# โครงร่างวิทยานิพนธ์

## (Thesis Proposal)

| | |
|---|---|
| **ชื่อเรื่อง (ภาษาไทย)** | แบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว |
| **ชื่อเรื่อง (ภาษาอังกฤษ)** | AN IP ADDRESS ANONYMIZATION SCHEME BASED ON PRIVACY LEVELS |


| | |
|---|---|
| **เสนอโดย** | นายวงศ์ยศ เกิดศรี |
| **เลขประจำตัวนิสิต** | 497 05416 21 |
| **หลักสูตร** | วิทยาศาสตรมหาบัณฑิต |
| **สาขาวิชา** | วิทยาศาสตร์คอมพิวเตอร์ |
| **ภาควิชา** | วิศวกรรมคอมพิวเตอร์ |
| **คณะ** | วิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย |
| **สถานที่ติดต่อ** | ห้องพัก 1306 หอพักนิสิตชาย (ตึกจำปี)<br>จุฬาลงกรณ์มหาวิทยาลัย ถนนพญาไท แขวงวังใหม่<br>เขตปทุมวัน กรุงเทพมหานคร 10330 |
| **โทรศัพท์** | 089-599-3490 (มือถือ) 027-76505980 (พีซีที) |
| **ไปรษณีย์อิเล็กทรอนิกส์** | wongyos@gmail.com, wongyos.k@student.chula.ac.th |
| **เว็บไซต์ส่วนบุคคล** | http://zeus.cp.eng.chula.ac.th/~g49wkr/ |

| | |
|---|---|
| **อาจารย์ที่ปรึกษาวิทยานิพนธ์** | อาจารย์ ดร.ยรรยง เต็งอำนวย |
| **อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม** | ดร.ภาสกร ประถมบุตร |



| | |
|---|---|
| **ทุนสนับสนุนวิทยานิพนธ์** | ทุนสถาบันบัณฑิตวิทยาศาสตร์และเทคโนโลยีไทย<br>(Thailand Graduate Institute of Science and Technology: TGIST) |

| | |
|---|---|
| **คำสำคัญ (ภาษาไทย)** | การปิดบังหมายเลขไอพี หมายเลขไอพีนิรนาม ระดับความเป็นส่วนตัว ความเป็นส่วนตัว ความปลอดภัย ความไม่ปรากฏนาม การตรวจตรา การตรวจจับ การวิเคราะห์เครือข่าย การจัดการเครือข่าย |
| **คำสำคัญ (ภาษาอังกฤษ)** | IP Address Anonymization, Anonymized IP Address, Privacy Levels, Privacy, Security, Anonymity, Trace, Sniffer, Network Analysis, Network Management |

# โครงร่างวิทยานิพนธ์

## หัวข้อวิทยานิพนธ์

**ภาษาไทย** แบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว

**ภาษาอังกฤษ** AN IP ADDRESS ANONYMIZATION SCHEME BASED ON PRIVACY LEVELS

## 1. ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันการวิเคราะห์และจัดการเครือข่ายมีความจำเป็นอย่างยิ่งในการดูแลและควบคุมระบบเครือข่ายให้สามารถทำงานได้อย่างปกติ มีความถูกต้อง และมีประสิทธิภาพ ซึ่งการวิเคราะห์และจัดการเครือข่ายนั้น จำเป็นจะต้องใช้ข้อมูลที่ได้จากการตรวจตราการจราจรในเครือข่าย (Network Traffic Traces) และการตรวจจับแพ็คเก็ต (Packets Sniffer) ซึ่งประกอบไปด้วยข้อมูลที่มีการรับเข้าและส่งออกมากมายหลายประเภท โดยข้อมูลจำพวกหนึ่งที่จะปรากฏอยู่เมื่อมีการตรวจตราและตรวจจับแพ็คเก็ตในระบบเครือข่ายก็คือ หมายเลขไอพี (IP Address) ซึ่งหมายเลขไอพีนี้จะปรากฏอยู่ในส่วนของเฮดเดอร์ (Header) ภายในแพ็คเก็ตทุกแพ็คเก็ตที่ทำงานอยู่ในระดับชั้นเครือข่าย (Network Layers) ของโครงสร้างระบบเครือข่าย โดยประกอบไปด้วยส่วนของหมายเลขไอพีต้นทาง (Source IP Address) และหมายเลขไอพีปลายทาง (Destination IP Address) แต่หมายเลขไอพีทั้งหมดที่กล่าวมานั้นเป็นหมายเลขไอพีดั้งเดิม (Original IP Address) หรือหมายเลขไอพีจริง (Real IP Address) ที่มาจากอุปกรณ์ในเครือข่าย ซึ่งเห็นได้ว่าข้อมูลที่ประกอบไปด้วยหมายเลขไอพีเหล่านี้เป็นข้อมูลที่สามารถระบุถึงตัวบุคคล [4] หรืออุปกรณ์ปลายทางหรือองค์กรที่ใช้งานระบบเครือข่าย เพราะเนื่องจากว่าหมายเลขไอพีสามารถบ่งบอกถึงความเป็นเจ้าของของบุคคลคนหนึ่งที่กำลังใช้งานอุปกรณ์ในเครือข่ายอยู่ ณ เวลาใดเวลาหนึ่ง หรือเป็นการแสดงว่าอุปกรณ์ในเครือข่ายกำลังเปิดใช้งานอยู่ ณ เวลานั้น และเมื่อมีการปิดใช้งานอุปกรณ์นั้นแล้ว หมายเลขไอพีดังกล่าวก็ยังจะถูกระบุและกำหนดให้กับอุปกรณ์เครื่องนั้นอยู่เสมอ ตราบใดที่ยังไม่ได้มีการเปลี่ยนแปลงหมายเลขไอพีไปเป็นหมายเลขอื่น

แต่อย่างไรก็ตามจะเห็นได้ว่า ข้อมูลที่เป็นหมายเลขไอพีที่ได้จากการตรวจตราและตรวจจับแพ็คเก็ตเหล่านั้นเป็นข้อมูลที่ไม่ได้มีการปิดบังหมายเลขไอพีเลยแม้แต่อย่างใด เมื่อมีการแสดงข้อมูลและผลลัพธ์ที่ได้จากการวิเคราะห์และจัดการเครือข่ายจะทำให้มองเห็นและทราบได้ว่าหมายเลขไอพีหมายเลขต่าง ๆ เป็นของบุคคลใดบ้าง ซึ่งในทางปฏิบัติแล้วผู้ที่ทำการวิเคราะห์และจัดการเครือข่ายไม่ควรล่วงรู้ข้อมูลที่มีความเป็นส่วนตัว (Privacy) แบบนั้นได้ แต่เพียงมีหน้าที่ในการตรวจสอบข้อมูลของระบบเครือข่ายว่ามีปัญหาอะไรเกิดขึ้นบ้างเท่านั้น ดังตัวอย่างเช่น สถานการณ์ที่ผู้ดูแลระบบเครือข่ายต้องการที่จะตรวจสอบสถิติการใช้บริการเว็บไซต์บนโปรโตคอลเอชทีทีพี (HTTP) ของสมาชิกในเครือข่ายแห่งหนึ่ง ซึ่งกระบวนการวิเคราะห์สถิติดังกล่าวอาจจะทำให้สามารถมองเห็นและทราบถึงรายละเอียดในการเข้าใช้งานเว็บไซต์ต่าง ๆ ของสมาชิกเป็นรายบุคคลได้ ซึ่งไม่ถูกต้องตามแนวทางที่ควรปฏิบัติ ผู้ดูแลระบบเครือข่ายไม่ควรล่วงรู้และละเมิดความเป็นส่วนตัวของสมาชิกเหล่านั้นได้ หรือสถานการณ์ที่หน่วยงานผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider) หรือไอเอสพี (ISP) ต้องการจะนำข้อมูลของลูกค้าและผู้ใช้บริการไปตรวจสอบค่าทางสถิติ ก็จำเป็นต้องปิดบังหมายเลขไอพีที่ปรากฏอยู่ในส่วนเฮดเดอร์แพ็คเก็ตก่อนทำการวิเคราะห์ เช่น หน่วยงานยูนิเน็ต (Uninet) ต้องการจะตรวจสอบค่าทางสถิติของเครือข่ายจุฬาลงกรณ์มหาวิทยาลัย หน่วยงานยูนิเน็ตจะต้องทำการปิดบังหมายเลขไอพีก่อนเริ่มกระบวนการทำงานและวิเคราะห์ผล ทั้งนี้เพื่อไม่เป็นการก้าวก่ายความเป็นส่วนตัวของสมาชิกในเครือข่ายเหล่านั้น

