ ซึ่งการวิเคราะห์และจัดการเครือข่ายนั้น จำเป็นต้องใช้ข้อมูลที่ได้จากการตรวจตราการจราจรในเครือข่าย (Network Traffic Tracers) และการสูบจับแพ็คเก็ต (Packets Sniffers) ที่ประกอบไปด้วยข้อมูลรับเข้าและส่งออกมากมายหลายประเภท ข้อมูลจำพวกหนึ่งที่ปรากฏอยู่เสมอเมื่อมีการตรวจตราและสูบจับแพ็คเก็ตก็คือ หมายเลขไอพี (IP Address) ซึ่งหมายเลขไอพีนี้ปรากฏอยู่ภายในเฮดเดอร์ (Header) ของแพ็คเก็ตทุกแพ็คเก็ตในระดับชั้นเครือข่าย (Network Layers) ของโครงสร้างระบบเครือข่าย โดยจะประกอบไปด้วยส่วนของหมายเลขไอพีต้นทาง (Source IP Address) และหมายเลขไอพีปลายทาง (Destination IP Address) ซึ่งหมายเลขไอพีเหล่านี้เป็นหมายเลขไอพีดั้งเดิม (Original IP Address) หรือหมายเลขไอพีจริง (Real IP Address) ที่มาจากอุปกรณ์ในเครือข่าย ซึ่งสามารถระบุถึงตัวบุคคล อุปกรณ์ปลายทาง และองค์กรที่ใช้งานในระบบเครือข่ายได้ หมายเลขไอพีจะถูกกำหนดให้กับอุปกรณ์ปลายทางในเครือข่ายและจะคงอยู่กับอุปกรณ์เครื่องนั้นเรื่อยไปตราบใดที่ยังไม่ได้เปลี่ยนแปลงหมายเลขไอพีให้เป็นหมายเลขอื่น

อย่างไรก็ตามจะเห็นได้ว่าข้อมูลที่ได้จากการตรวจตราและสูบจับแพ็คเก็ตเหล่านั้นเป็นข้อมูลที่ไม่ได้มีการปิดบังหมายเลขไอพีแม้แต่อย่างใด เมื่อมีการแสดงข้อมูลและผลลัพธ์ที่ได้จากการวิเคราะห์และจัดการเครือข่ายจะทำให้มองเห็นและทราบได้ว่าหมายเลขไอพีหมายเลขต่างๆ เป็นของบุคคลใดบ้าง ซึ่งในทางปฏิบัติแล้วผู้ที่ทำการวิเคราะห์และจัดการเครือข่ายไม่ควรล่วงรู้ข้อมูลที่มีความเป็นส่วนตัว (Privacy) แบบนั้นได้ แต่เพียงมีหน้าที่ในการตรวจสอบข้อมูลของระบบเครือข่ายว่ามีปัญหาในส่วนใดบ้างเท่านั้น ดังตัวอย่างเช่น ผู้ดูแลระบบเครือข่ายต้องการตรวจสอบสถิติการใช้บริการเว็บไซต์บนโปรโตคอลเอชทีทีพี (HTTP) ของสมาชิกในเครือข่าย ซึ่งกระบวนการวิเคราะห์สถิติดังกล่าวอาจทำให้สามารถมองเห็นและทราบถึงรายละเอียดในการเข้าใช้งานเว็บไซต์ต่างๆ ของสมาชิกเป็นรายบุคคลได้ ซึ่งไม่ถูกต้องตามแนวทางที่ควรปฏิบัติ ผู้ดูแลระบบเครือข่ายไม่ควรล่วงรู้และละเมิดความเป็นส่วนตัวของสมาชิกเหล่านั้นได้ หรือในกรณีที่หน่วยงานผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider) หรือไอเอสพี (ISP) ต้องการนำข้อมูลของลูกค้าและผู้ใช้บริการไปตรวจสอบค่าทางสถิติ ก็จำเป็นต้องปิดบังหมายเลขไอพีก่อนทำการวิเคราะห์ ยกตัวอย่างเช่น หน่วยงานยูนิเน็ต (Uninet) ต้องการจะตรวจสอบค่าทางสถิติของเครือข่ายจุฬาลงกรณ์มหาวิทยาลัย หน่วยงานยูนิเน็ตจะต้องทำการ

ปิดบังหมายเลขไอพีก่อนเริ่มกระบวนการวิเคราะห์ผล ทั้งนี้เพื่อไม่ให้ก้าวก่ายความเป็นส่วนตัวของสมาชิกในเครือข่าย

จากเหตุผลและตัวอย่างที่ได้กล่าวมานั้น ข้อมูลส่วนบุคคลที่เป็นหมายเลขไอพีนี้จึงต้องถูกปิดบังเอาไว้เพื่อให้เกิดความเป็นส่วนตัวแก่สมาชิกที่ใช้งานอยู่ในระบบเครือข่าย โดยวิธีการปิดบังหมายเลขไอพี (IP Address Anonymization) จะเป็นวิธีการที่ปกปิดความเป็นส่วนตัวของผู้ใช้และอุปกรณ์ที่เปิดใช้งานอยู่ในระบบเครือข่ายเมื่อมีการนำข้อมูลเหล่านั้นไปใช้เพื่อวิเคราะห์ผล การปิดบังหมายเลขไอพีเริ่มตั้งแต่การแปลงหมายเลขไอพีจริงที่ปรากฏในเฮดเดอร์ของแพ็คเก็ตที่ได้จากการตรวจตราและสูบจับแพ็คเก็ต ให้กลายเป็นหมายเลขไอพีปลอม (Faked IP Address) หรือหมายเลขไอพีนิรนาม (Anonymized IP Address) ก่อนที่จะนำไปใช้ทำการวิเคราะห์สถิติต่างๆ หรือทำการวิเคราะห์คุณลักษณะต่างๆ ของเครือข่ายต่อไป

วิธีการและแบบแผนในการปิดบังหมายเลขไอพีมีอยู่หลายวิธีการด้วยกันซึ่งจะได้กล่าวเพิ่มเติมในส่วนของบทที่ 2 ต่อไป โดยในแต่ละวิธีการปิดบังหมายเลขไอพีนั้นจะมีลักษณะการปิดบังที่แตกต่างกัน แต่อย่างไรก็ตามเมื่อพิจารณาถึงหลักการใช้งานหมายเลขไอพีนิรนามที่มีการปิดบังด้วยวิธีการใดวิธีการหนึ่งแล้ว ยังคงไม่เหมาะสมกับการทำงานบางประเภทของการวิเคราะห์และจัดการเครือข่าย เพราะในความเป็นจริงนั้นการปิดบังหมายเลขไอพีไม่มีความจำเป็นที่จะต้องปิดบังทั้ง 32 บิตของหมายเลขไอพี แต่สามารถปิดบังเพียงบางส่วนที่จำเป็นของหมายเลขไอพีได้ โดยขึ้นอยู่กับว่ามีความต้องการหรือความจำเป็นมากน้อยเพียงใดในการปิดบังหมายเลขไอพี โดยพิจารณาตามปัจจัยและเหตุผล 3 ประการ ดังนี้

1. โครงสร้างหมายเลขไอพีขององค์กรที่ต้องการแลกเปลี่ยนข้อมูลระหว่างกันมีความเหมือนหรือแตกต่างกันอย่างไรบ้าง
2. หน้าที่และประเภทของการวิเคราะห์และจัดการเครือข่ายแต่ละประเภทต้องใช้หมายเลขไอพีเพื่อวิเคราะห์ผลในเรื่องใดบ้าง และมองเห็นส่วนใดของหมายเลขไอพีบ้าง
3. กฎหมายหรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้กล่าวไว้อย่างไรบ้าง ในส่วนที่เกี่ยวข้องกับกระบวนการรักษาความเป็นส่วนตัวของข้อมูลส่วนบุคคล

จากปัจจัยและเหตุผล 3 ประการข้างต้นแสดงให้เห็นว่า การปิดบังหมายเลขไอพีนั้นสามารถปิดบังเพียงบางส่วนได้ตามความจำเป็นและความเหมาะสม และกระบวนการปิดบังดังกล่าวยังแสดงให้เห็นถึงระดับความเป็นส่วนตัว (Privacy Levels) ในการปิดบังหมายเลขไอพีที่แตกต่างกัน

ดังนั้นงานวิจัยเรื่องนี้จึงได้นำเสนอระดับความเป็นส่วนตัวขึ้นมา 5 ระดับในการปิดบังหมายเลขไอพี ได้แก่ ระดับที่ไม่มีการปิดบัง (Non-Anonymization Level) ระดับการปิดบังส่วน n บิตซ้าย (n-Left Anonymization Level) ระดับการปิดบังส่วน n บิตขวา (n-Right Anonymization Level) ระดับการปิดบังทั้ง 32 บิต (Full Anonymization Level) และ ระดับการปิดบังทั้ง 32 บิต แบบสุ่ม (Randomly Full Anonymization Level) ซึ่งกระบวนการปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวทั้ง 5 ระดับนี้จะพิจารณาเลือกใช้งานตามปัจจัย 3 ประการดังที่ได้กล่าวไว้ก่อนหน้านี้ซึ่งได้แก่ โครงสร้างต้นไม้ของความเป็นส่วนตัว (Privacy Tree Structures) รายการวิเคราะห์เครือข่าย (Network Analysis Functions) และ กฎหมายคอมพิวเตอร์ (Computer Law) โดยนำเอาปัจจัยทั้ง 3 ประการนี้มาผนวกเข้าด้วยกันโดยใช้วิธีการแบบกฎ (Rule-Based Method) เพื่อเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุดในการปิดบังหมายเลขไอพีต่อไป

การปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัวนี้ เหมาะสำหรับการแลกเปลี่ยนข้อมูลระหว่างสององค์กรใดๆ เพื่อใช้ในการวิเคราะห์ผลตามสภาพการใช้งานจริง สามารถเพิ่มประสิทธิภาพและความเร็วในการปิดบังหมายเลขไอพีในระบบการทำงานแบบช่วงเวลา (Batch Processing) และการทำงานแบบทันกาล (Real-Time Processing) และมีความปลอดภัยสูง

1.2 วัตถุประสงค์ของงานวิจัย

1. เพื่อกำหนดและนำเสนอระดับความเป็นส่วนตัว (Privacy Levels) ในการปิดบังหมายเลขไอพี
2. เพื่อกำหนดปัจจัยการปิดบัง (Anonymization Factors) เพื่อใช้เลือกระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพี
3. เพื่อสร้างแบบแผน (Scheme) การปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว

1.3 ขอบเขตของงานวิจัย

1. หมายเลขไอพีดั้งเดิมที่นำมาทำการปิดบังในงานวิจัยเรื่องนี้ใช้หมายเลขไอพีรุ่นที่ 4 ขนาด 32 บิต โดยกระบวนการทดลองและการทำงานต่างๆ ในการปิดบังหมายเลขไอพีจะอยู่บนระบบไอพีรุ่นที่ 4
2. งานวิจัยเรื่องนี้มีการศึกษาข้อมูลของรูปแบบและวิธีการปิดบังหมายเลขไอพีในซอฟต์แวร์สำเร็จรูปและเครื่องมือดูแลระบบเครือข่ายโดยจะพิจารณาเลือกซอฟต์แวร์ที่ได้รับความนิยมเช่น เอ็มอาร์ทีจี นากิออส และออปเมเนเจอร์ เป็นต้น

3. แบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัวมีขอบเขตสำหรับการทำงานดังต่อไปนี้

3.1 การวิเคราะห์เครือข่าย (Network Analysis) และการวิจัยเครือข่าย (Network Research) เช่น การวิเคราะห์การจราจร การตรวจตราการจราจร การตรวจจับผู้บุกรุก เป็นต้น

3.2 การจัดการเครือข่าย (Network Management) เช่น การใช้งานและการให้บริการในเครือข่าย การแสดงข้อมูลสรุปของเครือข่ายในรูปแบบของข้อความ กราฟ ตาราง และแผนที่เครือข่าย เป็นต้น

4. หมายเลขไอพีนิรนามที่ได้จากขั้นตอนของการปิดบังหมายเลขไอพี ไม่สามารถนำเอาไปใช้งานได้จริงในการสื่อสารและรับส่งข้อมูลในระแบบเครือข่าย แต่จะเป็นประโยชน์สำหรับนักวิจัยและนักวิเคราะห์ระบบเครือข่ายเท่านั้น

5. แบบแผนการปิดบังหมายเลขไอพีที่ได้จากงานวิจัยเรื่องนี้มีขอบเขตการใช้งานสำหรับองค์กรสององค์กรใดๆ ที่ต้องการแลกเปลี่ยนข้อมูลระหว่างกัน

6. อัลกอริทึมที่เลือกมาใช้ในการปิดบังหมายเลขไอพีได้มาจากอัลกอริทึมที่มีการนำเสนอในงานวิจัยต่างๆ และจากการพิจารณาเลือกอัลกอริทึมอื่นๆ ที่เหมาะสม

7. การวัดและทดสอบประสิทธิภาพการทำงานของแบบแผนการปิดบังหมายเลขไอพีจะใช้หลักการจำลองหมายเลขไอพีของเครือข่ายที่เป็นไปได้ทั้งหมดเพื่อใช้ทดสอบหรืออาจทดสอบกับระบบเครือข่ายจริง

8. การพัฒนาระบบการทำงานทั้งหมดจะกระทำภายใต้ระบบปฏิบัติการวินโดวส์ (Windows) และใช้ภาษาจาวาในกระบวนการพัฒนา

1.4 ขั้นตอนและวิธีดำเนินงานวิจัย

1. ศึกษาข้อมูลเอกสารและงานวิจัยที่เกี่ยวข้องกับหัวข้อของการปิดบังหมายเลขไอพี และศึกษาประเด็นของความเป็นส่วนตัว

2. ศึกษาลักษณะการทำงานของซอฟต์แวร์สำเร็จรูปต่างๆ ที่นิยมใช้ในการวิเคราะห์และจัดการเครือข่ายในปัจจุบัน และศึกษาการประยุกต์ใช้งานของการปิดบังหมายเลขไอพีในเครือข่ายตัวอย่าง

3. วิเคราะห์หลักการของการปิดบังหมายเลขไอพี วิเคราะห์ระดับความเป็นส่วนตัวของการปิดบังหมายเลขไอพี และวิเคราะห์ปัจจัยต่างๆ ที่ใช้พิจารณาในการปิดบังหมายเลขไอพี

4. ออกแบบและกำหนดระดับความเป็นส่วนตัวสำหรับการปิดบังหมายเลขไอพี และกำหนดปัจจัยที่ใช้พิจารณาในการปิดบังหมายเลขไอพี

5. ออกแบบแบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว

6. สร้างและบูรณาการแบบแผนการปิดบังหมายเลขไอพีด้วยระดับความเป็นส่วนตัว เพื่อให้เหมาะสมกับการวิเคราะห์และจัดการเครือข่าย

7. ทดสอบและตรวจสอบการทำงานและประสิทธิภาพของแบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว

8. ปรับปรุงแบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว

9. สรุปผลการวิจัยและตีพิมพ์ผลการทำวิจัย

10. เรียบเรียงและจัดทำเล่มวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับจากงานวิจัย

1. ได้แบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานระดับความเป็นส่วนตัวเพื่อใช้ในการวิเคราะห์และจัดการเครือข่าย

2. ได้แบบแผนการปิดบังหมายเลขไอพีที่สามารถประมวลผลได้เร็วและดีกว่าแบบแผนการปิดบังหมายเลขไอพีแบบเดิมที่ปิดบังทั้ง 32 บิตของหมายเลขไอพี

3. ได้แบบแผนการปิดบังหมายเลขไอพีที่สามารถรักษาความเป็นส่วนตัวของผู้ใช้งานในเครือข่ายได้เช่นเดียวกับกระบวนการปิดบังแบบเดิม แต่จะมีขั้นตอนและวิธีการปิดบังที่เหมาะสมตามสภาพความเป็นจริง

4. ได้แบบแผนการปิดบังหมายเลขไอพีที่เป็นประโยชน์สำหรับการรายงานผลและแสดงผลที่ไม่จำเป็นต้องแปลงย้อนกลับหมายเลขไอพี

5. ได้แบบแผนการปิดบังหมายเลขไอพีที่มีความปลอดภัยสูงต่อการถูกโจมตีและต่อการรักษาความลับของข้อมูล

6. สามารถนำหลักการของแบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัวไปประยุกต์ใช้ในงานด้านต่างๆ ได้อย่างเหมาะสม

1.6 ผลงานตีพิมพ์จากงานวิจัย

ส่วนหนึ่งของวิทยานิพนธ์เรื่องนี้ได้รับการตีพิมพ์ในประชุมวิชาการระดับชาติและระดับนานาชาติตามเอกสารในภาคผนวก ข โดยมีรายละเอียดดังต่อไปนี้

1. บทความเรื่อง “Defining Privacy Levels for IP Address Anonymization” โดย วงศ์ยศ เกิดศรี ยรรยง เต็งอำนวย และ ภาสกร ประถมบุตร ตีพิมพ์ในรายงานประชุมวิชาการระดับนานาชาติ 13th International ANnual Symposium on Computational Science

and Engineering (ANSCSE-13) ณ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ กรุงเทพมหานคร ระหว่างวันที่ 25-27 มีนาคม พ.ศ. 2552

2. บทคัดย่อเรื่อง “Defining Privacy Levels for IP Address Anonymization” โดย วงศ์ยศ เกิดศรี ยรรยง เต็งอำนวย และ ภาสกร ประถมบุตร ตีพิมพ์ในรายงานประชุมวิชาการระดับนานาชาติ 13th International ANnual Symposium on Computational Science and Engineering (ANSCSE-13) ณ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ กรุงเทพมหานคร ระหว่างวันที่ 25-27 มีนาคม พ.ศ. 2552

3. บทคัดย่อเรื่อง “Presenting Privacy Tree Structure for IP Address Anonymization Based on Privacy Levels” โดย วงศ์ยศ เกิดศรี ยรรยง เต็งอำนวย และ ภาสกร ประถมบุตร ตีพิมพ์ในรายงานประชุมวิชาการระดับนานาชาติ 13th International ANnual Symposium on Computational Science and Engineering (ANSCSE-13) ณ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ กรุงเทพมหานคร ระหว่างวันที่ 25-27 มีนาคม พ.ศ. 2552

4. บทความเรื่อง “Defining and Using Anonymization Factors for Anonymizing IP Address Based on Privacy Levels” โดย วงศ์ยศ เกิดศรี ยรรยง เต็งอำนวย และ ภาสกร ประถมบุตร ตีพิมพ์ในรายงานประชุมวิชาการระดับชาติ National Conference on Computing and Information Technology (NCCIT 2009) ณ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กรุงเทพมหานคร ระหว่างวันที่ 22-23 พฤษภาคม พ.ศ. 2552

บทที่ 2

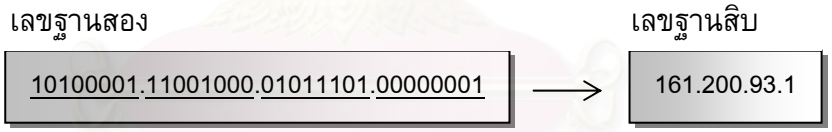
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ทฤษฎีและงานวิจัยที่เกี่ยวข้องกับวิทยานิพนธ์เรื่องนี้ประกอบไปด้วยส่วนของความรู้เบื้องต้นเกี่ยวกับหมายเลขไอพี หลักการปิดบังหมายเลขไอพี กระบวนการวิเคราะห์และจัดการเครือข่าย และบทวิจารณ์งานวิจัยต่างๆ ที่เกี่ยวข้อง โดยมีรายละเอียดดังต่อไปนี้

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 หมายเลขไอพี

หมายเลขไอพีหรือไอพีแอดเดรส (IP Address หรือ Internet Protocol Address) คือหมายเลขที่ใช้ในระบบเครือข่าย ซึ่งมีลักษณะคล้ายกับหมายเลขโทรศัพท์ที่ระบุถึงที่อยู่ของอุปกรณ์ในเครือข่าย [20] โดยจะเป็นตัวเลขฐานสองขนาด 32 บิต ซึ่งหมายเลขไอพีแบ่งออกเป็น 4 กลุ่ม โดยแต่ละกลุ่มใช้เลขฐานสองขนาด 8 บิต และมีสัญลักษณ์จุด (Dot) เป็นตัวแบ่งตัวเลขในแต่ละกลุ่มออกจากกัน โดยทั่วไปหมายเลขไอพีมักแสดงผลโดยใช้เลขฐานสิบ 4 กลุ่มแทนตัวเลขฐานสองดังตัวอย่างในรูปที่ 2.1

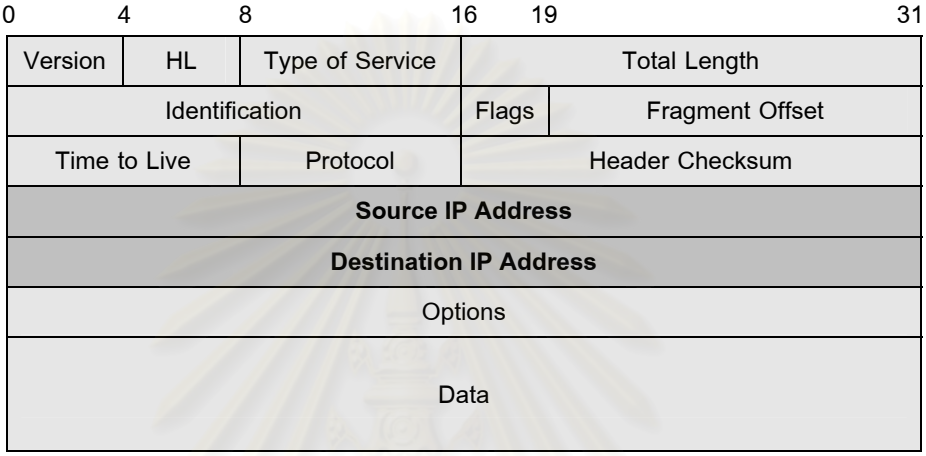


รูปที่ 2.1 ลักษณะของหมายเลขไอพี 32 บิตในรูปแบบของเลขฐานสองและเลขฐานสิบ

หมายเลขไอพีจะปรากฏอยู่ในส่วนของเฮดเดอร์ของแพ็คเก็ต (Packet Header) ที่ทำงานอยู่ในระดับชั้นเครือข่ายดังแสดงในส่วนโครงสร้างของเฮดเดอร์ในระดับชั้นเครือข่าย [8] ตามรูปที่ 2.2 ประกอบด้วยหมายเลขไอพีของเครื่องต้นทางและหมายเลขไอพีของเครื่องปลายทางซึ่งหมายเลขไอพีนี้จะถูกผนวกเข้าเป็นข้อมูลส่วนหนึ่งภายในแพ็คเก็ตที่ใช้ในการสื่อสารและแลกเปลี่ยนข้อมูลระหว่างกันของอุปกรณ์ในเครือข่าย

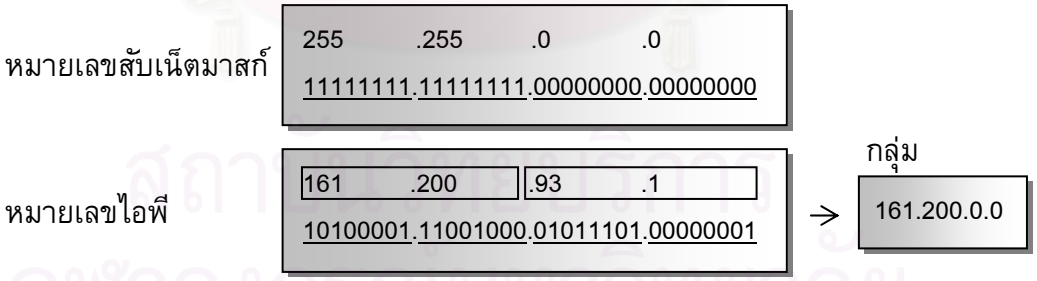
หมายเลขไอพีที่ใช้งานอยู่ในปัจจุบันนั้นเป็นระบบไอพีรุ่นที่ 4 (IPv4) ซึ่งมีรูปแบบตามโครงสร้างหมายเลขไอพีระบบ 32 บิตที่ได้กล่าวมาแล้วในตอนต้น โดยประกอบไปด้วยหมายเลขไอพีที่เป็นไปได้ทั้งหมด 2^{32} หมายเลข เริ่มตั้งแต่หมายเลข 0.0.0.0 จนถึงหมายเลข 255.255.255.255 แต่หมายเลขไอพีทั้ง 2^{32} หมายเลขนี้ไม่สามารถถูกกำหนดให้กับอุปกรณ์ในเครือข่ายได้ทั้งหมด เพราะเนื่องจากว่ามีหมายเลขไอพีบางหมายเลขที่สงวนไว้

สำหรับทำหน้าที่เฉพาะเช่น หมายเลข 127.0.0.0 หรือหมายเลข 255.255.255.255 เป็นต้น ในปัจจุบันนั้นได้มีอุปกรณ์ในเครือข่ายเพิ่มมากขึ้นอย่างรวดเร็วจนทำให้หมายเลขไอพีในระบบเดิมมีไม่เพียงพอ ดังนั้นจึงได้มีการออกแบบและพัฒนาระบบไอพีรุ่นที่ 6 (IPv6) ขึ้นมาใหม่เพื่อใช้ทดแทนระบบไอพีรุ่นที่ 4 เดิม ซึ่งในมาตรฐานของรุ่นที่ 6 นี้จะใช้ระบบ 128 บิตในการระบุหมายเลยไอพีทำให้มีหมายเลขไอพีที่เป็นไปได้ทั้งหมด 2^{128} หมายเลข



รูปที่ 2.2 โครงสร้างของเฮดเดอร์ในระดับชั้นเครือข่าย

ทั้งนี้ การจัดแบ่งและกำหนดขอบเขตของหมายเลขไอพีให้กับกลุ่มเครือข่ายหรือกลุ่มองค์กรหนึ่งๆ นั้น ในปัจจุบันจะใช้วิธีการจัดแบ่งด้วยหมายเลขสับเน็ตมาสก์ (Subnet Mask Address) ดังแสดงในรูปที่ 2.3



รูปที่ 2.3 การจัดแบ่งหมายเลขไอพีด้วยหมายเลขสับเน็ตมาสก์

หมายเลขสับเน็ตมาสก์สามารถแบ่งหมายเลขไอพีออกเป็น 2 ส่วนดังต่อไปนี้

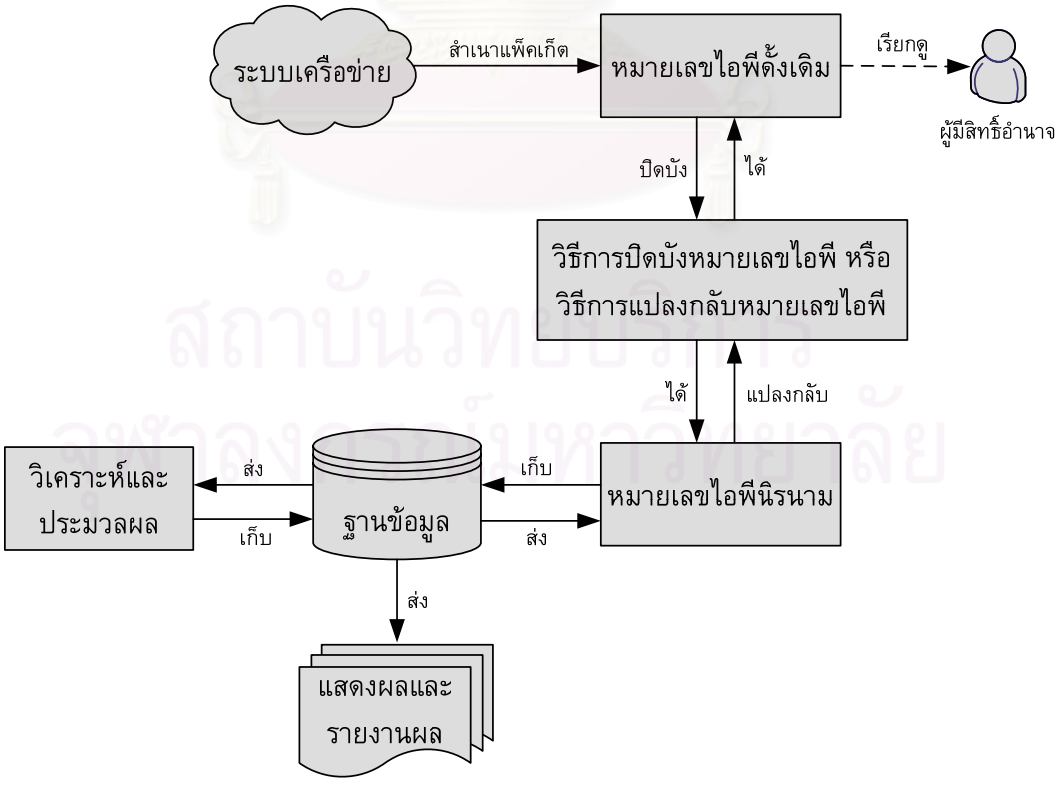
1. ส่วนเครือข่าย (Network Part) แสดงด้วยบิต 1 ของหมายเลขสับเน็ตมาสก์ ซึ่งเป็นกลุ่มของบิตทางซ้ายที่ระบุถึงความเป็นกลุ่มของเครือข่าย กลุ่มขององค์กร และหน่วยงานในเครือข่าย

2. ส่วนเครื่องหรือส่วนโฮส (Host Part) แสดงด้วยบิต 0 ของหมายเลขสับเน็ตมาสก์ ซึ่งเป็นกลุ่มของบิตทางขวาที่ระบุถึงจำนวนของเครื่องหรืออุปกรณ์ปลายทางในเครือข่าย

2.1.2 การปิดบังหมายเลขไอพี

การปิดบังหมายเลขไอพี (IP Address Anonymization) เป็นกระบวนการแปลงหมายเลขไอพีดั้งเดิม ทั้งหมายเลขไอพีต้นทางและปลายทางที่ปรากฏอยู่ในเฮดเดอร์ของแพ็คเก็ตให้กลายเป็นหมายเลขไอพีนิรนาม เพื่อเป็นการปกปิดข้อมูลส่วนบุคคล และปิดบังลักษณะต่างๆ ที่มีความเป็นส่วนตัวของอุปกรณ์ในเครือข่ายเอาไว้

โดยกระบวนการทำงานจะเริ่มเมื่อมีการสูบจับแพ็คเก็ตในเครือข่ายขึ้นมาเพื่อทำการวิเคราะห์ในเชิงสถิติ ซึ่งข้อมูลแพ็คเก็ตเหล่านั้นถูกจัดเก็บไว้ในฐานข้อมูล แต่ก่อนที่จะนำข้อมูลแพ็คเก็ตเหล่านั้นไปทำการวิเคราะห์และประมวลผล ข้อมูลจะถูกนำมาขจัดคุณลักษณะที่บ่งบอกถึงความเป็นส่วนตัวออกไปด้วยการปิดบังหมายเลขไอพี [17] ซึ่งลักษณะขั้นตอนทั่วไปของการปิดบังหมายเลขไอพีได้แสดงไว้ในรูปที่ 2.4 เมื่อกระบวนการวิเคราะห์ข้อมูลเหล่านั้นเสร็จสิ้นเป็นที่เรียบร้อย ข้อมูลส่วนที่เป็นผลลัพธ์และการรายงานผลต่างๆ จะถูกปิดบังลักษณะที่แสดงถึงความเป็นส่วนตัวเอาไว้ตามความเหมาะสม



รูปที่ 2.4 โครงสร้างขั้นตอนทั่วไปของการปิดบังหมายเลขไอพี

การปิดบังหมายเลขไอพีมีวัตถุประสงค์เพื่อปิดบังข้อมูลส่วนบุคคลให้กับนักวิจัยหรือนักวิเคราะห์ระบบเครือข่ายสามารถทำงานได้โดยไม่ก้าวก่ายความมนส่วนตัวของผู้ใช้งานในเครือข่าย ไม่ก่อให้เกิดการละเมิดสิทธิส่วนบุคคลและความเป็นส่วนตัวของผู้ใช้งานในเครือข่าย และเพื่อสร้างความน่าเชื่อถือ ความไว้วางใจในส่วนของข้อมูลของสมาชิก อุปกรณ์ และองค์กรในเครือข่ายที่อาจถูกนำไปแสดงผลต่อสาธารณะหรือใช้ในกระบวนการวิเคราะห์และจัดการเครือข่ายต่างๆ ต่อไปได้

การปิดบังหมายเลขไอพีนั้นมีหลายวิธีซึ่งจะได้กล่าวต่อไปในส่วนของงานวิจัยที่เกี่ยวข้อง โดยแต่ละวิธีการปิดบังนั้นจะมีแนวทางที่สอดคล้องตามกระบวนการขั้นตอนที่ได้แสดงไว้ในรูปที่ 2.4 ทั้งนี้กระบวนการปิดบังหมายเลขไอพีจะต้องได้หมายเลขไอพีนิรนามที่มีคุณสมบัติเช่นเดียวกับหมายเลขไอพีดั้งเดิมทุกประการ และอาจมีอัลกอริทึมที่สามารถแปลงหมายเลขไอพีนิรนามกลับเป็นหมายเลขไอพีดั้งเดิมได้

2.1.3 การวิเคราะห์และจัดการเครือข่าย

การวิเคราะห์และจัดการเครือข่าย (Network Analysis and Management) เป็นหลักการวิเคราะห์ ตรวจสอบ บริหารจัดการ ควบคุม และดูแลระบบเครือข่ายให้สามารถทำงานได้อย่างปกติ มีความถูกต้อง ปลอดภัย และมีประสิทธิภาพสูงสุด [5]

1) หลักการและทฤษฎี ประกอบไปด้วยแนวทางและรูปแบบการทำงาน [5, 21] ที่แบ่งออกได้เป็น 3 รูปแบบหลักดังนี้

1. การเรียกใช้งานโปรโตคอลเอสเอ็นเอ็มพี (Simple Network Management Protocol: SNMP) ซึ่งจะประกอบไปด้วยเครื่องจัดการ (Manager) ที่เป็นตัวกลางในการร้องขอข้อมูลการทำงานจากโปรแกรมตัวแทน (Agents) ที่อยู่กับอุปกรณ์ต่างๆ ในระบบเครือข่าย ซึ่งส่วนใหญ่แล้วจะกระทำกับอุปกรณ์จำพวกเราเตอร์ (Router) สวิตช์ (Switch) และ เซิร์ฟเวอร์ (Server) เป็นต้น

2. การสูบจับแพ็คเก็ต (Packet Sniffer) ซึ่งจะเป็นการสำเนาข้อมูลแพ็คเก็ตที่ถูกส่งมาในเครือข่ายขึ้นมาทำการวิเคราะห์ข้อมูลทางด้านสถิติต่างๆ หรือทำการตรวจจับข้อผิดพลาดของระบบเครือข่าย

3. การตรวจตราการจราจร (Traffic Traces) เป็นการตรวจตราข้อมูลของการใช้งานหรือตรวจติดตามพฤติกรรมของอุปกรณ์หนึ่งๆ ในเครือข่าย ว่ามีการทำงานและมีการเดินทางของข้อมูลไปในสถานที่ใดบ้าง เพื่อที่จะทราบถึงร่องรอยหรือการแกะรอยการทำงาน เพื่อวิเคราะห์หาสิ่งแปลกปลอมหรือหาสาเหตุบางประการที่เกิดขึ้นกับระบบเครือข่าย

จากรูปแบบของการวิเคราะห์และจัดการเครือข่ายเหล่านี้ได้ถูกนำออกไปประยุกต์ใช้กับระบบการทำงานจริง ซึ่งอยู่ในรูปแบบของซอฟต์แวร์สำเร็จรูปที่ใช้ดูแลเครือข่าย (Monitoring Tools) เช่น เอ็มอาร์ทีจี (MRTG) [13] พีอาร์ทีจี (PRTG) [21] นากิออส (Nagios) [11] และ ออปแมนเนเจอร์ (OpManager) [9] เป็นต้น ซึ่งซอฟต์แวร์สำเร็จรูปเหล่านี้ล้วนแล้วแต่มีลักษณะของการวิเคราะห์และจัดการเครือข่ายที่คล้ายคลึงกัน เช่น การวิเคราะห์การเข้าออกของข้อมูลในเครือข่าย การวิเคราะห์การใช้งานบริการต่างๆ ในเครือข่าย การตรวจสอบอุปกรณ์ในเครือข่าย ณ เวลาหนึ่งๆ เป็นต้น

2) ประเภทและบริการต่าง ๆ ในการวิเคราะห์และจัดการเครือข่าย ประกอบไปด้วยหลายรูปแบบ [1, 5] ดังนี้

1. ชนิดและประเภทของอุปกรณ์ เป็นการแสดงชนิดหรือประเภทของอุปกรณ์ และจำนวนของอุปกรณ์ที่ใช้งานอยู่ในระแบบเครือข่าย เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องพิมพ์ และเราเตอร์ เป็นต้น ซึ่งอาจจะแสดงอยู่ในรูปแบบของแผนที่เครือข่าย (Network Map)

2. กลุ่มผู้ใช้งาน เป็นการเลือกกลุ่มผู้ใช้งานเพื่อนำมาเปรียบเทียบข้อมูลการทำงานในแต่ละกลุ่ม

3. เวลาและช่วงเวลาการใช้งาน เป็นการสรุปข้อมูลทั้งรายวัน รายเดือน และรายปีของช่วงเวลาในการใช้งานอุปกรณ์และการเปิดให้บริการของอุปกรณ์ต่างๆ

4. ปริมาณข้อมูลการใช้งาน เป็นการคำนวณหาปริมาณของข้อมูลการรับเข้าและส่งออกในเครือข่าย หาค่าร้อยละของบริการต่างๆ ที่ถูกใช้งาน หาอัตราการประมวลผลของอุปกรณ์หนึ่งๆ หาอัตราการใช้ช่องสัญญาณ และหาความเร็วของการรับและส่งข้อมูล เป็นต้น

5. จำนวนและชนิดของบริการ เป็นการนับจำนวนของบริการที่เปิดให้บริการในเครือข่าย และแสดงจำนวนของการเรียกใช้งานบริการต่างๆ ในเครือข่าย

6. ข้อมูลความปลอดภัยและความมั่นคง เป็นการตรวจสอบและดูแลระบบเครือข่าย เช่นการตรวจจับผู้บุกรุก การค้นหาอุปกรณ์ที่ก่อกวนระบบ การตรวจหาหนอนอินเตอร์เน็ต (Worm) การตรวจหาไวรัส (Virus) และ การติดตามพฤติกรรมการทำงานของสมาชิกในเครือข่าย เป็นต้น

นอกจากนี้ ยังมีประเภทและลักษณะของการวิเคราะห์และจัดการเครือข่ายในรูปแบบอื่นๆ ที่ยังไม่ได้กล่าวไว้ในที่นี้จะแสดงรายละเอียดเพิ่มเติมในบทที่ 4 ต่อไป

2.2 งานวิจัยที่เกี่ยวข้อง

วิธีการและแบบแผนการปิดบังหมายเลขไอพีนั้นได้รับความสนใจเพิ่มมากยิ่งขึ้นในปัจจุบัน เพราะเนื่องจากว่า เมื่อระบบเครือข่ายคอมพิวเตอร์มีการขยายตัวอย่างแพร่หลายก็ย่อมต้องมีการคำนึงถึงความเป็นส่วนบุคคลของข้อมูลมากยิ่งขึ้นด้วยเช่นกัน หมายเลขไอพีนั้นจัดเป็นข้อมูลส่วนบุคคลประเภทหนึ่ง ดังนั้นข้อมูลเหล่านี้ต้องได้รับการปิดบังเอาไว้