ดังนั้นข้อมูลส่วนบุคคลที่เป็นหมายเลขไอพีนี้จึงต้องถูกปิดบังเอาไว้เพื่อให้เกิดความเป็นส่วนตัวแก่สมาชิกที่ใช้งานอยู่ในระบบเครือข่าย โดยวิธีการปิดบังหมายเลขไอพี (IP Address Anonymization) เป็นวิธีการปกปิดความเป็นส่วนตัวของผู้ใช้และอุปกรณ์ที่เปิดใช้งานอยู่ในระบบเครือข่ายเมื่อมีการนำข้อมูลเหล่านั้นไปใช้เพื่อวิเคราะห์และจัดการระบบเครือข่าย

การปิดบังหมายเลขไอพีเริ่มตั้งแต่การแปลงหมายเลขไอพีจริงที่ปรากฏในเฮดเดอร์ของแพ็คเก็ตที่ได้จากการตรวจตราและตรวจจับแพ็คเก็ต ให้กลายเป็นหมายเลขไอพีปลอม (Faked IP Address) หรือหมายเลขไอพีนิรนาม (Anonymized IP Address) ก่อนที่จะนำไปใช้ทำการวิเคราะห์สถิติต่าง ๆ หรือทำการวิเคราะห์คุณลักษณะต่าง ๆ ของเครือข่าย และจัดการกับระบบเครือข่ายต่อไปได้

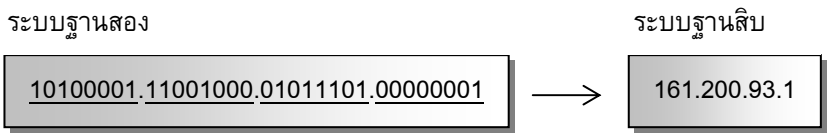
วิธีการและแบบแผนในการปิดบังหมายเลขไอพีมีอยู่หลายวิธีการด้วยกันซึ่งจะได้กล่าวเพิ่มเติมในส่วนของทฤษฎีและงานวิจัยที่เกี่ยวข้องต่อไป โดยในแต่ละวิธีการปิดบังหมายเลขไอพีนั้นจะมีลักษณะของความไม่ปรากฏนาม (Anonymity) หรือการปิดบังชื่อที่แตกต่างกันออกไป แต่อย่างไรก็ตามเมื่อมองถึงหลักการในการใช้งานหมายเลขไอพีนิรนามที่มีการปิดบังชื่อด้วยวิธีการใดวิธีการหนึ่งเป็นที่เรียบร้อยแล้วนั้น ยังคงไม่เหมาะสมกับการทำงานบางประเภทของการวิเคราะห์และจัดการเครือข่าย เพราะเนื่องจากว่าในทางปฏิบัติแล้วการปิดบังหมายเลขไอพีนั้นไม่มีความจำเป็นที่จะต้องปิดบังทั้งหมดหรือปิดบังในทุกประเภทของการวิเคราะห์และจัดการเครือข่าย แต่จะขึ้นอยู่กับว่ามีความจำเป็นมากหรือน้อยเพียงใดในการปิดบังหมายเลขไอพีตามประเภทของการวิเคราะห์และจัดการเครือข่ายประเภทต่าง ๆ ซึ่งขึ้นอยู่กับผู้ดูแลระบบเครือข่าย (Network Administrator) ที่จะจัดระดับความเป็นส่วนตัว (Privacy Levels) ในการปิดบังหมายเลขไอพีให้อยู่ในระดับใดบ้างและควรปิดบังหมายเลขไอพีในส่วนใดบ้าง ในขณะเดียวกันความต้องการที่จะนำข้อมูลแพ็คเก็ตมาทำการวิเคราะห์คุณลักษณะต่าง ๆ ของระบบเครือข่ายนั้นมีระดับความต้องการที่จะปิดบังหมายเลขไอพีที่แตกต่างกัน ซึ่งขึ้นอยู่กับว่าการวิเคราะห์ข้อมูลในแต่ละคุณลักษณะจะมองหรือสนใจถึงความเป็นส่วนตัวมากน้อยแค่ไหน หรือเกี่ยวข้องกับความเป็นส่วนตัวมากน้อยเพียงใด ถ้ามีความสนใจและเกี่ยวข้องในความเป็นส่วนตัวมากแสดงว่าต้องมีการปิดบังหมายเลขไอพีในส่วนนั้นให้มาก ซึ่งหมายความว่าข้อมูลแพ็คเก็ตที่จะใช้ทำการวิเคราะห์และจัดการเครือข่ายในประเภทและคุณลักษณะนั้นมีความต้องการสูงในการปิดบังหมายเลขไอพี

การจัดระดับความเป็นส่วนตัวในการปิดบังหมายเลขไอพีไม่ได้มีการเจาะจงถึงอัลกอริทึม (Algorithm) ของการปิดบังในรูปแบบใดรูปแบบหนึ่ง แต่จะพิจารณาว่าอัลกอริทึมและวิธีการปิดบังหมายเลขไอพีที่มีการนำเสนอมาในรูปแบบต่าง ๆ นั้น สามารถนำมาใช้กับการจัดระดับความเป็นส่วนตัวในการปิดบังหมายเลขไอพีได้ขึ้นอยู่กับว่าอัลกอริทึมใดจะเหมาะสมกับระดับความเป็นส่วนตัวระดับใด หรืออาจไม่มีความจำเป็นใด ๆ ที่ต้องใช้อัลกอริทึมในการปิดบังหมายเลขไอพี ซึ่งจะทำให้วิธีการและขั้นตอนการปิดบังหมายเลขไอพีถูกเลือกใช้งานได้อย่างเหมาะสมตรงตามความต้องการและความจำเป็นที่จะปิดบังหมายเลขไอพีไปตามประเภทของการวิเคราะห์และจัดการเครือข่ายได้ ทั้งยังทำให้การวิเคราะห์และจัดการเครือข่ายสามารถประมวลผลได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

## 2. ทฤษฎีที่เกี่ยวข้อง

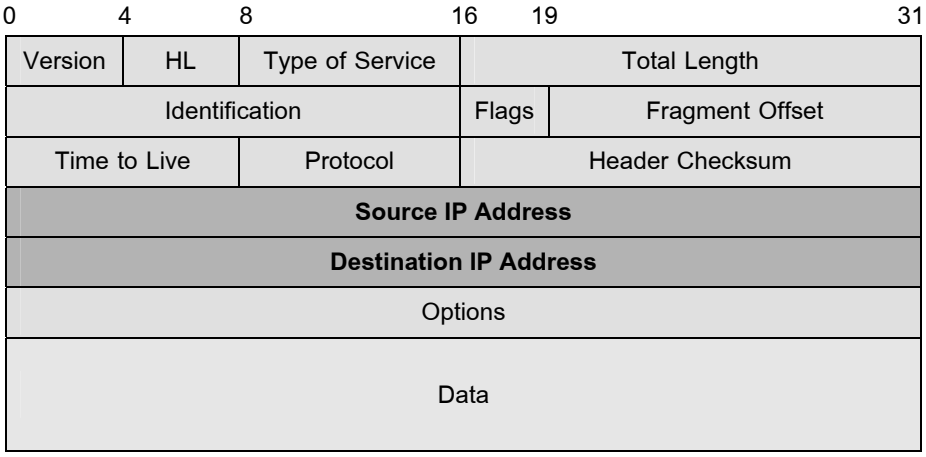
### 2.1 หมายเลขไอพี

หมายเลขไอพีหรือไอพีแอดเดรส (IP Address หรือ Internet Protocol Address) คือหมายเลขที่ใช้ในระบบเครือข่าย ซึ่งมีลักษณะคล้ายกับหมายเลขโทรศัพท์ที่จะระบุถึงที่อยู่ของอุปกรณ์ในเครือข่าย [18] โดยจะเป็นตัวเลขฐานสองขนาด 32 บิต ซึ่งหมายเลขไอพีแบ่งเป็น 4 กลุ่ม โดยแต่ละกลุ่มจะใช้เลขฐานสองขนาด 8 บิต และมีสัญลักษณ์จุด (Dot) เป็นตัวแบ่งตัวเลขในแต่ละกลุ่มเอาไว้ แต่โดยทั่วไปแล้วเพื่อความสะดวกจึงมักแสดงผลโดยการใช้เลขฐานสิบ 4 กลุ่มแทน ดังตัวอย่างในรูปที่ 1