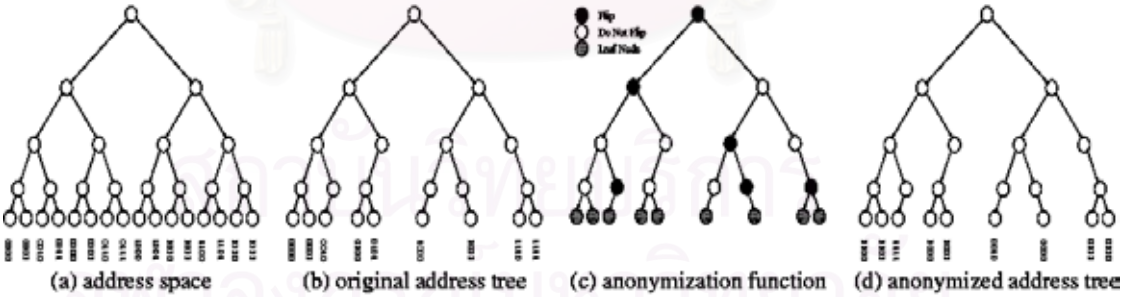
วิธีการและแบบแผนการปิดบังหมายเลขไอพีเกิดขึ้นมาเมื่อประมาณสิบปีเศษ โดยรูปแบบการปิดบังหมายเลขไอพีเริ่มแรกนั้นใช้หลักการพื้นฐานและอัลกอริทึมอย่างง่ายในการทำงาน [4] เช่น การใช้ฟังก์ชันแฮช (Hash Functions) การเข้ารหัสด้วยวิธีเอ็มดี 5 (MD5) การเข้ารหัสด้วยวิธีการของอาร์เอสเอ (RSA) และ การเข้ารหัสด้วยวิธีแบบซีซ่า (Caesar) เป็นต้น ซึ่งวิธีการเหล่านี้ต้องจับคู่ระหว่างหมายเลขไอพีต้นแบบกับหมายเลขไอพีนิรนามแต่ละคู่เข้าไว้ด้วยกันแบบหนึ่งต่อหนึ่ง (One-to-One Mapping) [22, 23, 25] และเก็บบันทึกหมายเลขไอพีในรูปแบบของตารางค้นหา (Table Lookup) เพื่อใช้ในการค้นคืนหมายเลขไอพีดั้งเดิม แต่วิธีการพื้นฐานเหล่านี้เป็นเพียงการแปลงหมายเลขไอพีดั้งเดิมให้กลายเป็นหมายเลขไอพีนิรนามเท่านั้น เมื่อนำไปใช้งานจริงในการวิเคราะห์และจัดการเครือข่ายแล้วจะทำได้ยากลำบากก่อให้เกิดปัญหาและความผิดพลาดขึ้นได้ เพราะเนื่องจากว่าหมายเลขไอพีนิรนามดังกล่าวไม่สามารถเป็นตัวแทนและสื่อความหมายของข้อมูลได้เช่นเดียวกับหมายเลขไอพีดั้งเดิม เช่น ไม่สามารถแยกแยะกลุ่มของเครือข่ายได้ เกิดการชนและซ้ำซ้อนของหมายเลขไอพี และต้องใช้ตารางในการจัดเก็บหมายเลขไอพีดั้งเดิมและหมายเลขไอพีนิรนามในแต่ละคู่ เป็นต้น

จนเมื่อปี ค.ศ. 1996 เกรก มินแชล [10] ได้คิดวิธีการปิดบังหมายเลขไอพีอย่างเป็นรูปแบบวิธีการแรกขึ้นมาซึ่งชื่อว่าทีซีพีดีไพรว์ (Tcpdpriv) และได้รับการโต้แย้งข้อผิดพลาดจากการทำงานโดยทาทุ โยลเน็น [24] ในปีเดียวกัน โดยวิธีการทีซีพีดีไพรว์นั้นจะเป็นอัลกอริทึมหนึ่งในโปรแกรมทีซีพีดัมพ์ (Tcpdump) ซึ่งถูกพัฒนาอยู่บนระบบยูนิกซ์ ตระกูลเน็ตบีเอสดี (NetBSD) ฟรีบีเอสดี (FreeBSD) ซันโอเอส (SunOS) และ โซลาริส (Solaris) จนเมื่อปี ค.ศ. 1999 เจอราล์ด คอมบ์ (Gerald Combs) [15] ได้ย้ายวิธีการทีซีพีดีไพรว์ไปใช้งานบนระบบลีนุกซ์ได้สำเร็จ

หลักการทำงานของทีซีพีดีไพรว์นั้นจะนำเอาหมายเลขไอพีต้นแบบมาทำการจับคู่แบบสุ่ม (Randomized Mapping) ตามระดับความปลอดภัยที่แตกต่างกันจนได้หมายเลขไอพีนิรนามออกมา ซึ่งวิธีการทีซีพีดีไพรว์นี้สามารถแก้ไขปัญหาของการสื่อความหมายของกลุ่ม

เครือข่ายได้ โดยหมายเลขไอพีนิรนามที่ได้สามารถแยกแยะกลุ่มของเครือข่ายได้เช่นเดียวกับหมายเลขไอพีดั้งเดิม แต่วิธีการดังกล่าวต้องมีการจับคู่ระหว่างหมายเลขไอพีดั้งเดิมกับหมายเลขไอพีนิรนามแบบหมายเลขต่อหมายเลขเช่นเดิม ซึ่งจะทำให้เกิดปัญหาในการทำงานขึ้นได้เมื่อมีหมายเลขไอพีจำนวนมาก และส่งผลให้เกิดการชนกันของหมายเลขไอพีนิรนามขึ้นได้เมื่อมีการกรองและจับแพ็คเก็ตในรอบถัดไปหรือเมื่อมีการทำงานหลายๆ รอบ

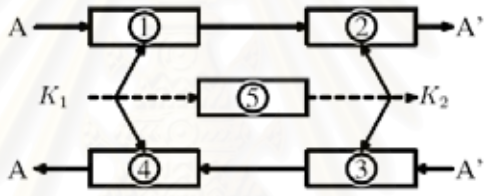
ดังนั้นจึงได้มีการคิดวิธีการปิดบังหมายเลขไอพีแบบใหม่ขึ้น โดยในปี ค.ศ. 2002 จุน ซิว และคณะ [22, 23] ได้นำหลักการเข้ารหัสลับ (Cryptography) เข้ามาใช้ในการปิดบังหมายเลขไอพี ซึ่งเป็นวิธีการที่เรียกว่าคริปโตแพน (Crypto-PAn) โดยใช้ทฤษฎีรูปแบบคาโนนิคอล (Canonical Form Theorem) ในการสร้างอัลกอริทึมการปิดบังหมายเลขไอพีขึ้นมาซึ่งมีรูปแบบเป็นต้นไม้ของการปิดบังหมายเลขไอพี (Address Anonymization Tree) ดังแสดงในรูปที่ 2.5 โดยมีการสร้างต้นไม้ของหมายเลขไอพีดั้งเดิม (Original Address Tree) และสร้างต้นไม้ฟังก์ชันการปิดบัง (Anonymization Function Tree) ซึ่งเปรียบเสมือนกุญแจที่ใช้สำหรับปิดบัง โดยการปิดบังหมายเลขไอพีเป็นการสลับค่าบิตของต้นไม้ของหมายเลขไอพีดั้งเดิมตามต้นไม้ฟังก์ชันการปิดบังซึ่งได้ระบุไว้ว่าส่วนบิตใดของหมายเลขไอพีดั้งเดิมที่ต้องสลับบิตบ้าง กระบวนการสลับบิตมีทั้งหมด 32 รอบ เพื่อให้ครบทั้ง 32 บิตของหมายเลขไอพี เมื่อสิ้นสุดกระบวนการปิดบังก็จะได้หมายเลขไอพีนิรนามตามแบบของต้นไม้ของหมายเลขไอพีนิรนาม (Anonymized Address Tree) วิธีการแบบคริปโตแพนสามารถแปลงหมายเลขไอพีดั้งเดิมให้เป็นหมายเลขไอพีนิรนามได้โดยไม่เกิดปัญหาการชนกัน และสามารถคงไว้ซึ่งข้อมูลในส่วนของบิตที่จะระบุถึงความแตกต่างของกลุ่มเครือข่าย (Prefix Preserving) เอาไว้ได้เช่นเดิม



รูปที่ 2.5 ต้นไม้ของการปิดบังหมายเลขไอพีตามทฤษฎีรูปแบบคาโนนิคอล

วิธีการปิดบังหมายเลขไอพีดังกล่าวทั้งสองวิธีก่อนหน้านี้ได้ถูกยอมรับและนำไปประยุกต์กับระบบการวิเคราะห์และจัดการเครือข่ายในกลุ่มวิจัยและองค์กรต่างๆ มากมาย แต่อย่างไรก็ตามยังมีนักวิจัยบางกลุ่มที่ได้คิดและพัฒนาระบบการปิดบังหมายเลขไอพีขึ้นมาอยู่เรื่อยๆ จนเมื่อปี ค.ศ. 2006 ที่ผ่านมาได้มีการคิดวิธีการและแบบแผนการปิดบังหมายเลขไอพีขึ้นมาใหม่อีกรูปแบบหนึ่ง ซึ่งได้นำเอาแนวคิดของวิธีการแบบคริปโตแพนและการจับคู่แบบหนึ่ง

ต่อหนึ่งมาประยุกต์ใช้โดยเคียนลี่ ชาง และคณะ [25] ได้ใช้หลักการแบ่งระดับการเข้าถึงหลายชั้น (Multiple Access Levels) มาใช้ในการทำงานดังแสดงตามรูปที่ 2.6 ซึ่งพิจารณาว่าการปิดบังหมายเลขไอพีมีหลากหลายระดับทำให้ต้องเข้ารหัสหมายเลขไอพีดั้งเดิมด้วยกุญแจที่แตกต่างกัน ซึ่งปลอดภัยมากยิ่งขึ้นในการปิดบังหมายเลขไอพี รายละเอียดของวิธีการทำงานเริ่มด้วยการนำเอาหมายเลขไอพีดั้งเดิมมาเข้ารหัสโดยใช้กุญแจแบบที่ 1 จนได้หมายเลขไอพีนิรนามแบบที่ 1 ออกมา ซึ่งบุคคลที่รู้หรือถือกุญแจแบบที่ 1 เท่านั้นที่จะสามารถแปลงหมายเลขไอพีนิรนามแบบที่ 1 กลับมาเป็นหมายเลขไอพีดั้งเดิม และเมื่อข้อมูลหมายเลขไอพีนิรนามเหล่านั้นถูกเข้ารหัสอีกครั้งด้วยกุญแจแบบที่ 2 ก็จะได้หมายเลขไอพีนิรนามใหม่เป็นแบบที่ 2 เช่นกัน ซึ่งบุคคลที่รู้หรือถือกุญแจแบบที่ 2 เท่านั้นที่จะสามารถแปลงหมายเลขไอพีนิรนามแบบที่ 2 กลับไปเป็นหมายเลขไอพีแบบที่ 1 แต่ก็ยังไม่สามารถทราบถึงหมายเลขไอพีดั้งเดิมที่แท้จริงได้ โดยกุญแจที่ใช้ในการเข้ารหัสก็จะถูกเข้ารหัสด้วยเช่นกัน ซึ่งหลักการดังกล่าวมองว่าการปิดบังหมายเลขไอพีมีระดับของการเข้าถึงและรับรู้ข้อมูลที่แตกต่างกัน



1: การปิดบังของแบบแผนที่หนึ่ง Sa1
2: การปิดบังของแบบแผนที่สอง Sa2
3: การแปลงกลับของแบบแผนที่สอง S2
4: การแปลงกลับของแบบแผนที่หนึ่ง S1
5: การสร้างกุญแจ

รูปที่ 2.6 หลักการแบ่งระดับการเข้าถึงหลายชั้น

ผลการทำงานของวิธีการแบ่งระดับการเข้าถึงหลายชั้นนี้เป็นที่น่าพอใจและสามารถที่จะทำให้เกิดความปลอดภัยมากยิ่งขึ้นในการวิเคราะห์และจัดการเครือข่าย แต่วิธีการดังกล่าวยังมีปัญหาในส่วนของกุญแจที่ใช้ในการแปลงหมายเลขไอพีซึ่งไม่สามารถแปลงข้ามระดับได้ โดยถ้าต้องการให้บุคคลที่ถือกุญแจระดับที่ 1 ทำการแปลงหมายเลขไอพีนิรนามในระดับที่ 2 นั้นไม่สามารถทำได้ โดยสามารถทำการแปลงหมายเลขไอพีได้ในระดับเดียวกันเท่านั้น นอกจากนี้ยังมีปัญหาในด้านของการทำงานและใช้งานจริง เพราะเนื่องจากว่าในบางกรณีหรือบางประเภทของการวิเคราะห์และจัดการเครือข่ายไม่มีความจำเป็นที่ต้องปิดบังหมายเลขไอพีอย่างมิดชิดและหลายระดับถึงขนาดนั้น และบางครั้งการปิดบังหมายเลขไอพีหลายระดับเกินไปจะทำให้ยากต่อการแปลงกลับ และทำให้เสียเวลาในการประมวลผลการ

ทำงาน ซึ่งต่อมาในปี ค.ศ. 2007 เคียนลี่ ชาง และคณะ [26] ได้ปรับปรุงวิธีการปิดบังดังกล่าวให้สามารถทำงานได้รวดเร็วยิ่งขึ้นโดยใช้หลักการทำงานของบิตสตริง (Bit String) และในปีเดียวกันรามัสเวมี [16] ก็ได้นำเสนอวิธีการปิดบังหมายเลขไอพีที่มีความรวดเร็ว ซึ่งเรียกว่าวิธีทีเอสเอ (TSA : Top-hash Subtree-replicated Anonymization) ซึ่งวิธีการปิดบังนี้ได้ประยุกต์ใช้หลักการของคริปโตแพนโดยนำวิธีการแบบแฮชฟังก์ชันเข้ามาช่วยในการปิดบัง ทั้งนี้เพื่อให้การประมวลผลสามารถทำได้อย่างรวดเร็วยิ่งขึ้น และสามารถประยุกต์ใช้กับระบบการปิดบังหมายเลขไอพีแบบทันกาลที่มีข้อมูลเข้ามาอย่างต่อเนื่อง

งานวิจัยอื่นๆ ที่ได้นำเสนอแนวคิด หลักการ และปัญหาที่เกี่ยวข้องกับการปิดบังหมายเลขไอพีที่น่าสนใจนอกเหนือจากที่ได้กล่าวมาข้างต้นประกอบไปด้วย งานวิจัยของเคาคิส และคณะ [7] ซึ่งได้นำเสนอถึงความเสี่ยงของการแสดงข้อมูลหมายเลขไอพีที่ถูกปิดบังแล้ว ซึ่งเคาคิสให้แนวคิดว่าข้อมูลที่ทำการปิดบังหมายเลขไอพีด้วยอัลกอริทึมแบบต่างๆ ไปแล้วยังสามารถถูกโจมตีและถูกแกะรอยเพื่อล้วงความลับออกมาได้เช่นเดิม เช่นการนำเอาผลลัพธ์จากการทำงานที่ใช้หมายเลขพีดั้งเดิมในการประมวลผล มาทำการเปรียบเทียบกับผลลัพธ์การทำงานที่ใช้หมายเลขไอพีนิรนามประมวลผลพบว่า ถ้าผลลัพธ์จากการทำงานที่ใช้หมายเลขไอพีนิรนามประมวลผลมีค่าที่เหมือนหรือสอดคล้องกับผลลัพธ์ที่ใช้หมายเลขไอพีดั้งเดิมประมวลผลก็ย่อมคาดเดาได้ว่าหมายเลขไอพีนิรนามหมายเลขนั้นอาจเป็นหมายเลขเดียวกับหมายเลขไอพีดั้งเดิมที่ตรวจพบ ดังนั้นจึงควรเปลี่ยนรูปแบบการระบุค่าหมายเลขไอพีดั้งเดิมมาเป็นการระบุค่าหมายเลขไอพีที่ไม่ได้ใช้งาน (Passive IP Address) ก่อนจะทำการปิดบังหมายเลขไอพีอย่างแท้จริง โดยนำหมายเลขไอพีดั้งเดิมมาผ่านฟังก์ชันอย่างง่ายเช่น เอชแมค (HMAC) เป็นต้น

งานวิจัยของเคาคิสมีผลสอดคล้องกับงานวิจัยของโตนเนส เบรคเนและคณะ [2] ที่ได้นำเสนอถึงวิธีการโจมตีและแสดงจุดอ่อนของหลักการปิดบังหมายเลขไอพีของทีซีพีดีไพรว์และคริปโตแพน ซึ่งสามารถถูกโจมตีได้ในหลายแนวทาง เช่น การโจมตีโดยอัดฉีดแพ็คเก็ตจำนวนมากแล้วทำการเปรียบเทียบค่า (Packet Injection Attack) หรือการวิเคราะห์ความถี่ของข้อมูลเพื่อทราบรูปแบบของข้อมูล (Frequency Analysis) เป็นต้น

จากงานวิจัยทั้งหมดที่ได้กล่าวมานั้นก่อให้เกิดแนวทางให้กับงานวิจัยเรื่องนี้ในการคิดแบบแผนการปิดบังหมายเลขไอพีขึ้นมาใหม่ โดยการสร้างและกำหนดระดับความเป็นส่วนตัวให้กับหมายเลขไอพี เพื่อทำการจัดกลุ่มและเลือกอัลกอริทึมของการปิดบังหมายเลขไอพีที่เหมาะสมกับระดับความเป็นส่วนตัวในการวิเคราะห์และจัดการเครือข่ายต่อไป

บทที่ 3

ระดับความเป็นส่วนตัว

บทนี้เป็นการนำเสนอระดับความเป็นส่วนตัว 5 ระดับ เพื่อใช้สำหรับการปิดบังหมายเลขไอพีตามแบบแผนการปิดบังซึ่งจะได้กล่าวต่อไปในบทที่ 5 โดยรายละเอียดของระดับความเป็นส่วนตัวมีดังต่อไปนี้

3.1 แนวคิดของระดับความเป็นส่วนตัว

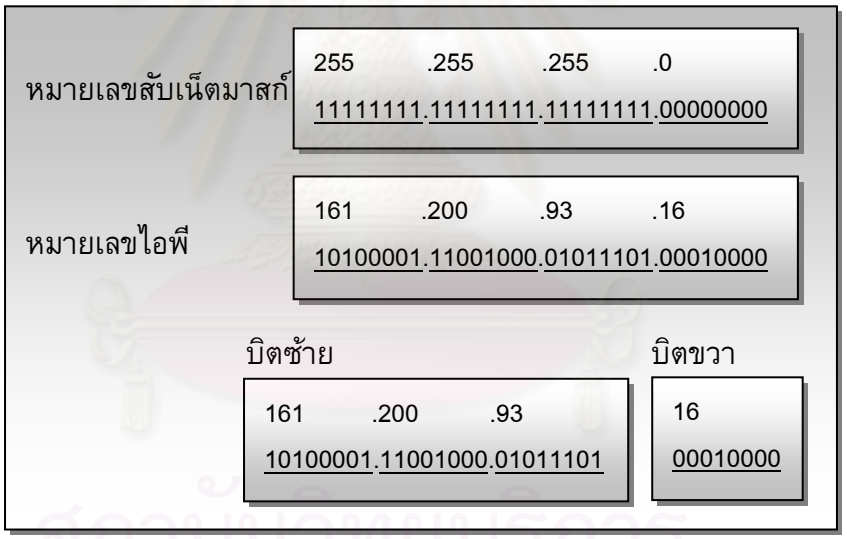
จากการศึกษากระบวนการปิดบังหมายเลขไอพีที่ได้นำเสนอจากงานวิจัยก่อนหน้านี้พบว่า หลักการปิดบังหมายเลขไอพีที่กล่าวมานั้นมีกระบวนการปิดบังทั้ง 32 บิตของหมายเลขไอพี ซึ่งเมื่อพิจารณาถึงหน้าที่การใช้งานและกระบวนการปิดบังหมายเลขไอพีในสภาพความเป็นจริงแล้วพบว่าไม่มีความจำเป็นที่ต้องปิดบังทั้ง 32 บิตของหมายเลขไอพี แต่อาจสามารถปิดบังเพียงบางบิตหรือเพียงบางส่วนของหมายเลขไอพีได้ตามความจำเป็น ซึ่งขึ้นอยู่กับระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบัง นอกจากนี้กระบวนการปิดบังหมายเลขไอพีส่วนใหญ่มุ่งเน้นในเรื่องของความมั่นคง (Security) มากเกินไป ในขณะที่ยังให้ความสำคัญและให้ความสนใจในเรื่องของความเป็นส่วนตัวที่ไม่เพียงพอ ในสภาพความเป็นจริงของการวิเคราะห์และจัดการเครือข่ายหนึ่ง ๆ จะประกอบไปด้วยวิธีการทำงานและประเภทของการทำงานที่หลากหลายรูปแบบและหลายคุณลักษณะ ซึ่งมีความต้องการและความจำเป็นในการปิดบังหมายเลขไอพีที่แตกต่างกัน เช่น ในการวิเคราะห์สถิติการใช้งานระบบเครือข่ายในภาพรวมหรือข้อมูลอย่างสรุปนั้น ไม่มีความจำเป็นมากในการปิดบังหมายเลขไอพี หรืออาจมีความจำเป็นเพียงแค่การปิดบังบางส่วนของหมายเลขไอพี เพราะในกระบวนการทำงานไม่ได้มีการเจาะจงหรือแสดงถึงรายละเอียดของข้อมูลของหมายเลขไอพีแต่อย่างใด แต่ในกรณีของการทำงานที่เป็นการตรวจสอบระบบเครือข่าย เช่น การค้นหาผู้บุกรุกในเครือข่าย ซึ่งต้องเจาะลงในรายละเอียดของหมายเลขไอพีแต่ละหมายเลข การทำงานแบบนี้จำเป็นอย่างยิ่งในการปิดบังหมายเลขไอพี นอกจากนั้นลักษณะบางประเภทของการวิเคราะห์และจัดการเครือข่ายอาจมีความจำเป็นในการปิดบังหมายเลขไอพีเพียงแค่บางส่วนเท่านั้น เช่น การปิดบังเพียงส่วนของบิตซ้ายหรือส่วนเครือข่ายและส่วนของบิตขวาหรือส่วนเครื่องของหมายเลขไอพี เป็นต้น ซึ่งขึ้นอยู่กับว่าประเภทของการวิเคราะห์และจัดการเครือข่ายประเภทใดจะเหมาะสมและสมควรปิดบังหมายเลขไอพีในส่วนใด

จากเหตุผลข้างต้นนั้น จึงเป็นที่มาของการนำเสนอระดับความเป็นส่วน 5 ระดับ ซึ่งประกอบไปด้วย ระดับที่ไม่มีการปิดบังหมายเลขไอพี ระดับการปิดบังหมายเลขไอพีในส่วน

ของ n บิตซ้าย ระดับการปิดบังหมายเลขไอพีในส่วนของ n บิตขวา ระดับการปิดบังหมายเลขไอพีทั้ง 32 บิต และ ระดับการปิดบังหมายเลขไอพีทั้ง 32 บิต แบบสุ่ม โดยรายละเอียดทั้งหมดจะกล่าวไว้ในหัวข้อถัดไป

3.2 ระดับความเป็นส่วนตัว (Privacy Levels)

ระดับความเป็นส่วนตัว คือ ระดับของการปิดบังหมายเลขไอพีโดยการพิจารณาปัจจัยของความเป็นส่วนตัว ซึ่งมีแนวคิดว่าหมายเลขไอพีประกอบด้วยกลุ่มเครือข่าย (Network Part) หรือกลุ่มบิตซ้ายที่แสดงถึงกลุ่มขององค์กรหรือหน่วยงานในเครือข่าย และกลุ่มเครื่อง (Host Part) หรือกลุ่มบิตขวาที่ระบุถึงจำนวนของเครื่องหรืออุปกรณ์ปลายทางในเครือข่ายทั้งนี้กลุ่มของบิตทั้งสองส่วนจะมีความยาวเท่าไรขึ้นอยู่กับการออกแบบลักษณะของเครือข่ายเหล่านั้นว่าต้องการให้มีรูปแบบเป็นอย่างไรโดยใช้หมายเลขสับเน็ตมาสก์เป็นตัวกำหนดดังแสดงในรูปที่ 3.1



รูปที่ 3.1 การแบ่งส่วนบิตซ้ายและขวาของหมายเลขไอพีโดยใช้หมายเลขสับเน็ตมาสก์

จากตัวอย่างในรูปที่ 3.1 หมายเลขไอพีหมายเลข 161.200.93.16 ถูกแบ่งออกเป็น 2 ส่วนโดยใช้หมายเลขสับเน็ตมาสก์ ดังรายละเอียดต่อไปนี้

1. 161.200.93 คือส่วนบิตซ้ายหรือส่วนเครือข่าย ซึ่งหมายถึงเครือข่ายของภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

2. 16 คือส่วนบิตขวาหรือส่วนเครื่อง ซึ่งหมายถึงหมายเลขเครื่องหรือเลขที่ของอุปกรณ์ที่ใช้งานอยู่ในเครือข่าย 161.200.93

ถ้าทำการปิดบังหมายเลขไอพีเพียงแค่ส่วนของบิตทางซ้ายเพียงอย่างเดียวก็จะสามารถปิดบังความเป็นส่วนตัวได้เพียงเล็กน้อย กล่าวคือ ส่วนของภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย จะถูกปิดบังเอาไว้ แต่ในขณะเดียวกันก็ยังทราบถึงรายละเอียดที่เป็นข้อมูลส่วนตัวที่สำคัญ คือ หมายเลขเครื่องหรือเลขที่ของอุปกรณ์ที่ใช้งานอยู่ในเครือข่ายได้เช่นเดิมเพราะยังไม่ถูกปิดบัง

ถ้าทำการปิดบังในส่วนของบิตทางขวาเพียงอย่างเดียวก็จะทำให้สามารถปิดบังในส่วนของหมายเลขเครื่องหรือเลขที่ของอุปกรณ์ที่ใช้งานอยู่ในเครือข่ายได้ซึ่งมีความเป็นส่วนตัวเพิ่มมากยิ่งขึ้น ถึงแม้ว่าในส่วนของเครือข่ายหรือส่วนของภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ยังไม่ได้ถูกปิดบังก็ตาม

ถ้ามีการปิดบังทั้ง 32 บิตของหมายเลขไอพี ทั้งในส่วนของบิตซ้ายและบิตขวาก็สามารถปิดบังความเป็นส่วนตัวได้สูงสุด ทำให้ไม่สามารถระบุข้อมูลของเครือข่ายและหมายเลขเครื่องที่แท้จริงได้จากรูปแบบของหมายเลขไอพีที่ถูกปิดบัง

จากรายละเอียดข้างต้นจึงสามารถแบ่งระดับความเป็นส่วนตัวออกเป็น 5 ระดับที่แตกต่างกันตามรายละเอียดดังต่อไปนี้

3.2.1 ระดับที่ไม่มีการปิดบัง (Non-Anonymization Level)

ระดับที่ไม่มีการปิดบังเป็นระดับที่ไม่ต้องการความเป็นส่วนตัวและไม่มีความจำเป็นใดๆ ในการปิดบังหมายเลขไอพี ดังนั้นหมายเลขไอพีนิรนามจะมีรูปแบบที่เหมือนกับหมายเลขไอพีดั้งเดิมดังแสดงตามรูปที่ 3.2

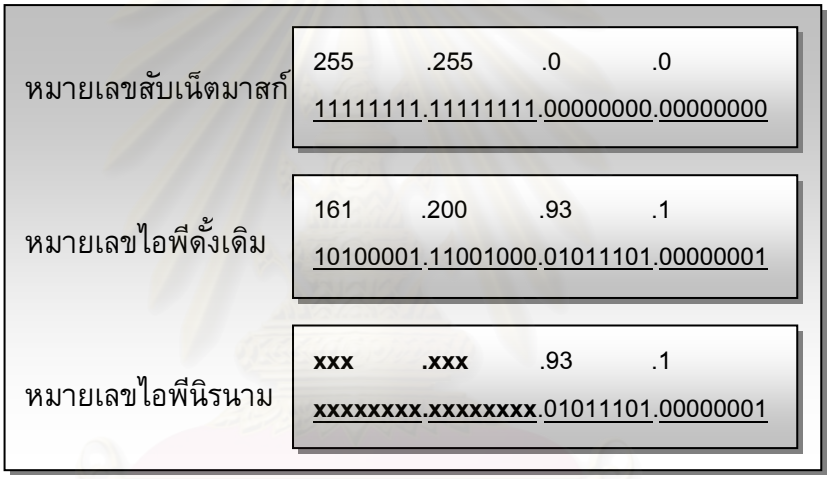
หมายเลขสับเน็ตมาสก์	255 .255 .0 .0 11111111.11111111.00000000.00000000
หมายเลขไอพีดั้งเดิม	161 .200 .93 .1 10100001.11001000.01011101.00000001
หมายเลขไอพีนิรนาม	161 .200 .93 .1 10100001.11001000.01011101.00000001

รูปที่ 3.2 การปิดบังหมายเลขไอพีตามระดับที่ไม่มีการปิดบัง

ระดับความเป็นส่วนตัวระดับนี้เหมาะสำหรับประเภทของการวิเคราะห์และจัดการเครือข่ายที่ไม่สนใจความเป็นส่วนตัวของหมายเลขไอพี เช่น การประมวลผลและสรุปผลค่าสถิติแบบเฉลี่ย หรือการสรุปผลลัพธ์ภาพรวมของเครือข่าย เป็นต้น ซึ่งจะได้นำเสนอรายละเอียดเพิ่มเติมในบทที่ 4 ต่อไป

3.2.2 ระดับการปิดบังส่วน n บิตซ้าย (n-Left Anonymization Level)

ระดับการปิดบังส่วน n บิตซ้าย เป็นระดับที่ต้องการความเป็นส่วนตัวในระดับเครือข่ายโดยปิดบังหมายเลขไอพีในส่วนของกลุ่มเครือข่ายหรือกลุ่มบิตซ้ายที่แสดงถึงกลุ่มขององค์กรหรือหน่วยงานในเครือข่ายดังแสดงตัวอย่างการปิดบังตามรูปที่ 3.3

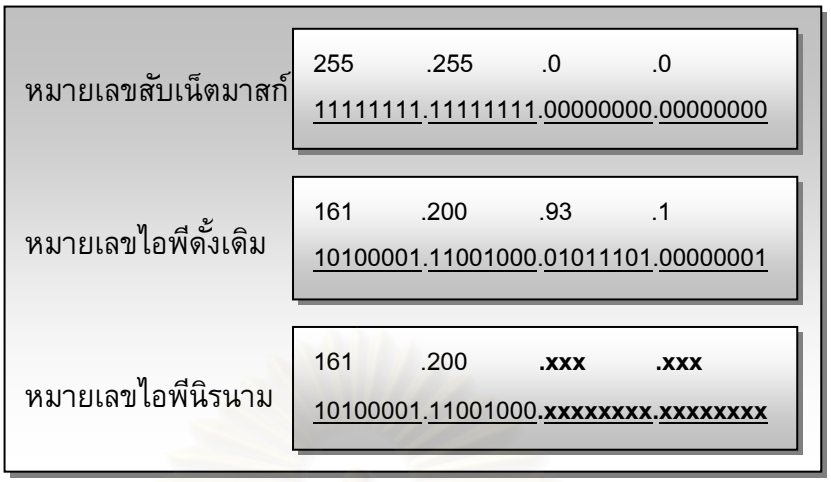


รูปที่ 3.3 การปิดบังหมายเลขไอพีตามระดับการปิดบังส่วน n บิตซ้าย

ระดับความเป็นส่วนตัวระดับนี้เหมาะกับประเภทของการวิเคราะห์และจัดการเครือข่ายที่มีความสนใจหรือมองเห็นความเป็นส่วนตัวของหมายเลขไอพีในส่วนของกลุ่มเครือข่าย เช่น การเปรียบเทียบสถิติการเรียกใช้งานบริการต่างๆ ขององค์กรย่อยในเครือข่าย การเปรียบเทียบข้อมูลทางสถิติระหว่างเครือข่าย เป็นต้น ซึ่งจะได้นำเสนอรายละเอียดเพิ่มเติมในบทที่ 4 ต่อไป

3.2.3 ระดับการปิดบังส่วน n บิตขวา (n-Right Anonymization Level)

ระดับการปิดบังส่วน n บิตขวาเป็นระดับที่ต้องการความเป็นส่วนตัวในระดับตัวเครื่องหรืออุปกรณ์ โดยปิดบังหมายเลขไอพีในส่วนของกลุ่มเครื่องหรือกลุ่มบิตทางขวาที่แสดงถึงหมายเลขเครื่องหรือหมายเลขอุปกรณ์ปลายทางในเครือข่ายดังแสดงตัวอย่างการปิดบังตามรูปที่ 3.4

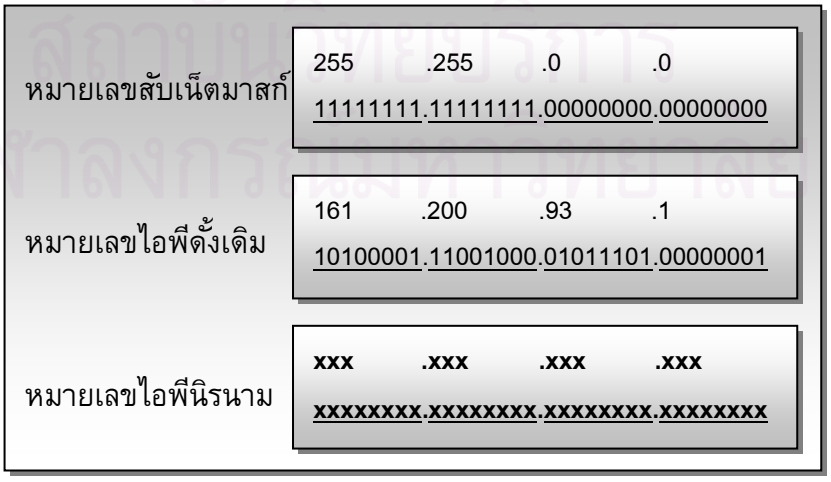


รูปที่ 3.4 การปิดบังหมายเลขไอพีตามระดับการปิดบังส่วน n บิตขวา

ระดับความเป็นส่วนตัวระดับนี้เหมาะกับประเภทของการวิเคราะห์และจัดการเครือข่ายที่มีความสนใจหรือมองเห็นความเป็นส่วนตัวของหมายเลขไอพีในส่วนของกลุ่มเครื่อง เช่น การตรวจสอบการใช้งานซีพียูของอุปกรณ์ การตรวจสอบการใช้งานหน่วยความจำของอุปกรณ์ การนับจำนวนเครื่องและอุปกรณ์ที่เปิดใช้งานในเครือข่าย เป็นต้น ซึ่งจะได้นำเสนอรายละเอียดเพิ่มเติมในบทที่ 4 ต่อไป

3.2.4 ระดับการปิดบังทั้ง 32 บิต (Full Anonymization Level)

ระดับการปิดบังทั้ง 32 บิต เป็นระดับที่ต้องการความเป็นส่วนตัวอย่างสมบูรณ์ โดยปิดบังหมายเลขไอพีทั้งในส่วนของกลุ่มเครือข่ายและกลุ่มเครื่อง ซึ่งทั้ง 32 บิตของหมายเลขไอพีดังแสดงตัวอย่างการปิดบังตามรูปที่ 3.5

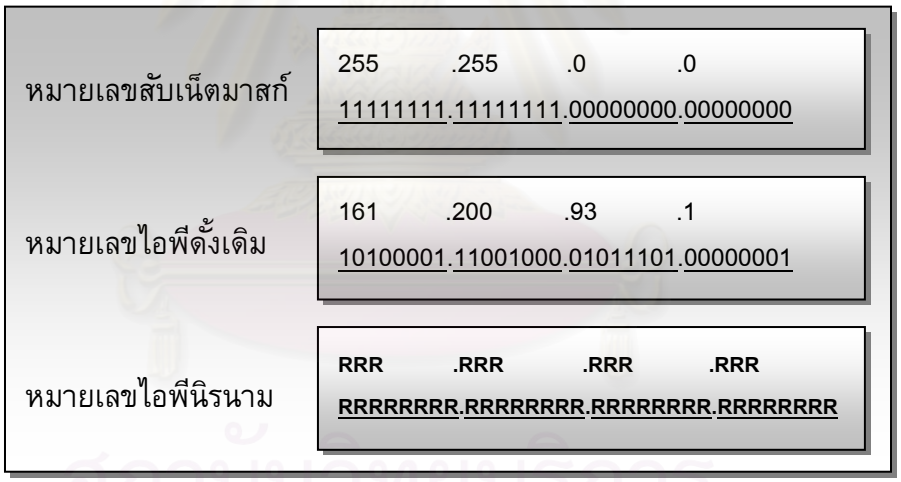


รูปที่ 3.5 การปิดบังหมายเลขไอพีตามระดับการปิดบังทั้ง 32 บิต

ระดับความเป็นส่วนตัวระดับนี้เหมาะกับประเภทของการวิเคราะห์และจัดการเครือข่ายที่มีความสนใจหรือมองเห็นความเป็นส่วนตัวของหมายเลขไอพีทั้งในส่วนของกลุ่มเครือข่ายและกลุ่มเครื่อง หรือทั้ง 32 บิต ของหมายเลขไอพี เช่น การตรวจจับผู้บุกรุก การวิเคราะห์ล็อกไฟล์ การตรวจตราและติดตามผู้ใช้ในเครือข่าย เป็นต้น ซึ่งจะได้นำเสนอรายละเอียดเพิ่มเติมในบทที่ 4 ต่อไป

3.2.5 ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม (Randomly Full Anonymization Level)

ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม เป็นระดับที่ต้องการความเป็นส่วนตัวอย่างสมบูรณ์แต่ไม่สนใจความหมายของหมายเลขไอพี หรือไม่สนใจความสัมพันธ์ของกลุ่มเครือข่าย ซึ่งจะปิดบังหมายเลขไอพีทั้งในส่วนของกลุ่มเครือข่ายและกลุ่มเครื่อง ทั้ง 32 บิตของหมายเลขไอพีแบบสุ่มค่า (Random) ทำให้ไม่คงไว้ซึ่งค่าของกลุ่มเครือข่าย ดังนั้นหมายเลขไอพีนิรนามในระดับนี้จะไม่มีคุณสมบัติเหมือนกับหมายเลขไอพีดั้งเดิมและยากอย่างยิ่งต่อการแปลงย้อนกลับมาเป็นหมายเลขไอพีดังเดิมดังแสดงตัวอย่างการปิดบังตามรูปที่ 3.6



รูปที่ 3.6 การปิดบังหมายเลขไอพีตามระดับการปิดบังทั้ง 32 บิตแบบสุ่ม

ระดับความเป็นส่วนตัวระดับนี้เหมาะกับประเภทของการวิเคราะห์และจัดการเครือข่ายที่แสดงผลต่อสาธารณะชน เช่น การแสดงผลและรายงานผล การส่งผลลัพธ์ที่ได้จากการประมวลผลไปยังบุคคลภายนอกเครือข่าย เป็นต้น ซึ่งจะได้นำเสนอรายละเอียดเพิ่มเติมในบทที่ 4 ต่อไป

จากระดับความเป็นส่วนตัวทั้ง 5 ระดับที่ได้กล่าวมานั้น สามารถสรุปเป็นตารางได้ดังตารางที่ 3.1 ต่อไปนี้

ตารางที่ 3.1 ตารางแสดงระดับความเป็นส่วนตัวของหมายเลขไอพี

ระดับที่	ระดับความเป็นส่วนตัว	นิยามการปิดบัง	ส่วนของการปิดบัง	
			ส่วนเครือข่าย	ส่วนเครื่อง
1	ระดับที่ไม่มีการปิดบัง	ไม่ปิดบังทั้ง 32 บิตของหมายเลขไอพี	ไม่ปิดบัง	ไม่ปิดบัง
2	ระดับการปิดบังส่วน n บิตซ้าย	ปิดบังเพียงส่วนบิตซ้ายหรือส่วนเครือข่ายของหมายเลขไอพี	ปิดบัง	ไม่ปิดบัง
3	ระดับการปิดบังส่วน n บิตขวา	ปิดบังเพียงส่วนบิตขวาหรือส่วนเครื่องของหมายเลขไอพี	ไม่ปิดบัง	ปิดบัง
4	ระดับการปิดบังทั้ง 32 บิต	ปิดบังทั้ง 32 บิตของหมายเลขไอพี	ปิดบัง	ปิดบัง
5	ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม	ปิดบังทั้ง 32 บิตของหมายเลขไอพีแบบสุ่ม	ปิดบังแบบสุ่ม	ปิดบังแบบสุ่ม

ในกระบวนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัวทั้ง 5 ระดับที่กล่าวมาในบทนี้ ต้องนำมาพิจารณาเลือกระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังโดยใช้ปัจจัยการปิดบังซึ่งจะได้กล่าวรายละเอียดในบทต่อไป