รูปที่ 1 ลักษณะของหมายเลขไอพี 32 บิตในรูปแบบของเลขฐานสองและเลขฐานสิบ

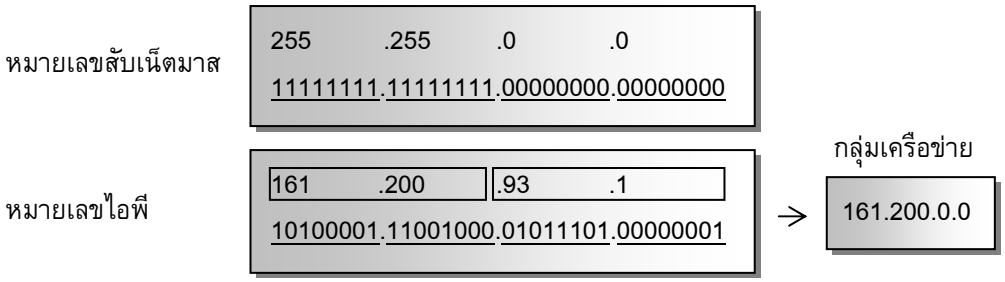
หมายเลขไอพีจะปรากฏอยู่ในส่วนของเฮดเดอร์ของแพ็คเก็ตที่ทำงานอยู่ในระดับชั้นเครือข่ายดังแสดงในส่วนโครงสร้างของเฮดเดอร์ในระดับชั้นเครือข่าย [7] ตามรูปที่ 2 ประกอบด้วยหมายเลขไอพีของเครื่องต้นทางและหมายเลขไอพีของเครื่องปลายทาง ซึ่งหมายเลขไอพีนี้จะถูกผนวกเข้าเป็นข้อมูลส่วนหนึ่งภายในแพ็คเก็ตที่ใช้ในการสื่อสารและแลกเปลี่ยนข้อมูลระหว่างกันของอุปกรณ์ในเครือข่าย




รูปที่ 2 โครงสร้างของเฮดเดอร์ในระดับชั้นเครือข่าย

หมายเลขไอพีที่ใช้งานอยู่ในปัจจุบันนั้นเป็นระบบไอพีรุ่นที่ 4 (IPv4) ซึ่งมีรูปแบบเป็นไปตามหมายเลขไอพีระบบ 32 บิตที่ได้กล่าวมาแล้วในตอนต้น โดยประกอบไปด้วยหมายเลขไอพีที่เป็นไปได้ทั้งหมด $2^{32}$ หมายเลข เริ่มตั้งแต่หมายเลข 0.0.0.0 จนถึงหมายเลข 255.255.255.255 แต่หมายเลขไอพีทั้ง $2^{32}$ หมายเลขนี้ไม่สามารถถูกกำหนดให้กับอุปกรณ์ในเครือข่ายได้ทั้งหมด เพราะเนื่องจากว่ามีหมายเลขไอพีบางหมายเลขที่สงวนไว้สำหรับทำหน้าที่เฉพาะเช่น 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

ทั้งนี้ การจัดแบ่งและกำหนดขอบเขตของหมายเลขไอพีให้กับกลุ่มเครือข่ายหรือกลุ่มองค์กรหนึ่ง ๆ นั้นในปัจจุบันจะใช้วิธีการจัดแบ่งด้วยหมายเลขสับเน็ตมาส (Subnet Mask Address) ดังแสดงในรูปที่ 3




รูปที่ 3 การจัดแบ่งหมายเลขไอพีด้วยหมายเลขสับเน็ตมาส

หมายเลขสับเน็ตมาสจะแบ่งหมายเลขไอพีออกเป็น 2 ส่วนดังนี้

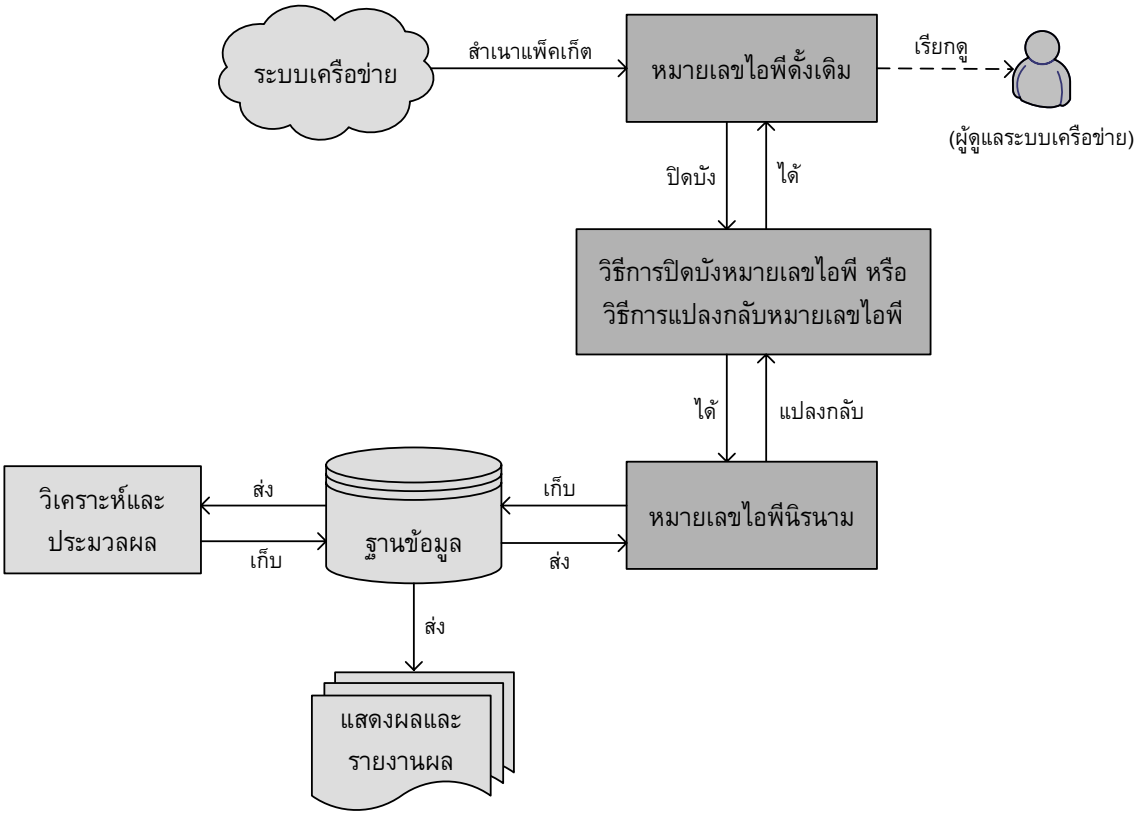
1. **ส่วนของกลุ่มเครือข่าย (Network Path)** แสดงด้วยบิต 1 ของหมายเลขสับเน็ตมาส ซึ่งเป็นกลุ่มของบิตทางซ้ายที่ระบุถึงความเป็นกลุ่มของเครือข่ายหรือกลุ่มขององค์กรหรือหน่วยงานในเครือข่าย

**2. ส่วนของกลุ่มเจ้าบ้าน (Host Path)** แสดงด้วยบิต 0 ของหมายเลขสับเน็ตมาส ซึ่งเป็นกลุ่มของบิตทางขวาที่ระบุถึงจำนวนของเครื่องหรืออุปกรณ์ปลายทางในเครือข่าย

### 2.2 การปิดบังหมายเลขไอพี

การปิดบังหมายเลขไอพี (IP Address Anonymization) เป็นกระบวนการแปลงหมายเลขไอพีดั้งเดิม ทั้งหมายเลขไอพีต้นทางและปลายทางที่ปรากฏอยู่ในเฮดเดอร์ของแพ็คเก็ตให้กลายเป็นหมายเลขไอพีนิรนาม เพื่อเป็นการปกปิดข้อมูลส่วนบุคคล และปิดบังลักษณะต่าง ๆ ที่มีความเป็นส่วนตัวของอุปกรณ์ในเครือข่ายเอาไว้

โดยกระบวนการทำงานจะเริ่มเมื่อมีการตรวจตราและตรวจจับแพ็คเก็ตในเครือข่ายขึ้นมาเพื่อทำการวิเคราะห์ในเชิงสถิติ ซึ่งข้อมูลแพ็คเก็ตเหล่านั้นถูกจัดเก็บไว้ในฐานข้อมูล แต่ก่อนที่จะนำข้อมูลแพ็คเก็ตเหล่านั้นไปทำการวิเคราะห์และประมวลผล ข้อมูลจะถูกนำมาขจัดคุณลักษณะที่บ่งบอกถึงความเป็นส่วนตัวออกไปด้วยการปิดบังหมายเลขไอพี โดยลักษณะขั้นตอนทั่วไปของการปิดบังหมายเลขไอพีได้แสดงไว้ในรูปที่ 4 เมื่อกระบวนการวิเคราะห์ข้อมูลเหล่านั้นเสร็จสิ้นเป็นที่เรียบร้อย ข้อมูลส่วนที่เป็นผลลัพธ์และการรายงานผลต่าง ๆ จะถูกปิดบังลักษณะที่แสดงถึงความเป็นส่วนตัวเอาไว้ตามความเหมาะสม