บทที่ 4

ปัจจัยการปิดบังหมายเลขไอพี

บทนี้เป็นการนำเสนอปัจจัยการปิดบังหมายเลขไอพี 3 ปัจจัย เพื่อใช้พิจารณาเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุดสำหรับการปิดบังหมายเลขไอพี โดยรายละเอียดของปัจจัยการปิดบังหมายเลขไอพีมีดังต่อไปนี้

4.1 ขอบเขตในการกำหนดปัจจัยการปิดบังหมายเลขไอพี

การพิจารณาเพื่อปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวทั้ง 5 ระดับที่กล่าวไว้ในบทที่ 3 นั้นมีขอบเขตและเหตุผล 3 ประการที่ใช้ในการกำหนดปัจจัยการปิดบัง ซึ่งมีรายละเอียดดังต่อไปนี้

1. ผู้ที่ต้องการใช้งานข้อมูลรับรู้และคุ้นเคยกับโครงสร้างของหมายเลขไอพีของเครือข่ายที่จะใช้งานมากน้อยเพียงใด

2. ผู้ที่ต้องการใช้งานข้อมูลต้องการใช้ข้อมูลส่วนใด และใช้อย่างไรในกระบวนการวิเคราะห์และจัดการเครือข่าย

3. กฎหมายคอมพิวเตอร์กล่าวไว้ว่าอย่างไรเกี่ยวกับการปิดบังหมายเลขไอพีและการใช้งานข้อมูลส่วนบุคคล

จากเหตุผล 3 ประการดังกล่าวได้มาซึ่งปัจจัยที่ใช้เพื่อพิจารณาในการปิดบังหมายเลขไอพีให้เป็นไปตามระดับความเป็นส่วนตัวที่เหมาะสม ซึ่งประกอบไปด้วย 3 ปัจจัยหลักดังต่อไปนี้

1. โครงสร้างของหมายเลขไอพี (IP Address Structure)

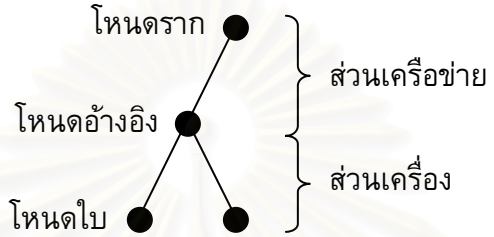
2. รายการวิเคราะห์เครือข่าย (Network Analysis Functions)

3. กฎหมายคอมพิวเตอร์ (Computer Law)

รายละเอียดของปัจจัยการปิดบังหมายเลขไอพีทั้ง 3 ปัจจัยจะกล่าวไว้ในหัวข้อที่ 4.2 ถึง 4.4 ตามลำดับ

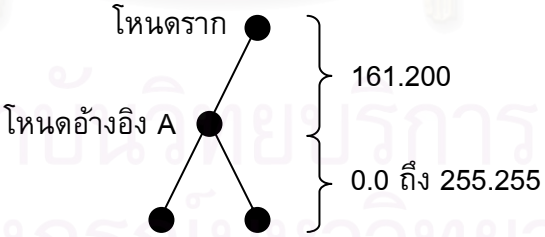
4.2 โครงสร้างของหมายเลขไอพี (IP Address Structure)

เมื่อพิจารณาโครงสร้างของหมายเลขไอพี่ขององค์กรใดๆ ที่ต้องการแลกเปลี่ยนข้อมูลกันนั้น พบว่ามีรูปแบบโครงสร้างของหมายเลขไอพี่ที่มีความสัมพันธ์กันในหลากหลายรูปแบบ โดยงานวิจัยเรื่องนี้ได้นำเสนอเป็นโครงสร้างต้นไม้ของความเป็นส่วนตัว (Privacy Tree Structures) โดยมีรายละเอียดและองค์ประกอบดังต่อไปนี้



รูปที่ 4.1 องค์ประกอบของโครงสร้างต้นไม้ของความเป็นส่วนตัว

กำหนดให้ ต้นไม้ (Tree) แทนโครงสร้างของของหมายเลขไอพีขององค์กรใดองค์กรหนึ่ง โหนด (Node) แทนจุดเชื่อม (Connector) ระหว่างส่วนเครือข่ายและส่วนเครื่องของหมายเลขไอพี และเส้นเชื่อม (Edge) แทนส่วน (Part) ของหมายเลขไอพีซึ่งได้แก่ส่วนเครือข่ายและส่วนเครื่อง จะได้ว่าเส้นทางจากโหนดรากจนถึงโหนดอ้างอิงคือส่วนเครือข่ายของหมายเลขไอพี และเส้นทางจากโหนดอ้างอิงถึงโหนดใบคือส่วนเครื่องของหมายเลขไอพี ถ้ากำหนดให้องค์กร A มีโครงสร้างของหมายเลขไอพีเป็น 161.200.0.0 และหมายเลขสับเน็ตมาสก์เป็น 255.255.0.0 จะได้รูปแบบของโครงสร้างต้นไม้ของความเป็นส่วนตัวดังรูปที่ 4.2

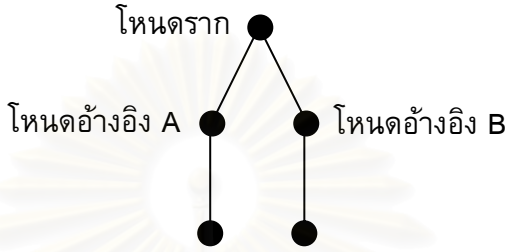


รูปที่ 4.2 โครงสร้างต้นไม้ของความเป็นส่วนตัวขององค์กร A ที่มีโครงสร้างของหมายเลขไอพีเป็น 161.200.0.0 และหมายเลขสับเน็ตมาสก์เป็น 255.255.0.0

จากโครงสร้างต้นไม้ของความเป็นส่วนตัว เมื่อนำโครงสร้างต้นไม้ของสององค์กรใดๆ มาพิจารณารูปแบบความสัมพันธ์ร่วมกัน โดยกำหนดให้องค์กร A แทนองค์กรที่เป็นผู้วิเคราะห์ข้อมูล และองค์กร B เป็นองค์กรที่ถูกวิเคราะห์ข้อมูลโดยองค์กร A จะทำให้ได้รูปแบบความสัมพันธ์เป็น 5 รูปแบบดังต่อไปนี้

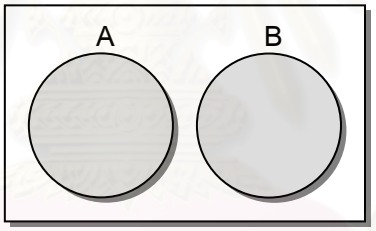
4.2.1 ต้นไม้ที่เป็นอิสระต่อกัน (Independent Subtree)

รูปแบบความสัมพันธ์ของต้นไม้ที่เป็นอิสระต่อกัน คือ ความสัมพันธ์ของโครงสร้างต้นไม้ของความเป็นส่วนตัวที่ได้จากโครงสร้างของหมายเลขไอพีขององค์กร A และองค์กร B ไม่มีส่วนเกี่ยวข้องกัน หรือไม่มีความสัมพันธ์ใดๆ ต่อกัน ดังแสดงในรูปที่ 4.3



รูปที่ 4.3 โครงสร้างต้นไม้ที่เป็นอิสระต่อกัน

จากโครงสร้างต้นไม้ที่เป็นอิสระต่อกันสามารถแสดงให้อยู่ในรูปของเซตที่เป็นอิสระต่อกัน (Independent Set) ได้ดังรูปที่ 4.4

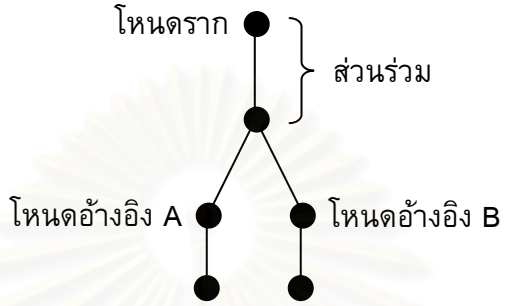


รูปที่ 4.4 โครงสร้างเซตที่เป็นอิสระต่อกัน

ตัวอย่างองค์กรสององค์กรที่มีความสัมพันธ์ในรูปแบบของต้นไม้ที่เป็นอิสระต่อกัน เช่น องค์กร A ซึ่งคือ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย มีโครงสร้างหมายเลขไอพีเป็น 161.200.93.0 และองค์กร B ซึ่งคือบริษัทไมโครซอฟต์ มีโครงสร้างหมายเลขไอพีเป็น 207.46.0.0 โดยองค์กรสององค์กรดังกล่าวมีโครงสร้างของหมายเลขไอพีที่เป็นอิสระต่อกันและไม่เกี่ยวข้องกันเลย ดังนั้นความสัมพันธ์รูปแบบนี้ใช้ระดับความเป็นส่วนตัวในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง (Non-Anonymization Levels) เหตุผลที่ใช้ระดับการปิดบังดังกล่าวเพราะว่า จากโครงสร้างของหมายเลขไอพีที่เป็นอิสระต่อกัน แสดงให้เห็นว่าสององค์กรดังกล่าวไม่ได้คุ้นเคย รู้จัก และเกี่ยวข้องกันมาก่อน ถ้าพิจารณาเพียงแค่ส่วนของโครงสร้างของหมายเลขไอพีโดยไม่ได้สนใจถึงความสัมพันธ์ในส่วนอื่น

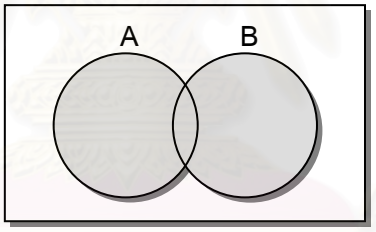
4.2.2 ต้นไม้ที่มีส่วนร่วมกัน (Intersection Subtree)

รูปแบบความสัมพันธ์ของต้นไม้ที่มีส่วนร่วมกัน คือ ความสัมพันธ์ของโครงสร้างต้นไม้ของความเป็นส่วนตัวที่ได้จากโครงสร้างของหมายเลขไอพีขององค์กร A และองค์กร B มีส่วนเครือข่ายหรือบางส่วนของส่วนเครือข่ายของหมายเลขไอพีที่เหมือนกัน ดังแสดงในรูปที่ 4.5



รูปที่ 4.5 โครงสร้างต้นไม้ที่มีส่วนร่วมกัน

จากโครงสร้างต้นไม้ที่มีส่วนร่วมกันสามารถแสดงให้อยู่ในรูปของเซตที่มีส่วนร่วมกัน (Intersection Set) ได้ดังรูปที่ 4.6



รูปที่ 4.6 โครงสร้างเซตที่มีส่วนร่วมกัน

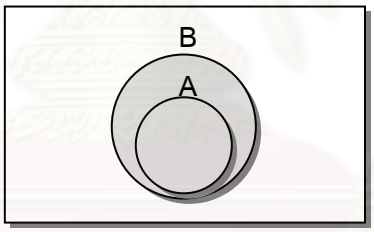
ตัวอย่างองค์กรสององค์กรที่มีความสัมพันธ์ในรูปแบบของต้นไม้ที่มีส่วนร่วมกัน เช่น องค์กร A ซึ่งคือ สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet) มีโครงสร้างหมายเลขไอพีเป็น 202.28.0.0 และองค์กร B ซึ่งคือมหาวิทยาลัยสงขลานครินทร์ มีโครงสร้างหมายเลขไอพีเป็น 202.12.0.0 ซึ่งองค์กรสององค์กรดังกล่าวมีโครงสร้างของหมายเลขไอพีที่มีส่วนที่ร่วมกันนั่นคือส่วนของ 202 โดยเป็นส่วนหนึ่งของส่วนเครือข่าย ดังนั้นความสัมพันธ์รูปแบบนี้ใช้ระดับความเป็นส่วนตัวในการปิดบังหมายเลขไอพีคือระดับที่มีการปิดบังส่วน n บิตซ้าย (*n*-Left Anonymization Levels) เหตุผลที่ใช้ระดับการปิดบังดังกล่าวเพราะว่า โครงสร้างของหมายเลขไอพีมีส่วนเกี่ยวข้องกันเพียงแค่ส่วนของเครือข่ายหรือส่วนของบิตซ้ายบางบิต ซึ่งถ้าพิจารณาเฉพาะโครงสร้างของหมายเลขไอพีโดยไม่ได้สนใจถึงความสัมพันธ์ในส่วนอื่นสามารถแสดงให้เห็นว่า สององค์กรดังกล่าวมีความคุ้นเคย รู้จัก และเกี่ยวข้องกันเฉพาะส่วนเครือข่ายเท่านั้น ระดับการปิดบังส่วน n บิตซ้ายจึงเหมาะสม

4.2.3 ต้นไม้ที่เป็นส่วนย่อยแท้แบบ A อยู่ใน B (Proper Subtree : A in B)

รูปแบบความสัมพันธ์ของต้นไม้ที่เป็นส่วนย่อยแท้แบบ A อยู่ใน B คือ ความสัมพันธ์ของโครงสร้างต้นไม้ของความเป็นส่วนตัวที่ได้จากโครงสร้างของหมายเลขไอพีขององค์กร A อยู่ภายในองค์กร B ดังแสดงในรูปที่ 4.7

รูปที่ 4.7 โครงสร้างต้นไม้ที่เป็นส่วนย่อยแท้แบบ A อยู่ใน B

จากโครงสร้างต้นไม้ที่เป็นส่วนย่อยแท้แบบ A อยู่ใน B สามารถแสดงให้อยู่ในรูปของเซตที่เป็นสับเซตแท้ (Proper Subset) ได้ดังรูปที่ 4.8



รูปที่ 4.8 โครงสร้างเซตที่เป็นสับเซตแท้แบบ A อยู่ใน B

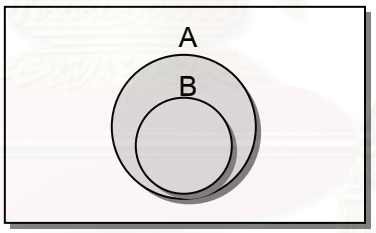
ตัวอย่างองค์กรสององค์กรที่มีความสัมพันธ์ในรูปแบบของต้นไม้ที่เป็นส่วนย่อยแท้แบบ A อยู่ใน B เช่น องค์กร A ซึ่งคือ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย มีโครงสร้างหมายเลขไอพีเป็น 161.200.93.0 และองค์กร B ซึ่งคือ จุฬาลงกรณ์มหาวิทยาลัย มีโครงสร้างหมายเลขไอพีเป็น 161.200.0.0 ซึ่งองค์กร A มีโครงสร้างของหมายเลขไอพีอยู่ภายในองค์กร B ดังนั้นความสัมพันธ์รูปแบบนี้ใช้ระดับความเป็นส่วนตัวในการปิดบังหมายเลขไอพีคือระดับที่มีการปิดบังส่วน n บิตขวา (*n*-Right Anonymization Levels) เหตุผลที่ใช้ระดับการปิดบังดังกล่าวเพราะว่า โครงสร้างของหมายเลขไอพีมีส่วนซ้อนทับกันซึ่งแสดงให้เห็นว่าองค์กร A เป็นหน่วยย่อยหนึ่งขององค์กร B ซึ่งถ้าพิจารณาเฉพาะโครงสร้างของหมายเลขไอพีโดยไม่ได้สนใจถึงความสัมพันธ์ในส่วนอื่นสามารถแสดงให้เห็นว่า สององค์กรดังกล่าวต้องรู้จักกันในระดับเครื่องเพราะว่าอยู่ในองค์กรใหญ่เดียวกัน ดังนั้นระดับการปิดบังส่วน n บิตขวาจึงเหมาะสม

4.2.4 ต้นไม้ที่เป็นส่วนย่อยแท้แบบ B อยู่ใน A (Proper Subtree : B in A)

รูปแบบความสัมพันธ์ของต้นไม้ที่เป็นส่วนย่อยแท้แบบ B อยู่ใน A คือ ความสัมพันธ์ของโครงสร้างต้นไม้ของความเป็นส่วนตัวที่ได้จากโครงสร้างของหมายเลขไอพีขององค์กร B อยู่ภายในองค์กร A หรือกล่าวอีกนัยคือ องค์กร A มีองค์กร B อยู่ภายใน ดังแสดงในรูปที่ 4.9

รูปที่ 4.9 โครงสร้างต้นไม้ที่เป็นส่วนย่อยแท้แบบ B อยู่ใน A

จากโครงสร้างต้นไม้ที่เป็นส่วนย่อยแท้แบบ B อยู่ใน A สามารถแสดงให้อยู่ในรูปของเซตที่เป็นสับเซตแท้ (Proper Subset) ได้ดังรูปที่ 4.10

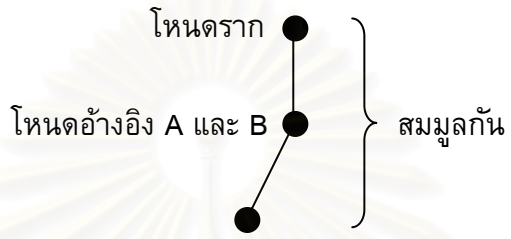


รูปที่ 4.10 โครงสร้างเซตที่เป็นสับเซตแท้แบบ B อยู่ใน A

ตัวอย่างองค์กรสององค์กรที่มีความสัมพันธ์ในรูปแบบของต้นไม้ที่เป็นส่วนย่อยแท้แบบ B อยู่ใน A เช่น องค์กร A ซึ่งคือ จุฬาลงกรณ์มหาวิทยาลัย มีโครงสร้างหมายเลขไอพีเป็น 161.200.0.0 และองค์กร B ซึ่งคือ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย มีโครงสร้างหมายเลขไอพีเป็น 161.200.93.0 ซึ่งองค์กร B มีโครงสร้างของหมายเลขไอพีอยู่ภายในองค์กร A ดังนั้นความสัมพันธ์รูปแบบนี้ใช้ระดับความเป็นส่วนตัวในการปิดบังหมายเลขไอพีคือระดับที่มีการปิดบังส่วน n บิตขวา เหตุผลที่ใช้ระดับการปิดบังดังกล่าวเพราะว่า โครงสร้างของหมายเลขไอพีมีส่วนซ้อนทับกันโดยที่องค์กร B เป็นหน่วยย่อยหนึ่งขององค์กร A ซึ่งถ้าพิจารณาเฉพาะโครงสร้างของหมายเลขไอพีโดยไม่สนใจถึงความสัมพันธ์ในส่วนอื่นสามารถแสดงให้เห็นว่า สององค์กรดังกล่าวต้องรู้จักกันในระดับเครือเพราะว่าอยู่ในองค์กรใหญ่เดียวกัน ดังนั้นระดับการปิดบังส่วน n บิตขวาจึงเหมาะสม

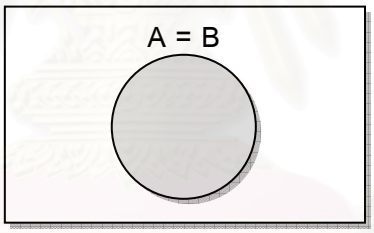
4.2.5 ต้นไม้ที่สมมูลกัน (Equivalent Subtree)

รูปแบบความสัมพันธ์ของต้นไม้ที่สมมูลกัน คือ ความสัมพันธ์ของโครงสร้างต้นไม้ของความเป็นส่วนตัวที่ได้จากโครงสร้างของหมายเลขไอพีขององค์กร A เท่ากับหรือเหมือนกันทุกประการกับองค์กร B ดังแสดงในรูปที่ 4.11



รูปที่ 4.11 โครงสร้างต้นไม้ที่สมมูลกัน

จากโครงสร้างต้นไม้ที่สมมูลกัน สามารถแสดงให้อยู่ในรูปของเซตที่สมมูลกัน (Equivalent Set) ได้ดังรูปที่ 4.12



รูปที่ 4.12 โครงสร้างเซตที่สมมูลกัน

ตัวอย่างองค์กรสององค์กรที่มีความสัมพันธ์ในรูปแบบของต้นไม้ที่สมมูลกัน เช่น องค์กร A ซึ่งคือ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย มีโครงสร้างหมายเลขไอพีเป็น 161.200.93.0 และองค์กร B ซึ่งคือ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย มีโครงสร้างหมายเลขไอพีเป็น 161.200.93.0 เช่นกัน ซึ่งองค์กร A มีโครงสร้างของหมายเลขไอพีที่เหมือนกันทุกประการกับองค์กร B ดังนั้นความสัมพันธ์รูปแบบนี้ใช้ระดับความเป็นส่วนตัวในการปิดบังหมายเลขไอพีคือระดับที่มีการปิดบังทั้ง 32 บิต (Full Anonymization Levels) เหตุผลที่ใช้ระดับการปิดบังดังกล่าวเพราะว่า โครงสร้างของหมายเลขไอพีเหมือนกันทุกประการ ซึ่งถ้าพิจารณาเฉพาะโครงสร้างของหมายเลขไอพีโดยไม่สนใจถึงความสัมพันธ์ในส่วนอื่นสามารถแสดงให้เห็นว่า สององค์กรดังกล่าวคือองค์กรเดียวกัน ดังนั้นระดับการปิดบังทั้ง 32 บิตจึงเหมาะสม

จากรูปแบบต้นไม้ของความเป็นส่วนตัวทั้ง 5 รูปแบบ สามารถสรุปรายละเอียดได้ตามตารางที่ 4.1 ดังต่อไปนี้

ตารางที่ 4.1 ตารางสรุปรายละเอียดของต้นไม้ของความเป็นส่วนตัว

รูปแบบ	ต้นไม้ของความเป็นส่วนตัว	ระดับความเป็นส่วนตัว
1	ต้นไม้ที่เป็นอิสระต่อกัน	ระดับที่ไม่มีการปิดบัง
2	ต้นไม้ที่มีส่วนร่วมกัน	ระดับการปิดบังส่วน n บิตซ้าย
3	ต้นไม้ที่เป็นส่วนย่อยแท้แบบ A อยู่ใน B	ระดับการปิดบังส่วน n บิตขวา
4	ต้นไม้ที่เป็นส่วนย่อยแท้แบบ B อยู่ใน A	ระดับการปิดบังส่วน n บิตขวา
5	ต้นไม้ที่สมมูลกัน	ระดับการปิดบังทั้ง 32 บิต

4.3 รายการวิเคราะห์เครือข่าย (Network Analysis Functions)

เมื่อทำการศึกษาถึงรายละเอียดของรายการวิเคราะห์เครือข่ายจากโปรแกรมและซอฟต์แวร์สำเร็จรูปที่ใช้งานในระบบเครือข่ายปัจจุบันซึ่งได้แก่ เอ็นท็อป (NTOP) [12] นากิออส (Nagios) [11] อ๊อปเมเนเจอร์ (OpManager) [9] ทีซีพีดัมพ์ (Tcpdump) [19] อีเทอเรียล (Ethereal) [3] เอ็มอาร์ทีจี (MRTG) [13] โอเพ็นเอ็นเอ็มเอส (OpenNMS) [14] และ อีโกเน็ต (EgoNet) [18] พบว่ารายการและหน้าที่งานของการวิเคราะห์เครือข่ายแต่ละรายการนั้นมีระดับการมองเห็นและใช้งานข้อมูลที่แตกต่างกัน บางกรณีต้องการวิเคราะห์ข้อมูลเพียงส่วนเครือข่ายของหมายเลขไอพีเท่านั้น บางกรณีก็เพียงส่วนเครื่องเท่านั้น หรือบางกรณีต้องการวิเคราะห์ทั้งส่วนเครือข่ายและส่วนเครื่อง ดังนั้นจึงแสดงให้เห็นว่ารายการวิเคราะห์เครือข่ายแต่ละรายการนั้นมีระดับความเป็นส่วนตัวที่แตกต่างกัน ซึ่งสอดคล้องกับระดับความเป็นส่วนตัวที่ได้นำเสนอไว้ในบทที่ 3 โดยจากการศึกษารายการวิเคราะห์เครือข่ายสามารถจำแนกออกได้เป็น 4 กลุ่มรายการ ซึ่งแต่ละกลุ่มรายการประกอบไปด้วยรายการวิเคราะห์เครือข่ายที่สำคัญดังรายละเอียดต่อไปนี้

4.3.1 การใช้งานทรัพยากรและปริมาณข้อมูล (Resource and Capacity Usages)

1. การวิเคราะห์ประสิทธิภาพของเครือข่าย (Network Performances Analysis) เป็นการวิเคราะห์ประสิทธิภาพการทำงานของเครือข่าย เช่น ดูความเร็ว ดูข้อมูลเข้าออก ซึ่งเป็นข้อมูลที่เป็นภาพรวมอย่างสรุปของเครือข่าย และไม่ได้เจาะจงในรายละเอียดของกลุ่มเครือข่ายและกลุ่มเครื่องหรือกลุ่มของผู้ใช้งานแต่อย่างใด ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง

2. การใช้งานแบนด์วิดธ์ของเครือข่าย (Network Bandwidth Usages) เป็นการตรวจดูและวิเคราะห์ปริมาณการจราจรของเครือข่ายหรือปริมาณเข้าออกของข้อมูลในเครือข่าย ณ เวลาหนึ่งๆ ซึ่งเป็นการใช้ข้อมูลอย่างสรุปของเครือข่ายเพื่อดูความหนาแน่นของช่องสัญญาณโดยไม่ได้เจาะจงในรายละเอียดของกลุ่มเครือข่ายและกลุ่มเครื่องหรือกลุ่มของผู้ใช้งานแต่อย่างใด ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง

3. การวางแผนปริมาณข้อมูล (Capacity Planning) เป็นการวางแผนเพื่อออกแบบ สร้าง และปรับปรุงระบบเครือข่าย และเป็นการวิเคราะห์ทรัพยากรที่ใช้งานในเครือข่าย เช่น ความเร็วในการส่งข้อมูล ขนาดของแบนด์วิดธ์ และข้อมูลพื้นฐานต่างๆ ของระบบเครือข่าย ซึ่งใช้ข้อมูลอย่างสรุปของเครือข่ายและไม่ได้เจาะจงในรายละเอียดของกลุ่มเครือข่ายและกลุ่มเครื่องหรือกลุ่มของผู้ใช้งานแต่อย่างใด ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง

4. การวิเคราะห์การจราจรมัลติคาสท์ (Multicast Traffic Analysis) เป็นการวิเคราะห์กลุ่มมัลติคาสท์ และการส่งข้อมูลภายในกลุ่มมัลติคาสท์เดียวกันของเครือข่าย ซึ่งการทำงานแบบนี้จะสนใจในส่วนเครือข่ายของหมายเลขไอพีเพื่อดูความสัมพันธ์ของกลุ่มมัลติคาสท์ที่มาจากกลุ่มเดียวกัน ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตซ้าย

5. การใช้งานซีพียู (CPU Usages) เป็นการตรวจสอบผลการใช้งานซีพียูของอุปกรณ์หรือของผู้ใช้งานในเครือข่าย ซึ่งจะสนใจเฉพาะส่วนของเครื่องของหมายเลขไอพีเพื่อเป็นการระบุหมายเลขเครื่องหรือหมายเลขอุปกรณ์ว่ามีสถิติการใช้ซีพียูเป็นอย่างไรบ้าง ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

6. การใช้งานหน่วยความจำ (Memory Usages) เป็นการตรวจสอบผลการใช้งานหน่วยความจำของอุปกรณ์หรือของผู้ใช้งานในเครือข่าย ซึ่งจะสนใจเฉพาะส่วนของเครื่องของหมายเลขไอพี เพื่อเป็นการระบุหมายเลขเครื่องหรือหมายเลขอุปกรณ์ว่ามีข้อมูลการใช้งานหน่วยความจำเป็นอย่างไรบ้าง ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

7. การใช้งานดิสก์ (Disk Usages) เป็นการตรวจสอบผลการใช้งานฮาร์ดดิสของอุปกรณ์หรือของผู้ใช้ในเครือข่าย ซึ่งจะสนใจเฉพาะส่วนของเครื่องของหมายเลขไอพี เพื่อเป็นการระบุหมายเลขเครื่องหรือหมายเลขอุปกรณ์ว่ายังมีพื้นที่ของหน่วยความจำที่ใช้

แล้วและยังไม่ใช้เป็นเท่าใดบ้าง ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

8. การใช้งานของบัญชีผู้ใช้ (Accounting Usages) เป็นการบริหารจัดการการใช้ทรัพยากรของผู้ใช้งานในเครือข่าย เช่น การใช้งานเครื่องพิมพ์ การบันทึกจำนวนชั่วโมงการใช้งานเครือข่าย การบันทึกสถิติการเปิดใช้อุปกรณ์ เป็นต้น ซึ่งการใช้งานแบบนี้จะสนใจเฉพาะส่วนของเครื่องของหมายเลขไอพี เพื่อเป็นการระบุหมายเลขเครื่องหรือหมายเลขอุปกรณ์ว่ามีบัญชีการใช้ทรัพยากรของระบบเป็นอย่างไรบ้าง ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

9. การจัดการพร๊อกซี่ (Proxy Management) เป็นการบริหารจัดการและตรวจสอบการทำงานของพร๊อกซี่ของระบบเครือข่าย เช่น การแบ่งประเภทของพร๊อกซี่ตามลักษณะการทำงาน การปรับแต่งพร็อกซีของเครือข่าย การจำกัดการควบคุมการเข้าสู่เว็บไซต์จากเครื่องพร็อกซี่เซิร์ฟเวอร์ (Proxy Server) เป็นต้น ซึ่งการจัดการพร๊อกซี่นี้จะเกี่ยวข้องกับข้อมูลหมายเลขไอพีทั้งในส่วนเครือข่ายและส่วนเครื่อง ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต

4.3.2 สถิติของบริการที่เปิดใช้และให้บริการ (Service Statistics)

1. บริการเอชทีทีพี (HTTP Service) เป็นบริการของการใช้งานเว็บไซต์โดยประกอบไปด้วยการวิเคราะห์ผลลัพธ์ในภาพรวมของบริการเอชทีทีพีในเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง การวิเคราะห์ผลลัพธ์ของกลุ่มเครือข่ายย่อยในเครือข่ายหลัก ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตซ้าย และการวิเคราะห์ผลลัพธ์ของบริการเอชทีทีพีจากเครื่องแต่ละเครื่อง ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

2. บริการเอสเอ็นเอ็มพี (SNMP Service) เป็นบริการของการจัดการและดูแลเครือข่ายผ่านทางโปรโตคอลเอสเอ็นเอ็มพี โดยประกอบไปด้วยการจัดการเครือข่ายในภาพรวม ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง การจัดการของกลุ่มเครือข่ายย่อยในเครือข่ายหลัก ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตซ้าย และการจัดการเครื่องแต่ละเครื่องในเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

3. บริการเทลเน็ต (TELNET Service) เป็นบริการของการติดต่อเข้าไปทำงานในเครื่องบริการผ่านทางพอร์ต (Port) หมายเลข 23 โดยประกอบไปด้วยการวิเคราะห์ข้อมูลการเทลเน็ตในภาพรวมของเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง การวิเคราะห์ผลลัพธ์ของกลุ่มเครือข่ายย่อยในเครือข่ายหลัก ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตซ้าย และการวิเคราะห์ข้อมูลการเทลเน็ตของเครื่องแต่ละเครื่องในเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

4. บริการพีโอพีสามหรือป๊อปสาม (POP3 Service) เป็นบริการทางด้านการจัดการอีเมลล์ (E-Mail) โดยประกอบไปด้วยการวิเคราะห์ข้อมูลบริการป๊อปสามในภาพรวมของเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง การวิเคราะห์ข้อมูลบริการของกลุ่มเครือข่ายย่อยในเครือข่ายหลัก ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตซ้าย และการวิเคราะห์ข้อมูลบริการป๊อปสามของเครื่องแต่ละเครื่องในเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

5. บริการเอ็นเอ็นทีพี (NNTP Service) เป็นบริการของการถ่ายโอนข้อมูลแบบใหม่โดยใช้โปรโตคอลเอ็นเอ็นทีพี โดยประกอบไปด้วยการวิเคราะห์ข้อมูลเอ็นเอ็นทีพีในภาพรวมของเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง การวิเคราะห์ข้อมูลของกลุ่มเครือข่ายย่อยในเครือข่ายหลัก ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตซ้าย และการวิเคราะห์ข้อมูลเอ็นเอ็นทีพีของเครื่องแต่ละเครื่องในเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

6. การใช้โปรโตคอลเออาร์พี/ไอซีเอ็มพี (ARP/ICMP Usages) เป็นการใช้งานการปิง (Ping) เพื่อตรวจสอบการมีอยู่ของเครื่อง โดยในการวิเคราะห์นั้นอาจเป็นการวิเคราะห์การใช้โปรโตคอลเออาร์พี/ไอซีเอ็มพีในภาพรวมของเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง หรือการวิเคราะห์ข้อมูลของกลุ่มเครือข่ายย่อยในเครือข่ายหลัก ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตซ้าย หรืออาจเป็นการวิเคราะห์การใช้โปรโตคอลเออาร์พี/ไอซีเอ็มพีของเครื่องแต่ละเครื่องในเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

7. บริการเอฟทีพี (FTP Service) เป็นการบริการของการถ่ายโอนไฟล์ข้อมูลระหว่างอุปกรณ์ในเครือข่ายผ่านทางโปรโตคอลเอฟทีพี โดยในการวิเคราะห์บริการของเอฟทีพี

นั้นอาจเป็นการวิเคราะห์ในภาพรวมของเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง หรือการวิเคราะห์ข้อมูลของกลุ่มเครือข่ายย่อยในเครือข่ายหลัก ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตซ้าย หรืออาจเป็นการวิเคราะห์ของเครื่องแต่ละเครื่องในเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

8. บริการเอสเอสเอช (SSH Service) เป็นบริการของการติดต่อระหว่างเครื่องในเครือข่ายอย่างปลอดภัย โดยในการวิเคราะห์บริการของเอสเอสเอชนั้นอาจเป็นการวิเคราะห์ในภาพรวมของเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง หรือการวิเคราะห์ข้อมูลของกลุ่มเครือข่ายย่อยในเครือข่ายหลัก ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตซ้าย หรืออาจเป็นการวิเคราะห์ของเครื่องแต่ละเครื่องในเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

9. บริการวีโอไอพี (VoIP Service) เป็นบริการของการส่งข้อมูลเสียงผ่านทางระบบเครือข่าย โดยในการวิเคราะห์บริการของวีโอไอพีนั้นอาจเป็นการวิเคราะห์ในภาพรวมของเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง หรือการวิเคราะห์ข้อมูลของกลุ่มเครือข่ายย่อยในเครือข่ายหลัก ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตซ้าย หรืออาจเป็นการวิเคราะห์ของเครื่องแต่ละเครื่องในเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

10. บริการพีทูพี (P2P Service) เป็นบริการแบบเพียร์ทูเพียร์ (Peer-to-Peer) ของระบบเครือข่าย เช่น บิตทอเร็นท์ (Bittorrent) โดยในการวิเคราะห์บริการของพีทูพีนั้นอาจเป็นการวิเคราะห์ในภาพรวมของเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง หรือการวิเคราะห์ข้อมูลของกลุ่มเครือข่ายย่อยในเครือข่ายหลัก ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตซ้าย หรืออาจเป็นการวิเคราะห์ของเครื่องแต่ละเครื่องในเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

11. การบันทึกสถานะของทีซีพี (TCP Session History) เป็นการเก็บบันทึกเหตุการณ์และสถานะของโปรโตคอลทีซีพี โดยในการวิเคราะห์สถิติของโปรโตคอลทีซีพีนั้นอาจเป็นการวิเคราะห์ในภาพรวมของเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง หรือการวิเคราะห์ข้อมูลของกลุ่มเครือข่ายย่อยในเครือข่ายหลัก ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการ

ปิดบังส่วน n บิตซ้าย หรืออาจเป็นการวิเคราะห์ของเครื่องแต่ละเครื่องในเครือข่าย ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

12. บริการดีเอ็นเอส (DNS Service) เป็นการบริการทางด้านโดเมนเนม เพื่อเปลี่ยนชื่อที่อยู่ของเครื่องในเครือข่ายที่ระบุด้วยหมายเลขไอพีให้เป็นชื่อภาษาอังกฤษที่จำได้ง่ายยิ่งขึ้น โดยในการวิเคราะห์การให้บริการดีเอ็นเอสนั้นจะต้องสนใจทั้งในส่วนของเครือข่ายและส่วนเครื่องของหมายเลขไอพี ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต

4.3.3 การวินิจฉัยระบบและการตรวจจับความผิดปกติ (System Diagnosis and Anomaly Detection)

1. การตรวจจับผู้บุกรุก (Intrusion Detection) เป็นการวิเคราะห์และตรวจจับผู้บุกรุกที่เข้ามาโจมตีในเครือข่าย โดยในการวิเคราะห์และตรวจจับผู้บุกรุกนั้นจะต้องสนใจทั้งในส่วนของเครือข่ายและส่วนเครื่องของหมายเลขไอพี ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต

2. การตรวจจับความผิดพลาด เป็นการวิเคราะห์และตรวจจับความผิดพลาดที่จะเกิดขึ้นกับอุปกรณ์ในเครือข่ายแต่ละเครื่อง โดยในการวิเคราะห์และตรวจจับความผิดพลาดนั้นจะต้องสนใจทั้งในส่วนของเครือข่ายและส่วนเครื่องของหมายเลขไอพี ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต

3. การวิเคราะห์ล็อก (Log Analysis) เป็นการวิเคราะห์ข้อมูลจากล็อกไฟล์ (Log File) ซึ่งอาจต้องพาดพิงถึงหมายเลขไอพีของผู้ใช้งานแต่ละคนในเครือข่าย โดยในการวิเคราะห์ล็อกนั้นจะต้องสนใจทั้งในส่วนของเครือข่ายและส่วนเครื่องของหมายเลขไอพี ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต

4. การวิเคราะห์เครือข่ายเชิงสังคม (Social Network Analysis) เป็นการวิเคราะห์การใช้งานที่เกี่ยวข้องกับสังคมในเครือข่ายของผู้ใช้งานแต่ละคน เช่น ศึกษาถึงพฤติกรรมผู้ใช้ในเครือข่าย ศึกษากิจกรรมผู้ใช้ในเครือข่าย เป็นต้น ซึ่งการวิเคราะห์เครือข่ายเชิงสังคมนั้นจะต้องสนใจทั้งในส่วนของเครือข่ายและส่วนเครื่องของหมายเลขไอพี ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต

5. การวิเคราะห์พฤติกรรม (Behavior Analysis) เป็นการวิเคราะห์พฤติกรรมและติดตามพฤติกรรมของเครื่องหรือผู้ใช้งานในเครือข่ายที่มีพฤติกรรมน่าสงสัย หรือมีพฤติกรรมเสี่ยง ซึ่งการวิเคราะห์พฤติกรรมนั้นจะต้องสนใจทั้งในส่วนของเครือข่ายและส่วน

เครื่องของหมายเลขไอพี ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต

4.3.4 การรายงานผลและแสดงผลของระบบ (System Report and Display)

1. แผนผังเครือข่าย (Network Map) เป็นการแสดงแผนผังของเครือข่ายที่ระบุหมายถึงหมายเลขไอพีของอุปกรณ์ทั้งหมดที่ใช้งานในเครือข่าย ซึ่งการแสดงผลดังกล่าวต้องสื่อความหมายของหมายเลขไอพีทั้งในส่วนของเครือข่ายและส่วนเครื่องของหมายเลขไอพี ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต

2. รายงานผ่านเว็บ (Web Report) เป็นการแสดงข้อมูลของเครือข่ายหรือข้อมูลของผู้ใช้งานในเครือข่ายที่ได้ทำการวิเคราะห์ผลลัพธ์แล้วผ่านทางระบบประยุกต์บนเว็บ (Web Application System) ซึ่งการแสดงผลดังกล่าวอาจต้องการสื่อถึงความหมายของหมายเลขไอพีทั้งในส่วนของเครือข่ายและส่วนเครื่องของหมายเลขไอพี ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต หรืออาจไม่ต้องการสื่อถึงความหมายของหมายเลขไอพีทั้งในส่วนของเครือข่ายและส่วนเครื่องของหมายเลขไอพี ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต แบบสุ่ม