รูปที่ 4 โครงสร้างขั้นตอนทั่วไปของการปิดบังหมายเลขไอพี

การปิดบังหมายเลขไอพีมีวัตถุประสงค์เพื่อที่จะปิดบังข้อมูลที่เป็นส่วนบุคคลให้กับนักวิจัยหรือนักวิเคราะห์ระบบเครือข่ายสามารถทำงานได้โดยไม่ก้าวก่ายข้อมูลส่วนบุคคลของผู้ใช้งานในเครือข่าย ไม่ก่อให้เกิดการละเมิดสิทธิส่วนบุคคลและความเป็นส่วนตัวของผู้ใช้งานในเครือข่าย และเพื่อสร้างความน่าเชื่อถือความไว้วางใจในส่วนของข้อมูลของสมาชิก อุปกรณ์ และองค์กรในเครือข่ายที่อาจถูกนำไปแสดงผลต่อสาธารณะหรือใช้ในกระบวนการวิเคราะห์และจัดการเครือข่ายต่าง ๆ ต่อไปได้

การปิดบังหมายเลขไอพีนั้นมีหลายวิธีซึ่งจะได้กล่าวต่อไปในส่วนของงานวิจัยที่เกี่ยวข้อง โดยแต่ละวิธีการปิดบังนั้นจะมีแนวทางที่สอดคล้องตามกระบวนการขั้นตอนที่ได้แสดงไว้ในรูปที่ 4 ทั้งนี้กระบวนการปิดบังหมายเลขไอพีจะต้องได้หมายเลขไอพีนิรนามที่มีคุณสมบัติเช่นเดียวกับหมายเลขไอพีดั้งเดิมทุกประการ และควรมีอัลกอริทึมที่จะสามารถแปลงหมายเลขไอพีนิรนามกลับเป็นหมายเลขไอพีดั้งเดิมได้

### 2.3 การวิเคราะห์และจัดการเครือข่าย

การวิเคราะห์และจัดการเครือข่าย (Network Analysis and Management) เป็นหลักการวิเคราะห์ ตรวจสอบ บริหารจัดการ ควบคุม และดูแลระบบเครือข่ายให้สามารถทำงานได้อย่างปกติ มีความถูกต้อง ปลอดภัย และมีประสิทธิภาพสูงสุด [2]

#### 2.3.1 หลักการและทฤษฎีที่เกี่ยวข้องในการวิเคราะห์และจัดการเครือข่าย

ประกอบไปด้วยแนวทางและรูปแบบการทำงาน [16] ที่แบ่งออกได้เป็น 3 รูปแบบหลักดังนี้

1. **การใช้โปรโตคอลเอสเอ็นเอ็มพี (Simple Network Management Protocol: SNMP)** ซึ่งจะประกอบไปด้วยเครื่องจัดการ (Manager) ที่เป็นตัวกลางในการร้องขอข้อมูลการทำงานจากโปรแกรมตัวแทน (Agents) ที่อยู่กับอุปกรณ์ต่าง ๆ ในระบบเครือข่าย ซึ่งส่วนใหญ่แล้วจะกระทำกับอุปกรณ์จำพวกเราเตอร์ (Router) สวิตช์ (Switch) และ เซิร์ฟเวอร์ (Server) เป็นต้น
2. **การตรวจจับแพ็คเก็ต (Packet Sniffer)** ซึ่งจะเป็นการสำเนาข้อมูลแพ็คเก็ตที่ถูกส่งมาในเครือข่ายขึ้นมาทำการวิเคราะห์ข้อมูลทางด้านสถิติต่างๆ หรือทำการตรวจจับข้อผิดพลาดของระบบเครือข่าย
3. **การตรวจตราการจราจร (Traffic Traces)** เป็นการตรวจตราข้อมูลของการใช้งานหรือตรวจติดตามพฤติกรรมของอุปกรณ์หนึ่ง ๆ ในเครือข่าย ว่ามีการทำงานและมีการเดินทางของข้อมูลไปในสถานที่ใดบ้าง เพื่อที่จะทราบถึงร่องรอยหรือการแกะรอยการทำงาน เพื่อวิเคราะห์หาสิ่งแปลกปลอมหรือหาสาเหตุบางประการที่เกิดขึ้นกับระบบเครือข่าย

จากรูปแบบของการวิเคราะห์และจัดการเครือข่ายเหล่านี้ได้ถูกนำออกไปประยุกต์ใช้กับระบบการทำงานจริง ซึ่งอยู่ในรูปแบบของซอฟต์แวร์สำเร็จรูปที่ใช้ดูแลเครือข่าย (Monitoring Tools) เช่น เอ็มอาร์ทีจี (MRTG) [15] พีอาร์ทีจี (PRTG) [16] นากิออส (Nagios) [17] และ ออปแมนเนเจอร์ (OpManager) [12] เป็นต้น ซึ่งซอฟต์แวร์สำเร็จรูปเหล่านี้ล้วนแล้วแต่มีลักษณะของการวิเคราะห์และจัดการเครือข่ายที่คล้ายคลึงกัน เช่น การวิเคราะห์การเข้าออกของข้อมูลในเครือข่าย การวิเคราะห์การใช้งานบริการต่างๆ ในเครือข่าย การตรวจสอบอุปกรณ์ในเครือข่าย ณ เวลาหนึ่งๆ เป็นต้น

#### 2.3.2 ประเภทและบริการต่าง ๆ ในการวิเคราะห์และจัดการเครือข่าย

ประเภทและบริการต่าง ๆ ในการวิเคราะห์และจัดการเครือข่ายนั้นประกอบไปด้วยหลายรูปแบบ [1,2] ซึ่งประกอบไปด้วย

1. **ชนิดและประเภทของอุปกรณ์** เป็นการแสดงชนิดหรือประเภทของอุปกรณ์ และจำนวนของอุปกรณ์ที่ใช้งานอยู่ในระแบบเครือข่าย เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องพิมพ์ และเราเตอร์ เป็นต้น ซึ่งอาจจะแสดงอยู่ในรูปแบบของแผนที่เครือข่าย (Network Map)
2. **กลุ่มผู้ใช้งาน** เป็นการเลือกกลุ่มผู้ใช้งานเพื่อนำมาเปรียบเทียบข้อมูลการทำงานในแต่ละกลุ่ม
3. **ระยะเวลาและช่วงเวลาการใช้งาน** เป็นการสรุปข้อมูลทั้งรายวัน รายเดือน และรายปีของระยะเวลาและช่วงเวลาในการใช้งานอุปกรณ์และการเปิดให้บริการของอุปกรณ์ต่าง ๆ
4. **ปริมาณข้อมูลการใช้งาน** เป็นการคำนวณหาปริมาณของข้อมูลการรับเข้าและส่งออกในเครือข่าย หาค่าร้อยละของบริการต่าง ๆ ที่ถูกใช้งาน หาอัตราการใช้งานซีพียู (CPU) ของอุปกรณ์หนึ่ง ๆ หาอัตราการใช้ช่องสัญญาณ และหาความเร็วของการรับและส่งข้อมูล เป็นต้น

**5. จำนวนและชนิดของบริการ** เป็นการนับจำนวนของบริการที่เปิดให้บริการในเครือข่าย และแสดงจำนวนของการเรียกใช้งานบริการต่าง ๆ ในเครือข่าย

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

นอกจากนี้ ยังมีประเภทและลักษณะของการวิเคราะห์และจัดการเครือข่ายในรูปแบบอื่น ๆ ที่ยังไม่ได้กล่าวไว้ในที่นี้ซึ่งจะศึกษาวิจัยและสรุปเพิ่มเติมในรายงานวิจัยต่อไป

## 3. งานวิจัยที่เกี่ยวข้อง

วิธีการและแบบแผนการปิดบังหมายเลขไอพีนั้นได้รับความสนใจเพิ่มมากยิ่งขึ้นในปัจจุบัน เพราะเนื่องจากว่า เมื่อระบบเครือข่ายคอมพิวเตอร์มีการขยายตัวอย่างแพร่หลายก็ย่อมต้องมีการคำนึงถึงความเป็นส่วนบุคคลของข้อมูลมากยิ่งขึ้นด้วยเช่นกัน หมายเลขไอพีนั้นจัดเป็นข้อมูลส่วนบุคคลประเภทหนึ่ง ดังนั้นข้อมูลเหล่านี้ต้องได้รับการปิดบังเอาไว้