3. รายงานผ่านโปรแกรมประยุกต์ (Application Report) เป็นการแสดงข้อมูลของเครือข่ายหรือข้อมูลของผู้ใช้งานในเครือข่ายที่ได้ทำการวิเคราะห์ผลลัพธ์แล้วผ่านทางโปรแกรมประยุกต์ (Application Program) ซึ่งการแสดงผลดังกล่าวอาจต้องการสื่อถึงความหมายของหมายเลขไอพีทั้งในส่วนของเครือข่ายและส่วนเครื่องของหมายเลขไอพี ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต หรืออาจไม่ต้องการสื่อถึงความหมายของหมายเลขไอพีทั้งในส่วนของเครือข่ายและส่วนเครื่องของหมายเลขไอพี ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิตแบบสุ่ม

4. รายงานผ่านเล่มเอกสาร (Book Report) เป็นการแสดงข้อมูลของเครือข่ายหรือข้อมูลของผู้ใช้งานในเครือข่ายที่ได้ทำการวิเคราะห์ผลลัพธ์แล้วในรูปแบบของเล่มเอกสาร (Document) หรือหนังสือ (Book) ซึ่งการแสดงผลดังกล่าวอาจต้องการสื่อถึงความหมายของหมายเลขไอพีทั้งในส่วนของเครือข่ายและส่วนเครื่องของหมายเลขไอพี ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต หรืออาจไม่ต้องการสื่อถึงความหมายของหมายเลขไอพีทั้งในส่วนของเครือข่ายและส่วนเครื่องของ

หมายเลขไอพี ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิตแบบสุ่ม

จากข้อมูลรายการวิเคราะห์เครือข่ายที่ได้นำเสนอตามรายละเอียดข้างต้น สามารถสรุปได้ตามตารางที่ 4.2 ดังต่อไปนี้

ตารางที่ 4.2 ตารางสรุปการปิดบังหมายเลขไอพีตามรายการวิเคราะห์เครือข่าย

กลุ่มรายการวิเคราะห์เครือข่าย	**รายการวิเคราะห์เครือข่าย**	**ระดับความเป็นส่วนตัว**
1. การใช้งานทรัพยากรและปริมาณงาน (Resource and Capacity Usages)	▪ การวิเคราะห์ประสิทธิภาพของเครือข่าย (Network Performances Analysis) ▪ การใช้งานแบนด์วิดท์ของเครือข่าย (Network Bandwidth Usages) ▪ การวางแผนปริมาณข้อมูล (Capacity Planning)	ระดับที่ไม่มีการปิดบัง
	▪ การวิเคราะห์การจราจรมัลติคาสท์ (Multicast Traffic Analysis)	ระดับการปิดบังส่วน n บิตซ้าย
	▪ การใช้งานซีพียู (CPU Usages) ▪ การใช้งานหน่วยความจำ (Memory Usages) ▪ การใช้งานดิสก์ (Disk Usages) ▪ การใช้งานจากบัญชีผู้ใช้ (Accounting Usages)	ระดับการปิดบังส่วน n บิตขวา
	▪ การจัดการพร็อกซี่ (Proxy Management)	ระดับการปิดบังทั้ง 32 บิต
2. สถิติของบริการที่เปิดใช้และให้บริการ (Service Statistics)	▪ บริการเอชทีทีพี (HTTP Service) ▪ บริการเอสเอ็นเอ็มพี (SNMP	▪ ระดับที่ไม่มีการปิดบัง (ใช้ในกรณีที่ต้องการวิเคราะห์ข้อมูลของทั้งเครือข่าย)

กลุ่มรายการวิเคราะห์เครือข่าย	รายการวิเคราะห์เครือข่าย	ระดับความเป็นส่วนตัว
	Service) ▪ บริการเทลเน็ต (TELNET Service) ▪ บริการพีโอพีสามหรือป๊อปสาม (POP3 Service) ▪ บริการเอ็นเอ็นทีพี (NNTP Service) ▪ การใช้โปรโตคอลเออาร์พี/ไอซีเอ็มพี (ARP/ICMP Usages) ▪ บริการเอฟทีพี (FTP Service) ▪ บริการเอสเอสเอช (SSH Service) ▪ บริการวีโอไอพี (VoIP Service) ▪ บริการพีทูพี (P2P Service) ▪ การบันทึกสถานะของทีซีพี (TCP Session History)	▪ ระดับการปิดบังส่วน n บิตซ้าย (ใช้ในกรณีที่ต้องการวิเคราะห์ข้อมูลของกลุ่มเครือข่ายย่อย) ▪ ระดับการปิดบังส่วน n บิตขวา (ใช้ในกรณีที่ต้องการวิเคราะห์ข้อมูลรายเครื่อง)
	▪ บริการดีเอ็นเอส (DNS Service)	ระดับการปิดบังทั้ง 32 บิต
3. การวินิจฉัยระบบและการตรวจจับความผิดปกติ (System Diagnosis and Anomaly Detection)	▪ การตรวจจับผู้บุกรุก (Intrusion Detection) ▪ การตรวจจับความผิดพลาด (Fault Detection) ▪ การวิเคราะห์ล็อก (Log Analysis) ▪ การวิเคราะห์เครือข่ายเชิงสังคม (Social Network Analysis) ▪ การวิเคราะห์พฤติกรรม (Behavior Analysis)	ระดับการปิดบังทั้ง 32 บิต

กลุ่มรายการวิเคราะห์เครือข่าย	รายการวิเคราะห์เครือข่าย	ระดับความเป็นส่วนตัว
4. การรายงานผลและแสดงผลของระบบ (System Report and Display)	▪ แผนผังเครือข่าย (Network Map)	ระดับการปิดบังทั้ง 32 บิต
	▪ รายงานผ่านเว็บ (Web Report) ▪ รายงานผ่านโปรแกรมประยุกต์ (Application Report) ▪ รายงานผ่านเล่มเอกสาร (Book Report)	▪ ระดับการปิดบังทั้ง 32 บิต (ใช้ในกรณีที่ต้องการแสดงผลลัพธ์ที่สื่อถึงความสัมพันธ์ของกลุ่มเครือข่ายหรือผู้ใช้ในเครือข่าย) ▪ ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม (ใช้ในกรณีที่ไม่ต้องการแสดงผลลัพธ์ที่สื่อถึงความสัมพันธ์ของกลุ่มเครือข่ายหรือผู้ใช้ในเครือข่าย)

4.4 กฎหมายคอมพิวเตอร์ (Computer Law)

จากปัจจัยการปิดบังหมายเลขไอพีที่ได้กล่าวมาทั้ง 2 ปัจจัยข้างต้น ซึ่งได้แก่ ต้นไม้ของความเป็นส่วนตัว และรายการวิเคราะห์เครือข่าย จำเป็นต้องอยู่ภายใต้การควบคุมดูแลของกฎหมายคอมพิวเตอร์ ดังนั้นงานวิจัยเรื่องนี้จึงได้ใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อใช้เป็นกฎหมายอ้างอิงในการปิดบังหมายเลขไอพี โดยการตีความพระราชบัญญัติดังกล่าวเพื่อกำหนดระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบัง งานวิจัยเรื่องนี้ได้พิจารณารายละเอียดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เฉพาะในหมวดที่ 2 ซึ่งเกี่ยวข้องกับพนักงานเจ้าหน้าที่เท่านั้น ซึ่งประกอบไปด้วย 13 มาตรา โดยสามารถแจกแจงรายละเอียดเฉพาะมาตราที่เกี่ยวข้องในการปิดบังหมายเลขไอพีได้ดังต่อไปนี้

1. มาตราที่ 18 (2) ได้กล่าวไว้ว่า “เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง” จากมาตราที่ 18 (2) สามารถตีความได้ว่า การเรียกข้อมูลจราจรทางคอมพิวเตอร์อาจสามารถเรียกได้จากกลุ่มเครือข่ายหรือจากตัวบุคคล ถ้ามีการเรียกข้อมูลการจราจรจากกลุ่มเครือข่าย แสดงว่าต้องการเรียกดูข้อมูลในภาพรวมของเครือข่ายใดๆ ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสม

ในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง แต่ถ้ามีการเรียกข้อมูลการจราจรจากตัวบุคคล แสดงว่าต้องการเรียกดูข้อมูลเฉพาะอุปกรณ์หรือเฉพาะบุคคลใดบุคคลหนึ่ง ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต

2. มาตราที่ 18 (3) ได้กล่าวไว้ว่า “สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่” สามารถตีความได้ว่า การสั่งให้ผู้ให้บริการซึ่งที่นี้หมายถึงผู้ให้บริการอินเตอร์เน็ต (ISP: Internet Service Provider) ส่งมอบข้อมูลการจราจรในเครือข่ายซึ่งประกอบไปด้วยข้อมูลการจราจรของผู้ใช้บริการจากองค์กรหรือจากหน่วยงานต่างๆ มากมาย ให้กับพนักงานเจ้าหน้าที่ ดังนั้นจึงขึ้นอยู่กับข้อมูลที่ต้องการแลกเปลี่ยนและส่งมอบนั้นเป็นข้อมูลขององค์กรใดและจะส่งมอบให้กับองค์กรใด ซึ่งระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีจะเป็นไปตามความสัมพันธ์ของต้นไม้ของความเป็นส่วนตัวดังที่ได้กล่าวไว้ในหัวข้อที่ 4.2

3. มาตราที่ 18 (4) ได้กล่าวไว้ว่า “ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่” สามารถตีความได้ว่า การทำสำเนา (Capture) และการสูบจับ (Sniffer) ข้อมูลจราจรของระบบคอมพิวเตอร์หรือระบบเครือข่ายใดๆ ของพนักงานเจ้าหน้าที่นั้น ขึ้นอยู่กับว่าพนักงานเจ้าหน้าที่ต้องการใช้ข้อมูลเหล่านั้นเพื่อวิเคราะห์ผลในเรื่องใดและในประเด็นใด ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีจะเป็นไปตามรายการวิเคราะห์เครือข่ายดังที่ได้กล่าวไว้ในหัวข้อที่ 4.3

4. มาตราที่ 18 (5) ได้กล่าวไว้ว่า “สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่” สามารถตีความได้ว่า การที่พนักงานเจ้าหน้าที่สั่งให้ตัวบุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง ส่งมอบข้อมูลให้กับพนักงานเจ้าหน้าที่ ซึ่งข้อมูลเหล่านั้นเป็นข้อมูลส่วนบุคคล ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต

5. มาตราที่ 18 (6) ได้กล่าวไว้ว่า “ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้” สามารถตีความได้ว่า การตรวจสอบและการเข้าถึงข้อมูลจาก

ระบบคอมพิวเตอร์ของบุคคลใดบุคคลหนึ่งนั้น เป็นการเข้าถึงที่สามารถระบุถึงตัวบุคคลหรืออุปกรณ์ที่ใช้งานในเครือข่ายได้ ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต

6. มาตราที่ 26 วรรค 1 ได้กล่าวไว้ว่า "ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้" สามารถตีความได้ว่า การเก็บรักษาข้อมูลจราจรของผู้ให้บริการไม่ว่าจะเป็นระยะเวลานานเท่าใดก็ตาม ถ้ายังไม่มีกระบวนวิเคราะห์หรือการนำข้อมูลเหล่านั้นไปกระทำการอย่างใดอย่างหนึ่งแล้ว ก็ไม่จำเป็นต้องปิดบังหมายเลขไอพีแต่อย่างใด ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง

7. มาตราที่ 26 วรรค 2 ได้กล่าวไว้ว่า "ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง" สามารถตีความได้ว่า การที่ผู้ให้บริการเก็บรักษาข้อมูลจราจรของเครือข่ายที่เกี่ยวข้องกับตัวผู้ใช้บริการแต่ละคนเพื่อให้สามารถระบุตัวผู้ใช้บริการได้นั้น เป็นการใช้ข้อมูลซึ่งแสดงอยู่ในส่วนของเครื่องของหมายเลขไอพี ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

จากรายละเอียดการตีความและการพิจารณาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ทั้งที่เกี่ยวข้องกับการปิดบังหมายเลขไอพีที่ได้นำเสนอตามรายละเอียดข้างต้นและที่ไม่เกี่ยวข้องกับการปิดบังหมายเลขไอพี สามารถสรุปรวมไว้ตามตารางที่ 4.3 ได้ดังต่อไปนี้

ตารางที่ 4.3 ตารางสรุปการปิดบังหมายเลขไอพีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

มาตรา	รายละเอียดจากพระราชบัญญัติ	ระดับความเป็นส่วนตัว
18	ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐาน	ไม่เกี่ยวข้องกับการปิดบัง

มาตรา	รายละเอียดจากพระราชบัญญัติ	ระดับความเป็นส่วนตัว
	เกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด	
18 (1)	มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้	ไม่เกี่ยวข้องกับการปิดบัง
18 (2)	เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิว-เตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง	ระดับที่ไม่มีการปิดบัง และระดับการปิดบังทั้ง 32 บิต
18 (3)	สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่	ปิดบังตามต้นไม้ของความเป็นส่วนตัว
18 (4)	ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่	ปิดบังตามรายการวิเคราะห์เครือข่าย
18 (5)	สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิว-เตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่	ระดับการปิดบังทั้ง 32 บิต
18 (6)	ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอม-พิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้	ระดับการปิดบังทั้ง 32 บิต
18 (7)	ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับ	ไม่เกี่ยวข้องกับการปิดบัง

มาตรา	รายละเอียดจากพระราชบัญญัติ	ระดับความเป็นส่วนตัว
	ดังกล่าว	
18 (8)	ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้	ไม่เกี่ยวข้องกับการปิดบัง
19 วรรค 1	การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) และ (8) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว	เป็นไปตามรายละเอียดการปิดบังที่ระบุไว้ในมาตราที่ 18
19 วรรค 2	เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา 18 (4) (5) (6) (7) และ (8) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้	เป็นไปตามรายละเอียดการปิดบังที่ระบุไว้ในมาตราที่ 18
19 วรรค 3	ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา 18 (4) (5) (6) (7) และ (8) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน	เป็นไปตามรายละเอียดการปิดบังที่ระบุไว้ในมาตราที่ 18
19 วรรค 4	การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา 18 (4) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้	เป็นไปตามรายละเอียดการปิดบังที่ระบุไว้ในมาตราที่ 18

มาตรา	รายละเอียดจากพระราชบัญญัติ	ระดับความเป็นส่วนตัว
	ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น	
19 วรรค 5	การยึดหรืออายัดตามมาตรา 18 (8) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้วพนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน	เป็นไปตามรายละเอียดการปิดบังที่ระบุไว้ในมาตราที่ 18
19 วรรค 6	หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง	ไม่เกี่ยวข้องกับการปิดบัง
20 วรรค 1	ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสองลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้	ไม่เกี่ยวข้องกับการปิดบัง
20 วรรค 2	ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้	ไม่เกี่ยวข้องกับการปิดบัง
21 วรรค 1	ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงาน	ไม่เกี่ยวข้องกับการปิดบัง

มาตรา	รายละเอียดจากพระราชบัญญัติ	ระดับความเป็นส่วนตัว
	เจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูล คอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้	
21 วรรค 2	ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือเพิ่มเติมขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวงทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้นตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา	ไม่เกี่ยวข้องกับการปิดบัง
22 วรรค 1	ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา 18 ให้แก่บุคคลใด	เป็นไปตามรายละเอียดการปิดบังที่ระบุไว้ในมาตราที่ 18
22 วรรค 2	ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล	เป็นไปตามรายละเอียดการปิดบังที่ระบุไว้ในมาตราที่ 18
22 วรรค 3	พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ	ไม่เกี่ยวข้องกับการปิดบัง
23	พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา 18 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ	ไม่เกี่ยวข้องกับการปิดบัง

มาตรา	รายละเอียดจากพระราชบัญญัติ	ระดับความเป็นส่วนตัว
24	ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา 18 และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ	ไม่เกี่ยวข้องกับการปิดบัง
25	ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจมีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น	ไม่เกี่ยวข้องกับการปิดบัง
26 วรรค 1	ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้	ระดับที่ไม่มีการปิดบัง
26 วรรค 2	ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง	ระดับการปิดบังส่วน n บิตขวา
26 วรรค 3	ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา	ไม่เกี่ยวข้องกับการปิดบัง
26 วรรค 4	ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท	ไม่เกี่ยวข้องกับการปิดบัง
27	ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา 18 หรือมาตรา 20 หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา 21 ต้องระวางโทษปรับไม่เกินสองแสนบาทและปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง	ไม่เกี่ยวข้องกับการปิดบัง

มาตรา	รายละเอียดจากพระราชบัญญัติ	ระดับความเป็นส่วนตัว
28	การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด	ไม่เกี่ยวข้องกับการปิดบัง
29 วรรค 1	ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้	ไม่เกี่ยวข้องกับการปิดบัง
29 วรรค 2	ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป	ไม่เกี่ยวข้องกับการปิดบัง
29 วรรค 3	ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง	ไม่เกี่ยวข้องกับการปิดบัง
30 วรรค 1	ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง	ไม่เกี่ยวข้องกับการปิดบัง
30 วรรค 2	บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา	ไม่เกี่ยวข้องกับการปิดบัง

จากตารางสรุปการปิดบังหมายเลขไอพีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น ในมาตราที่ 19 วรรค 1 ถึง 19 วรรค 5 จะมีกระบวนการพิจารณาการปิดบังหมายเลขไอพีตามรายละเอียดที่ระบุไว้ในมาตราที่ 18 ซึ่งขึ้นอยู่กับสถานการณ์การปิดบังว่าจะสอดคล้องกับมาตราและอนุมาตราใดบ้าง

รายละเอียดของปัจจัยการปิดบังทั้ง 3 ปัจจัยที่ได้กล่าวมาในบทนี้ จะนำมาพิจารณาร่วมกันในการตัดสินเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุด โดยใช้หลักการของวิธีการแบบกฎซึ่งจะได้กล่าวโดยละเอียดในบทต่อไป

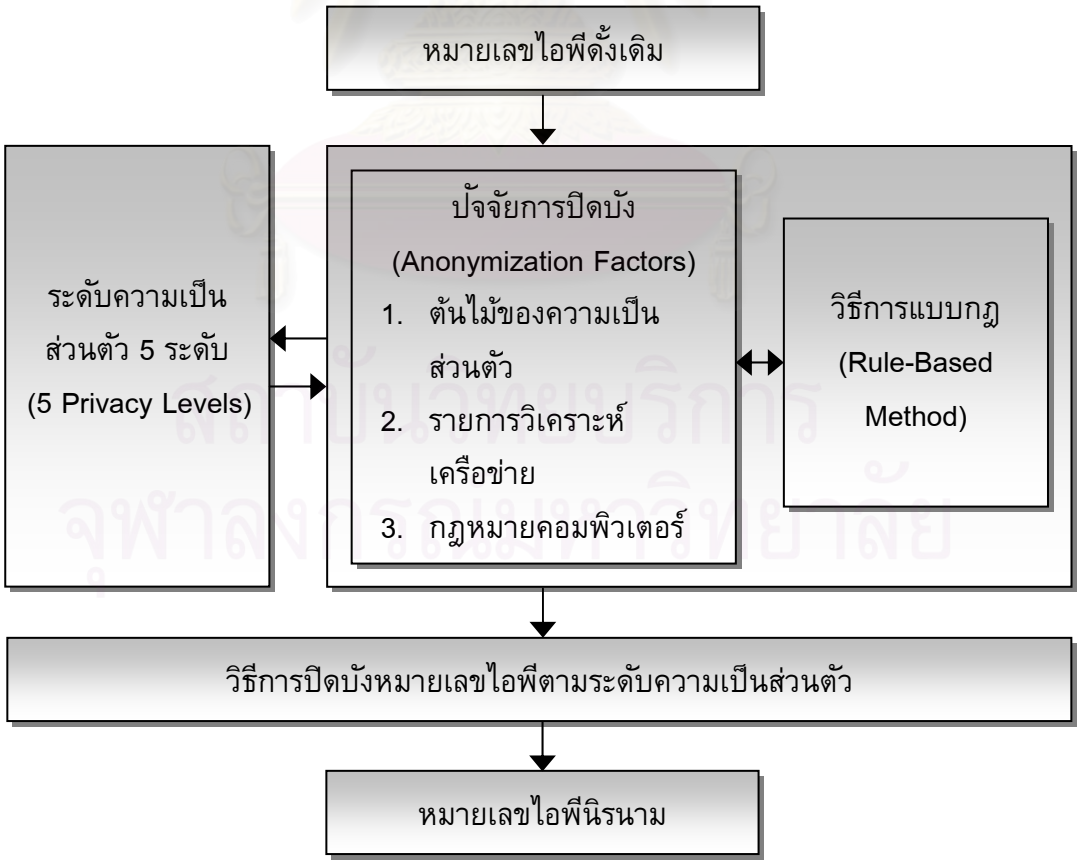
บทที่ 5

แบบแผนการปิดบังหมายเลขไอพี

บทนี้เป็นการสร้างแบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว ซึ่งใช้ปัจจัยการปิดบังหมายเลขไอพีทั้ง 3 ปัจจัยในบทที่ 4 เพื่อพิจารณาเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุดโดยใช้วิธีการแบบกฎ ซึ่งมีรายละเอียดดังต่อไปนี้

5.1 แบบแผนการปิดบังหมายเลขไอพี (IP Address Anonymization Scheme)

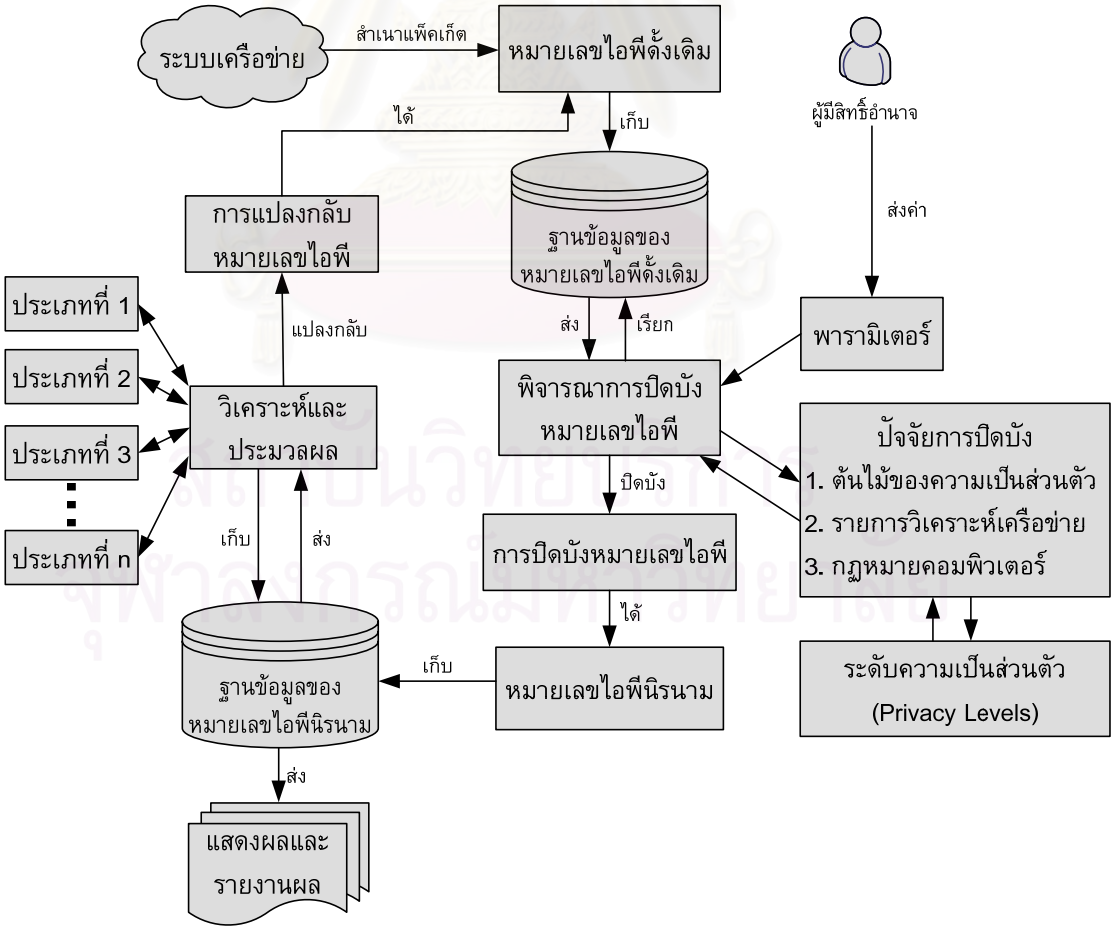
แบบแผนการปิดบังหมายเลขไอพีของงานวิจัยเรื่องนี้เป็นแบบแผนการปิดบังหมายเลขไอพีแบบใหม่ที่อยู่บนพื้นฐานของระดับความเป็นส่วนตัวตามที่ได้นำเสนอไว้ในบทที่ 3 และจะพิจารณาเลือกระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังโดยใช้ปัจจัยการปิดบังทั้ง 3 ปัจจัยที่ได้นำเสนอไว้ในบทที่ 4 โดยใช้วิธีการแบบกฎ (Rule-Based Method) ในการเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุด รายละเอียดโดยสรุปของแบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัวนี้ได้แสดงไว้ในรูปที่ 5.1



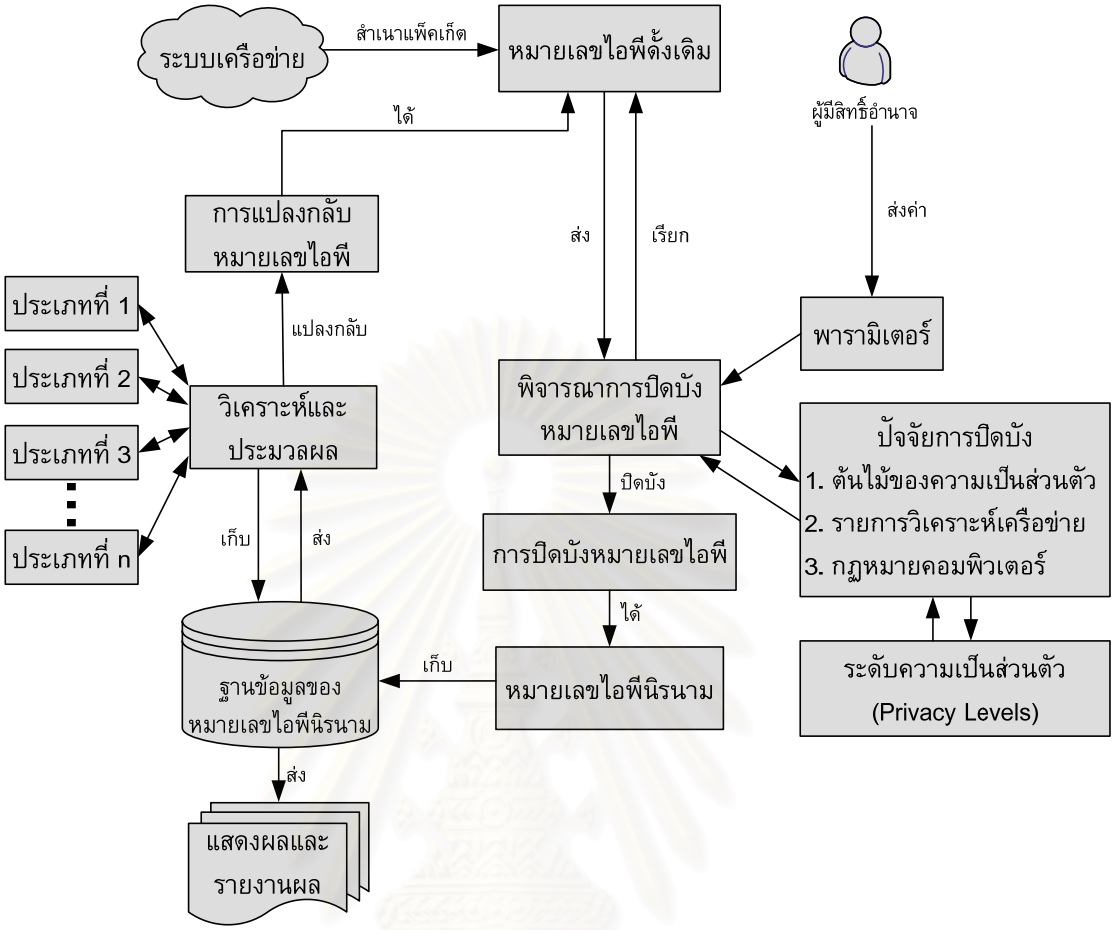
รูปที่ 5.1 แบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว

จากแบบแผนการปิดบังหมายเลขไอพีตามรูปที่ 5.1 หมายเลขไอพีดั้งเดิมจะถูกพิจารณาถึงระดับความเป็นส่วนตัวที่เหมาะสมก่อนการปิดบังหมายเลขไอพี โดยใช้ปัจจัยการปิดบัง 3 ปัจจัยอันได้แก่ ต้นไม้ของความเป็นส่วนตัว รายการวิเคราะห์เครือข่าย และกฎหมายคอมพิวเตอร์ เข้ามาพิจารณาร่วมกันโดยใช้วิธีการแบบกฎเพื่อเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุดจาก 5 ระดับ และใช้ระดับความเป็นส่วนตัวที่เลือกนั้นในการปิดบังหมายเลขไอพี ซึ่งวิธีการปิดบังอาจใช้วิธีการของคริปโตแพน วิธีการแบบสุ่ม และวิธีการที่ไม่ต้องปิดบัง ทั้งนี้ขึ้นอยู่กับระดับความเป็นส่วนตัวที่เลือกใช้งาน โดยจะได้กล่าวถึงรายละเอียดในหัวข้อที่ 5.2 และ 5.3 ต่อไป

แบบแผนการปิดบังหมายเลขไอพีนี้สามารถใช้งานได้ทั้งในระบบการทำงานแบบช่วงเวลา (Batch Processing) และระบบการทำงานแบบทันกาล (Real-Time Processing) ซึ่งมีขั้นตอนการปิดบังหมายเลขไอพีตามรูปที่ 5.2 และ 5.3 ตามลำดับ โดยระบบการทำงานแบบช่วงเวลานั้นจะมีการสำเนาแพ็คเก็ตซึ่งมีหมายเลขไอพีปรากฏอยู่เข้ามาเก็บไว้ในฐานข้อมูลก่อนทำการปิดบัง ส่วนระบบการทำงานแบบทันกาลนั้นจะทำการปิดบังหมายเลขไอพีขณะที่มีการสำเนาแพ็คเก็ตโดยทันที

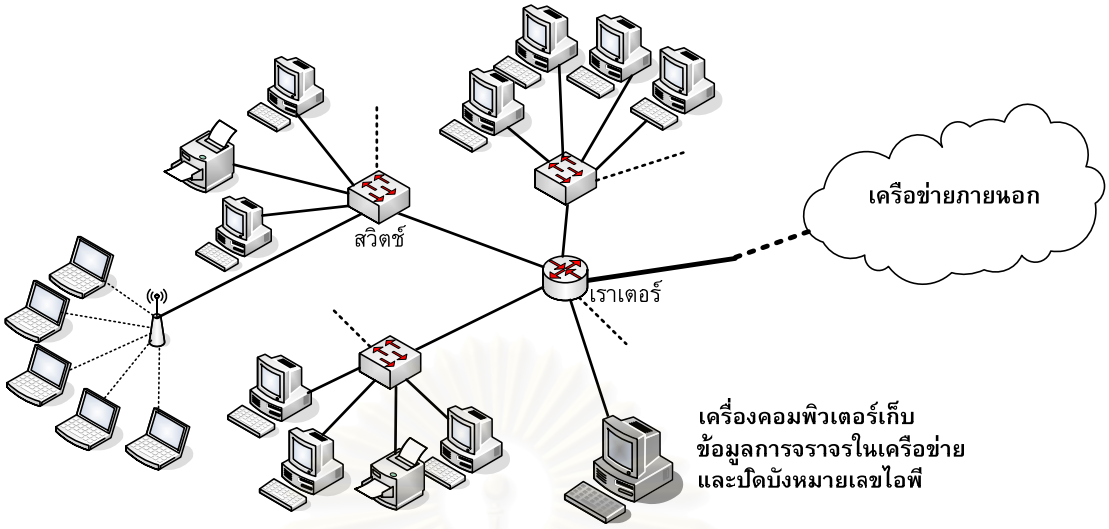


รูปที่ 5.2 แบบแผนการปิดบังหมายเลขไอพีในระบบการทำงานแบบช่วงเวลา



รูปที่ 5.3 แบบแผนการปิดบังหมายเลขไอพีในระบบการทำงานแบบทันกาล

จากแบบแผนการปิดบังหมายเลขไอพีในระบบการทำงานแบบช่วงเวลาและระบบการทำงานแบบทันกาลนั้น ในกระบวนการปิดบังและใช้งานจริงจะทำการติดตั้งโปรแกรมที่พัฒนาตามแบบแผนการปิดบังหมายเลขไอพีที่ได้นำเสนอลงบนเครื่องคอมพิวเตอร์ที่ทำหน้าที่สูบจับและจัดเก็บข้อมูลการจราจรในเครือข่าย ซึ่งเครื่องคอมพิวเตอร์เครื่องนี้ถูกต่อเข้ากับเราเตอร์ทางออกของเครื่องข่ายดังแสดงตามรูปที่ 5.4 โดยกระบวนการปิดบังและใช้งานจริงที่ได้กำหนดไว้ในงานวิจัยเรื่องนี้ยังเป็นเพียงแนวทางที่เป็นไปได้เท่านั้น ยังคงไม่ได้ทดสอบกับระบบจริงแต่อย่างใด ซึ่งกระบวนการปิดบังและใช้งานกับระบบจริงจะได้ทำการทดลองและศึกษาวิจัยต่อไปในอนาคต



รูปที่ 5.4 แผนผังการปิดบังหมายเลขไอพีบนระบบเครือข่ายจริง

5.2 วิธีการแบบกฎ (Rule-Based Method)

วิธีการแบบกฎที่นำมาใช้กับงานวิจัยเรื่องนี้ คือ การสร้างกฎในการเลือกระดับความเป็นส่วนตัวจากปัจจัยแต่ละปัจจัยแล้วนำมาเปรียบเทียบและผนวกเข้าด้วยกันเพื่อเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุด โดยพิจารณาจากสถานการณ์การปิดบังและความต้องการใช้ข้อมูล เช่น ศาลแต่งตั้งให้จุฬาลงกรณ์มหาวิทยาลัยเป็นพนักงานเจ้าหน้าที่เพื่อให้จุฬาลงกรณ์มหาวิทยาลัย สั่งให้บริษัทไมโครซอฟต์เก็บข้อมูลการจราจรทางคอมพิวเตอร์ไว้อย่างน้อย 90 วัน เป็นต้น ซึ่งสถานการณ์ดังกล่าวจะถูกพิจารณาด้วยปัจจัยการปิดบัง 3 ปัจจัย และเลือกระดับความเป็นส่วนตัวในการปิดบังต่อไป โดยรายละเอียดของวิธีการแบบกฎมีดังต่อไปนี้

5.2.1 วิธีการแบบกฎของต้นไม้ของความเป็นส่วนตัว

วิธีการแบบกฎของต้นไม้ของความเป็นส่วนตัวเพื่อใช้เลือกระดับความเป็นส่วนตัวมีรายละเอียดดังอัลกอริทึมที่ 5.1 ซึ่งเริ่มต้นโดยการกำหนดค่าหมายเลขไอพีอ้างอิงและหมายเลขสับเน็ตมาสก์จากเครือข่าย A ซึ่งเป็นองค์กรที่เป็นผู้วิเคราะห์ข้อมูล และเครือข่าย B ซึ่งเป็นองค์กรที่เป็นผู้ถูกวิเคราะห์ข้อมูล จากนั้นทำการตรวจสอบโครงสร้างหมายเลขไอพีขององค์กร A และ B เพื่อหาความสัมพันธ์และจำนวนบิตที่มีส่วนร่วมกัน โดยถ้ามีจำนวนบิตน้อยกว่า 4 บิตที่มีส่วนร่วมกัน ซึ่งเป็นจำนวนบิตที่น้อยที่สุดของกลุ่มเครือข่ายที่เป็นไปได้ [6] จะถือว่าโครงสร้างหมายเลขไอพีของทั้งสององค์กรไม่มีส่วนเกี่ยวข้องกันหรือเป็นอิสระต่อกัน แต่ถ้าไม่เช่นนั้นแสดงว่าโครงสร้างหมายเลขไอพีของทั้งสององค์กรมีส่วนเกี่ยวข้องกัน และมีความสัมพันธ์ตามต้นไม้ของความเป็นส่วนตัวในหัวข้อที่ 4.2 ซึ่งต้นไม้ของความเป็นส่วนตัวแต่

ละรูปแบบมีการกำหนดให้มีระดับความเป็นส่วนตัวที่แตกต่างกันตามรายละเอียดที่ได้กล่าวไว้ในหัวข้อที่ 4.2

อัลกอริทึมที่ 5.1 อัลกอริทึมของวิธีการแบบกฎของต้นไม้ของความเป็นส่วนตัว

```
1   //A is referenced IP address of organization which analyzes B
2   // B is referenced IP address of organization which is analyzed by A
3   OriginalIP-A ← Input A's IP Address
4   Subnet-A ← Input A's Subnet Mask Address
5   OriginalIP-B ← Input B's IP Address
6   Subnet-B ← Input B's Subnet Mask Address
7   LeftPart-A ← binary(OriginalIP-A) AND binary(Subnet-A)
8   RightPart-A ← substring(LeftPart-A.length, 32)
9   LeftPart-B ← binary(OriginalIP-B) AND binary(Subnet-B)
10  RightPart-B ← substring(LeftPart-B.length, 32)
11  PTS //Privacy Tree Structure
12  n ← binary(OriginalIP-A) ∩ binary(OriginalIP-B
13  If (n Greater Than or Equal 4)
14          IF ((n Greater Than or Equal LeftPart-A.length) AND
15          (n Less Than LeftPart-B.length) AND
16          (LeftPart-A.length Not Equal LeftPart-B.length))
17                  PTS ← 3 //Proper Subtree (A in B)
18          Else IF ((n Less Than or Equal LeftPart-A.length) AND
19          (n Greater Than LeftPart-B.length))
20                  PTS ← 4 //Proper Subtree (B in A)
21          Else IF ((n Equal LeftPart-A.length) AND
22          (n Equal LeftPart-B.length))
23                  PTS ← 5 //Equivalent Subtree
24          Else //Otherwise
25                  PTS ← 2 //Intersection Subtree
26          End If
27  Else //Otherwise
28          PTS ← 1 //Independent Subtree
29  End If
30  LevelFromPTS ← 0 //Privacy Level from PTS
```

```
31  If (PTS is 1)
32      LevelFromPTS ← 1 //Non-Anonymization
33  Else If (PTS is 2)
34      LevelFromPTS ← 2 //n-Left Anonymization
35  Else If (PTS is 3)
36      LevelFromPTS ← 3 //n-Right Anonymization
37  Else If (PTS is 4)
38      LevelFromPTS ← 3 //n-Right Anonymization
39  Else If (PTS is 5)
40      LevelFromPTS ← 4 //Full Anonymization
41  Else //Undefined PTS
42      LevelFromPTS ← 1 //Non-Anonymization
43  End If
```

5.2.2 วิธีการแบบกฎของรายการวิเคราะห์เครือข่าย

วิธีการแบบกฎของต้นไม้ของรายการวิเคราะห์เครือข่ายเพื่อใช้เลือกระดับความเป็นส่วนตัวมีรายละเอียดดังอัลกอริทึมที่ 5.2 ซึ่งเริ่มต้นโดยการระบุรายการวิเคราะห์เครือข่ายทั้งหมดที่ต้องการพิจารณาเพื่อตรวจสอบเงื่อนไขและกฎที่กำหนดขึ้นกับรายการวิเคราะห์เครือข่ายว่ามีความสัมพันธ์กับระดับความเป็นส่วนตัวระดับใด และในบางรายการวิเคราะห์เครือข่ายอาจมีระดับความเป็นส่วนตัวที่เป็นไปได้หลายระดับ ดังนั้นจึงต้องระบุความต้องการเพิ่มเติมเพื่อกำหนดและพิจารณาเลือกระดับความเป็นส่วนตัวที่เหมาะสม