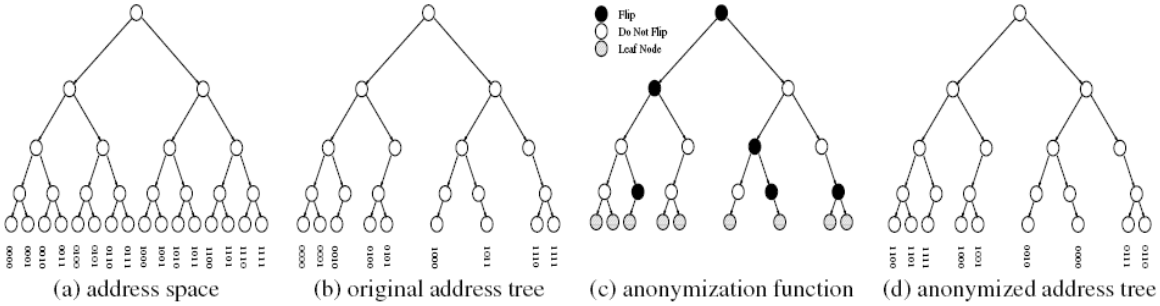
วิธีการและแบบแผนการปิดบังหมายเลขไอพีเกิดขึ้นมาเมื่อประมาณสิบปีเศษ โดยรูปแบบการปิดบังหมายเลขไอพีเริ่มแรกนั้นใช้หลักการพื้นฐานและอัลกอริทึมอย่างง่ายในการทำงาน [4] เช่น การใช้ฟังก์ชันแฮช (Hash Function) การเข้ารหัสด้วยวิธีเอ็มดี 5 (MD5) การเข้ารหัสด้วยวิธีการของอาร์เอสเอ (RSA) และ การเข้ารหัสด้วยวิธีแบบซีซ่า (Caesar) เป็นต้น ซึ่งวิธีการเหล่านี้ต้องจับคู่ระหว่างหมายเลขไอพีต้นแบบกับหมายเลขไอพีนิรนามแต่ละคู่เข้าไว้ด้วยกันแบบหนึ่งต่อหนึ่ง (One-to-One Mapping) [8,9,13] และเก็บบันทึกหมายเลขไอพีในรูปแบบของตารางค้นหา (Table Lookup) เพื่อใช้ในการค้นคืนหมายเลขไอพีดั้งเดิม แต่วิธีการพื้นฐานเหล่านี้เป็นเพียงการแปลงหมายเลขไอพีดั้งเดิมให้กลายเป็นหมายเลขไอพีนิรนามเท่านั้น เมื่อนำไปใช้งานจริงในการวิเคราะห์และจัดการเครือข่ายแล้วจะทำได้ยากลำบาก ก่อให้เกิดปัญหาและความผิดพลาดขึ้นได้ เพราะเนื่องจากว่าหมายเลขไอพีนิรนามดังกล่าวไม่สามารถเป็นตัวแทนและสื่อความหมายของข้อมูลได้เช่นเดียวกับหมายเลขไอพีดั้งเดิม เช่น ไม่สามารถแยกแยะกลุ่มของเครือข่ายได้ เกิดการชนและซ้ำซ้อนของหมายเลขไอพีและต้องมีตารางในการเก็บหมายเลขไอพีดั้งเดิมและหมายเลขไอพีนิรนามในแต่ละคู่ เป็นต้น

จนเมื่อปี ค.ศ. 1996 เกรก มินแชล (Greg Minshall) [6] ได้คิดวิธีการปิดบังหมายเลขไอพีอย่างเป็นรูปแบบวิธีการแรกขึ้นมาซึ่งชื่อว่าทีซีพีดีไพรว์ (Tcpdpriv) และได้รับการโต้แย้งข้อผิดพลาดจากการทำงานโดยทาทุ โยลเน็น (Tatu Ylonen) [11] ในปีเดียวกัน โดยวิธีการทีซีพีดีไพรว์นั้นจะเป็นอัลกอริทึมหนึ่งในโปรแกรมทีซีพีดัมพ์ (Tcpdump) ซึ่งถูกพัฒนาอยู่บนระบบยูนิกซ์ (UNIX) ตระกูลเน็ตบีเอสดี (NetBSD) ฟรีบีเอสดี (FreeBSD) ซัน (SunOS) และ โซลาริส (Solaris) จนเมื่อปี ค.ศ. 1999 เจอราล์ด คอมบ์ (Gerald Combs) [5] ได้ย้ายวิธีการทีซีพีดีไพรว์ไปใช้งานบนระบบลีนุกซ์ (Linux) ได้สำเร็จ

หลักการทำงานของทีซีพีดีไพรว์นั้นจะนำเอาหมายเลขไอพีต้นแบบมาทำการจับคู่แบบสุ่ม (Randomized Mapping) ตามระดับความปลอดภัยที่แตกต่างกันจนได้หมายเลขไอพีนิรนามออกมา ซึ่งวิธีการทีซีพีดีไพรว์นี้สามารถแก้ไขปัญหาของการสื่อความหมายของกลุ่มเครือข่ายได้ โดยหมายเลขไอพีนิรนามที่ได้จะสามารถแยกแยะกลุ่มของเครือข่ายได้เช่นเดียวกับหมายเลขไอพีดั้งเดิม แต่วิธีการดังกล่าวจะต้องมีการจับคู่ระหว่างหมายเลขไอพีดั้งเดิมกับหมายเลขไอพีนิรนามแบบหมายเลขต่อหมายเลขเช่นเดิม ซึ่งจะทำให้เกิดปัญหาในการทำงานขึ้นได้เมื่อมีหมายเลขไอพีจำนวนมาก และส่งผลให้เกิดการชนกันของหมายเลขไอพีนิรนามขึ้นได้เมื่อมีการกรองและจับแพ็คเก็ตในรอบถัดไปหรือเมื่อมีการทำงานหลาย ๆ รอบ

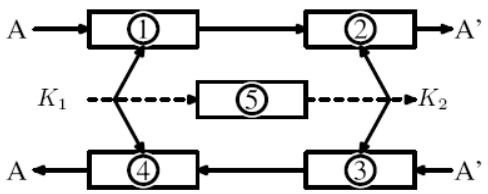
ดังนั้นจึงได้มีการคิดวิธีการปิดบังหมายเลขไอพีแบบใหม่ขึ้น โดยในปี ค.ศ. 2002 จุน ซือ (Jun Xu) และคณะ [8,9] ได้นำหลักการทางวิทยาการเข้ารหัสลับ (Cryptography) เข้ามาช่วยในการแปลงหมายเลขไอพี ซึ่งเป็นวิธีการที่เรียกว่าคริปโตแพน (Crypto-PAn) โดยใช้ทฤษฎีรูปแบบคาโนนิคอล (Canonical Form Theorem) ในการ

สร้างอัลกอริทึมการแปลงหมายเลขไอพีขึ้นมาซึ่งมีรูปแบบเป็นต้นไม้ของการปิดบังหมายเลขไอพี (Address Anonymization Tree) ดังแสดงในรูปที่ 5 และทั้งยังนำหลักการของทีซีพีดีไพรว์เข้ามาพัฒนาร่วมด้วย ซึ่งได้ผลเป็นที่น่าพอใจ โดยสามารถแปลงหมายเลขไอพีดั้งเดิมให้เป็นหมายเลขไอพีนิรนามได้โดยไม่เกิดปัญหาการชนกัน และสามารถคงไว้ซึ่งข้อมูลในส่วนของบิตที่จะระบุถึงความแตกต่างของกลุ่มเครือข่าย (Prefix Preserving) เอาไว้ได้เช่นเดิม




รูปที่ 5 ต้นไม้ของการปิดบังหมายเลขไอพีตามทฤษฎีรูปแบบคาโนนิคอล

วิธีการปิดบังหมายเลขไอพีดังกล่าวทั้งสองวิธีได้ถูกยอมรับและนำไปประยุกต์กับระบบการวิเคราะห์และจัดการเครือข่ายในกลุ่มวิจัยและองค์กรต่าง ๆ มากมาย แต่อย่างไรก็ตามยังมีนักวิจัยบางกลุ่มที่ได้คิดและพัฒนาระบบการปิดบังหมายเลขไอพีขึ้นมาอยู่เรื่อย ๆ จนเมื่อปี ค.ศ. 2006 ที่ผ่านมาได้มีการคิดวิธีการและแบบแผนการปิดบังหมายเลขไอพีขึ้นมาใหม่อีกรูปแบบหนึ่ง ซึ่งได้นำเอาแนวคิดของวิธีการแบบคริปโตแพนและการจับคู่แบบหนึ่งต่อหนึ่งมาประยุกต์ใช้โดยเคียนลี่ จาง (Qianli Zhang) และคณะ [13] ได้ใช้หลักการแบ่งระดับการเข้าถึงหลายชั้น (Multiple Access Levels) มาใช้ในการทำงานดังแสดงตามรูปที่ 6 ซึ่งจะมองว่าการปิดบังหมายเลขไอพีมีหลากหลายระดับของการเข้ารหัสหมายเลขไอพีดั้งเดิมด้วยกุญแจที่แตกต่างกัน ซึ่งทำให้เกิดความปลอดภัยมากยิ่งขึ้นในการปิดบังหมายเลขไอพี 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: Anonymization of the first scheme Sa1*