อัลกอริทึมที่ 5.2 อัลกอริทึมของวิธีการแบบกฎของรายการวิเคราะห์เครือข่าย

```
1   /* ================== List of Network Analysis ==================
2   [1]  Network Performances Analysis   [2]  Network Bandwidth Usages
3   [3]  Capacity Planning               [4]  Multicast Traffic Analysis
4   [5]  CPU Usages                      [6]  Memory Usages
5   [7]  Disk Usages                     [8]  Accounting Usages
6   [9]  Proxy Management                [10] HTTP Service
7   [11] SNMP Service                    [12] TELNET Service
8   [13] POP3 Service                    [14] NNTP Service
9   [15] ARP/ICMP Usages                 [16] FTP Service
10  [17] SSH Service                     [18] VoIP Service
```

```
11  [19] P2P Service                    [20] TCP Session History
12  [21] DNS Service                    [22] Intrusion Detection
13  [23] Fault Detection                [24] Log Analysis
14  [25] Social Network Analysis        [26] Behavior Analysis
15  [27] Network Map                    [28] Web Report
16  [29] Application Report             [30] Book Report
17  ========================================================== */
18  FN ← -1 //Function Number of Network Analysis (NTA)
19  CheckLeftPart ← False
20  CheckRightPart ← False
21  CheckRandom ← False
22  While (FN Not Equal 0)
23          FN ← Input FN from User
24          IF (FN Equal 1 to 3)
25                  //Don't Do Anything
26          Else If (FN Equal 4)
27                  If (CheckLeftPart is False)  CheckLeftPart ← True
28          Else If (FN Equal 5 to 8)
29                  If (CheckRightPart is False)  CheckRightPart ← True
30          Else If (FN Equal 9)
31                  If (CheckLeftPart is False)  CheckLeftPart ← True
32                  If (CheckRightPart is False)  CheckRightPart ← True
33          Else If (FN Equal 10 to 20)
34                  Rq ← Input Requirement from User
35                  //[1] Network Summary
36                  //[2] Sub-Network Summary
37                  //[3] Device Summary
38                  If (Rq Equal 1)  //Don't Do Anything
39                  Else If (Rq Equal 2)
40                          If (CheckLeftPart is False)  CheckLeftPart ← True
41                  Else If (Rq Equal 3)
42                          If (CheckRightPart is False)  CheckRightPart ← True
43                  Else //Don't Do Anything
44                  End If
```

```
45          Else If (FN Equal 21 to 27)
46                  If (CheckLeftPart is False)  CheckLeftPart ← True
47                  If (CheckRightPart is False)  CheckRightPart ← True
48          Else If (FN Equal 28 to 30)
49                  Rq ← Input Requirement from User
50                  //[1] Prefix-Preserving
51                  //[2] Non Prefix-Preserving (Random)
52                  If (Rq Equal 1)
53                          If (CheckLeftPart is False)  CheckLeftPart ← True
54                          If (CheckRightPart is False)  CheckRightPart ← True
55                  Else If (Rq Equal 2)
56                          If (CheckRandom is False)  CheckRandom ← False
57                  Else //Don't Do Anything
58                  End If
59          Else //Don't Do Anything
60          End If
61  End While
62  LevelFromNTA ← 0 //Privacy Level from NTA
63  If (CheckRandom is True)
64          LevelFromNTA ← 5 //Randomly Full Anonymization
65  Else
66          If (CheckLeftPart is False AND CheckRightPart is False)
67                  LevelFromNTA ← 1 //Non-Anonymization
68          Else If (CheckLeftPart is True AND CheckRightPart is False)
69                  LevelFromNTA ← 2 //n-Left Anonymization
70          Else If (CheckLeftPart is False AND CheckRightPart is True)
71                  LevelFromNTA ← 3 //n-Right Anonymization
72          Else If (CheckLeftPart is True AND CheckRightPart is True)
73                  LevelFromNTA ← 4 //Full Anonymization
74          Else //Don't Do Anything
75          End If
76  End If
```

5.2.3 วิธีการแบบกฎของกฎหมายคอมพิวเตอร์

วิธีการแบบกฎของกฎหมายคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อใช้เลือกระดับความเป็นส่วนตัวมีรายละเอียดดังอัลกอริทึมที่ 5.3 ซึ่งเริ่มต้นโดยการระบุมาตรากฎหมายที่เกี่ยวข้อง โดยการพิจารณาจากสถานการณ์การปิดบัง ซึ่งมีตัวอย่างอยู่ในหัวข้อที่ 6.1.3 ซึ่งมาตราแต่ละมาตราถูกกำหนดด้วยกฎเพื่อพิจารณาเลือกระดับความเป็นส่วนตัวที่เหมาะสม โดยที่มาตรา 18 (3) ต้องใช้ข้อมูลการทำงานของต้นไม้ของความเป็นส่วนตัว มาตรา 18 (4) ต้องใช้ข้อมูลการทำงานของรายการวิเคราะห์เครือข่าย และมาตรา 19 และ 22 มีการทำงานที่เป็นไปตามมาตารา 18

อัลกอริทึมที่ 5.3 อัลกอริทึมของวิธีการแบบกฎของกฎหมายคอมพิวเตอร์

```
1  /* ============== List of Law Sections ==============
2  [1]  Section 18 (2)              [2]  Section 18 (3)
3  [3]  Section 18 (4)              [4]  Section 18 (5)
4  [5]  Section 18 (6)              [6]  Section 19 Paragragh 1
5  [7]  Section 19 Paragragh 2      [8]  Section 19 Paragragh 3
6  [9]  Section 19 Paragragh 4      [10] Section 19 Paragragh 5
7  [11] Section 22 Paragragh 1      [12] Section 22 Paragragh 2
8  [13] Section 26 Paragragh 1      [14] Section 26 Paragragh 2
9  ================================================ */
10 LAW ← -1 //Number of Law Sections (LWS)
11 CheckLeftPart ← False
12 CheckRightPart ← False
13 While (LAW Not Equal 0)
14       LAW ← Input LAW from User
15       IF (LAW Equal 1)
16             Rq ← Input Requirement from User
17             //[1] Network Information
18             //[2] Device/User Information
19             If (Rq Equal 1) //Don't Do Anything
20             Else If (Rq Equal 2)
21                   If (CheckLeftPart is False)  CheckLeftPart ← True
22                   If (CheckRightPart is False)  CheckRightPart ← True
23             Else //Don't Do Anything
```

24	End If
25	Else If (LAW Equal 2)
26	//Follow By PTS
27	Else If (LAW Equal 3)
28	//Follow By NTA
29	Else If (LAW Equal 4 to 5)
30	If (CheckLeftPart is False) CheckLeftPart ← True
31	If (CheckRightPart is False) CheckRightPart ← True
32	Else If (LAW Equal 6 to 12)
33	//Follow By Section 18
34	Else If (LAW Equal 13)
35	//Don't Do Anything
36	Else If (LAW Equal 14)
37	If (CheckRightPart is False) CheckRightPart ← True
38	Else //Don't Do Anything
39	End If
40	End While
41	LevelFromLWS ← 0 //Privacy Level from LWS
42	If (CheckLeftPart is False AND CheckRightPart is False)
43	LevelFromLWS ← 1 //Non-Anonymization
44	Else If (CheckLeftPart is False AND CheckRightPart is True)
45	LevelFromLWS ← 3 //n-Right Anonymization
46	Else If (CheckLeftPart is True AND CheckRightPart is True)
47	LevelFromLWS ← 4 //Full Anonymization
48	Else
49	LevelFromLWS ← 1 //Non-Anonymization
50	End If

5.2.4 วิธีการแบบกฎโดยการรวม 3 ปัจจัยการปิดบัง

วิธีการแบบกฎโดยการรวมปัจจัยการปิดบังทั้ง 3 ปัจจัยเข้าด้วยกันเพื่อใช้เลือกระดับความเป็นส่วนตัวขั้นสุดท้ายมีรายละเอียดดังอัลกอริทึมที่ 5.4 โดยกระบวนการดังกล่าวเป็นขั้นตอนสุดท้ายในการพิจารณาเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุดจากสถานการณ์การปิดบังที่ถูกกำหนดขึ้น

ลำดับในการพิจารณาปัจจัยการปิดบังเริ่มต้นด้วยการพิจารณาต้นไม้ของความเป็นส่วนตัว ตามด้วยรายการวิเคราะห์เครือข่าย และลำดับสุดท้ายเป็นกฎหมายคอมพิวเตอร์ โดยจะนำผลลัพธ์ที่ได้จากการทำงานของแต่ละปัจจัยมารวมเข้าด้วยกันเพื่อตัดสินระดับความเป็นส่วนตัวที่ดีและเหมาะสมที่สุด

อัลกอริทึมที่ 5.4 อัลกอริทึมของวิธีการแบบกฎโดยการรวม 3 ปัจจัยการปิดบัง

```
1   CheckLeftPart ← False
2   CheckRightPart ← False
3   CheckRandom ← False
4   LevelFromPTS ← Input from PTS Function
5   LevelFromNTA ← Input from NTA Function
6   LevelFromLWS ← Input from LWS Function
7   LevelFromFactor[ ] ← { LevelFromPTS, LevelFromNTA, LevelFromLWS }
8   Level ← 0 //Final Privacy Level
9   For (i ← 0 to 2)
10          If (LevelFromFactor[i] is 1)  //Don't Do Anything
11          Else If (LevelFromFactor[i] is 2)
12                  If (CheckLeftPart is False)  CheckLeftPart ← True
13          Else If (LevelFromFactor[i] is 3)
14                  If (CheckRightPart is False)  CheckRightPart ← True
15          Else If (LevelFromFactor[i] is 4)
16                  If (CheckLeftPart is False)  CheckLeftPart ← True
17                  If (CheckRightPart is False)  CheckRightPart ← True
18          Else If (LevelFromFactor[i] is 5)
19                  If (CheckRandom is False)  CheckRandom ← True
20          Else  //Don't Do Anything
21          End If
22  End for
23  If (CheckRandom is True)
24          Level ← 5 //Randomly Full Anonymization
25  Else
26          If (CheckLeftPart is False AND CheckRightPart is False)
27                  Level ← 1 //Non-Anonymization
28          Else If (CheckLeftPart is True AND CheckRightPart is False)
```

29	Level ← 2 //n-Left Anonymization
30	Else If (CheckLeftPart is False AND CheckRightPart is True)
31	Level ← 3 //n-Right Anonymization
32	Else If (CheckLeftPart is True AND CheckRightPart is True)
33	Level ← 4 //Full Anonymization
34	Else //Don't Do Anything
35	End If
36	End If

5.3 วิธีการปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัว

หลังจากผ่านกระบวนการเลือกระดับความเป็นส่วนตัวที่เหมาะสมโดยใช้วิธีการแบบกฎแล้ว ก็จะเข้าสู่กระบวนการปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวที่ถูกเลือกจาก 5 ระดับที่ได้นำเสนอ โดยการปิดบังหมายเลขไอพีในแต่ละระดับนั้นจะมีขั้นตอนวิธีหรืออัลกอริทึมการปิดบังที่แตกต่างกันดังรายละเอียดต่อไปนี้

1. ระดับที่ไม่มีการปิดบัง เป็นระดับที่ไม่ต้องปิดบังหมายเลขไอพีดังนั้นจึงไม่มีอัลกอริทึมสำหรับการปิดบัง

2. ระดับการปิดบังส่วน n บิตซ้าย ใช้อัลกอริทึมคริปโตแพนในการปิดบัง เพราะระดับความเป็นส่วนตัวนี้ต้องปิดบังส่วนบิตซ้ายที่ต้องคงไว้ซึ่งความสัมพันธ์ของหมายเลขไอพีดั้งเดิม

3. ระดับการปิดบังส่วน n บิตขวา ใช้อัลกอริทึมคริปโตแพนในการปิดบัง เพราะระดับความเป็นส่วนตัวนี้ต้องปิดบังส่วนบิตขวาที่ต้องคงไว้ซึ่งความสัมพันธ์ของหมายเลขไอพีดั้งเดิม

4. ระดับการปิดบังทั้ง 32 บิต ใช้อัลกอริทึมคริปโตแพนในการปิดบัง เพราะระดับความเป็นส่วนตัวนี้ต้องปิดบังทั้ง 32 บิตของหมายเลขไอพี ที่ต้องคงไว้ซึ่งความสัมพันธ์ของหมายเลขไอพีดั้งเดิม

5. ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม ใช้อัลกอริทึมแบบสุ่มในการปิดบัง เพราะระดับความเป็นส่วนตัวนี้ต้องปิดบังทั้ง 32 บิตของหมายเลขไอพีแบบสุ่ม และไม่จำเป็นต้องคงไว้ซึ่งความสัมพันธ์ของหมายเลขไอพีดั้งเดิม

การปิดบังหมายเลขไอพีเริ่มต้นจากการแบ่งหมายเลขไอพีดั้งเดิมออกเป็น 2 ส่วน คือส่วนบิตซ้ายและส่วนบิตขวา โดยใช้การดำเนินการระดับบิตระหว่างหมายเลขไอพีดั้งเดิมและหมายเลขสับเน็ตมาสก์ พร้อมทั้งกำหนดกุญแจสำหรับการปิดบังที่มีจำนวนบิตเป็น 32 บิตทวีคูณ ซึ่งอาจเป็น 32 บิต 64 บิต ฯลฯ และกระบวนการต่อจากนี้คือการพิจารณาระดับความเป็นส่วนตัวที่เหมาะสมซึ่งมีรายละเอียดอยู่ในหัวข้อที่ 5.2 กระบวนการปิดบังหมายเลขไอพีจะปิดบังตามระดับความเป็นส่วนตัวที่ถูกเลือกและตามอัลกอริทึมที่ระบุไว้ในระดับความเป็นส่วนตัวเหล่านั้น โดยรายละเอียดของกระบวนการปิดบังหมายเลขไอพีทั้งหมดแสดงได้ไว้ในอัลกอริทึมที่ 5.5

อัลกอริทึมที่ 5.5 อัลกอริทึมการปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัว

```
1  OriginalIP ← Input from Previous Function
2  Subnet ← Input from Previous Function
3  LeftPart ← Input from Previous Function
4  RightPart ← Input from Previous Function
5  Level ← ruleBased(OriginalIP, Subnet)
6  Key ← keyGeneration()
7  If (Level is 1)
8          AnonymizedIP ← OriginalIP
9  Else If (Level is 2)
10         AnonymizedIP ← cryptopan(LeftPart, Key) + RightPart
11 Else If (Level is 3)
12         AnonymizedIP ← LeftPart  + cryptopan(RightPart, Key)
13 Else If (Level is 4)
14         AnonymizedIP ← cryptopan(OriginalIP, Key)
15 Else If (Level is 5)
16         AnonymizedIP ← random(OriginalIP, Key)
17 Else //Undefined Level
18         AnonymizedIP ← OriginalIP
19 End If
```

5.4 วิธีการแปลงกลับหมายเลขไอพีตามระดับความเป็นส่วนตัว

การแปลงกลับหมายเลขไอพี (IP Address Recovery) จะเกี่ยวข้องกับขั้นตอนการแสดงผลและรายงานผลที่ต้องการทราบข้อมูลเดิมก่อนการปิดบังหลังจากที่ผ่านกระบวนการ

วิเคราะห์ผลลัพธ์เรียบร้อยแล้ว โดยการแปลงกลับหมายเลขไอพีนั้นจะแปลงจากหมายเลขไอพีนิรนามให้กลับมาเป็นหมายเลขไอพีดั้งเดิม ซึ่งมีการทำงานตรงข้ามกับการปิดบังหมายเลขไอพี โดยในงานวิจัยเรื่องนี้ได้แปลงกลับหมายเลขไอพีเฉพาะระดับความเป็นส่วนตัวระดับที่ 2 ระดับที่ 3 และ ระดับที่ 4 เท่านั้น ส่วนระดับความเป็นส่วนตัวนอกเหนือจากนี้จะไม่แปลงกลับหมายเลขไอพีแต่อย่างใด ซึ่งรายละเอียดและเหตุผลจะได้กล่าวต่อไปในหัวข้อที่ 6.6 โดยรายละเอียดการแปลงกลับหมายเลขไอพีแสดงไว้ในอัลกอริทึมที่ 5.6

อัลกอริทึมที่ 5.6 อัลกอริทึมการแปลงกลับหมายเลขไอพีตามระดับความเป็นส่วนตัว

```
1   AnonymizedIP ← Input IP Address
2   Subnet ← Input Subnet Mask Address
3   Level ← Input Privacy Level
4   Key ← Input Key
5   LeftPart ← binary(AnonymizedIP) AND binary(AnonymizedIP)
6   RightPart ← substring(LeftPart.length, 32)
7   If (Level is 2)
8           OriginalIP ← recover_cryptopan(LeftPart, Key) + RightPart
9   Else If (Level is 3)
10          OriginalIP ← LeftPart  + recover_cryptopan(RightPart, Key)
11  Else If (Level is 4)
12          OriginalIP ← recover_cryptopan(AnonymizedIP, Key)
13  Else //Other Levels
14          Print “No recovery function”
15  End If
```

จากแบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของความเป็นส่วนตัวในบทนี้ได้ผลลัพธ์และการประเมินผลการทำงานตามรายละเอียดในบทที่ 6 ซึ่งจะได้กล่าวต่อไป

บทที่ 6

ผลการทดลอง

บทนี้เป็นการแสดงผลการทดลองจากการปิดบังหมายเลขไอพีด้วยระดับความเป็นส่วนตัว ผลการใช้วิธีการแบบกฎเพื่อตัดสินใจเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุด และประสิทธิภาพการทำงานของแบบแผนการปิดบัง โดยมีรายละเอียดดังต่อไปนี้

6.1 ผลการเลือกระดับความเป็นส่วนตัวจากปัจจัยการปิดบัง

จากการพิจารณาเลือกระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีนั้น จะพิจารณาจากปัจจัยการปิดบังทั้ง 3 ปัจจัย โดยผลลัพธ์ที่ได้จากการทำงานในแต่ละปัจจัยมีดังต่อไปนี้

6.1.1 ผลการเลือกระดับความเป็นส่วนตัวโดยใช้ต้นไม้ของความเป็นส่วนตัว

จากการทดลองเพื่อหาระดับความเป็นส่วนตัวที่เหมาะสมโดยการพิจารณาเลือกระดับความเป็นส่วนตัวด้วยต้นไม้ของความเป็นส่วนตัว จะต้องพิจารณาจากโครงสร้างของหมายเลขไอพีจากสององค์กรที่ต้องการแลกเปลี่ยนข้อมูลระหว่างกัน ซึ่งประกอบไปด้วยองค์กรที่เป็นผู้ร้องขอหรือเป็นผู้วิเคราะห์ข้อมูล และองค์กรที่ถูกร้องขอหรือถูกวิเคราะห์ข้อมูล โดยมีตัวอย่างรายละเอียดผลลัพธ์ดังตารางที่ 6.1

ตารางที่ 6.1 ตารางตัวอย่างผลลัพธ์การพิจารณาเลือกระดับความเป็นส่วนตัวโดยใช้ต้นไม้ของความเป็นส่วนตัว

ตัวอย่าง	องค์กร	หมายเลขไอพี	หมายเลขสับเน็ตมาสก์	ต้นไม้ของความเป็นส่วนตัว	ระดับความเป็นส่วนตัว
1	A คือจุฬาลงกรณ์มหาวิทยาลัย	161.200.0.0	255.255.0.0	ต้นไม้ที่เป็นอิสระต่อกัน	ระดับที่ไม่มีการปิดบัง
	B คือบริษัทไมโครซอฟต์	207.46.0.0	255.255.0.0		
2	A คือสำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา	202.28.0.0	255.255.0.0	ต้นไม้ที่มีส่วนร่วมกัน	ระดับการปิดบังส่วน n บิตซ้าย
	B คือมหาวิทยาลัยสงขลานครินทร์	202.12.0.0	255.255.0.0		
3	A คือภาควิชาวิศวกรรมคอมพิว-เตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย	161.200.93.0	255.255.254.0	ต้นไม้ที่เป็นส่วนย่อยแท้แบบ A อยู่ใน B	ระดับการปิดบังส่วน n บิตขวา

ตัวอย่าง	องค์กร	หมายเลขไอพี	หมายเลขสับเน็ตมาสก์	ต้นไม้ของความเป็นส่วนตัว	ระดับความเป็นส่วนตัว
	B คือจุฬาลงกรณ์มหาวิทยาลัย	161.200.0.0	255.255.0.0		
4	A คือจุฬาลงกรณ์มหาวิทยาลัย	161.200.0.0	255.255.0.0	ต้นไม้ที่เป็นส่วนย่อยแท้แบบ B อยู่ใน A	ระดับการปิดบังส่วน n บิตขวา
	B คือภาควิชาวิศวกรรมคอมพิว-เตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย	161.200.93.0	255.255.254.0		
5	A คือภาควิชาวิศวกรรมคอมพิว-เตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย	161.200.93.0	255.255.254.0	ต้นไม้ที่สมมูลกัน	ระดับการปิดบังทั้ง 32 บิต
	B คือภาควิชาวิศวกรรมคอมพิว-เตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย	161.200.93.0	255.255.254.0		

กำหนดให้ A แทนองค์กรผู้วิเคราะห์ และ B แทนองค์กรผู้ถูกวิเคราะห์

6.1.2 ผลการเลือกระดับความเป็นส่วนตัวโดยใช้รายการวิเคราะห์เครือข่าย

จากการทดลองเพื่อหาระดับความเป็นส่วนตัวที่เหมาะสมโดยการพิจารณาเลือกระดับความเป็นส่วนตัวด้วยรายการวิเคราะห์เครือข่าย จะต้องพิจารณารายการวิเคราะห์เครือข่ายตามรายละเอียดในหัวข้อที่ 4.3 โดยมีตัวอย่างผลลัพธ์ดังตารางที่ 6.2

ตารางที่ 6.2 ตารางตัวอย่างผลลัพธ์จากการพิจารณาเลือกระดับความเป็นส่วนตัวโดยใช้รายการวิเคราะห์เครือข่าย

ตัวอย่าง	รายการวิเคราะห์เครือข่าย	หมายเลขระดับความเป็นส่วนตัว	ระดับความเป็นส่วนตัว
1	Network Performances Analysis	1	ระดับการปิดบังส่วน n บิตขวา
	Capacity Planning	1	
	Network Bandwidth Usages	1	
	CPU Usages	3	
2	Memory Usages	3	ระดับการปิดบังทั้ง 32 บิต
	Disk Usages	3	
	HTTP Service (Network Summary)	1	
	FTP Service (Network Summary)	1	
	Multicast Traffic Analysis	2	
3	SNMP Service (Device Summary)	4	ระดับการปิดบังทั้ง 32 บิต
	POP3 Service (Device Summary)	4	
	P2P Service (Subnetwork Summary)	2	
4	VoIP Service (Network Summary)	1	ระดับการปิดบังส่วน n บิตซ้าย
	Multicast Traffic Analysis	2	
5	Intrusion Detection	4	ระดับการปิดบังทั้ง 32 บิต
	Log Analysis	4	
	Network Map	4	
6	Web Report (Public)	5	ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม
	Application Report (Public)	5	
7	Network Bandwidth Usages	1	ระดับที่ไม่มีการปิดบัง
	Capacity Planning	1	

6.1.3 ผลการเลือกระดับความเป็นส่วนตัวโดยใช้กฎหมายคอมพิวเตอร์

จากการทดลองเพื่อหาระดับความเป็นส่วนตัวที่เหมาะสมโดยการพิจารณาเลือกระดับความเป็นส่วนตัวด้วยกฎหมายคอมพิวเตอร์ ซึ่งในที่นี้คือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยมีตัวอย่างผลลัพธ์ดังตารางที่ 6.3

ตารางที่ 6.3 ตารางตัวอย่างผลลัพธ์จากการพิจารณาเลือกระดับความเป็นส่วนตัวโดยใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ตัวอย่าง	สถานการณ์ที่เกี่ยวข้องกับพระราชบัญญัติ	มาตรา	ระดับความเป็นส่วนตัว
1	จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ เรียกดูข้อมูลจากเครือข่ายของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ	18 (2)	ระดับที่ไม่มีการปิดบัง
2	จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ ต้องการเรียกดูข้อมูลจากเครือข่ายของมหาวิทยาลัยเกษตรศาสตร์ จึงสั่งให้มหาวิทยาลัยเกษตรศาสตร์ ส่งข้อมูลดังกล่าวไปยังจุฬาลงกรณ์มหาวิทยาลัย	18 (2) 18 (3)	ตามความสัมพันธ์ของต้นไม้ของความเป็นส่วนตัว
3	กระทรวงยุติธรรมซึ่งเป็นพนักงานเจ้าหน้าที่ สั่งให้บริษัททรูบิสซิเนสคอร์เปอร์เรชั่นเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน	26 วรรค 1	ระดับที่ไม่มีการปิดบัง
4	สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษาซึ่งเป็นพนักงานเจ้าหน้าที่ เข้ามาตรวจสอบข้อมูลระบบคอมพิวเตอร์ และข้อมูลจราจรทางคอมพิวเตอร์ของอุปกรณ์ที่ใช้รายบุคคล ในกระทรวงศึกษาธิการ	18 (6)	ระดับการปิดบังทั้ง 32 บิต
5	นาย ก. ซึ่งเป็นพนักงานเจ้าหน้าที่ที่ได้รับการแต่งตั้งตาม พระราชบัญญัติ ทำสำเนาข้อมูลคอมพิวเตอร์ และข้อมูลจราจรจากระบบคอมพิวเตอร์ เพื่อนำมาวิเคราะห์ค่าทางสถิติ	18 (4)	ตามรายการวิเคราะห์เครือข่าย

6.2 ผลการเลือกระดับความเป็นส่วนตัวจากสถานการณ์การปิดบังหมายเลขไอพี

จากตัวอย่างผลลัพธ์ในหัวข้อที่ 6.1 ซึ่งมีกระบวนการพิจารณาการเลือกระดับความเป็นส่วนตัวที่แตกต่างกันตามปัจจัยการปิดบัง ผลลัพธ์จากแต่ละปัจจัยการปิดบังนั้นจะถูกพิจารณาร่วมกันในขั้นตอนสุดท้ายเพื่อตัดสินและเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุด ต่อไปนี้เป็นตัวอย่างสถานการณ์การปิดบังหมายเลขไอพี และผลลัพธ์สุดท้ายของการพิจารณาร่วมกันจากทุกปัจจัยการปิดบัง

1. สถานการณ์ที่ 1 ศาลแต่งตั้งให้จุฬาลงกรณ์มหาวิทยาลัยเป็นพนักงานเจ้าหน้าที่เพื่อให้จุฬาลงกรณ์มหาวิทยาลัย สั่งให้บริษัทไมโครซอฟต์เก็บข้อมูลการจราจรทางคอมพิวเตอร์ไว้อย่างน้อย 90 วัน มีผลลัพธ์ดังแสดงในตารางที่ 6.4

ตารางที่ 6.4 ตารางตัวอย่างผลลัพธ์จากการพิจารณาเลือกระดับความเป็นส่วนตัวจากสถานการณ์การปิดบังสถานการณ์ที่ 1

ข้อมูลรับเข้า		
1.	หมายเลขไอพีของจุฬาลงกรณ์มหาวิทยาลัย	161.200.0.0 (10100001110010000000000000000000)
2.	หมายเลขสับเน็ตมาสก์ของจุฬาลงกรณ์มหาวิทยาลัย	255.255.0.0 (11111111111111110000000000000000)
3.	หมายเลขไอพีของบริษัทไมโครซอฟต์	207.46.0.0 (11001111001011100000000000000000)
4.	หมายเลขสับเน็ตมาสก์ของบริษัทไมโครซอฟต์	255.255.0.0 (11111111111111110000000000000000)
ระดับความเป็นส่วนตัวจากปัจจัยการปิดบัง		
1.	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับที่ไม่มีการปิดบัง (ต้นไม้ที่เป็นอิสระต่อกัน)
2.	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับที่ไม่มีการปิดบัง
3.	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ระดับที่ไม่มีการปิดบัง (มาตรา 26 วรรค 1)
ระดับความเป็นส่วนตัวสุดท้ายที่เลือก คือ ระดับที่ไม่มีการปิดบัง		

2. สถานการณ์ที่ 2 จุฬาลงกรณ์มหาวิทยาลัยเป็นพนักงานเจ้าหน้าที่เรียกดูข้อมูลจราจรในระบบเครือข่ายคอมพิวเตอร์ของภาควิชาวิศวกรรมคอมพิวเตอร์ เพื่อใช้ในการวิเคราะห์สถิติการใช้งานโปรโตคอลเอชทีทีพี และโปรโตคอลเอฟทีพี ของเครือข่ายภาควิชาวิศวกรรมคอมพิวเตอร์ มีผลลัพธ์ดังแสดงในตารางที่ 6.5

ตารางที่ 6.5 ตารางตัวอย่างผลลัพธ์จากการพิจารณาเลือกระดับความเป็นส่วนตัวจากสถานการณ์การปิดบังสถานการณ์ที่ 2

ข้อมูลรับเข้า		
1.	หมายเลขไอพีของจุฬาลงกรณ์มหาวิทยาลัย	161.200.0.0 (10100001110010000000000000000000)
2.	หมายเลขสับเน็ตมาสก์ของจุฬาลงกรณ์มหาวิทยาลัย	255.255.0.0 (11111111111111110000000000000000)
3.	หมายเลขไอพีของภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาฯ	161.200.93.0 (10100001110010000101110100000000)
4.	หมายเลขสับเน็ตมาสก์ของภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาฯ	255.255.254.0 (11111111111111111111111000000000)
ระดับความเป็นส่วนตัวจากปัจจัยการปิดบัง		
1.	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับการปิดบังส่วน n บิตขวา (ต้นไม้ที่เป็นส่วนย่อยแท้แบบ B อยู่ใน A)
2.	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับที่ไม่มีการปิดบัง
3.	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ระดับที่ไม่มีการปิดบัง (มาตรา 18 (2))
ระดับความเป็นส่วนตัวสุดท้ายที่เลือก คือ ระดับการปิดบังส่วน n บิตขวา		

3. สถานการณ์ที่ 3 กระทรวงยุติธรรมซึ่งเป็นพนักงานเจ้าหน้าที่ สั่งให้บริษัทชินคอร์เปอร์เรชั่นเก็บรักษาข้อมูลการจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน และได้ทำสำเนาข้อมูลคอมพิวเตอร์ และข้อมูลจราจรจากระบบคอมพิวเตอร์ เพื่อนำมาวิเคราะห์การใช้งานแบนด์วิดท์ของเครือข่าย การใช้งานซีพียู การใช้งานหน่วยความจำ และ การใช้งานดิสก์ ของเครือข่ายบริษัทชินคอร์เปอร์เรชั่น มีผลลัพธ์ดังแสดงในตารางที่ 6.6

ตารางที่ 6.6 ตารางตัวอย่างผลลัพธ์จากการพิจารณาเลือกระดับความเป็นส่วนตัวจากสถานการณ์การปิดบังสถานการณ์ที่ 3

ข้อมูลรับเข้า		
1.	หมายเลขไอพีของกระทรวงยุติธรรม	210.246.159.0 (11010010111101101001111100000000)
2.	หมายเลขสับเน็ตมาสก์ของกระทรวงยุติธรรม	255.255.254.0 (11111111111111111111111000000000)
3.	หมายเลขไอพีของบริษัทชินคอร์เปอร์เรชั่น	202.183.253.0 (11001010101101111111110100000000)
4.	หมายเลขสับเน็ตมาสก์ของบริษัทชินคอร์เปอร์เรชั่น	255.255.255.0 (11111111111111111111111100000000)
ระดับความเป็นส่วนตัวจากปัจจัยการปิดบัง		
1.	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับที่ไม่มีการปิดบัง (ต้นไม้ที่เป็นอิสระต่อกัน)
2.	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับการปิดบังส่วน n บิตขวา
3.	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ตามรายการวิเคราะห์เครือข่าย (มาตรา 26 วรรค 1 และ มาตรา 18 (4))
ระดับความเป็นส่วนตัวสุดท้ายที่เลือก คือ ระดับการปิดบังส่วน n บิตขวา		

ตัวอย่างสถานการณ์การปิดบังหมายเลขไอพีในสถานการณ์อื่นๆ นอกเหนือจากที่ได้ยกอย่างอย่างไว้ข้างต้น ได้แจกแจงเพิ่มเติมไว้ในส่วนของภาคผนวก ก

6.3 ผลการปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัว

จากผลลัพธ์ในหัวข้อที่ 6.2 ซึ่งก็คือระดับความเป็นส่วนตัวในการปิดบังหมายเลขไอพี โดยผลลัพธ์จากการปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวที่ถูกเลือกมีรายละเอียดดังต่อไปนี้

กำหนดให้ หมายเลขไอพีของเครือข่ายเป็น 161.200.92.0 (10100001110010000101110000000000) และ หมายเลขสับเน็ตมาสก์เป็น 255.255.255.0 (11111111111111111111111100000000) และกุญแจในการปิดบังเป็น 11101010010011010010110110010010 จะได้ผลลัพธ์จากการปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวแต่ละระดับดังแสดงในตัวอย่างตามตารางที่ 6.7

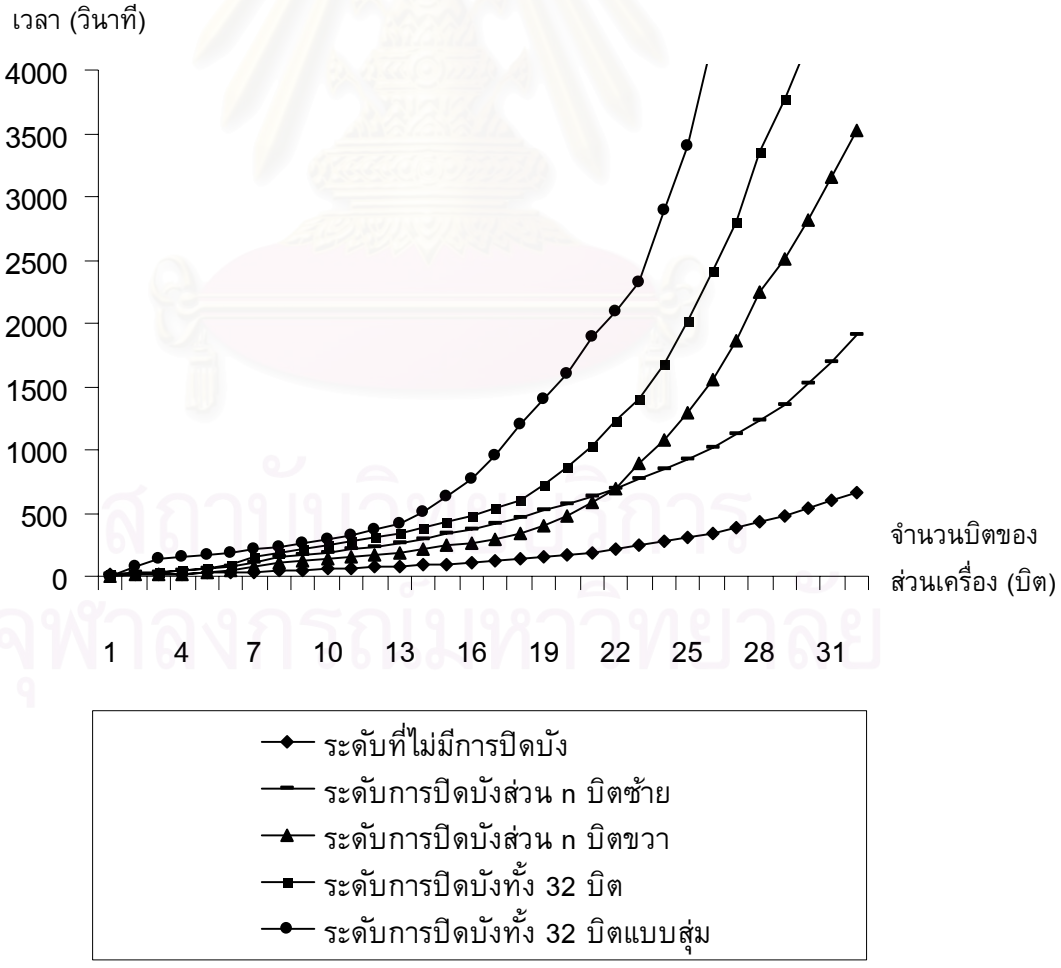
ตารางที่ 6.7 ตารางตัวอย่างผลลัพธ์ของการปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวแต่ละระดับ

ระดับที่ไม่มีการปิดบัง	ระดับการปิดบังส่วน n บิตซ้าย	ระดับการปิดบังส่วน n บิตขวา	ระดับการปิดบังทั้ง 32 บิต	ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม
161.200.92.0	75.133.113.0	161.200.92.146	75.133.113.146	47.168.34.128
161.200.92.1	75.133.113.1	161.200.92.147	75.133.113.147	170.45.182.23
161.200.92.2	75.133.113.2	161.200.92.144	75.133.113.144	95.156.134.221
161.200.92.3	75.133.113.3	161.200.92.145	75.133.113.145	163.223.31.131
161.200.92.4	75.133.113.4	161.200.92.150	75.133.113.150	24.142.23.41
161.200.92.5	75.133.113.5	161.200.92.151	75.133.113.151	230.69.82.31
161.200.92.6	75.133.113.6	161.200.92.148	75.133.113.148	138.171.158.170
161.200.92.7	75.133.113.7	161.200.92.149	75.133.113.149	181.57.77.28
161.200.92.8	75.133.113.8	161.200.92.154	75.133.113.154	161.244.21.11
161.200.92.9	75.133.113.9	161.200.92.155	75.133.113.155	143.196.186.11
161.200.92.10	75.133.113.10	161.200.92.152	75.133.113.152	18.255.210.79
161.200.92.11	75.133.113.11	161.200.92.153	75.133.113.153	75.130.151.108
161.200.92.12	75.133.113.12	161.200.92.158	75.133.113.158	24.115.131.239
161.200.92.13	75.133.113.13	161.200.92.159	75.133.113.159	170.123.63.59
161.200.92.14	75.133.113.14	161.200.92.156	75.133.113.156	1.232.73.240
161.200.92.15	75.133.113.15	161.200.92.157	75.133.113.157	20.78.3.15
161.200.92.16	75.133.113.16	161.200.92.130	75.133.113.130	158.8.51.53
161.200.92.17	75.133.113.17	161.200.92.131	75.133.113.131	254.197.52.62
161.200.92.18	75.133.113.18	161.200.92.128	75.133.113.128	23.156.204.118
161.200.92.19	75.133.113.19	161.200.92.129	75.133.113.129	64.205.203.231
161.200.92.20	75.133.113.20	161.200.92.134	75.133.113.134	187.196.145.5
161.200.92.21	75.133.113.21	161.200.92.135	75.133.113.135	98.241.123.94
161.200.92.22	75.133.113.22	161.200.92.132	75.133.113.132	64.25.63.109
161.200.92.23	75.133.113.23	161.200.92.133	75.133.113.133	169.145.4.66
161.200.92.24	75.133.113.24	161.200.92.138	75.133.113.138	61.205.254.74
161.200.92.25	75.133.113.25	161.200.92.139	75.133.113.139	174.132.215.39
161.200.92.26	75.133.113.26	161.200.92.136	75.133.113.136	145.244.59.185
161.200.92.27	75.133.113.27	161.200.92.137	75.133.113.137	39.216.119.84
161.200.92.28	75.133.113.28	161.200.92.142	75.133.113.142	71.224.245.108
161.200.92.29	75.133.113.29	161.200.92.143	75.133.113.143	125.38.37.114