*2: Anonymization of the second scheme Sa2*

*3: Recovering of the second scheme S2*

*4: Recovering of the first scheme S1*

*5: Key generation*

รูปที่ 6 หลักการแบ่งระดับการเข้าถึงหลายชั้น

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

งานวิจัยอื่น ๆ ที่ได้นำเสนอแนวคิด หลักการ และปัญหาที่เกี่ยวข้องกับการปิดบังหมายเลขไอพีที่น่าสนใจนอกเหนือจากที่ได้กล่าวมาข้างต้นประกอบไปด้วย งานวิจัยของเคาคิส (D. Koukis) และคณะ [3] ซึ่งได้นำเสนอถึงความเสี่ยงของการแสดงข้อมูลหมายเลขไอพีที่ถูกปิดบังแล้ว ซึ่งเคาคิสให้แนวคิดว่าข้อมูลที่ทำการปิดบังหมายเลขไอพีด้วยอัลกอริทึมแบบต่าง ๆ ไปแล้ว ยังสามารถถูกโจมตีและถูกแกะรอยเพื่อล้วงความลับออกมาได้เช่นเดิม เช่นการนำเอาผลลัพธ์จากการทำงานที่ใช้หมายเลขพีดั้งเดิมในการประมวลผล มาทำการเปรียบเทียบกับผลลัพธ์การทำงานที่ใช้หมายเลขไอพีนิรนามประมวลผลพบว่า ถ้าผลลัพธ์จากการทำงานที่ใช้หมายเลขไอพีนิรนามประมวลผลมีค่าที่เหมือนหรือสอดคล้องกับผลลัพธ์ที่ใช้หมายเลขไอพีดั้งเดิมประมวลผล ก็ย่อมคาดเดาได้ว่าหมายเลขไอพีนิรนามหมายเลขนั้นอาจเป็นหมายเลขเดียวกับหมายเลขไอพีดั้งเดิมที่ตรวจพบ ดังนั้นจึงควรเปลี่ยนรูปแบบการระบุค่าหมายเลขไอพีดั้งเดิมมาเป็นการระบุค่าหมายเลขไอพีทางอ้อม (Passive IP Address) ก่อนจะทำการปิดบังหมายเลขไอพีอย่างแท้จริง โดยนำหมายเลขไอพีดั้งเดิมมาผ่านฟังก์ชันอย่างง่าย เช่น เอชแมค (HMAC) เป็นต้น

งานวิจัยของเคาคิสมีผลสอดคล้องกับงานวิจัยของโตนเนส เบรคเน (Tonnes Brekne) และคณะ [10] ที่ได้นำเสนอถึงวิธีการโจมตีและแสดงจุดอ่อนของหลักการปิดบังหมายเลขไอพีของทีซีพีดีไพรว์และคริปโตแพน ซึ่งสามารถถูกโจมตีได้ในหลายแนวทาง เช่น การโจมตีโดยอัดฉีดแพ็คเก็ตจำนวนมากแล้วทำการเปรียบเทียบค่า (Packet Injection Attack) หรือการวิเคราะห์ความถี่ของข้อมูลเพื่อทราบรูปแบบของข้อมูล (Frequency Analysis) เป็นต้น

จากงานวิจัยทั้งหมดที่ได้กล่าวมานั้นก่อให้เกิดแนวทางให้กับงานวิจัยเรื่องนี้ในการคิดแบบแผนการปิดบังหมายเลขไอพีขึ้นมาใหม่ โดยการสร้างและกำหนดระดับความเป็นส่วนตัวให้กับหมายเลขไอพี เพื่อทำการจัดกลุ่มและเลือกอัลกอริทึมของการปิดบังหมายเลขไอพีที่เหมาะสมกับระดับความเป็นส่วนตัวในการวิเคราะห์และจัดการเครือข่ายต่อไป

## 4. วัตถุประสงค์ของการวิจัย

4.1 เพื่อกำหนดระดับความเป็นส่วนตัว (Privacy Levels) ให้กับหมายเลขไอพี

4.2 เพื่อสร้างแบบแผน (Scheme) ที่ระบุถึงระดับความเป็นส่วนตัวในการปิดบังหมายเลขไอพี

4.3 เพื่อจัดกลุ่มประเภทของการวิเคราะห์และจัดการเครือข่ายที่เหมาะสมกับระดับความเป็นส่วนตัว

4.4 เพื่อเลือกอัลกอริทึมและวิธีการปิดบังหมายเลขไอพีที่เหมาะสมกับระดับความเป็นส่วนตัว และเหมาะสมกับประเภทของการวิเคราะห์และจัดการเครือข่าย

## 5. แนวคิดและวิธีการวิจัย

จากทฤษฎีและงานวิจัยที่เกี่ยวข้องจะเห็นได้ว่า หลักการทั้งหมดยังขาดปัจจัยและคุณสมบัติของความเป็นส่วนตัวที่แท้จริงแต่ไปมุ่งเน้นในเรื่องของความปลอดภัย (Security) มากกว่า โดยให้ความสำคัญและสนใจในเรื่องของความเป็นส่วนตัวไม่เพียงพอ เมื่อคำนึงถึงสถานการณ์จริงและการทำงานในสภาพความเป็นจริงแล้วจะ

พบว่า การวิเคราะห์และจัดการเครือข่ายหนึ่ง ๆ ประกอบไปด้วยวิธีการทำงานและประเภทของการทำงานหลากหลายรูปแบบและหลายคุณลักษณะ ซึ่งมีความต้องการและความจำเป็นในการปิดบังหมายเลขไอพีที่แตกต่างกันเช่น ในการวิเคราะห์สถิติการใช้งานระบบเครือข่ายในภาพรวมหรือข้อมูลอย่างสรุปนั้น ไม่มีความจำเป็นมากในการปิดบังหมายเลขไอพี เพราะในการทำงานไม่ได้มีการเจาะจงหรือแสดงถึงรายละเอียดของข้อมูลของหมายเลขไอพีแม้แต่อย่างใด แต่ถ้าเป็นการทำงานที่เป็นการตรวจสอบระบบเครือข่ายเช่น การค้นหาผู้บุกรุกในเครือข่าย ซึ่งต้องเจาะรายละเอียดเข้าไปในแต่ละหมายเลขไอพีของสมาชิกในเครือข่าย การทำงานแบบนี้จำเป็นอย่างยิ่งในการปิดบังหมายเลขไอพีก่อนนำไปใช้งาน นอกจากนั้นลักษณะบางประเภทของการวิเคราะห์และจัดการเครือข่ายอาจมีความจำเป็นในการปิดบังหมายเลขไอพีเพียงแค่บางส่วนเท่านั้นเช่น การปิดบังเพียงแค่ส่วนของบิตทางซ้ายหรือบิตทางขวาของหมายเลขไอพีเป็นต้น ซึ่งขึ้นอยู่กับว่าประเภทของการวิเคราะห์และจัดการเครือข่ายประเภทใดจะเหมาะสมและสมควรปิดบังมากน้อยเพียงใด

ดังนั้นหลักการทำงานโดยทั่วไปจึงต้องมีการพิจารณาถึงระดับความเป็นส่วนตัวของการทำงานในแต่ละกรณีว่าอยู่ในระดับใดและมีความต้องการและความจำเป็นมากน้อยเพียงใดในการปิดบังหมายเลขไอพี ทั้งนี้เพื่อทำให้การวิเคราะห์และจัดการเครือข่ายสามารถประมวลผลได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

แนวคิดและวิธีการวิจัยของการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัวนั้น สามารถแจกแจงออกได้เป็น 5 ประเด็นหลักดังจะได้กล่าวในรายละเอียดตามลำดับดังนี้

### 5.1 คุณสมบัติพื้นฐานในการปิดบังหมายเลขไอพี

ในกระบวนการปิดบังหมายเลขไอพีจะต้องมีคุณสมบัติเบื้องต้นของหมายเลขไอพีและการปิดบังหมายเลขไอพีดังต่อไปนี้