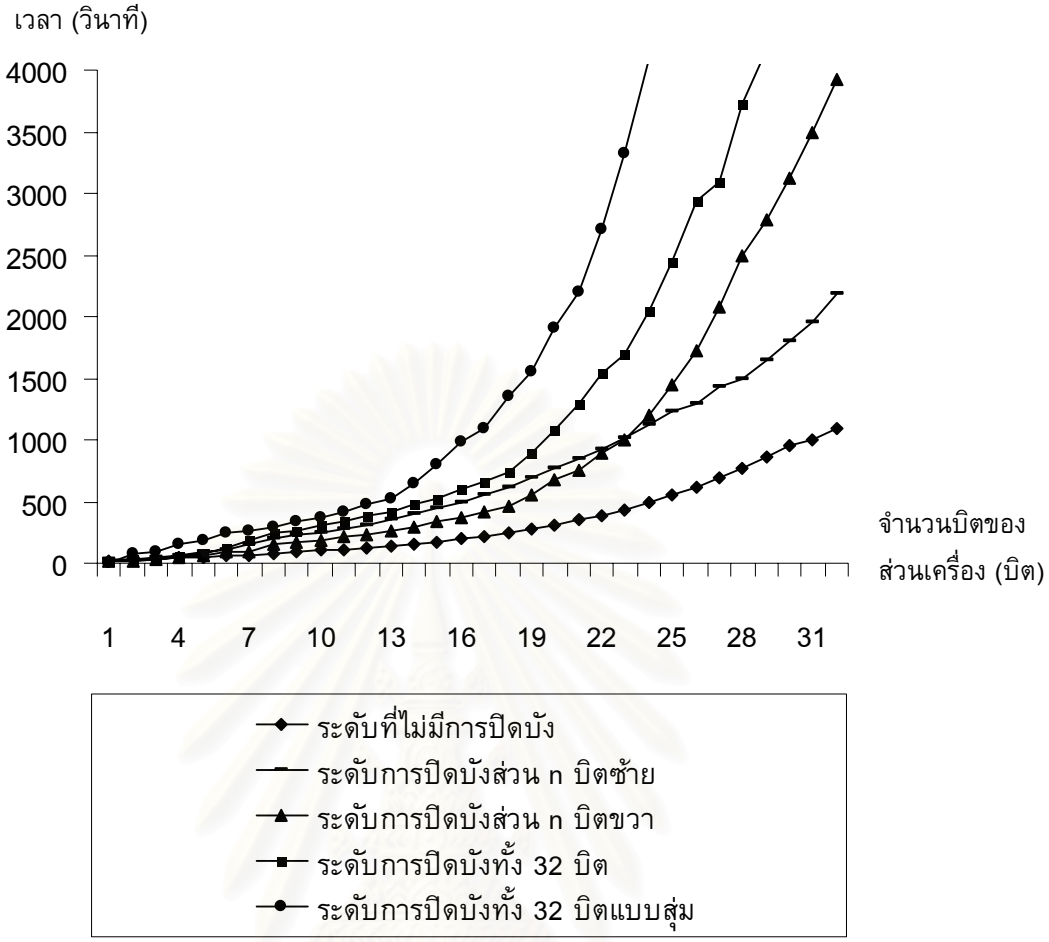
ระดับที่ไม่มีการปิดบัง	ระดับการปิดบังส่วน n บิตซ้าย	ระดับการปิดบังส่วน n บิตขวา	ระดับการปิดบังทั้ง 32 บิต	ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม
161.200.92.30	75.133.113.30	161.200.92.140	75.133.113.140	8.93.170.176
161.200.92.31	75.133.113.31	161.200.92.141	75.133.113.141	131.214.252.253
161.200.92.32	75.133.113.32	161.200.92.178	75.133.113.178	142.240.124.200
161.200.92.33	75.133.113.33	161.200.92.179	75.133.113.179	148.253.167.189
161.200.92.34	75.133.113.34	161.200.92.176	75.133.113.176	47.146.109.94
161.200.92.35	75.133.113.35	161.200.92.177	75.133.113.177	127.220.206.32
161.200.92.36	75.133.113.36	161.200.92.182	75.133.113.182	99.183.24.21
161.200.92.37	75.133.113.37	161.200.92.183	75.133.113.183	85.2.192.113
161.200.92.38	75.133.113.38	161.200.92.180	75.133.113.180	71.163.22.122
161.200.92.39	75.133.113.39	161.200.92.181	75.133.113.181	41.41.170.100
161.200.92.40	75.133.113.40	161.200.92.186	75.133.113.186	209.34.48.35
161.200.92.41	75.133.113.41	161.200.92.187	75.133.113.187	244.233.212.61
161.200.92.42	75.133.113.42	161.200.92.184	75.133.113.184	136.225.121.12
161.200.92.43	75.133.113.43	161.200.92.185	75.133.113.185	185.123.170.79
161.200.92.44	75.133.113.44	161.200.92.190	75.133.113.190	71.62.132.173
161.200.92.45	75.133.113.45	161.200.92.191	75.133.113.191	203.157.202.149
161.200.92.46	75.133.113.46	161.200.92.188	75.133.113.188	255.108.170.227
161.200.92.47	75.133.113.47	161.200.92.189	75.133.113.189	179.233.155.215
161.200.92.48	75.133.113.48	161.200.92.162	75.133.113.162	30.219.155.43
161.200.92.49	75.133.113.49	161.200.92.163	75.133.113.163	106.246.45.90
161.200.92.50	75.133.113.50	161.200.92.160	75.133.113.160	216.195.229.196
161.200.92.51	75.133.113.51	161.200.92.161	75.133.113.161	250.239.35.109
161.200.92.52	75.133.113.52	161.200.92.166	75.133.113.166	242.46.76.167
161.200.92.53	75.133.113.53	161.200.92.167	75.133.113.167	41.217.148.50
161.200.92.54	75.133.113.54	161.200.92.164	75.133.113.164	55.69.86.197
161.200.92.55	75.133.113.55	161.200.92.165	75.133.113.165	15.108.72.89
161.200.92.56	75.133.113.56	161.200.92.170	75.133.113.170	173.181.39.40
161.200.92.57	75.133.113.57	161.200.92.171	75.133.113.171	217.237.82.48
161.200.92.58	75.133.113.58	161.200.92.168	75.133.113.168	75.50.157.196
161.200.92.59	75.133.113.59	161.200.92.169	75.133.113.169	45.27.44.251
161.200.92.60	75.133.113.60	161.200.92.174	75.133.113.174	192.244.149.0
161.200.92.61	75.133.113.61	161.200.92.175	75.133.113.175	177.137.29.77
161.200.92.62	75.133.113.62	161.200.92.172	75.133.113.172	164.169.71.144

6.4 ความเร็วในการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว

ผลลัพธ์จากการปิดบังหมายเลขไอพีตามแบบแผนการปิดบังของงานวิจัยเรื่องนี้มีรูปแบบหมายเลขไอพี 5 รูปแบบ ตามระดับความเป็นส่วนตัว 5 ระดับ ซึ่งกระบวนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัวนี้สามารถเพิ่มประสิทธิภาพในด้านความเร็วได้ดียิ่งขึ้น โดยสามารถลดระยะเวลาในการประมวลผลลงและเพิ่มความเร็วในการปิดบังให้เร็วยิ่งขึ้น ที่เป็นเช่นนี้เพราะว่า แบบแผนการปิดบังหมายเลขไอพีดังกล่าวสามารถปิดบังเฉพาะบางบิตหรือบางส่วนของหมายเลขไอพีที่จำเป็นได้ ซึ่งกราฟการวัดค่าเวลาในการปิดบังได้แสดงไว้ในรูปที่ 6.1 และ 6.2 ตามลำดับ โดยรูปที่ 6.1 เป็นกราฟค่าเวลาในการปิดบังหมายเลขไอพีแบบช่วงเวลา และรูปที่ 6.2 เป็นกราฟค่าเวลาในการปิดบังหมายเลขไอพีแบบทันกาล ซึ่งกระบวนการทดลองนี้กระทำภายใต้เครื่องคอมพิวเตอร์ Intel® Core 2 Duo Processor 1.6 GHz หน่วยความจำขนาด 1.0 GB ระบบปฏิบัติการ Windows Vista และกระบวนการทดลองทั้งหมดกระทำภายใต้ระบบจำลอง เพื่อสร้างและกำหนดหมายเลขไอพีที่เป็นไปได้ทั้งหมดในการปิดบัง



รูปที่ 6.1 กราฟค่าเวลาในการปิดบังหมายเลขไอพีแบบช่วงเวลา



รูปที่ 6.2 กราฟค่าเวลาในการปิดบังหมายเลขไอพีแบบทันกาล

จากรายละเอียดของกราฟตามรูปที่ 6.1 และรูปที่ 6.2 แสดงให้เห็นรายละเอียดหลายประการกล่าวคือ การปิดบังหมายเลขไอพีโดยใช้ระดับที่ไม่มีการปิดบัง ระดับการปิดบังส่วน n บิตซ้าย และระดับการปิดบังส่วน n บิตขวา สามารถประมวลผลและปิดบังหมายเลขไอพีโดยใช้ระยะเวลาในการประมวลผลที่น้อยกว่าระดับการปิดบังทั้ง 32 บิต ที่เป็นวิธีการแบบเดิมของอัลกอริทึมที่ได้นำเสนอก่อนหน้านี้ โดยจะเห็นได้ว่ายิ่งมีจำนวนเครื่องในเครือข่ายมากขึ้นก็จะทำให้สามารถลดระยะเวลาในการประมวลผลได้มากขึ้น

ดังนั้นจึงสามารถกล่าวได้ว่าแบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัวที่ได้นำเสนอในงานวิจัยเรื่องนี้สามารถเพิ่มความเร็วในการปิดบังหมายเลขไอพีได้ตามความเหมาะสมกับสภาพการใช้งานจริงของการปิดบังข้อมูล

6.5 ประสิทธิภาพในการป้องกันการถูกโจมตี

แบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัวที่ได้นำเสนอนี้มีความมั่นคงและความปลอดภัยจากการถูกโจมตีสูงกว่าแบบแผนการปิดบังแบบเดิมที่ปิดบังทั้ง 32 บิตของหมายเลขไอพี เพราะผู้โจมตีไม่สามารถทราบได้ว่าบิตใดหรือส่วนใดของหมายเลขไอพีที่ถูกปิดบังบ้าง และถูกปิดบังจำนวนกี่บิต

ตัวอย่างของอัลกอริทึมอย่างง่ายในการสุ่มโจมตีข้อมูลที่แสดงหมายเลขไอพีนิรนามเพื่อให้ได้มาซึ่งหมายเลขไอพีดั้งเดิมแสดงไว้ในอัลกอริทึมที่ 6.1 และ 6.2 ตามลำดับ โดยอัลกอริทึมที่ 6.1 เป็นอัลกอริทึมการโจมตีข้อมูลที่แสดงหมายเลขไอพีนิรนามตามการปิดบังแบบเดิมที่ปิดบังทั้ง 32 บิต ของหมายเลขไอพี และอัลกอริทึมที่ 6.2 เป็นอัลกอริทึมการโจมตีข้อมูลที่แสดงหมายเลขไอพีนิรนามตามการปิดบังที่นำเสนอ ซึ่งสามารถปิดบังเพียงบางบิตหรือบางส่วนของหมายเลขไอพีได้

อัลกอริทึมที่ 6.1 อัลกอริทึมการโจมตีข้อมูลที่แสดงหมายเลขไอพีนิรนามตามการปิดบังแบบเดิม

```
1  N ← 2^32 //Possible Number of IP Address
2  For (Key ← 1 to N)
3      Key ← keyGeneration()
4      For (OriginalIP ← 1 to N)
5          TestIP ← cryptopan(OriginalIP, Key)
6          If (AnonymizedIP equals TestIP) Return TestIP
7      End For
8  End For
```

อัลกอริทึมที่ 6.2 อัลกอริทึมการโจมตีข้อมูลที่แสดงหมายเลขไอพีนิรนามตามการปิดบังที่นำเสนอ

```
1  N ← 2^32 //Possible Number of IP Address
2  For (Key ← 1 to N)
3      Key ← keyGeneration()
4      For (OriginalIP ← 1 to N)
5          TestIP ← cryptopan(OriginalIP, Key)
6          For (BitIndex ← 1 to 32)
7              If (AnonymizedIP equals TestIP) Return TestIP
```

8	End For
9	For (BitIndex ← 32 to 1)
10	If (AnonymizedIP equals TestIP) Return TestIP
11	End For
12	End For
13	End For

จากอัลกอริทึมที่ 6.1 จะต้องใช้จำนวนครั้งในการสุ่มโจมตีหมายเลขไอพีทั้งหมด N^2 ครั้ง ส่วนอัลกอริทึมที่ 6.2 จะต้องใช้จำนวนครั้งในการสุ่มโจมตีหมายเลขไอพีทั้งหมด $64N^2$ ครั้ง เพราะว่าในอัลกอริทึมที่ 6.2 นั้นจะต้องใช้เวลาในการสลับบิตจากซ้ายไปขวาและจากขวาไปซ้ายอย่างละ 32 ครั้ง รวมเป็น 64 ครั้ง เพิ่มเข้ามา ดังนั้นจึงแสดงให้เห็นว่าแบบแผนการปิดบังหมายเลขไอพีที่นำเสนอนี้ ถูกโจมตีได้ยากกว่าแบบแผนการปิดบังหมายเลขไอพีแบบเดิมอยู่ 64 เท่า ในขณะที่ไม่ต้องปิดบังทั้ง 32 บิตของหมายเลขไอพี

6.6 ผลการวิเคราะห์การแปลงกลับหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว

การแปลงกลับหมายเลขไอพีนั้นส่วนใหญ่แล้วจะเกี่ยวข้องกับกระบวนการแสดงผลและรายงานผลหลังจากที่ผ่านกระบวนการวิเคราะห์ผลลัพธ์เรียบร้อยแล้ว จากผลการศึกษาวิจัยพบว่า กระบวนการแปลงกลับหมายเลขไอพีมีความสำคัญเพียงส่วนน้อย เพราะเนื่องจากว่าแบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัวที่ได้นำเสนอนั้น ปิดบังหมายเลขไอพีได้อย่างเหมาะสมตามสถานการณ์และความต้องการการใช้ข้อมูล ซึ่งเมื่อปิดบังแล้วก็ยังสามารถสื่อความหมายและใช้งานในกระบวนการวิเคราะห์เครือข่ายได้อย่างถูกต้อง และการแสดงผลลัพธ์ด้วยหมายเลขไอพีนิรนามนั้นก็ยังให้ค่าและความหมายเช่นเดียวกับหมายเลขไอพีดั้งเดิม จึงมีความจำเป็นน้อยหรือไม่มีความจำเป็นใดเลยในการแปลงกลับหมายเลขไอพี เช่น ถ้าผลลัพธ์ที่ได้อยู่ในรูปของตัวเลขหรือข้อมูลเชิงสรุป กระบวนการแปลงกลับหมายเลขไอพีก็ไม่มีความจำเป็นแต่ประการใด หรือการปิดบังโดยใช้ระดับความเป็นส่วนตัวระดับที่ 1 คือ ระดับที่ไม่มีการปิดบัง ซึ่งไม่ต้องการกระบวนการแปลงกลับหมายเลขไอพีแม้แต่น้อย หรือการแสดงผลลัพธ์ต่อที่สาธารณะโดยใช้การปิดบังด้วยระดับความเป็นส่วนตัวระดับที่ 5 คือ ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม ก็ไม่ต้องการการแปลงกลับหมายเลขไอพี หรือแม้กระทั่งการแสดงผลโดยใช้การปิดบังด้วยระดับความเป็นส่วนตัวระดับที่ 4 คือ ระดับการปิดบังทั้ง 32 บิต ก็ไม่มีความจำเป็นในการแปลงกลับหมายเลขไอพี เพราะหมายเลขไอพีนิรนามที่ได้นั้นยังคงไว้ซึ่งค่าที่ต้องการแสดงผลและรักษาความเป็นส่วนตัวได้อย่างสมบูรณ์ครบถ้วน ในขณะที่การปิดบังหมายเลขไอพีด้วยระดับความเป็นส่วนตัวระดับที่ 2 และ 3 ซึ่งมีการปิดบังเพียงบางบิตและบางส่วนของหมายเลขไอพี ก็มีความจำเป็นน้อยในการแปลงกลับหมายเลขไอ

พี เพราะหมายเลขไอพีนิรนามที่ได้นั้นยังสื่อความหมายได้เช่นเดียวกับหมายเลขไอพีดั้งเดิมทั้งในส่วนที่ถูกปิดบังและส่วนที่ไม่ถูกปิดบัง

การแปลงกลับหมายเลขไอพีจะถูกใช้ก็ต่อเมื่อต้องการทราบถึงค่าของข้อมูลก่อนการปิดบังหมายเลขไอพี ซึ่งหมายถึงการทราบหมายเลขไอพีจริงและทราบถึงอุปกรณ์หรือตัวบุคคลที่แท้จริง การกระทำเช่นนี้มีความละเอียดอ่อน ดังนั้นการแปลงกลับหมายเลขไอพีจึงต้องระมัดระวัง

จากที่ได้กล่าวมาทั้งหมดในบทนี้คือผลลัพธ์ที่ได้และประสิทธิภาพการทำงานของแบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว ซึ่งบทสรุปของงานวิจัยเรื่องนี้จะได้กล่าวไว้ในบทต่อไป

บทที่ 7

สรุปผลการวิจัยและข้อเสนอแนะ

7.1 สรุปผลการวิจัย

งานวิจัยเรื่องนี้ได้นำเสนอระดับความเป็นส่วนตัว 5 ระดับเพื่อใช้ในกระบวนการปิดบังหมายเลขไอพีอันได้แก่ ระดับที่ไม่มีการปิดบัง ระดับการปิดบังส่วน n บิตซ้าย ระดับการปิดบังส่วน n บิตขวา ระดับการปิดบังทั้ง 32 บิต และระดับการปิดบังทั้ง 32 บิตแบบสุ่ม โดยได้ประยุกต์ใช้ระดับความเป็นส่วนตัวเหล่านี้กับวิธีการปิดบังที่คงไว้ซึ่งกลุ่มเครือข่ายซึ่งเลือกวิธีคริปโตแพนในการทดสอบและใช้งาน งานวิจัยเรื่องนี้ยังได้นำเสนอปัจจัยการปิดบัง 3 ปัจจัยเพื่อใช้สำหรับพิจารณาเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุดในการปิดบังหมายเลขไอพี ได้แก่ โครงสร้างต้นไม้ของความเป็นส่วนตัว รายการวิเคราะห์เครือข่าย และกฎหมายคอมพิวเตอร์ ซึ่งปัจจัยการปิดบังทั้ง 3 ปัจจัยถูกผนวกเข้าด้วยกันโดยใช้วิธีการแบบกฎ หลักการทั้งหมดนี้ได้มาซึ่งแบบแผนการปิดบังหมายเลขไอพีแบบใหม่บนพื้นฐานของระดับความเป็นส่วนตัว

ผลลัพธ์ที่ได้จากการทดลองสามารถสรุปได้ว่าแบบแผนการปิดบังหมายเลขไอพีที่ได้นำเสนอในงานวิจัยเรื่องนี้มีประสิทธิภาพที่ดีกว่าแบบแผนการปิดบังหมายเลขไอพีแบบเดิมที่ได้นำเสนอก่อนหน้านี้หลายประการดังต่อไปนี้

1. แบบแผนการปิดบังหมายเลขไอพีที่ได้นำเสนอสามารถปิดบังหมายเลขไอพีได้ตามความเหมาะสมในสภาพความเป็นจริงของการใช้งานข้อมูล และสามารถพิจารณาเลือกปิดบังเพียงบางส่วน ปิดบังทั้ง 32 บิต หรือไม่ปิดบังหมายเลขไอพีได้ตามความเหมาะสม ซึ่งแบบแผนการปิดบังดังกล่าวสามารถรักษาความลับและความเป็นส่วนตัวได้เหมือนกับวิธีการปิดบังแบบเดิมทุกประการ

2. แบบแผนการปิดบังหมายเลขไอพีที่ได้นำเสนอสามารถประมวลผลได้เร็วและดีกว่าแบบแผนการปิดบังแบบเดิม และเหมาะสำหรับการใช้งานในการสูบจับแพ็คเก็ตทั้งแบบช่วงเวลา (Batch) และแบบทันกาล (Real-Time) ได้อย่างมีประสิทธิภาพ ทั้งยังเหมาะสำหรับการสูบจับแพ็คเก็ตที่มีขนาดมหาศาลได้

3. แบบแผนการปิดบังหมายเลขไอพีที่ได้นำเสนอมีความมั่นคงและความปลอดภัยที่สูงกว่าแบบแผนการปิดบังแบบเดิม เพราะไม่สามารถทราบได้ว่าบิตใดหรือส่วนใดของหมายเลขไอพีที่ถูกปิดบังบ้าง และปิดบังบิตจำนวนเท่าใด

4. แบบแผนการปิดบังหมายเลขไอที่ได้นำเสนอสามารถปิดบังหมายเลขไอพีได้อย่างเหมาะสมตามสถานการณ์และความต้องการการใช้ข้อมูล และสามารถสื่อความหมายและใช้งานในกระบวนการวิเคราะห์เครือข่ายได้อย่างถูกต้อง อีกทั้งการแสดงผลลัพธ์ด้วยหมายเลขไอพีนิรนามนั้นก็ยังให้ค่าและความหมายเช่นเดียวกับหมายเลขไอพีดั้งเดิม จึงมีความจำเป็นน้อยหรือไม่มีความจำเป็นใดเลยในการแปลงกลับหมายเลขไอพี

5. แบบแผนการปิดบังหมายเลขไอพีที่ได้นำเสนอเป็นประโยชน์สำหรับองค์กรสององค์กรใดๆ ในการแลกเปลี่ยนข้อมูลระหว่างกัน

7.2 ข้อเสนอแนะและแนวทางการทำวิจัยในอนาคต

ในงานวิจัยเรื่องนี้มีข้อเสนอแนะและแนวทางในการทำวิจัยในอนาคตดังต่อไปนี้

1. งานวิจัยเรื่องนี้ยังไม่ได้มีการทดสอบการใช้งานกับเครื่องมือวิเคราะห์เครือข่ายและเครื่องมือจัดการเครือข่ายจริง ดังนั้นในอนาคตจะต้องทดลองและประยุกต์ใช้แบบแผนการปิดบังที่ได้นำเสนอนี้กับเครื่องมือเหล่านั้น

2. งานวิจัยเรื่องนี้ยังไม่ได้มีการตรวจวัดประสิทธิภาพในการทำงานกับระบบเครือข่ายจริงซึ่งจำเป็นต้องเพิ่มการวัดผลและประเมินผลการทำงานของแบบแผนการปิดบังที่ได้นำเสนอนี้กับระบบเครือข่ายจริงต่อไปในอนาคต

3. งานวิจัยเรื่องนี้ยังไม่ได้ครอบคลุมแบบแผนการปิดบังหมายเลขไอพีรุ่นที่ 6 ซึ่งจะใช้งานกันอย่างแพร่หลายในอนาคต ดังนั้นอาจจำเป็นต้องพัฒนาแบบแผนการปิดบังที่ได้นำเสนอนี้ให้เข้ากับหมายเลขไอพีรุ่นที่ 6 ด้วยเช่นกัน

รายการอ้างอิง

[1] ภาณุพันธ์ สุวรรณมาตร์. การวิเคราะห์สถิติการใช้งานอินเตอร์เน็ตในระบบเครือข่ายระดับสถาบันอุดมศึกษา. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2541.

[2] Brekne, T., Arnes, A., and Oslebo, A. Anonymization of IP Traffic Monitoring Data: Attacks on Two Prefix-preserving Anonymization Schemes and Some Proposed Remedies. In Proceedings of Workshop on Privacy Enhancing Technologies (PET), 2005.

[3] Ethereal. Ethereal Online Documentation [Online]. Available from: http://www.ethereal.com/docs/ [18 January 2009]

[4] Haibl, F., and Dressler, F. Anonymization of Measurement and Monitoring Data: Requirements and Solutions. Praxis der Informationsverarbeitung und Kommunikation (PIK), 2006.

[5] Keardsri, W. A Prototype of Completed Network Management System Using SNMP and Ping/Port Checking for Monitoring of Managed and Unmanaged Devices. In Proceedings of 5th International Joint Conference on Computer Science and Software Engineering (JCSSE), 2008.

[6] Kohler, E., Li, J., Paxson, V., and Shenker, S. Observed Structure of Addresses in IP Traffic. IEEE/ACM Transactions on Networking (TON), 2006.

[7] Koukis, D., Antonatos, S., and Anagnostakis, K.G. On the Privacy Risks of Publishing Anonymized IP Network Traces. In Proceedings of 10th Conference in the Communications and Multimedia Security (CMS), 2006.

[8] Kurose, J.F., and Ross, K.W. Computer Networking: A Top-Down Approach Featuring the Internet. 2nd ed., Addison-Wesley Publishing Company, New York, 2003.

[9] Manage Engine. OpManager: Network Monitoring Software [Online]. Available from: http://manageengine.adventnet.com/products/opmanager/ [21 March 2008]

[10] Minshall, G. Tcpdpriv Command Manual, 1996.

[11] Nagios. Nagios Documentation [Online]. Available from: http://www.nagios.org/docs/ [18 January 2009]

[12] NTOP. NTOP Documentation [Online]. Available from: http://www.ntop.org/documentation.html [18 January 2009]

[13] Oetiker, T. MRTG: Multi Router Traffic Grapher [Online]. Available from: http://oss.oetiker.ch/mrtg/ [18 January 2009]

[14] OpenNMS. OpenNMS Documentation [Online]. Available from: http://www.opennms.org/index.php/Documentation/ [18 January 2009]

[15] Potorti, F. Tcpdpriv [Online]. Available from: http://fly.isti.cnr.it/software/tcpdpriv/ [10 February 2008]

[16] Ramaswamy, R., and Wolf, T. High-Speed Prefix-Preserving IP Address Anonymization for Passive Measurement Systems. IEEE/ACM Transactions on Networking (TON), 2007.

[17] Smith, R. IP Address: Your Internet Identity [Online]. Available from: http://www.ntia.doc.gov/ntiahome/privacy/files/smith.htm [21 March 2008]

[18] SourceForge. EgoNet [Online]. Available from: http://sourceforge.net/projects/egonet/ [18 January 2009]

[19] Tcpdump. TCPDUMP/LIBPCAP public repository [Online]. Available from: http://www.tcpdump.org/ [18 January 2009]

[20] Wikipedia, IP Address [Online]. Available from: http://en.wikipedia.org/wiki/IP_Address [21 March 2008]

[21] Wikipedia, Paessler Router Traffic Grapher [Online]. Available from: http://en.wikipedia.org/wiki/PRTG [21 March 2008]

[22] Xu, J., Fan, J., Ammar, M.H., and Moon, S.B. On the design and performance of prefix-preserving IP traffic trace anonymization. In Proceedings of ACM SIGCOMM Internet Measurement Workshop, 2001.

[23] Xu, J., Fan, J., Ammar, M.H., and Moon, S.B. Prefix-preserving IP address anonymization: measurement based security evaluation and a new cryptographybased scheme. In Proceedings of IEEE International Conference on Network Protocols (ICNP), 2002.

[24] Ylonen, T. Thoughts on how to mount an attack on TPCpdriv's ''-a50'' option, 1996.

[25] Zhang, Q., and Li, X. An IP Address Anonymization Scheme with Multiple Access Levels. In Proceedings of International Conference on Information Networking (ICOIN), 2006.

[26] Zhang, Q., Wang, J., and Li, X. On the Design of Fast Prefix-Preserving IP Address Anonymization Scheme. In Proceedings of 6th International Conferences on Information, Communications and Signal Processing (ICICS), 2007.

ภาคผนวก

ภาคผนวก ก
ตัวอย่างสถานการณ์การปิดบังหมายเลขไอพี

ลำดับ	สถานการณ์	ผู้วิเคราะห์ข้อมูล	ผู้ถูกวิเคราะห์ข้อมูล	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ระดับความเป็นส่วนตัวที่เลือก
1	จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ ได้รับคำสั่งจากศาลให้เพื่อสั่งให้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติเก็บข้อมูลการจรา-จรทางคอมพิวเตอร์ในเครือข่ายทั้งหมดไว้อย่างน้อย 90 วัน	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	ศูนย์เทคโนโลยีอิเล็ก-ทรอนิกส์และคอมพิว-เตอร์แห่งชาติ IP: 203.185.132.0 SM: 255.255.255.0	ระดับที่ไม่มีการปิดบัง (ต้นไม้ที่เป็นอิสระต่อกัน)	ระดับที่ไม่มีการปิดบัง	ระดับที่ไม่มีการปิดบัง	ระดับที่ไม่มีการปิดบัง
2	จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ สั่งให้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ส่งมอบข้อมูลการจราจรในเครือข่ายเพื่อวิเคราะห์บริการเอชทีทีพี บริการพีทูพี และบริการวีโอไอพีของเครื่องในเครือข่าย	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	ศูนย์เทคโนโลยีอิเล็ก-ทรอนิกส์และคอมพิว-เตอร์แห่งชาติ IP: 203.185.132.0 SM: 255.255.255.0	ระดับที่ไม่มีการปิดบัง (ต้นไม้ที่เป็นอิสระต่อกัน)	ระดับการปิดบังส่วน n บิตขวา	ตามต้นไม้ของความเป็นส่วนตัว	ระดับการปิดบังส่วน n บิตขวา

ลำดับ	สถานการณ์	ผู้วิเคราะห์ข้อมูล	ผู้ถูกวิเคราะห์ข้อมูล	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ระดับความเป็นส่วนตัวที่เลือก
3	จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ สั่งให้นาย ก ซึ่งใช้งานคอมพิวเตอร์อยู่ในเครือข่ายของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ เพื่อตรวจสอบการใช้งานซีพียู และหน่วยความจำและดิสก์	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ IP: 203.185.132.0 SM: 255.255.255.0	ระดับที่ไม่มีการปิดบัง (ต้นไม้ที่เป็นอิสระต่อกัน)	ระดับการปิดบังส่วน n บิตขวา	ระดับการปิดบังทั้ง 32 บิต	ระดับการปิดบังทั้ง 32 บิต
4	จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ สั่งให้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ส่งมอบรายงานผลการวิเคราะห์การจราจรในเครือข่ายผ่านเว็บสาธารณะและแฟ้มเอกสาร	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ IP: 203.185.132.0 SM: 255.255.255.0	ระดับที่ไม่มีการปิดบัง (ต้นไม้ที่เป็นอิสระต่อกัน)	ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม	ระดับการปิดบังทั้ง 32 บิต	ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม

ลำดับ	สถานการณ์	ผู้วิเคราะห์ข้อมูล	ผู้ถูกวิเคราะห์ข้อมูล	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ระดับความเป็นส่วนตัวที่เลือก
5	สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษาซึ่งเป็นพนักงานเจ้าหน้าที่ เรียกดูข้อมูลจากล็อกของมหาวิทยาลัยสงขลานครินทร์	สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา IP: 202.28.18.0 SM: 255.255.255.0	มหาวิทยาลัย สงขลานครินทร์ IP: 202.12.74.0 SM: 255.255.255.0	ระดับการปิดบังส่วน n บิตซ้าย (ต้นไม้ที่มีส่วนร่วมกัน)	ระดับการปิดบังทั้ง 32 บิต	ระดับที่ไม่มีการปิดบัง	ระดับการปิดบังทั้ง 32 บิต
6	สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษาซึ่งเป็นพนักงานเจ้าหน้าที่ เรียกดูข้อมูลการจราจรของมหาวิทยา-ลัยสงขลานครินทร์เพื่อวิเคราะห์สถิติการใช้งานแบนด์วิดท์ และการจราจรของการมัลติคาสท์	สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา IP: 202.28.18.0 SM: 255.255.255.0	มหาวิทยาลัยสงขลานครินทร์ IP: 202.12.74.0 SM: 255.255.255.0	ระดับการปิดบังส่วน n บิตซ้าย (ต้นไม้ที่มีส่วนร่วมกัน)	ระดับการปิดบังส่วน n บิตซ้าย	ระดับที่ไม่มีการปิดบัง	ระดับการปิดบังส่วน n บิตซ้าย
7	สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษาซึ่งเป็นพนักงานเจ้าหน้าที่ เรียกดู	สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา	มหาวิทยาลัยสงขลานครินทร์ IP: 202.12.74.0	ระดับการปิดบังส่วน n บิตซ้าย	ระดับการปิดบังส่วน n บิตขวา	ระดับที่ไม่มีการปิดบัง	ระดับการปิดบังทั้ง 32 บิต

ลำดับ	สถานการณ์	ผู้วิเคราะห์ข้อมูล	ผู้ถูกวิเคราะห์ข้อมูล	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ระดับความเป็นส่วนตัวที่เลือก
	ข้อมูลการจราจรของมหาวิทยา-ลัยสงขลานครินทร์เพื่อวิเคราะห์สถิติการใช้งานบริการเอฟทีพีในรายเครื่อง	IP: 202.28.18.0 SM: 255.255.255.0	SM: 255.255.255.0	(ต้นไม้ที่มีส่วนร่วมกัน)			
8	สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษาซึ่งเป็นพนักงานเจ้าหน้าที่ ทำสำเนาข้อมูลการจราจรของมหาวิทยาลัยสงขลานครินทร์ เพื่อวิเคราะห์ข้อมูลการใช้งานเว็บแบบสรุปของเครือข่าย	สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา IP: 202.28.18.0 SM: 255.255.255.0	มหาวิทยาลัยสงขลานครินทร์ IP: 202.12.74.0 SM: 255.255.255.0	ระดับการปิดบังส่วน n บิตซ้าย (ต้นไม้ที่มีส่วนร่วมกัน)	ระดับที่ไม่มีการปิดบัง	ตามรายการวิเคราะห์เครือข่าย	ระดับการปิดบังส่วน n บิตซ้าย
9	ภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ ได้รับคำสั่งจากศาลให้ เรียกดูข้อมูลการ	ภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.93.0	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	ระดับการปิดบังส่วน n บิตขวา (ต้นไม้ที่เป็น	ระดับที่ไม่มีการปิดบัง	ระดับที่ไม่มีการปิดบัง	ระดับการปิดบังส่วน n บิตขวา

ลำดับ	สถานการณ์	ผู้วิเคราะห์ข้อมูล	ผู้ถูกวิเคราะห์ข้อมูล	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ระดับความเป็นส่วนตัวที่เลือก
	จราจรของจุฬาลงกรณ์มหา-วิทยาลัยเพื่อวิเคราะห์ประสิทธิภาพของเครือข่าย	SM: 255.255.254.0		ส่วนย่อยแท้แบบ A อยู่ใน B)			
10	ภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ ได้รับคำสั่งจากศาลให้ เพื่อสั่งให้จุฬาลงกรณ์มหาวิทยาลัย เก็บข้อมูลการจราจรทางคอมพิวเตอร์ในเครือข่ายทั้งหมดไว้อย่างน้อย 90 วัน	ภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.93.0 SM: 255.255.254.0	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	ระดับการปิดบังส่วน n บิตขวา (ต้นไม้ที่เป็นส่วนย่อยแท้แบบ A อยู่ใน B)	ระดับที่ไม่มีการปิดบัง	ระดับที่ไม่มีการปิดบัง	ระดับการปิดบังส่วน n บิตขวา
11	ภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ ทำสำเนาข้อมูลการจราจรของเครือข่าย	ภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.93.0	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	ระดับการปิดบังส่วน n บิตขวา (ต้นไม้ที่เป็น	ระดับที่ไม่มีการปิดบัง	ตามรายการวิเคราะห์เครือข่าย	ระดับการปิดบังส่วน n บิตขวา

ลำดับ	สถานการณ์	ผู้วิเคราะห์ข้อมูล	ผู้ถูกวิเคราะห์ข้อมูล	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ระดับความเป็นส่วนตัวที่เลือก
	จุฬาลงกรณ์มหาวิทยาลัยเพื่อวิเคราะห์ข้อมูลการใช้งานอีเมลล์และการแลกเปลี่ยนไฟล์แบบสรุปของเครือข่าย	SM: 255.255.254.0		ส่วนย่อยแท้แบบ A อยู่ใน B)			
12	ภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ ต้องการเรียกดูข้อมูลการจาราจรของเครือข่ายจุฬาลงกรณ์มหาวิทยา-ลัย จึงสั่งให้จุฬาลงกรณ์มหาวิทยาลัย ส่งข้อมูลดังกล่าวมาให้เพื่อใช้วิเคราะห์ค่าสถิติของโปรโตคอลเอสเอสเอช โปรโต-คอลพีโอพีสาม และโปรโตคอลเทลเน็ตในระดับเครื่อง	ภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.93.0 SM: 255.255.254.0	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	ระดับการปิดบังส่วน n บิตขวา (ต้นไม้ที่เป็นส่วนย่อยแท้แบบ A อยู่ใน B)	ระดับการปิดบังส่วน n บิตขวา	ตามต้นไม้ของความเป็นส่วนตัว	ระดับการปิดบังส่วน n บิตขวา

ลำดับ	สถานการณ์	ผู้วิเคราะห์ข้อมูล	ผู้ถูกวิเคราะห์ข้อมูล	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ระดับความเป็นส่วนตัวที่เลือก
13	จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ ได้ทำสำเนาข้อมูลจราจรจากระบบคอมพิว-เตอร์ของคณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เพื่อนำมาวิเคราะห์ค่าทางสถิติของเครือข่ายจากโปรโตคอลเอสเอ็นเอ็มพี และโปรโตคอลเอสเอสเอช	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.118.0 SM: 255.255.254.0	ระดับการปิดบังส่วน n บิตขวา (ต้นไม้ที่เป็นส่วนย่อยแท้แบบ B อยู่ใน A)	ระดับที่ไม่มีการปิดบัง	ตามรายการวิเคราะห์เครือข่าย	ระดับการปิดบังส่วน n บิตขวา
14	จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ ได้ทำสำเนาข้อมูลจราจรจากระบบคอมพิว-เตอร์ของคณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เพื่อนำมาวิเคราะห์สำหรับจัดการพร๊อกซี่ของเครือข่าย	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.118.0 SM: 255.255.254.0	ระดับการปิดบังส่วน n บิตขวา (ต้นไม้ที่เป็นส่วนย่อยแท้แบบ B อยู่ใน A)	ระดับการปิดบังทั้ง 32 บิต	ตามรายการวิเคราะห์เครือข่าย	ระดับการปิดบังทั้ง 32 บิต

ลำดับ	สถานการณ์	ผู้วิเคราะห์ข้อมูล	ผู้ถูกวิเคราะห์ข้อมูล	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ระดับความเป็นส่วนตัวที่เลือก
15	จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ ได้ทำสำเนาข้อมูลจราจรจากระบบคอมพิว-เตอร์ของคณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เพื่อนำมาวิเคราะห์ข้อมูลการจราจรของมัลติคาสท์	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.118.0 SM: 255.255.254.0	ระดับการปิดบังส่วน n บิตขวา (ต้นไม้ที่เป็นส่วนย่อยแท้แบบ B อยู่ใน A)	ระดับการปิดบังส่วน n บิตซ้าย	ตามรายการวิเคราะห์เครือข่าย	ระดับการปิดบังทั้ง 32 บิต
16	จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ ได้ทำสำเนาข้อมูลจราจรจากระบบคอมพิว-เตอร์ของคณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เพื่อนำมาวิเคราะห์การวางแผนปริมาณข้อมูล และการใช้งานแบนด์วิดท์ของเครือข่าย	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.118.0 SM: 255.255.254.0	ระดับการปิดบังส่วน n บิตขวา (ต้นไม้ที่เป็นส่วนย่อยแท้แบบ B อยู่ใน A)	ระดับที่ไม่มีการปิดบัง	ตามรายการวิเคราะห์เครือข่าย	ระดับการปิดบังส่วน n บิตขวา

ลำดับ	สถานการณ์	ผู้วิเคราะห์ข้อมูล	ผู้ถูกวิเคราะห์ข้อมูล	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ระดับความเป็นส่วนตัวที่เลือก
17	จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ เรียกดูข้อมูลการจราจรจากระบบคอมพิวเตอร์ของเครือข่ายจุฬาลงกรณ์มหาวิทยาลัยเพื่อนำมาวิเคราะห์การเชื่อมต่อโดยการเทลเน็ตแบบรายเครื่อง	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	ระดับการปิดบังทั้ง 32 บิต (ต้นไม้ที่สมมูลกัน)	ระดับการปิดบังทั้ง 32 บิต	ระดับที่ไม่มีการปิดบัง	ระดับการปิดบังทั้ง 32 บิต
18	จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ เรียกดูข้อมูลการจราจรของนางสาว ข จากระบบคอมพิวเตอร์ของเครือข่ายจุฬาลงกรณ์มหาวิทยาลัยเพื่อนำมาวิเคราะห์พฤติกรรมการใช้งานเครื่องบนเครือข่าย และการใช้บิตทอร์เรนต์	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	ระดับการปิดบังทั้ง 32 บิต (ต้นไม้ที่สมมูลกัน)	ระดับการปิดบังทั้ง 32 บิต	ระดับการปิดบังทั้ง 32 บิต	ระดับการปิดบังทั้ง 32 บิต

ลำดับ	สถานการณ์	ผู้วิเคราะห์ข้อมูล	ผู้ถูกวิเคราะห์ข้อมูล	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ระดับความเป็นส่วนตัวที่เลือก
19	จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ เรียกดูข้อมูลการจราจรจากระบบคอมพิวเตอร์ของเครือข่ายจุฬาลงกรณ์มหาวิทยาลัยเพื่อนำมาวิเคราะห์ประสิทธิภาพของเครือข่าย	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	ระดับการปิดบังทั้ง 32 บิต (ต้นไม้ที่สมมูลกัน)	ระดับที่ไม่มีการปิดบัง	ระดับที่ไม่มีการปิดบัง	ระดับการปิดบังทั้ง 32 บิต
20	จุฬาลงกรณ์มหาวิทยาลัยซึ่งเป็นพนักงานเจ้าหน้าที่ ทำสำเนาข้อมูลการจราจรจากระบบคอมพิวเตอร์ของเครือข่ายจุฬาลง-กรณ์มหาวิทยาลัยเพื่อนำมาวิเคราะห์บริการโดเมนเนม	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	จุฬาลงกรณ์มหาวิทยาลัย IP: 161.200.0.0 SM: 255.255.0.0	ระดับการปิดบังทั้ง 32 บิต (ต้นไม้ที่สมมูลกัน)	ระดับการปิดบังทั้ง 32 บิต	ตามรายการวิเคราะห์เครือข่าย	ระดับการปิดบังทั้ง 32 บิต

กำหนดให้ IP คือ หมายเลขไอพี และ SM คือ หมายเลยสับเน็ตมาสก์

ภาคผนวก ข

ผลงานตีพิมพ์จากงานวิจัย

ผลงานตีพิมพ์จากงานวิจัย

1. บทความเรื่อง “Defining Privacy Levels for IP Address Anonymization” โดย วงศ์ยศ เกิดศรี ยรรยง เต็งอำนวย และ ภาสกร ประถมบุตร ตีพิมพ์ในรายงานประชุมวิชาการระดับนานาชาติ 13th International ANnual Symposium on Computational Science and Engineering (ANSCSE-13) ณ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ กรุงเทพมหานคร ระหว่างวันที่ 25-27 มีนาคม พ.ศ. 2552

2. บทคัดย่อเรื่อง “Defining Privacy Levels for IP Address Anonymization” โดย วงศ์ยศ เกิดศรี ยรรยง เต็งอำนวย และ ภาสกร ประถมบุตร ตีพิมพ์ในรายงานประชุมวิชาการระดับนานาชาติ 13th International ANnual Symposium on Computational Science and Engineering (ANSCSE-13) ณ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ กรุงเทพมหานคร ระหว่างวันที่ 25-27 มีนาคม พ.ศ. 2552

3. บทคัดย่อเรื่อง “Presenting Privacy Tree Structure for IP Address Anonymization Based on Privacy Levels” โดย วงศ์ยศ เกิดศรี ยรรยง เต็งอำนวย และ ภาสกร ประถมบุตร ตีพิมพ์ในรายงานประชุมวิชาการระดับนานาชาติ 13th International ANnual Symposium on Computational Science and Engineering (ANSCSE-13) ณ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ กรุงเทพมหานคร ระหว่างวันที่ 25-27 มีนาคม พ.ศ. 2552

4. บทความเรื่อง “Defining and Using Anonymization Factors for Anonymizing IP Address Based on Privacy Levels” โดย วงศ์ยศ เกิดศรี ยรรยง เต็งอำนวย และ ภาสกร ประถมบุตร ตีพิมพ์ในรายงานประชุมวิชาการระดับชาติ National Conference on Computing and Information Technology (NCCIT 2009) ณ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กรุงเทพมหานคร ระหว่างวันที่ 22-23 พฤษภาคม พ.ศ. 2552

Defining Privacy Levels for IP Address Anonymization

Wongyos Keardsri,[1, C1] **Yunyong Teng-amnuay**,[1, C2] **and Passakon Prathombutr** [2, C3]

[1] *Information System Engineering Laboratory (ISEL), Center of Excellence in Software Engineering*
Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University
Phayathai Road, Pathumwan, Bangkok 10330, Thailand

[2] *National Electronics and Computer Technology Center (NECTEC)*
National Science and Technology Development Agency (NSTDA), Ministry of Science and Technology
Thailand Science Park, Phaholyothin Road, Klong Luang, Pathumthani 12120, Thailand

E-mail: [C1]g49wkr@cp.eng.chula.ac.th, [C2]Yunyong.T@Chula.ac.th, [C3]prathom@nectec.or.th

ABSTRACT

Nowadays, an IP address anonymization is an important technique for network analysis and Internet research. The method of anonymization is the changing of original IP address to anonymized IP address. This can prevent sensitive information of users from disclosure. However, most current anonymization techniques are unsuitable for network analysis functions. They anonymize all 32 bits of IP address unnecessarily. In this paper, we propose 5 privacy levels that anonymize a part of IP address in a different scheme. We apply these privacy levels to prefix-preserving IP address anonymization. Our anonymization scheme benefits any organizations in exchanging network data, and also appropriates for packet tracers and sniffers.