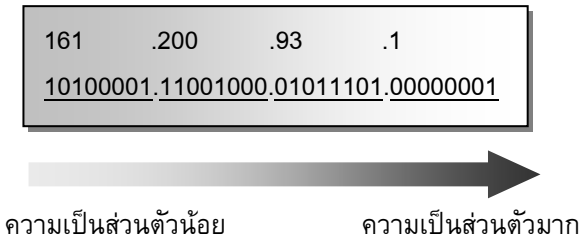
1. หมายเลขไอพีที่เกิดจากการปิดบังต้องถูกเปลี่ยนรูปแบบจากหมายเลขไอพีจริงหรือหมายเลขไอพีดั้งเดิมให้เป็นหมายเลขไอพีปลอมหรือหมายเลขไอพีนิรนามด้วยอัลกอริทึมและวิธีการปิดบังแบบต่าง ๆ เพื่อปิดบังลักษณะที่เป็นส่วนตัวเอาไว้
2. หมายเลขไอพีนิรนามต้องมีคุณสมบัติเช่นเดียวกับหมายเลขไอพีดั้งเดิมทุกประการ โดยสามารถระบุถึงกลุ่มของเครือข่ายและสามารถแยกแยะกลุ่มของเครือข่ายได้เช่นเดิม นั่นคือสามารถคงไว้ซึ่งข้อมูลในส่วนของบิตที่ระบุถึงความแตกต่างของกลุ่มเครือข่ายเอาไว้ได้
3. หมายเลขไอพีนิรนามต้องไม่มีการชนกันและไม่เกิดความซ้ำซ้อนในการทำงาน
4. หมายเลขไอพีนิรนามต้องสามารถแปลงกลับคืน (Recovery) ให้อยู่ในรูปของหมายเลขไอพีดั้งเดิมได้เช่นเดิมถ้ามีความจำเป็นที่จะต้องทราบหมายเลขไอพีดั้งเดิม
5. หมายเลขไอพีนิรนามสามารถใช้งานในกระบวนการวิเคราะห์และจัดการเครือข่ายได้เท่านั้น ไม่สามารถนำไปใช้งานในกระบวนการสื่อสาร รับส่งข้อมูล และเชื่อมต่อระหว่างอุปกรณ์ต่าง ๆ ในเครือข่ายได้

ทั้งนี้กระบวนการปิดบังหมายเลขไอพีทั้งหมดที่กล่าวมา ต้องคำนึงถึงความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นสำคัญ

### 5.2 ระดับความเป็นส่วนตัว

ระดับความเป็นส่วนตัว (Privacy Levels) คือ ระดับของการปิดบังหมายเลขไอพีโดยการพิจารณาคุณสมบัติของความเป็นส่วนตัว ซึ่งมีแนวคิดว่าหมายเลขไอพีประกอบด้วยกลุ่มเครือข่ายหรือกลุ่มบิตทางซ้ายที่แสดงถึงกลุ่มขององค์กรหรือหน่วยงานในเครือข่าย และกลุ่มเจ้าบ้านหรือกลุ่มบิตทางขวาที่ระบุถึงจำนวนของเครื่องหรืออุปกรณ์ปลายทางในเครือข่ายทั้งนี้กลุ่มของบิตทั้งสองส่วนจะมีขนาดเท่าไรก็ขึ้นอยู่กับการออกแบบลักษณะของเครือข่ายเหล่านั้นว่าต้องการให้มีรูปแบบเป็นอย่างไร โดยใช้หมายเลขสับเน็ตมาสเป็นตัวกำหนด

พบว่าค่าระดับความเป็นส่วนตัวหรือระดับความสามารถในการแยกแยะเครื่องหรืออุปกรณ์มีค่าระดับที่แตกต่างกัน โดยหมายเลขไอพีในกลุ่มของบิตทางซ้ายจะมีค่าความเป็นส่วนตัวน้อยกว่ากลุ่มของบิตทางขวา และจะมีค่าความเป็นส่วนตัวเพิ่มมากยิ่งขึ้นไปตามกลุ่มของบิตทางขวา ดังแสดงในทิศทางระดับความเป็นส่วนตัวของหมายเลขไอพีตามรูปที่ 7




รูปที่ 7 ทิศทางระดับความเป็นส่วนตัวของหมายเลขไอพี

จากรูปที่ 7 จะทำการยกตัวอย่างหมายเลขไอพีหมายเลข 161.200.93.1 เพื่อใช้อธิบายถึงระดับความเป็นส่วนตัว โดยหมายเลขไอพีดังกล่าวมีความหมายของส่วนต่าง ๆ ดังต่อไปนี้

161 แสดงถึงข้อมูลประเทศไทย
200 แสดงถึงข้อมูลของจุฬาลงกรณ์มหาวิทยาลัย
93 แสดงถึงหน่วยงานย่อยภายในมหาวิทยาลัยเช่น คณะ ภาควิชา เป็นต้น
1 แสดงถึงชื่อเครื่องหรือหมายเลขของอุปกรณ์ที่กำลังใช้งาน

กำหนดให้
161 และ 200 เป็นกลุ่มบิตทางซ้าย
93 และ 1 เป็นกลุ่มบิตทางขวา

ถ้าทำการปิดบังหมายเลขไอพีเพียงแค่ส่วนของบิตทางซ้ายเพียงอย่างเดียวก็จะสามารถปิดบังความเป็นส่วนตัวได้เพียงเล็กน้อยหรือมีความสามารถในการแยกแยะเครื่องได้มาก กล่าวคือ ส่วนของประเทศไทยและส่วนของจุฬาลงกรณ์มหาวิทยาลัยจะถูกปิดบังเอาไว้ แต่ในขณะเดียวกันก็ยังทราบถึงรายละเอียดที่เป็นข้อมูลส่วนตัวที่สำคัญคือ หน่วยงาน คณะ หรือภาควิชาและหมายเลขของอุปกรณ์ได้เช่นเดิมเพราะยังไม่ถูกปิดบัง

ถ้าทำการปิดบังในส่วนของบิตทางขวาเพียงอย่างเดียวก็จะทำให้สามารถปิดบังในส่วนของหน่วยงานและหมายเลขของอุปกรณ์เอาไว้ได้ซึ่งมีความเป็นส่วนตัวเพิ่มมากยิ่งขึ้น หรือสามารถแยกแยะเครื่องได้น้อยลงถึงแม้ว่าในส่วนของประเทศไทยและส่วนของจุฬาลงกรณ์มหาวิทยาลัยยังไม่ได้ถูกปิดบังก็ตาม

ถ้ามีการปิดบังทั้งหมด ทั้งในส่วนของบิตทางซ้ายและบิตทางขวาก็จะทำให้สามารถปิดบังความเป็นส่วนตัวได้สูงสุดหรือไม่สามารถแยกแยะเครื่องได้จากรูปแบบของหมายเลขไอพีแบบเดิม กล่าวคือ ไม่สามารถทราบและก้าวก่ายความเป็นส่วนตัวของหมายเลขไอพีได้อีกต่อไป

จากการวิเคราะห์ทิศทางระดับความเป็นส่วนตัวของหมายเลขไอพีพบว่า สามารถแบ่งระดับความเป็นส่วนตัวออกเป็น 5 ระดับตามตารางที่ 1 โดยพิจารณาลักษณะความต้องการและความจำเป็นในการปิดบังหมายเลขไอพีสำหรับการวิเคราะห์และจัดการเครือข่ายเพื่อใช้กำหนดค่าระดับความเป็นส่วนตัว และพิจารณาจากจำนวนบิตของหมายเลขไอพีตั้งแต่บิตตำแหน่งที่ 1 จนถึงบิตตำแหน่งที่ 32 ซึ่งมีค่าความเป็นส่วนตัวแตกต่างกัน โดยในแต่ละระดับความเป็นส่วนตัวจะทำการการเลือกอัลกอริทึมและวิธีการปิดบังหมายเลขไอพีที่เหมาะสม

ตารางที่ 1 ระดับความเป็นส่วนตัวของหมายเลขไอพี

| ค่าระดับ | ระดับ | รายละเอียด |
|---|---|---|
| 1 | ไม่มีความเป็นส่วนตัว | เป็นระดับที่ไม่ต้องการความเป็นส่วนตัวและไม่มีความจำเป็นใด ๆ ในการปิดบังหมายเลขไอพี |
| 2 | ความเป็นส่วนตัวน้อย | เป็นระดับที่ต้องการความเป็นส่วนตัวในระดับต่ำ กล่าวคือจะทำการปิดบังหมายเลขไอพีในส่วนของกลุ่มเครือข่ายหรือกลุ่มบิตทางซ้ายที่แสดงถึงกลุ่มขององค์กรหรือหน่วยงานในเครือข่าย |
| 3 | ความเป็นส่วนตัวปานกลาง | เป็นระดับที่ต้องการความเป็นส่วนตัวในระดับปานกลาง กล่าวคือจะทำการปิดบังหมายเลขไอพีในส่วนของกลุ่มเจ้าบ้านหรือกลุ่มบิตทางขวาที่แสดงถึงหมายเลขตำแหน่งหรือจำนวนของเครื่องหรือจำนวนอุปกรณ์ปลายทางในเครือข่าย |
| 4 | ความเป็นส่วนตัวมาก | เป็นระดับที่ต้องการความเป็นส่วนตัวในระดับสูง กล่าวคือจะทำการปิดบังหมายเลขไอพีทั้งในส่วนของกลุ่มเครือข่าย และกลุ่มเจ้าบ้าน ซึ่งการปิดบังจะเกี่ยวเนื่องกันทั้งสองส่วน |
| 5 | ความเป็นส่วนตัวมากที่สุด | เป็นระดับที่ต้องการความเป็นส่วนตัวในระดับสูงสุด กล่าวคือจะทำการปิดบังหมายเลขไอพีทั้งในส่วนของกลุ่มเครือข่าย และกลุ่มเจ้าบ้านโดยใช้หลักการสุ่มค่า (Random) หรือไม่คงไว้ซึ่งค่าของกลุ่มเครือข่าย |

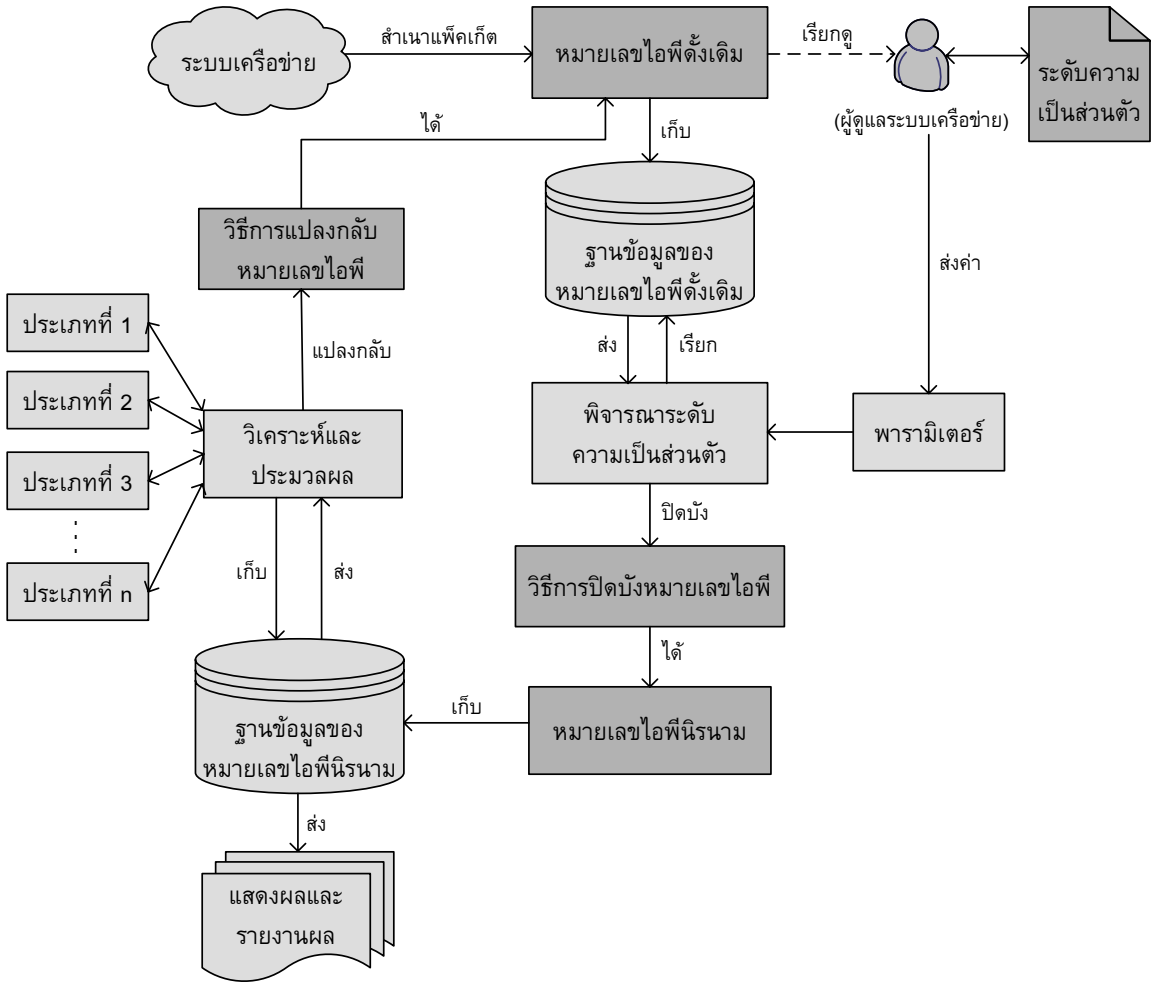
ระดับความเป็นส่วนตัวทั้ง 5 ระดับ มีการพิจารณาถึงองค์ประกอบดังต่อไปนี้

1. ค่าระดับความเป็นส่วนตัวและคุณสมบัติของความเป็นส่วนตัวในการปิดบังหมายเลขไอพีตั้งแต่ระดับที่ 1 ถึงระดับที่ 5
2. อัลกอริทึมและวิธีการปิดบังที่เหมาะสมกับค่าระดับความเป็นส่วนตัวทั้ง 5 ระดับ โดยจะพิจารณาอัลกอริทึมที่ได้นำเสนอตามหัวข้อที่ 5.4
3. ประเภทและลักษณะการทำงานของการวิเคราะห์และจัดการเครือข่ายที่เหมาะสมกับค่าระดับความเป็นส่วนตัวทั้ง 5 ระดับ

องค์ประกอบในข้อที่ 2 และ 3 ยังอยู่ในช่วงของการศึกษาวิจัยและทำการทดลองซึ่งจะได้นำเสนอรายละเอียดเพิ่มเติมต่อไปในอนาคต

### 5.3 แบบแผนการปิดบังหมายเลขไอพี

จากหลักการของระดับความเป็นส่วนตัวสามารถนำมาสร้างเป็นแบบแผนการปิดบังหมายเลขไอพีที่มีกระบวนการทำงานอยู่บนพื้นฐานของระดับความเป็นส่วนตัว ซึ่งพัฒนาจากรูปแบบขั้นตอนทั่วไปของการปิดบังหมายเลขไอพีเดิม โดยมีโครงสร้างการทำงานโดยรวมดังแสดงไว้ในรูปที่ 8 ซึ่งขั้นตอนต่าง ๆ นั้นจะมีเพียงผู้ดูแลระบบเครือข่ายหรือกลุ่มของผู้ดูแลระบบเครือข่ายเท่านั้นที่อยู่ในขอบเขตการทำงานดังกล่าว




รูปที่ 8 โครงสร้างขั้นตอนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว

จากโครงสร้างขั้นตอนการปิดบังหมายเลขไอพีตามรูปที่ 8 พบว่า ข้อมูลหมายเลขไอพีมีโอกาสที่จะถูกเปิดเผยหรือละเมิดความเป็นส่วนตัวได้ใน 2 ขั้นตอน คือ ขั้นตอนการวิเคราะห์และประมวลผล และขั้นตอนการแสดงผลและรายงานผล ดังนั้นขั้นตอนทั้งสองต้องมีการปิดบังหมายเลขไอพีโดยการพิจารณาระดับความเป็นส่วนตัวในแต่ละระดับ ต่อไปนี้จะเป็นการแสดงรายละเอียดของแบบแผนการปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวทั้ง 5 ระดับดังนี้

**1. ระดับที่ 1 หรือ ระดับที่ไม่มีความเป็นส่วนตัว**

การปิดบังหมายเลขไอพีโดยการพิจารณาระดับความเป็นส่วนตัวระดับที่ 1 เป็นระดับที่ไม่ต้องการความเป็นส่วนตัวและไม่มีความจำเป็นใด ๆ ในการปิดบังหมายเลขไอพี ดังนั้นหมายเลขไอพีนิรนามจะมีรูปแบบที่เหมือนกับหมายเลขไอพีดั้งเดิมดังแสดงตามรูปที่ 9

| | |
|---|---|
| หมายเลขสับเน็ตมาส | 255 .255 .0 .0<br>11111111.