Keywords: IP address anonymization, privacy, privacy levels, sensitive information, network analysis, Internet research, packet tracer, packet sniffer

INTRODUCTION

Nowadays, packet tracers and sniffers are a crucial tool for network analysis and Internet research such as traffic analysis, system diagnosis, network performance evaluation, and more generally network analysis functions, to analyze and evaluate the condition of network system. The packet data from the traces which contain the source and destination IP addresses can link to users who are in the network. To prevent user privacy which may be inferred from the trace, the IP address must be removed or closed by using an anonymization technique. The IP address anonymization is the replacing of original IP address to anonymized IP address to keep the private information of users in network and to prevent suitable a disclosure and violation of user privacy. The well-known anonymization techniques are TCPdpriv [1], Crypto-PAn [2], Multiple Access Level [3], and TSA [4]; however, they are unsuitable for network analysis functions. Because they do not consider the appropriate bits or parts of IP address to anonymize and also anonymize all 32 bits of IP address unnecessarily. In fact, the anonymization depend on the packet data which need to analyze and parts of IP address which need to see.

In this paper, we anonymize the necessary bits or parts of IP address according to different privacy levels and views. We propose 5 privacy levels for anonymization scheme. The first level is non-anonymization; all 32 bits of IP address are not anonymized. The second level is n-left anonymization; only n bits of IP address from network part are anonymized. The third level is n-right anonymization; only n bits of IP address from host part are anonymized. The fourth level is full anonymization; all 32 bits of IP address, which consist of host and network parts, are anonymized. The last level is randomly full anonymization; all 32 bits of IP address are randomized before being anonymized. We apply 5 privacy levels to prefix-preserving IP address anonymization, the technique which can preserve network relationship among the same network domain from original IP addresses. Our anonymization scheme is applicable to an administrator who analyzes packet data. The scheme benefits any organizations in exchanging network data, and also appropriates for packet tracers and sniffers.

THEORY AND RELATED WORKS

IP Address Structure

An IP address is a data structure which uniquely identifies a node within the network. Each IP address consists of two parts. First is a network part; it identifies a network domain and a group of organization. Second is a host part; it identifies a host number within a local network of each organization. In the IPv4 [5], network address is identified as a bit-wise logical AND of the 32-bit IPv4 address with 32-bit subnet mask or netmask address. The netmask has a "1" bit for each bit that is a part of the network number, and a "0" bit for each bit which is a part of the host number. All systems within the same network domain share the same subnet mask address. When each IP address is calculated with subnet mask address, it can be separated into network and host parts. These above-mentioned details show in Figure 1.

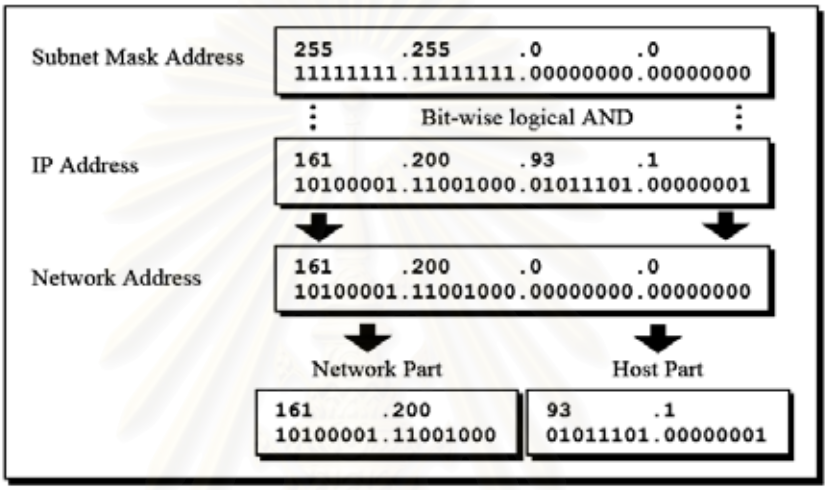


Figure 1. IP address structure

IP Address Anonymization

An IP address anonymization was first proposed in 1990s. The basic approach is one-to-one mapping [1], which maps each IP address to random 32 bits of IP address. The examples of this approach are Blowfish [6], MD5 [6, 7], and Hashing function. One-to-one mapping can only preserve privacy requirement, however, the results from anonymization cannot preserve the prefix relationships among original IP addresses. To apply anonymization scheme to be prefix preserving, it should anonymize two of original IP addresses to share a k-bit prefix, and their anonymized mappings will also share a k-bit prefix. First approach to such prefix preserving anonymization is a TCPdpriv (tcpdump privacy). It was developed by Greg Minshall [1]. The TCPdpriv was implemented to anonymize IP addresses with different security levels. In level 0, it maps different addresses to integers (counting from 1). In level 1, it maps the upper and lower 16 bits of IP address, separately, to integers (counting from 1); the upper and lower maps are independent. In level 2, it maps each byte of the address separately; each byte map is independent. Level 50 is prefix-preserving anonymization scheme. The TCPdpriv can be viewed as a table-based approach, it stores a set of raw IP address, and anonymized IP address binding pairs of IP addresses to maintain the consistency of the anonymization within one trace. The binding is generated randomly when a new address is anonymized. Therefore, it may produce an inconsistency of anonymized address (i.e., same original prefix is mapped into different anonymized prefixes) when the same IP address is used more than one trace.

To improve TCPdpriv scheme, Jun Xu [2] et al proposed a new prefix-preserving anonymization by using cryptographic concepts. They called Crypto-PAn. It is the well-known deterministic prefix preserving anonymization which maps raw addresses to anonymized addresses with the same key, so it can anonymize IP address consistently. The Crypto-PAn algorithm is based on the canonical form theorem. It represents the distinct IPv4 addresses with a *complete binary tree* of height 32 as show in Figure 2(a). The set of distinct original addresses

can be represented by *original address tree* as show in Figure 2(b). It uses *anonymization function* in Figure 2(c) to anonymize original IP address. This function can be generated by specifying a binary variable for each non-leaf node (including the root node) of the original address tree. This variable specifies whether the function "flips" this bit or not. The result from anonymization function is the *anonymized address tree* as show in Figure 2(d).

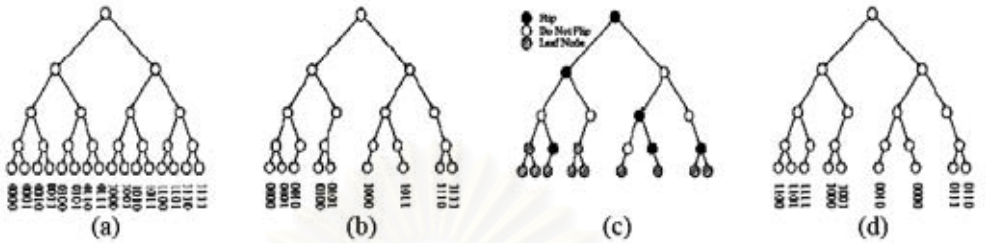


Figure 2. Address trees and anonymization function: (a) complete binary tree (using 4-bit addresses for simplicity); (b) original address tree; (c) anonymization function; (d) anonymized address tree.

The Crypto-PAn uses cryptographic key in 32-bit steps (e.g., 32-bit, 64-bit, 128-bit, etc.) to anonymization function. The same address which appears in two different traces will be mapped to the same anonymized address if the same key is used. Therefore, this scheme is consistent in prefix-preserving anonymization. However, Crypto-PAn is low efficiency for a heavy packet tracer on real time high speed network because of time which generates address trees is long. It needs 32 rounds of encryption, thus makes it unsuitable for real time anonymization.

The prefix-preserving anonymization is an interesting method to many researchers. Qianli Zhang [3] and et al are one which proposed the anonymization scheme by using multiple access levels of the traces. This scheme is made more secure by different keys, but it may be complex to access data if the levels and keys increase. Therefore, they are complicated to recover and unsuitable for real time anonymization.

In the previous problem, Ramaswamy Ramaswamy [4] and et al proposed the top-hash subtree-replicated anonymization (TSA), the high-speed prefix-preserving anonymization, by using pre-computation, replicated subtrees, and top hashing, to improve the computation time of anonymization algorithm. Moreover, Qianli Zhang [7] and et al also proposed fast prefix-preserving anonymization by using bit string algorithm to improve anonymization performance.

PRIVACY LEVELS

Previous proposed techniques always anonymize all 32 bits of IP address. When we studied and surveyed in the network analysis processes, we found that some processes do not require anonymization; some processes require anonymizing only some parts of IP address. Therefore, we can consider the appropriate bit numbers and appropriate parts of IP address to anonymization. Consequently, we propose the privacy levels to anonymization scheme. We define these privacy levels into 5 levels as follows.

Non-Anonymization

Non-anonymization is the first level which all 32 bits of original IP address are not anonymized. This level is used to anonymize IP address in packet data which needs to analyze the network summary results such as bandwidth usage, network service summary, and capacity planning. These analysis processes are not related to users or specific network, so it is unnecessary to anonymize the IP address. The anonymized IP address by using non-anonymization level is shown in Figure 3(a).

n-Left Anonymization

n-Left anonymization is the second level which only n bits of IP address from network part are anonymized. This level is used to anonymize IP address in packet data which needs to

analyze the results that specify the network part during analysis process such as comparing network resource usage, and comparing network service statistics. The anonymized IP address by using n-left anonymization level is shown in Figure 3(b).

n-Right Anonymization

n-Right anonymization is the third level which only n bits of IP address from host part are anonymized. This level is used to anonymize IP address in packet data which needs to analyze the results that specify the host part during analysis process such as CPU usage, memory usage, and device services summary. The anonymized IP address by using n-right anonymization level is shown in Figure 3(c).

Full Anonymization

Full anonymization is the fourth level which all 32 bits of IP address, which consist of the host network parts, are anonymized. This level is used to anonymize IP address in packet data which needs to analyze the results that specify both of network host parts during analysis process such as user behavior analysis, intrusion detection, log analysis, and social network analysis. The anonymized IP address by using full anonymization level is shown in Figure 3(d).

Randomly Full Anonymization

Randomly full anonymization is the fifth level which all 32 bits of IP address are randomized by random algorithm. This has been done before they are anonymized and be consistent by table lookup. This level is used to anonymize IP address in packet data which needs to analyze the results that do not require prefix-preserving and display the results to the public such as list of device services, web application report, and network map. The anonymized IP address by using randomly full anonymization level is shown in Figure 3(e).

ANONYMIZATION SCHEME

We apply the privacy levels to prefix-preserving anonymization, specifically to Crypto-PAn. The Crypto-PAn uses the trees to anonymize all 32 bits of IP address. In our scheme, we implement the anonymization algorithm to anonymize n bits of IP address by applying Crypto-PAn algorithm for n-left, n-right and full anonymization, and using the random algorithm for randomly full anonymization. This algorithm shows in Table 1.

Table 1. Anonymization algorithm based on privacy levels

```
1  originalIP ← input IP address
2  subnet ← input subnet mask address
3  netPart ← binary(originalIP) AND binary(subnet)
4  hostPart ← substring(netPart.length, 32)
5  level ← input privacy level
6  if (level is 1)
7     anonymizedIP ← originalIP
8  else if (level is 2)
9     anonymizedIP ← cryptopan(netPart)
10 else if (level is 3)
11    anonymizedIP ← cryptopan(hostPart)
12 else if (level is 4)
13    anonymizedIP ← cryptopan(originalIP)
14 else if (level is 5)
15    anonymizedIP ← random(originalIP)
16 else //undefined level
17    anonymizedIP ← originalIP
```

This anonymization scheme depends on the packet data which is used to analyze, and is related to a network part, a host part, or unrelated. It can be applied to either batch or real-time anonymization.

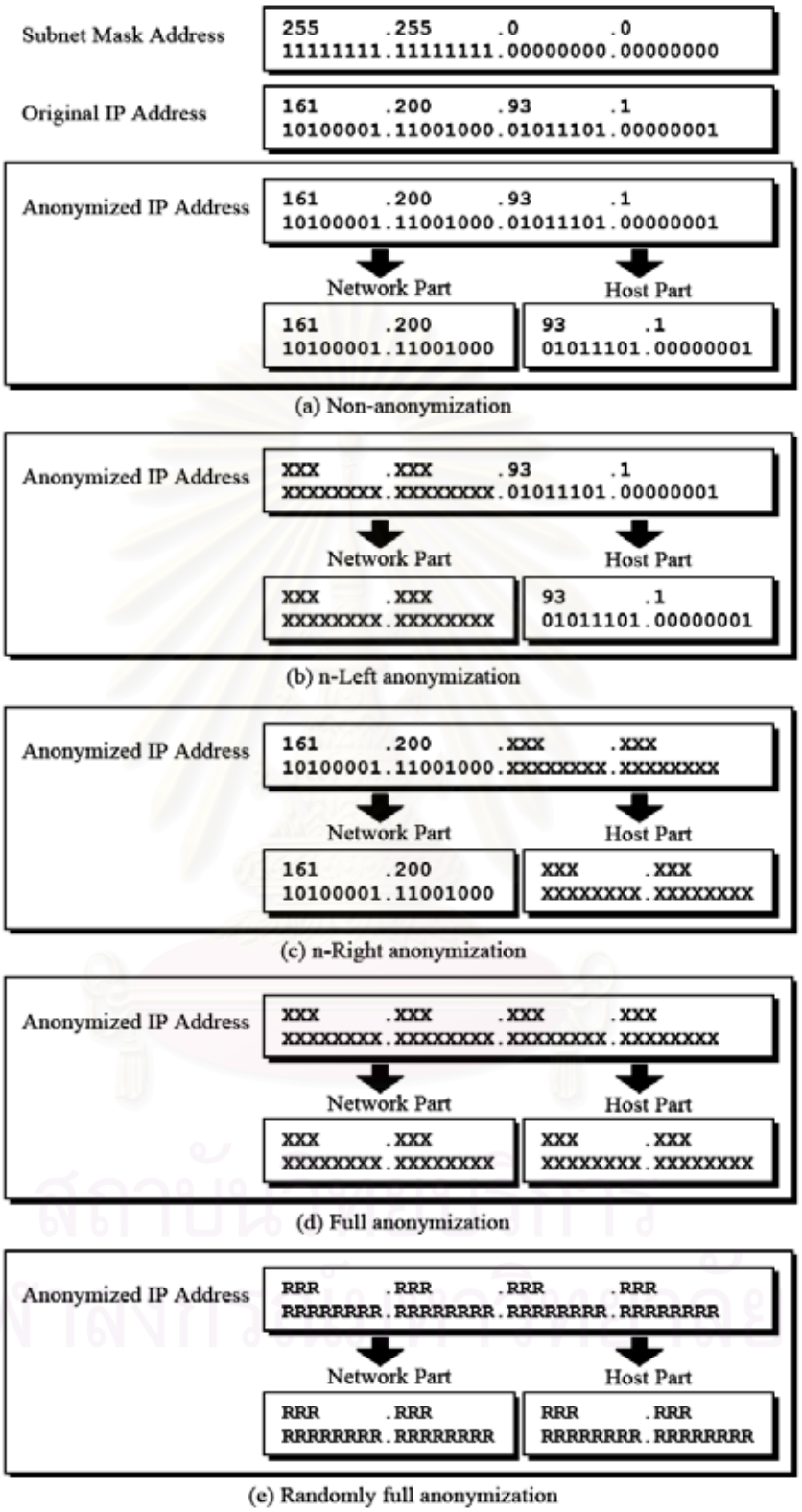


Figure 3. Privacy levels; (a) non-anonymization; (b) n-left anonymization; (c) n-right anonymization; (d) full anonymization; (e) randomly full anonymization

RESULTS AND DISCUSSION

The results from our anonymization scheme based on privacy levels are different from the level which is used. Table 2 is an example of possible results from 5 levels.

Given the data which are used in anonymization process are as follows.

1. Network address 161.200.93.0
2. Subnet mask 255.255.255.0

The network in binary format is 10100001110010000101110100000000, and subnet mask is 11111111111111111111111100000000. Therefore, the network part is the first 24 bits and the host part is the final 8 bits. The anonymized IP address can be anonymized with 32-bit key (11101010010011010010110110010010).

Table 2. An example of possible results from 5 levels

Non-Anonymization	n-Left Anonymization	n-Right Anonymization	Full Anonymization	Randomly Full Anonymization
161.200.93.0	75.133.112.0	161.200.93.146	75.133.112.146	50.204.154.136
161.200.93.1	75.133.112.1	161.200.93.147	75.133.112.147	151.33.86.11
161.200.93.2	75.133.112.2	161.200.93.144	75.133.112.144	192.37.246.138
161.200.93.3	75.133.112.3	161.200.93.145	75.133.112.145	91.154.158.81
161.200.93.4	75.133.112.4	161.200.93.150	75.133.112.150	251.28.175.177
161.200.93.5	75.133.112.5	161.200.93.151	75.133.112.151	238.131.107.78
161.200.93.6	75.133.112.6	161.200.93.148	75.133.112.148	66.126.74.200
161.200.93.7	75.133.112.7	161.200.93.149	75.133.112.149	253.214.9.219
161.200.93.8	75.133.112.8	161.200.93.154	75.133.112.154	37.226.102.49
161.200.93.9	75.133.112.9	161.200.93.155	75.133.112.155	226.2.206.69
161.200.93.10	75.133.112.10	161.200.93.152	75.133.112.152	108.208.137.21
161.200.93.11	75.133.112.11	161.200.93.153	75.133.112.153	117.143.52.30
161.200.93.12	75.133.112.12	161.200.93.158	75.133.112.158	60.113.106.222
161.200.93.13	75.133.112.13	161.200.93.159	75.133.112.159	14.42.186.251
161.200.93.14	75.133.112.14	161.200.93.156	75.133.112.156	203.190.237.11
161.200.93.15	75.133.112.15	161.200.93.157	75.133.112.157	245.15.120.136
161.200.93.16	75.133.112.16	161.200.93.130	75.133.112.130	104.170.90.1
161.200.93.17	75.133.112.17	161.200.93.131	75.133.112.131	158.54.30.228
161.200.93.18	75.133.112.18	161.200.93.128	75.133.112.128	192.22.47.232
161.200.93.19	75.133.112.19	161.200.93.129	75.133.112.129	27.116.57.62
161.200.93.20	75.133.112.20	161.200.93.134	75.133.112.134	83.188.20.57

From Table 1, the result levels 1 to 4 are consistent in prefix-preserving anonymization; they can preserve the network prefix among the same network domain from original IP addresses. The result of the last level is consistent in non-prefix-preserving anonymization. However, this level of anonymization is used to analyze the results that do not require prefix-preserving such as reporting to the public.

The benefits of this scheme are following as;

1. It appropriates for two organizations which have different views in exchanging network data by using privacy levels
2. It appropriates for packet tracers and sniffers, and suite for real-time high speed network. Because it can anonymize some bits or parts of IP address. This can reduce the computation times.

CONCLUSION AND FUTURE WORKS

In this paper, we propose 5 levels of privacy for IP address anonymization: non-anonymization, n-left anonymization, n-right anonymization, full anonymization, and randomly full anonymization. We apply these privacy levels to prefix-preserving anonymization, specifically to Crypto-PAn. Our scheme anonymizes the necessary bits or parts of IP address by considering different privacy levels and views. It benefits any organizations in exchanging network data and also appropriates for packet tracers and sniffers.

Our future works are defining the factors concerning IP address structure, network analysis functions, and cyber laws to consider and select the appropriate privacy levels for our anonymization scheme and combining such factors by using rule-based method.

REFERENCES

1. G. Minshall, *TCPdpriv Command Manual*, July 1996.
2. J. Xu, J. Fan, M. H. Ammar, and S. B. Moon, *Prefix-preserving IP Address Anonymization: Measurement based Security Evaluation and a New Cryptography based Scheme*, IEEE International Conference on Network Protocols (ICNP), 2002, 280-289.
3. Q. Zhang and X. Li, *An IP Address Anonymization Scheme with Multiple Access Levels*, Lecture Notes in Computer Science (LNCS), Springer-Verlag Berlin/Heidelberg, International Conference on Information Networking (ICOIN), 2006, 793-802.
4. R. Ramaswamy, T. Wolf, High-Speed Prefix-Preserving IP Address Anonymization for Passive Measurement Systems, *IEEE/ACM Transactions on Networking (TON)*, 2007, **15**(1), 26-39.
5. J.F. Kurose and K.W. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, 2nd Edition, Addison- Wesley Publishing Company, New York, 2003, 331-342.
6. M. Peuhkuri, *A Method to Compress and Anonymize Packet Traces*, ACM SIGCOMM Internet Measurement Workshop, 2001, 257-261.
7. Q. Zhang, J. Wang, and X. Li, *On the Design of Fast Prefix-Preserving IP Address Anonymization Scheme*, Lecture Notes in Computer Science (LNCS), Springer-Verlag Berlin/Heidelberg, 6th International Conferences on Information, Communications and Signal Processing (ICICS), 2007, 177-188.

ACKNOWLEDGMENTS

The financial support from Thailand Graduate Institute of Science and Technology (TGIST) is gratefully acknowledged. The scholar ID is TG-44-09-50-076M and the grant number is TGIST 01-50-076.

Defining Privacy Levels for IP Address Anonymization

Wongyos Keardsri[1] Yunyong Teng-amnuay[1] and Passakon Prathombutr[2]

[1] *Information System Engineering Laboratory (ISEL), Center of Excellence in Software Engineering*
Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University
Phayathai Road, Pathumwan, Bangkok 10330, Thailand

[2] *National Electronics and Computer Technology Center (NECTEC)*
National Science and Technology Development Agency (NSTDA)
Thailand Science Park, Phaholyothin Road, Klong Luang, Pathumthani 12120, Thailand

E-mail: g49wkr@cp.eng.chula.ac.th, Yunyong.T@Chula.ac.th, prathom@nectec.or.th

Nowadays, an IP address anonymization is an important technique for network analysis and Internet research. The method of anonymization is the changing of original IP address to anonymized IP address to keep the private information of users in network and to prevent suitable a disclosure and violation of user privacy. The well-known anonymization techniques are TCPdpriv [1], Crypto-PAn [2], Multiple Access Level [3], and TSA [4]; however, they are unsuitable for network analysis functions. The current techniques anonymize all 32 bits of IP address unnecessarily. In fact, we can anonymize the necessary bits or parts of IP address for different privacy levels. In this paper, we propose 5 privacy levels for anonymization scheme. The first level is non-anonymization; all 32 bits of IP address are not anonymized. The second level is n-left anonymization; only n bits of IP address from network part are anonymized. The third level is n-right anonymization; only n bits of IP address from host part are anonymized. The fourth level is full anonymization; all 32 bits of IP address, which consist of host and network parts, are anonymized. The last level is randomly full anonymization; all 32 bits of IP address are randomized before being anonymized. We apply these privacy levels to prefix-preserving IP address anonymization, the technique which can preserve network relationship among the same network group from original IP addresses. Our anonymization scheme is applicable to an administrator who analyzes packet data. The scheme benefits any organizations in exchanging network data, and also appropriates for packet tracers and sniffers.

REFERENCES

1. G. Minshall, *TCPdpriv Command Manual*, July 1996.
2. J. Xu, J. Fan, M. H. Ammar, and S. B. Moon, *Prefix-preserving IP Address Anonymization: Measurement based Security Evaluation and a New Cryptography based Scheme*, IEEE International Conference on Network Protocols (ICNP), 2002, 280-289.
3. Q. Zhang and X. Li, *An IP Address Anonymization Scheme with Multiple Access Levels*, Lecture Notes in Computer Science (LNCS), Springer-Verlag Berlin/Heidelberg, International Conference on Information Networking (ICOIN), 2006, 793-802.
4. R. Ramaswamy, T. Wolf, High-Speed Prefix-Preserving IP Address Anonymization for Passive Measurement Systems, *IEEE/ACM Transactions on Networking (TON)*, 2007, **15**(1), 26-39.

ACKNOWLEDGMENTS

The financial support from Thailand Graduate Institute of Science and Technology (TGIST) is gratefully acknowledged. The scholar ID is TG-44-09-50-076M and the grant number is TGIST 01-50-076.

Presenting Privacy Tree Structure for IP Address Anonymization Based on Privacy Levels

Wongyos Keardsri[1] Yunyong Teng-amnuay[1] and Passakon Prathombutr[2]

[1] *Information System Engineering Laboratory (ISEL), Center of Excellence in Software Engineering*
Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University
Phayathai Road, Pathumwan, Bangkok 10330, Thailand

[2] *National Electronics and Computer Technology Center (NECTEC)*
National Science and Technology Development Agency (NSTDA)
Thailand Science Park, Phaholyothin Road, Klong Luang, Pathumthani 12120, Thailand

E-mail: g49wkr@cp.eng.chula.ac.th, Yunyong.T@Chula.ac.th, prathom@nectec.or.th

Privacy becomes more and more serious concern in network traffic analysis. Because of an analysis process is related to private information of users in network system. It is a significant issue in determining what we can and cannot access in packet data that include the sensitive information, for example, IP address. Recently, IP address anonymizations become an interesting topic. They can anonymize original IP addresses and reform as anonymized IP addresses. Most methods are prefix-preserving anonymization [1, 2], which can preserve the network relationship among the same network group from the original IP addresses. However, these methods anonymize all 32 bits of IP address unnecessarily. In fact, we can anonymize only some bits or parts of IP address for different privacy levels. In this paper, we study and develop the privacy levels to anonymization scheme, and present a factor, a privacy tree structure, to consider and select appropriate privacy level. Our idea is the IP address structures between any two organizations have different privacy levels and each organization has different views of packet data. We represent the different views as a tree and IP address structure as nodes and edges. The operation results of two tree structures from each organization will be the results which are used in the selecting appropriate privacy level. This privacy tree structure is good factor for anonymization scheme based on privacy levels.

REFERENCES

1. G. Minshall, *TCPdpriv Command Manual*, July 1996.
2. J. Xu, J. Fan, M. H. Ammar, and S. B. Moon, *Prefix-preserving IP Address Anonymization: Measurement based Security Evaluation and a New Cryptography based Scheme*, IEEE International Conference on Network Protocols (ICNP), 2002, 280-289.

ACKNOWLEDGMENTS

The financial support from Thailand Graduate Institute of Science and Technology (TGIST) is gratefully acknowledged. The scholar ID is TG-44-09-50-076M and the grant number is TGIST 01-50-076.

การกำหนดและใช้งานปัจจัยการปิดบังสำหรับปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว

Defining and Using Anonymization Factors for Anonymizing IP Address Based on Privacy Levels

วงศ์ยศ เกิดศรี[1] ยรรยง เต็งอำนวย[1] และ ภาสกร ประถมบุตร[2]

[1] ห้องปฏิบัติการวิศวกรรมระบบสารสนเทศ ศูนย์เชี่ยวชาญทางวิศวกรรมซอฟต์แวร์
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพมหานคร 10330

[2] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค)
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)
ถนนพหลโยธิน ตำบลคลองหนึ่ง อำเภอคลองหลวง จังหวัดปทุมธานี 12120

อีเมล: g49wkr@cp.eng.chula.ac.th, prathom@nectec.or.th, Yunyong.T@Chula.ac.th

บทคัดย่อ

การปิดบังหมายเลขไอพีเป็นกระบวนการหนึ่งที่สำคัญในขั้นตอนการสูบจับแพ็คเก็ตสำหรับการวิเคราะห์เครือข่าย กระบวนการนี้สามารถป้องกันการละเมิดความเป็นส่วนตัวของผู้ใช้ได้ ปัจจุบันการปิดบังหมายเลขไอพีคำนึงถึงลักษณะการใช้งานมากยิ่งขึ้น ซึ่งขึ้นอยู่กับว่าผู้วิเคราะห์เครือข่ายต้องการวิเคราะห์สิ่งใดและมองเห็นส่วนใดของหมายเลขไอพีบ้าง หมายเลขไอพีประกอบด้วยส่วนของกลุ่มผู้ใช้และกลุ่มเครือข่าย ซึ่งมีระดับความเป็นส่วนตัวที่แตกต่างกัน งานวิจัยเรื่องนี้จึงได้นำเสนอระดับความเป็นส่วนตัว 5 ระดับเพื่อใช้ปิดบังหมายเลขไอพี และนำเสนอปัจจัยการปิดบังหมายเลขไอพี 3 ปัจจัยอันได้แก่ ต้นไม้ของความเป็นส่วนตัว รายการวิเคราะห์เครือข่าย และกฎหมายคอมพิวเตอร์ เพื่อใช้เลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุด แบบแผนการปิดบังหมายเลขไอพีนี้เป็นประโยชน์ต่อองค์กรในการแลกเปลี่ยนข้อมูล และช่วยให้ผู้วิเคราะห์สามารถใช้ข้อมูลได้ตามสถานการณ์ที่เหมาะสม

คำสำคัญ: การปิดบังหมายเลขไอพี ความเป็นส่วนตัว ระดับความเป็นส่วนตัว ข้อมูลส่วนบุคคล การวิเคราะห์เครือข่าย การวิเคราะห์การจราจร การสูบจับแพ็คเก็ต

Abstract

An IP address anonymization is one of important process in packet sniffers for network analysis. It can prevent a violation of user privacy. Currently, IP address anonymization is more considered to packet data usages which are used to analysis. They depend on the network analysts need to process these data to which analysis functions or view which parts of IP address. Generally, 32-bit IPv4 address contains the host and network parts which have a different privacy levels. This paper presents 5 privacy levels for IP address anonymization scheme and 3 anonymization factors; privacy tree structures, network analysis functions and computer law, for selecting the most appropriate privacy level. This scheme benefits any organizations in exchanging network data and helps the analyst able to use the packet data in suitable scenarios.

Keyword: IP Address Anonymization, Privacy, Privacy Levels, Private Information, Network Analysis, Traffic Analysis, Packet Sniffer

1. บทนำ

ปัจจุบันการวิเคราะห์และจัดการเครือข่ายมีความจำเป็นอย่างยิ่งในการดูแลและควบคุมระบบเครือข่ายให้สามารถทำงานได้อย่างปกติ มีความถูกต้อง และมีประสิทธิภาพ ซึ่งการวิเคราะห์และจัดการเครือข่ายนั้น จำเป็นต้องใช้ข้อมูลแพ็คเก็ต (Packet) จากการตามรอยการจราจรในเครือข่าย (Network Traffic Tracers) และการสูบจับแพ็คเก็ต (Packets Sniffers) ในกระบวนการวิเคราะห์ผล โดยข้อมูลแพ็คเก็ตเหล่านั้นประกอบไปด้วยหมายเลขไอพี (IP Address) ของผู้ใช้และของอุปกรณ์ในเครือข่าย ซึ่งสามารถระบุถึงตัวบุคคล อุปกรณ์ปลายทาง และองค์กรที่ใช้งานในเครือข่ายได้ ดังนั้นหมายเลขไอพีดังกล่าวจึงต้องถูกปิดบังก่อนการใช้งาน เพื่อไม่ให้ถูกละเมิดและก้าวก่ายความเป็นส่วนตัว (Privacy) ของสมาชิกในเครือข่ายได้ และเพื่อรักษาสิทธิ์ส่วนบุคคลเอาไว้

โดยทั่วไปกระบวนการวิเคราะห์และจัดการเครือข่ายอาจทำให้มองเห็นและทราบได้ว่าหมายเลขไอพีหมายเลขต่างๆ เป็นของบุคคลใดบ้าง ซึ่งในทางปฏิบัติแล้วผู้ที่ทำการวิเคราะห์และจัดการเครือข่ายไม่ควรล่วงรู้ข้อมูลที่มีความเป็นส่วนตัวแบบนั้นได้ แต่เพียงมีหน้าที่ในการตรวจสอบข้อมูลของระบบเครือข่ายว่ามีปัญหาในส่วนใดบ้างเท่านั้น เช่น ผู้ดูแลระบบเครือข่ายต้องการตรวจสอบสถิติการใช้บริการเว็บไซต์บนโปรโตคอลเอชทีทีพี (HTTP) ของสมาชิกในเครือข่าย โดยกระบวนการวิเคราะห์สถิติดังกล่าวอาจทำให้สามารถมองเห็นและทราบถึงรายละเอียดในการเข้าใช้งานเว็บไซต์ต่างๆ ของสมาชิกเป็นรายบุคคลได้ ซึ่งไม่ถูกต้องตามแนวทางที่ควรปฏิบัติ ผู้ดูแลระบบเครือข่ายไม่ควรล่วงรู้และละเมิดความเป็นส่วนตัวของสมาชิกเหล่านั้น

จากเหตุผลและตัวอย่างที่กล่าวมา หมายเลขไอพีที่อ้างถึงข้างต้นจึงต้องถูกปิดบังเอาไว้เพื่อรักษาความเป็นส่วนตัวแก่สมาชิกที่ใช้งาน โดยวิธีการปิดบังหมายเลขไอพี (IP Address Anonymization) เป็นการเปลี่ยนหมายเลขไอพีดั้งเดิม (Original IP Address) ให้กลายเป็นหมายเลขไอพีนิรนาม (Anonymized IP Address) โดยที่วิธีการปิดบังหมายเลขไอพีที่มีชื่อเสียงนั้นมีอยู่หลายวิธีการด้วยกัน ได้แก่ ทีซีพีดีไพรว์ (Tcpdpriv) [1] คริปโตแพน (Crypto-PAn) [2] การเข้าถึงแบบหลายชั้น (Multiple Access Levels) [3] และทีเอสเอ (TSA) [4] แต่อย่างไรก็ตามเมื่อพิจารณาถึงการใช้งานหมายเลขไอพีนิรนามที่ถูกปิดบังด้วยวิธีการเหล่านั้นแล้วพบว่า ยังคงไม่เหมาะสมกับการทำงานบางประเภทของการวิเคราะห์และจัดการเครือข่าย จากการศึกษาทำให้ทราบว่าการปิดบังหมายเลขไอพีไม่มีความจำเป็นเสมอไปในการปิดบังทั้ง 32 บิต แต่อาจสามารถปิดบังเพียงบางบิตหรือบางส่วนที่จำเป็นของหมายเลขไอพีได้ โดยขึ้นอยู่กับความต้องการและความจำเป็นในการปิดบัง ซึ่งพิจารณาตามเหตุผล 3 ประการดังต่อไปนี้

1. โครงสร้างหมายเลขไอพีขององค์กรที่ต้องการปิดบังมีรูปแบบเป็นอย่างไร
2. ประเภทของรายการวิเคราะห์และจัดการเครือข่ายแต่ละประเภทใช้หมายเลขไอพีวิเคราะห์ผลในเรื่องใดและมองเห็นส่วนใดของหมายเลขไอพี
3. กฎหมายคอมพิวเตอร์กล่าวไว้อย่างไรในกระบวนการรักษาความเป็นส่วนตัวของข้อมูลส่วนบุคคล

จากเหตุผล 3 ประการข้างต้นแสดงให้เห็นว่ากระบวนการปิดบังหมายเลขไอพีมีระดับความเป็นส่วนตัว (Privacy Levels) หรือระดับการปิดบังที่แตกต่างกัน ดังนั้นงานวิจัยเรื่องนี้จึงได้นำเสนอระดับความเป็นส่วนตัว 5 ระดับในการปิดบังหมายเลขไอพี อันได้แก่ ระดับที่ไม่มีการปิดบัง (Non-Anonymization) ระดับการปิดบังส่วน n บิตซ้าย (n-Left Anonymization) ระดับการปิดบังส่วน n บิตขวา (n-Right Anonymization) ระดับการปิดบังทั้ง 32 บิต (Full Anonymization) และ ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม (Randomly Full Anonymization) ซึ่งระดับความเป็นส่วนตัวแต่ละระดับมีอัลกอริทึมในการปิดบังที่แตกต่างกัน ดังนั้นจึงต้องมีการกำหนดปัจจัยเพื่อใช้เลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุด โดยประกอบด้วยปัจจัย 3 ประการอันได้แก่ โครงสร้างต้นไม้ของความเป็นส่วนตัว (Privacy Tree Structures) รายการวิเคราะห์เครือข่าย (Network Analysis Functions) และกฎหมายคอมพิวเตอร์ (Computer Law) ซึ่งจะได้นำเสนอในรายละเอียดต่อไป

2. งานวิจัยที่เกี่ยวข้อง

วิธีการปิดบังหมายเลขไอพีเกิดขึ้นมาเมื่อประมาณสิบปีเศษ โดยแรกเริ่มนั้นใช้หลักการพื้นฐานและอัลกอริทึมอย่างง่ายในการปิดบัง [5] เช่น การใช้ฟังก์ชันแฮช (Hash Function) การ

เข้ารหัสด้วยวิธีเอ็มดี 5 (MD5) เป็นต้น แต่เมื่อนำไปใช้งานจริงในกระบวนการวิเคราะห์และจัดการเครือข่ายแล้วหมายเลขไอพีนิรนามที่ได้ไม่สามารถแยกแยะกลุ่มของเครือข่ายได้ ทั้งยังเกิดการชนกันและเกิดการซ้ำซ้อนของหมายเลขไอพีขึ้น และต้องมีตารางในการจัดเก็บอีกด้วย จนเมื่อปี ค.ศ. 1996 เกรก มินแชล [1] ได้คิดวิธีการปิดบังหมายเลขไอพีแบบแรกขึ้นซึ่งเรียกว่าทีซีพีดีไพรว์ โดยนำหมายเลขไอพีต้นแบบมาทำการจับคู่และสลับบิตหลายๆ รอบจนได้หมายเลขไอพีนิรนามที่สามารถแยกแยะกลุ่มของเครือข่ายได้ แต่วิธีการดังกล่าวต้องมีการจับคู่ระหว่างหมายเลขไอพีดั้งเดิมกับหมายเลขไอพีนิรนามแบบหมายเลขต่อหมายเลข อาจทำให้เกิดการชนกันของหมายเลขไอพีนิรนามได้เมื่อมีการกรองและจับแพ็คหลายๆ รอบ ดังนั้นจึงได้มีการคิดวิธีการปิดบังหมายเลขไอพีแบบใหม่ขึ้น โดยในปี ค.ศ. 2002 จุน ซิว และคณะ [2][6] ได้นำหลักการเข้ารหัสลับ (Cryptography) มาใช้ในการปิดบังหมายเลขไอพีซึ่งเรียกว่าคริปโตแพน โดยมีการกำหนดกุญแจและอัลกอริทึมในการปิดบังในรูปของโครงสร้างต้นไม้ (Tree Structure) และใช้หลักการสลับบิตแบบเดียวกับวิธีทีซีพีดีไพรว์ในการปิดบัง โดยหมายเลขไอพีนิรนามที่ได้ไม่มีปัญหาการชนกัน และสามารถคงไว้ซึ่งความสัมพันธ์ของบิตที่ระบุถึงกลุ่มเครือข่ายได้ ในปี ค.ศ. 2006 ได้มีการคิดวิธีการปิดบังหมายเลขไอพีโดยเตียนลี่ ชาง และคณะ [3] โดยใช้หลักการแบ่งระดับการเข้าถึงหลายชั้น ซึ่งพิจารณาว่าการปิดบังหมายเลขไอพีมีหลายระดับและมีกุญแจการเข้ารหัสที่แตกต่างกัน วิธีนี้มีความปลอดภัยแต่มีความซับซ้อนในการปิดบัง ซึ่งการวิเคราะห์และจัดการเครือข่ายไม่มีความจำเป็นที่ต้องปิดบังหมายเลขไอพีมากระดับเพราะยากและเสียเวลาในการแปลงกลับ ในปี ค.ศ. 2007 รามาสเวมี่ ได้นำเสนอการปิดบังหมายเลขไอพีที่เรียกว่าทีเอสเอ ซึ่งประยุกต์ใช้วิธีของคริปโตแพนโดยนำแฮชฟังก์ชันและการแบ่งย่อยโครงสร้างต้นไม้เข้ามาใช้ในการปิดบัง เพื่อเพิ่มความเร็วในการประมวลผล

จากงานวิจัยที่ผ่านมาจะเห็นได้ว่า หลักการปิดบังหมายเลขไอพีที่กล่าวมานั้นมีกระบวนการปิดบังทั้ง 32 บิตของหมายเลขไอพีอย่างไม่จำเป็น ในความเป็นจริงสามารถปิดบังเพียงบางบิตหรือบางส่วนของหมายเลขไอพีได้ตามระดับความเป็นส่วนตัวที่เหมาะสมและตามความจำเป็นในการใช้งานหมายเลขไอพี โดยจะได้กล่าวในรายละเอียดในหัวข้อถัดไป

3. ระดับความเป็นส่วนตัว

งานวิจัยเรื่องนี้มีแนวคิดที่ว่าในการปิดบังหมายเลขไอพีสามารถเลือกใช้อัลกอริทึมใดก็ได้ แต่กระบวนการปิดบังนั้นจำเป็นต้องพิจารณาถึงความต้องการใช้งานและความสามารถในการมองเห็นหมายเลขไอพีเพิ่มเติม งานวิจัยเรื่องนี้จึงได้นำเสนอระดับความเป็นส่วนตัว 5 ระดับ ซึ่งแต่ละระดับมีความต้องการความเป็นส่วนตัวและสถานการณ์ใช้งานข้อมูลที่แตกต่างกัน หมายเลขไอพีประกอบด้วยกลุ่มเครือข่ายหรือกลุ่มบิตซ้ายที่แสดงถึงกลุ่มขององค์กรหรือหน่วยงานในเครือข่ายและกลุ่มเครื่องหรือกลุ่มบิตขวาที่ระบุถึงจำนวนของเครื่องหรืออุปกรณ์ปลายทางในเครือข่าย ทั้งนี้กลุ่มของบิตทั้งสองส่วนจะมีขนาดเท่าไรก็ขึ้นอยู่กับการออกแบบลักษณะของเครือข่ายเหล่านั้นว่าต้องการให้มีรูปแบบเป็นอย่างไร โดยใช้หมายเลขสับเน็ตมาสเป็นตัวกำหนดดังแสดงในรูปที่ 1

รูปที่ 1: การแบ่งส่วนบิตซ้ายและส่วนบิตขวาของหมายเลขไอพีโดยใช้หมายเลขสับเน็ตมาส

จากรายละเอียดข้างต้น เมื่อพิจารณาส่วนบิตซ้ายและส่วนบิตขวาของหมายเลขไอพีแล้วพบว่า แต่ละส่วนอาจถูกมองเห็นและใช้งานในสถานการณ์ที่แตกต่างกันได้ เช่น บางสถานการณ์มองเห็นและใช้งานเพียงแค่ส่วนบิตซ้าย บางสถานการณ์เพียงแค่ส่วนบิตขวา บางสถานการณ์อาจทั้งสองส่วน หรือบางสถานการณ์อาจไม่ต้องการการมองเห็นหรือใช้งานเลย ซึ่งสอดคล้องกับระดับความเป็นส่วนตัว 5 ระดับที่ได้กล่าวไว้โดยมีรายละเอียดดังต่อไปนี้

1. **ระดับที่ไม่มีการปิดบัง (Non-Anonymization Level)** เป็นระดับที่ไม่ต้องการความเป็นส่วนตัวและไม่มีความจำเป็นใดเลยในการปิดบังหมายเลขไอพี ดังนั้นหมายเลขไอพีนิรนามจะมีรูปแบบที่เหมือนกับหมายเลขไอพีดั้งเดิม

2. ระดับการปิดบังส่วน n บิตซ้าย (n-Left Anonymization Level) เป็นระดับที่ต้องการความเป็นส่วนตัวในระดับเครือข่ายโดยปิดบังหมายเลขไอพีในส่วนของกลุ่มเครือข่ายหรือกลุ่มบิตซ้ายที่แสดงถึงกลุ่มองค์กรหรือหน่วยงานในเครือข่าย ซึ่งอัลกอริทึมที่ใช้ในการปิดบังคือคริปโตแพน

3. ระดับการปิดบังส่วน n บิตขวา (n-Right Anonymization Level) เป็นระดับที่ต้องการความเป็นส่วนตัวในระดับเครื่องหรืออุปกรณ์ โดยปิดบังหมายเลขไอพีในส่วนของกลุ่มเครื่องหรือกลุ่มบิตขวาที่แสดงถึงหมายเลขเครื่องหรือหมายเลขอุปกรณ์ปลายทางในเครือข่าย ซึ่งอัลกอริทึมที่ใช้ในการปิดบังคือคริปโตแพน

4. ระดับการปิดบังทั้ง 32 บิต (Full Anonymization Level) เป็นระดับที่ต้องการความเป็นส่วนตัวอย่างสมบูรณ์ โดยปิดบังหมายเลขไอพีทั้งในส่วนของกลุ่มเครือข่ายและกลุ่มเครื่อง หรือปิดบังทั้ง 32 บิตของหมายเลขไอพี ซึ่งอัลกอริทึมที่ใช้ในการปิดบังคือคริปโตแพน

5. ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม (Randomly Full Anonymization Level) เป็นระดับที่ต้องการความเป็นส่วนตัวอย่างสมบูรณ์แต่ไม่สนใจความสัมพันธ์ของกลุ่มเครือข่ายหรือกลุ่มเครื่อง ซึ่งปิดบังหมายเลขไอพีทั้งสองส่วนหรือทั้ง 32 บิตแบบสุ่ม (Random) โดยใช้อัลกอริทึมแบบสุ่ม ทำให้ไม่สามารถคงไว้ซึ่งความสัมพันธ์ของกลุ่มเครือข่ายของหมายเลขไอพี ดังนั้นหมายเลขไอพีนิรนามในระดับนี้จึงไม่มีคุณสมบัติเหมือนกับหมายเลขไอพีดั้งเดิม

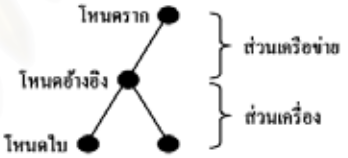
จากระดับความเป็นส่วนตัวทั้ง 5 ระดับที่ได้กล่าวมานั้น สามารถสรุปได้ดังตารางที่ 1

4. ปัจจัยการปิดบังหมายเลขไอพี

จากการนำเสนอระดับความเป็นส่วนตัวทั้ง 5 ระดับในหัวข้อที่ 3 นั้น การเลือกใช้ระดับความเป็นส่วนตัวระดับต่างๆ ให้เหมาะสมกับกระบวนการปิดบังหมายเลขไอพีจะต้องอยู่ภายใต้การพิจารณาปัจจัยการปิดบัง 3 ปัจจัยซึ่งได้แก่ โครงสร้างต้นไม้ของความเป็นส่วนตัว (Privacy Tree Structures) รายการวิเคราะห์เครือข่าย (Network Analysis Functions) และ กฎหมายคอมพิวเตอร์ (Computer Law) โดยงานวิจัยเรื่องนี้ได้กำหนดรายละเอียดของปัจจัยการปิดบังหมายเลขไอพีไว้ดังต่อไปนี้

4.1 โครงสร้างต้นไม้ของความเป็นส่วนตัว

เมื่อพิจารณาโครงสร้างของหมายเลขไอพีขององค์กรใดๆ ที่ต้องการแลกเปลี่ยนข้อมูลซึ่งกันพบว่า รูปแบบโครงสร้างของหมายเลขไอพีมีความสัมพันธ์กันในหลายรูปแบบ ซึ่งงานวิจัยเรื่องนี้ได้นำเสนอในลักษณะของโครงสร้างต้นไม้ของความเป็นส่วนตัวโดยมีรายละเอียดและองค์ประกอบดังรูปที่ 2



รูปที่ 2: องค์ประกอบของโครงสร้างต้นไม้ของความเป็นส่วนตัวตามโครงสร้างหมายเลขไอพีขององค์กรใดๆ

ตารางที่ 1: ตารางแสดงระดับความเป็นส่วนตัว 5 ระดับ ในการปิดบังหมายเลขไอพี

ระดับที่	ระดับความเป็นส่วนตัว	นิยามการปิดบัง	ส่วนของการปิดบัง	
			ส่วนเครือข่าย	ส่วนเครื่อง
1	ระดับที่ไม่มีการปิดบัง	ไม่ปิดบังทั้ง 32 บิตของหมายเลขไอพี	ไม่ปิดบัง	ไม่ปิดบัง
2	ระดับการปิดบังส่วน n บิตซ้าย	ปิดบังเพียงส่วนบิตซ้ายหรือส่วนเครือข่ายของหมายเลขไอพี	ปิดบัง	ไม่ปิดบัง
3	ระดับการปิดบังส่วน n บิตขวา	ปิดบังเพียงส่วนบิตขวาหรือส่วนเครื่องของหมายเลขไอพี	ไม่ปิดบัง	ปิดบัง
4	ระดับการปิดบังทั้ง 32 บิต	ปิดบังทั้ง 32 บิตของหมายเลขไอพี	ปิดบัง	ปิดบัง
5	ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม	ปิดบังทั้ง 32 บิตของหมายเลขไอพีแบบสุ่ม	ปิดบังแบบสุ่ม	ปิดบังแบบสุ่ม

ตารางที่ 2: ตารางสรุปรายละเอียดของต้นไม้ของความเป็นส่วนตัว

รูปแบบ	ต้นไม้ของความเป็นส่วนตัว	ความสัมพันธ์ในรูปแบบเซต	ระดับความเป็นส่วนตัว
1	ต้นไม้ที่เป็นอิสระต่อกัน	เซตที่เป็นอิสระต่อกัน (Independent Set)	ระดับที่ไม่มีการปิดบัง
2	ต้นไม้ที่มีส่วนร่วมกัน	เซตที่มีส่วนร่วมกัน (Intersection Set)	ระดับการปิดบังส่วน n บิตซ้าย
3	ต้นไม้ที่เป็นส่วนย่อยแท้แบบ A อยู่ใน B	เซตที่เป็นสับเซตแท้ (Proper Subset)	ระดับการปิดบังส่วน n บิตขวา
4	ต้นไม้ที่เป็นส่วนย่อยแท้แบบ B อยู่ใน A	เซตที่เป็นสับเซตแท้ (Proper Subset)	ระดับการปิดบังส่วน n บิตขวา
5	ต้นไม้ที่สมมูลกัน	เซตที่สมมูลกัน (Equivalent Set)	ระดับการปิดบังทั้ง 32 บิต

จากโครงสร้างต้นไม้ของความเป็นส่วนตัว เมื่อนำโครงสร้างต้นไม้ของสององค์กรใดๆ มาพิจารณารูปแบบความสัมพันธ์ร่วมกัน โดยกำหนดให้องค์กร A แทนองค์กรที่เป็นผู้วิเคราะห์ข้อมูล และองค์กร B เป็นองค์กรที่ถูกวิเคราะห์ข้อมูล ทำให้ได้รูปแบบความสัมพันธ์เป็น 5 รูปแบบ โดยแต่ละรูปแบบนั้นมีระดับความเป็นส่วนตัวในการปิดบังหมายเลขไอพีที่แตกต่างกัน ซึ่งขอกล่าวอย่างสรุปไว้ในตารางที่ 2

4.2 รายการวิเคราะห์เครือข่าย

เมื่อทำการศึกษาถึงรายละเอียดของรายการวิเคราะห์เครือข่ายจากโปรแกรมสำเร็จรูปที่ใช้งานในระบบเครือข่ายปัจจุบันพบว่า รายการวิเคราะห์เครือข่ายแต่ละรายการนั้นมีระดับการมองเห็นและวิธีการใช้งานข้อมูลที่แตกต่างกัน บางกรณีต้องการวิเคราะห์ข้อมูลเพียงส่วนเครือข่ายของหมายเลขไอพี บางกรณีก็เพียงส่วนเครื่องเท่านั้น หรือบางกรณีต้องการวิเคราะห์ทั้งส่วนเครือข่ายและส่วนเครื่อง โดยงานวิจัยเรื่องนี้ได้กำหนดรายการวิเคราะห์เครือข่ายออกเป็น 4 กลุ่มรายการ ซึ่งแต่ละกลุ่มประกอบไปด้วยรายการย่อยที่แตกต่างกัน และแต่ละรายการย่อยก็ยังมีระดับความเป็นส่วนตัวที่ใช้พิจารณาในการปิดบังหมายเลขไอพีที่แตกต่างกันด้วย ซึ่งเป็นไปตามหน้าที่การใช้งานหมายเลขไอพี โดยได้กล่าวไว้อย่างสรุปในตารางที่ 3

ตารางที่ 3: ตารางสรุปรายละเอียดของรายการวิเคราะห์เครือข่าย

กลุ่มรายการวิเคราะห์เครือข่าย	รายการวิเคราะห์เครือข่าย	ระดับความเป็นส่วนตัว
1. การใช้งานทรัพยากรและปริมาณงาน (Resource and Capacity Usages)	▪ การวิเคราะห์ประสิทธิภาพเครือข่าย (Network Performances Analysis) ▪ การใช้งานแบนด์วิดท์ของเครือข่าย (Network Bandwidth Usages) ▪ การวางแผนปริมาณข้อมูล (Capacity Planning)	ระดับที่ไม่มีการปิดบัง
	▪ การวิเคราะห์การจราจรมัลติคาสท์ (Multicast Traffic Analysis)	ระดับการปิดบังส่วน n บิตซ้าย
	▪ การใช้งานซีพียู (CPU Usages) ▪ การใช้งานหน่วยความจำ (Memory Usages) ▪ การใช้งานดิสก์ (Disk Usages) ▪ การใช้งานจากบัญชีผู้ใช้ (Accounting Usages)	ระดับการปิดบังส่วน n บิตขวา
	▪ การจัดการพร็อกซี่ (Proxy Management)	ระดับการปิดบังทั้ง 32 บิต
2. สถิติของบริการที่เปิดใช้และให้บริการ	▪ บริการเอชทีทีพี (HTTP Service) ▪ บริการเอสเอ็นเอ็มพี (SNMP Service)	▪ ระดับที่ไม่มีการปิดบัง (ใช้ในกรณีที่ต้องการวิเคราะห์ข้อมูลของทั้งเครือข่าย)

กลุ่มรายการวิเคราะห์เครือข่าย	รายการวิเคราะห์เครือข่าย	ระดับความเป็นส่วนตัว
(Service Statistics)	▪ บริการเทลเน็ต (TELNET Service) ▪ บริการพีโอพีสามหรือป๊อปสาม (POP3 Service) ▪ บริการเอ็นเอ็นทีพี (NNTP Service) ▪ การใช้โปรโตคอลเออาร์พี/ไอซีเอ็มพี (ARP/ICMP Usages) ▪ บริการเอฟทีพี (FTP Service) ▪ บริการเอสเอสเอช (SSH Service) ▪ บริการวีโอไอพี (VoIP Service) ▪ บริการพีทูพี (P2P Service) ▪ การบันทึกสถานะของทีซีพี (TCP Session History)	▪ ระดับการปิดบังส่วน n บิตซ้าย (ใช้ในกรณีที่ต้องการวิเคราะห์ข้อมูลของกลุ่มเครือข่ายย่อย) ▪ ระดับการปิดบังส่วน n บิตขวา (ใช้ในกรณีที่ต้องการวิเคราะห์ข้อมูลรายเครื่อง)
	▪ บริการดีเอ็นเอส (DNS Service)	ระดับการปิดบังทั้ง 32 บิต
3. การวินิจฉัยระบบและการตรวจจับความผิดปกติ (System Diagnosis and Anomaly Detection)	▪ การตรวจจับผู้บุกรุก (Intrusion Detection) ▪ การตรวจจับความผิดพลาด (Fault Detection) ▪ การวิเคราะห์ล็อก (Log Analysis) ▪ การวิเคราะห์เครือข่ายเชิงสังคม (Social Network Analysis) ▪ การวิเคราะห์พฤติกรรม (Behavior Analysis)	ระดับการปิดบังทั้ง 32 บิต
4. การรายงานผลและแสดงผลของระบบ (System Report and Display)	▪ แผนผังเครือข่าย (Network Map)	ระดับการปิดบังทั้ง 32 บิต
	▪ รายงานผ่านเว็บ (Web Report) ▪ รายงานผ่านโปรแกรมประยุกต์ (Application Report) ▪ รายงานผ่านเล่มเอกสาร (Book Report)	▪ ระดับการปิดบังทั้ง 32 บิต (ใช้ในกรณีที่ต้องการแสดงผลลัพธ์ที่สื่อถึงความสัมพันธ์ของกลุ่มเครือข่ายหรือผู้ใช้ในเครือข่าย) ▪ ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม (ใช้ในกรณีที่ไม่ต้องการแสดงผลลัพธ์ที่สื่อถึงความสัมพันธ์ของกลุ่มเครือข่ายหรือผู้ใช้ในเครือข่าย)

4.3 กฎหมายคอมพิวเตอร์

งานวิจัยเรื่องนี้ได้นำพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 [7] มาใช้เป็นปัจจัยหนึ่งในการพิจารณาเลือกระดับความเป็นส่วนตัวสำหรับการปิดบังหมายเลขไอพี โดยการตีความจากพระราชบัญญัติดังกล่าวเพื่อกำหนดระดับความเป็นส่วนตัวที่เหมาะสม ซึ่งพิจารณาเฉพาะหมวดที่ 2 ที่เกี่ยวกับพนักงานเจ้าหน้าที่เท่านั้น โดยขอยกเฉพาะมาตราที่เกี่ยวข้องในการปิดบังหมายเลขไอพีดังต่อไปนี้

1. มาตราที่ 18 (2) ได้กล่าวไว้ว่า "เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง" จากมาตราที่ 18 (2) สามารถตีความได้ว่า การเรียกข้อมูลจราจรทางคอมพิวเตอร์อาจสามารถเรียกได้จากกลุ่มเครือข่ายหรือจากตัวบุคคล

ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง และระดับการปิดบังทั้ง 32 บิตตามลำดับ

2. **มาตราที่ 18 (3)** ได้กล่าวไว้ว่า "สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่" สามารถตีความได้ว่า การสั่งให้ผู้ให้บริการซึ่งในที่นี้หมายถึงผู้ให้บริการอินเตอร์เน็ต (ISP: Internet Service Provider) ส่งมอบข้อมูลการจราจรนั้น จะขึ้นอยู่กับข้อมูลที่ต้องการแลกเปลี่ยนและส่งมอบว่าเป็นข้อมูลขององค์กรใด ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีจึงเป็นไปตามความสัมพันธ์ของต้นไม้ของความเป็นส่วนตัวดังที่ได้กล่าวไว้ในหัวข้อที่ 4.1

3. **มาตราที่ 18 (4)** ได้กล่าวไว้ว่า "ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่" สามารถตีความได้ว่า การทำสำเนา (Capture) ข้อมูลจราจรของระบบคอมพิวเตอร์หรือระบบเครือข่ายใดๆ นั้น ขึ้นอยู่กับพนักงานเจ้าหน้าที่ว่าต้องการใช้ข้อมูลเหล่านั้นเพื่อวิเคราะห์ผลในเรื่องใด ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีจึงเป็นไปตามรายการวิเคราะห์เครือข่ายดังที่ได้กล่าวไว้ในหัวข้อที่ 4.2

4. **มาตราที่ 18 (5)** ได้กล่าวไว้ว่า "สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่" สามารถตีความได้ว่า การที่พนักงานเจ้าหน้าที่สั่งให้ตัวบุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง ส่งมอบข้อมูลให้กับพนักงานเจ้าหน้าที่ ซึ่งข้อมูลเหล่านั้นเป็นข้อมูลส่วนบุคคล ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต

5. **มาตราที่ 18 (6)** ได้กล่าวไว้ว่า "ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้" สามารถตีความได้ว่า การตรวจสอบและการเข้าถึงข้อมูลจากระบบคอมพิวเตอร์ของบุคคลใดบุคคลหนึ่งนั้น เป็นการเข้าถึงที่สามารถระบุถึงตัวบุคคลหรืออุปกรณ์ที่ใช้งานในเครือข่ายได้ ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังทั้ง 32 บิต

6. **มาตราที่ 26 วรรค 1** ได้กล่าวไว้ว่า "ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้" สามารถตีความได้ว่า การเก็บรักษาข้อมูลจราจรของผู้ให้บริการไม่ว่าจะเป็นระยะเวลานานเท่าใดก็ตาม ถ้ายังไม่ใช้งาน ก็ไม่จำเป็นต้องปิดบังหมายเลขไอพี ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับที่ไม่มีการปิดบัง

7. **มาตราที่ 26 วรรค 2** ได้กล่าวไว้ว่า "ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง" สามารถตีความได้ว่า การที่ผู้ให้บริการเก็บรักษาข้อมูลจราจรของเครือข่ายที่เกี่ยวข้องกับตัวผู้ใช้บริการแต่ละคนเพื่อให้สามารถระบุตัวผู้ใช้บริการได้นั้น เป็นการใช้ข้อมูลซึ่งแสดงอยู่ในส่วนเครื่องของหมายเลขไอพี ดังนั้นระดับความเป็นส่วนตัวที่เหมาะสมในการปิดบังหมายเลขไอพีคือระดับการปิดบังส่วน n บิตขวา

ปัจจัยการปิดบังหมายเลขไอพีทั้ง 3 ปัจจัยที่กล่าวมานี้จะถูกพิจารณาร่วมกันในการเลือกระดับความเป็นส่วนตัวที่เหมาะสมเพื่อใช้สำหรับการปิดบังหมายเลขไอพี โดยกระบวนการและผลลัพธ์ที่ได้แสดงไว้ในหัวข้อถัดไป

5. กระบวนการปิดบังและผลการปิดบังหมายเลขไอพี

กระบวนการพิจารณาเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุดในการปิดบังหมายเลขไอพีจะพิจารณาตามปัจจัยการ

ปิดบัง 3 ปัจจัยในหัวข้อก่อนหน้านี้ โดยจะมีสถานการณ์ในการปิดบังหมายเลขไอพีแต่ละสถานการณ์ที่แตกต่างกันเพื่อนำมาวิเคราะห์และพิจารณาหาระดับความเป็นส่วนตัวสุดท้าย

ต่อไปนี้เป็นตัวอย่างสถานการณ์การปิดบังหมายเลขไอพีและผลลัพธ์สุดท้ายจากการพิจารณาปัจจัยการปิดบังทุกปัจจัย

1. สถานการณ์ที่ 1 บริษัท ก ซึ่งเป็นพนักงานเจ้าหน้าที่ สั่งให้บริษัท ข เก็บรักษาข้อมูลของการจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน และได้ทำสำเนาข้อมูลคอมพิวเตอร์ และข้อมูลจราจรจากระบบคอมพิวเตอร์ เพื่อนำมาวิเคราะห์การใช้งานแบนด์วิดท์ของเครือข่าย การใช้งานซีพียู การใช้งานหน่วยความจำ และ การใช้งานดิสก์ ของเครือข่ายของบริษัท ข โดยมีผลการวิเคราะห์ดังแสดงในตารางที่ 4

2. สถานการณ์ที่ 2 ศาลแต่งตั้งให้บริษัท ค เป็นพนักงานเจ้าหน้าที่เพื่อให้บริษัท ค สั่งให้บริษัท ง เก็บข้อมูลการจราจรทางคอมพิวเตอร์ไว้อย่างน้อย 90 วัน โดยบริษัท ค อาจจะขอเรียกดูข้อมูลในอนาคต มีผลการวิเคราะห์ดังแสดงในตารางที่ 5

ระดับความเป็นส่วนตัวสุดท้ายที่ถูกเลือก จะนำมาใช้งานในขั้นตอนของการปิดบังหมายเลขไอพีตามอัลกอริทึมการปิดบังในตารางที่ 6 โดยตัวอย่างผลลัพธ์ที่เป็นไปได้ทั้งหมดของระดับความเป็นส่วนทั้ง 5 ระดับแสดงไว้ในตารางที่ 7

ตารางที่ 4: ตารางตัวอย่างผลการวิเคราะห์การพิจารณาเลือกระดับความเป็นส่วนตัวจากสถานการณ์ที่ 1

ข้อมูลรับเข้า		
1.	หมายเลขไอพีของบริษัท ก	210.246.159.0 (11010010111101101001111100000000)
2.	หมายเลขสับเน็ตมาสของบริษัท ก	255.255.254.0 (11111111111111111111111000000000)
3.	หมายเลขไอพีของบริษัท ข	202.183.253.0 (11001010101101111111110100000000)
4.	หมายเลขสับเน็ตมาสของบริษัท ข	255.255.255.0 (11111111111111111111111100000000)
ระดับความเป็นส่วนตัวจากปัจจัยการปิดบัง		
1.	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับที่ไม่มีการปิดบัง (ต้นไม้ที่เป็นอิสระต่อกัน)
2.	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับการปิดบังส่วน n บิตขวา
3.	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ตามรายการวิเคราะห์เครือข่าย (มาตรา 26 วรรค 1 และ 18 (4))
ระดับความเป็นส่วนตัวสุดท้ายที่เลือก คือ ระดับการปิดบังส่วน n บิตขวา		

ตารางที่ 5: ตารางตัวอย่างผลการวิเคราะห์การพิจารณาเลือกระดับความเป็นส่วนตัวจากสถานการณ์ที่ 2

ข้อมูลรับเข้า		
1.	หมายเลขไอพีของบริษัท ค	161.200.0.0 (10100001110010000000000000000000)
2.	หมายเลขสับเน็ตมาสของบริษัท ค	255.255.0.0 (11111111111111110000000000000000)
3.	หมายเลขไอพีของบริษัท ง	207.46.0.0 (11001111001011100000000000000000)
4.	หมายเลขสับเน็ตมาสของบริษัท ง	255.255.0.0 (11111111111111110000000000000000)
ระดับความเป็นส่วนตัวจากปัจจัยการปิดบัง		
1.	ระดับความเป็นส่วนตัวจากต้นไม้ของความเป็นส่วนตัว	ระดับที่ไม่มีการปิดบัง (ต้นไม้ที่เป็นอิสระต่อกัน)
2.	ระดับความเป็นส่วนตัวจากรายการวิเคราะห์เครือข่าย	ระดับที่ไม่มีการปิดบัง
3.	ระดับความเป็นส่วนตัวจากกฎหมายคอมพิวเตอร์	ระดับที่ไม่มีการปิดบัง (มาตรา 26 วรรค 1)
ระดับความเป็นส่วนตัวสุดท้ายที่เลือก คือ ระดับที่ไม่มีการปิดบัง		

ตารางที่ 6: ตารางของอัลกอริทึมการปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัว

```
1   OriginalIP ← Input
2   Subnet ← Input
3   LeftPart ← binary(OriginalIP) AND binary(Subnet)
4   RightPart ← substring(LeftPart.length, 32)
5   Level ← Input
6   Key ← keyGeneration()
7   If (Level is 1)
8           AnonymizedIP ← OriginalIP
9   Else If (Level is 2)
10          AnonymizedIP ← cryptopan(LeftPart, Key) + RightPart
11  Else If (Level is 3)
12          AnonymizedIP ← LeftPart + cryptopan(RightPart, Key)
13  Else If (Level is 4)
14          AnonymizedIP ← cryptopan(OriginalIP, Key)
15  Else If (Level is 5)
16          AnonymizedIP ← random(OriginalIP, Key)
17  Else //Undefined Level
18          AnonymizedIP ← OriginalIP
19  End If
```

ตารางที่ 7: ตารางตัวอย่างผลลัพธ์ของการปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวแต่ละระดับ

ระดับที่ไม่มีการปิดบัง	ระดับการปิดบังส่วน n บิตซ้าย	ระดับการปิดบังส่วน n บิตขวา	ระดับการปิดบังทั้ง 32 บิต	ระดับการปิดบังทั้ง 32 บิตแบบสุ่ม
161.200.92.0	75.133.113.0	161.200.92.146	75.133.113.146	47.168.34.128
161.200.92.1	75.133.113.1	161.200.92.147	75.133.113.147	170.45.182.23
161.200.92.2	75.133.113.2	161.200.92.144	75.133.113.144	95.156.134.221
161.200.92.3	75.133.113.3	161.200.92.145	75.133.113.145	163.223.31.131
161.200.92.4	75.133.113.4	161.200.92.150	75.133.113.150	24.142.23.41
161.200.92.5	75.133.113.5	161.200.92.151	75.133.113.151	230.69.82.31
161.200.92.6	75.133.113.6	161.200.92.148	75.133.113.148	138.171.158.170
161.200.92.7	75.133.113.7	161.200.92.149	75.133.113.149	181.57.77.28
161.200.92.8	75.133.113.8	161.200.92.154	75.133.113.154	161.244.21.11
161.200.92.9	75.133.113.9	161.200.92.155	75.133.113.155	143.196.186.11
161.200.92.10	75.133.113.10	161.200.92.152	75.133.113.152	18.255.210.79
161.200.92.11	75.133.113.11	161.200.92.153	75.133.113.153	75.130.151.108
161.200.92.12	75.133.113.12	161.200.92.158	75.133.113.158	24.115.131.239

โดยกำหนดให้ หมายเลขไอพีของเครือข่ายทดสอบเป็น 161.200.92.0 (10100001110010000101110000000000) และหมายเลขสับเน็ตมาสเป็น 255.255.255.0 (11111111111111111111111100000000) และกุญแจในการปิดบังเป็น 11101010010011010010110110010010 จะได้ผลลัพธ์จากการปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวแต่ละระดับที่แตกต่างกันตามตารางที่ 7 ที่ได้แสดงไว้ข้างต้น

6. บทสรุปและแนวทางการวิจัยในอนาคต

งานวิจัยเรื่องนี้ได้นำเสนอระดับความเป็นส่วนตัว 5 ระดับในกระบวนการปิดบังหมายเลขไอพี อันได้แก่ ระดับที่ไม่มีการปิดบัง ระดับการปิดบังส่วน n บิตซ้าย ระดับการปิดบังส่วน n บิตขวา ระดับการปิดบังทั้ง 32 บิต และระดับการปิดบังทั้ง 32 บิตแบบสุ่ม และกำหนดปัจจัยการปิดบัง 3 ปัจจัยเพื่อใช้สำหรับพิจารณาเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุดในการ

ปิดบัง อันได้แก่ โครงสร้างต้นไม้ของความเป็นส่วนตัว รายการวิเคราะห์เครือข่าย และกฎหมายคอมพิวเตอร์ ในกระบวนการปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวแต่ละระดับมีอัลกอริทึมในการปิดบังที่แตกต่างกันตามความเหมาะสม ซึ่งหลักการปิดบังหมายเลขไอพีที่นำเสนอนี้ สามารถปิดบังหมายเลขไอพีได้ตรงตามสภาพความเป็นจริงของสถานการณ์การปิดบัง

แนวทางการทำวิจัยในอนาคตคือการสร้างกฎเพื่อใช้ในการกำหนดเงื่อนไขสำหรับเลือกระดับความเป็นส่วนตัวจากปัจจัยการปิดบังทั้ง 3 ปัจจัย และการทดสอบประสิทธิภาพการปิดบังหมายเลขไอพีตามวิธีการที่ได้นำเสนอ

7. กิตติกรรมประกาศ

งานวิจัยเรื่องนี้ได้รับการสนับสนุนเงินทุนจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ตามสัญญารับทุนสนับสนุนการศึกษาระดับบัณฑิตศึกษา โครงการทุนสถาบันบัณฑิตวิทยาศาสตร์และเทคโนโลยีไทย (TGIST) เลขที่ทุน TGIST 01-50-076

8. เอกสารอ้างอิง

[1] G. Minshall, TCPdpriv Command Manual, July 1996.

[2] J. Xu, J. Fan, M. H. Ammar, and S. B. Moon, "Prefix-preserving IP Address Anonymization: Measurement based Security Evaluation and a New Cryptography based Scheme", In Proc. of IEEE Int. Conf. on Network Protocols (ICNP), 2002.

[3] Q. Zhang and X. Li, An IP Address Anonymization Scheme with Multiple Access Levels, In Proc. of Int. Conf. on Information Networking (ICOIN), 2006.

[4] R. Ramaswamy, T. Wolf, High-Speed Prefix-Preserving IP Address Anonymization for Passive Measurement Systems, IEEE/ACM Transactions on Networking, 2007.

[5] F. Haibl and F. Dressler. "Anonymization of Measurement and Monitoring Data: Requirements and Solutions", Praxis der Informationsverarbeitung und Kommunikation (PIK), 2006.

[6] J. Xu, J. Fan, M. H. Ammar, and S. B. Moon. "On the design and performance of prefix-preserving IP traffic trace anonymization", In Proc. of ACM SIGCOMM Internet Measurement Workshop, 2001.

[7] Thailand Computer Crimes Act B.E. 2550, 2007.

ประวัติผู้เขียนวิทยานิพนธ์

นายวงศ์ยศ เกิดศรี เกิดเมื่อวันที่ 13 มิถุนายน พ.ศ. 2526 ที่จังหวัดสงขลา สำเร็จการศึกษาระดับประถมศึกษาในปี พ.ศ. 2538 จากโรงเรียนบ้านควนเนียง จังหวัดสงขลา โดยสอบได้เป็นลำดับที่ 1 ของโรงเรียน สำเร็จการศึกษาระดับมัธยมศึกษาตอนต้นในปี พ.ศ. 2541 จากโรงเรียนหาดใหญ่วิทยาลัยสมบูรณ์กุลกันยา (ญ.ส.) จังหวัดสงขลา ด้วยผลการเรียนเฉลี่ย 3.13 และสำเร็จการศึกษาระดับมัธยมศึกษาตอนปลายสายวิทยาศาสตร์-คณิตศาสตร์ ในปี พ.ศ. 2544 จากโรงเรียนหาดใหญ่วิทยาลัยสมบูรณ์กุลกันยาเช่นเดียวกัน ด้วยผลการเรียนเฉลี่ย 3.40 ซึ่งเป็นลำดับที่ 12 ของโรงเรียน

นายวงศ์ยศ เกิดศรี มีความสนใจด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศเป็นพิเศษ ในปี พ.ศ. 2545 ได้เข้าศึกษาต่อในระดับปริญญาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์ จังหวัดสงขลา และสำเร็จการศึกษาในสาขาวิชาดังกล่าวในปี พ.ศ. 2548 ด้วยปริญญาบัณฑิตเกียรตินิยมอันดับหนึ่ง ผลการเรียนเฉลี่ย 3.63 ซึ่งเป็นลำดับที่ 3 ของสาขาวิชา ต่อมาได้เข้าศึกษาต่อในระดับปริญญามหาบัณฑิต สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย กรุงเทพมหานคร ในปี พ.ศ. 2549 และสำเร็จการศึกษาปริญญามหาบัณฑิตในสาขาวิชาดังกล่าวในปี พ.ศ. 2551 ด้วยผลการเรียนเฉลี่ย 3.58 และผลสอบวิทยานิพนธ์ระดับดี ต่อมาในปี พ.ศ. 2552 ได้เข้าศึกษาต่อในระดับปริญญาดุษฎีบัณฑิตในสาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

นอกจากนี้ นายวงศ์ยศ เกิดศรี ยังสำเร็จการศึกษาในระดับปริญญาบัณฑิต สาขาวิชาบริหารธุรกิจ วิชาเอกการจัดการทั่วไป คณะวิทยาการจัดการ มหาวิทยาลัยสุโขทัยธรรมาธิราช ในปี พ.ศ. 2551 และกำลังศึกษาในระดับปริญญาบัณฑิตอีก 2 สาขาวิชา ได้แก่ สาขาวิชาศิลปศาสตร์ วิชาเอกภาษาอังกฤษ คณะมนุษยศาสตร์ มหาวิทยาลัยรามคำแหง และสาขาวิชาเศรษฐศาสตร์ วิชาเอกเศรษฐศาสตร์ธุรกิจ คณะเศรษฐศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช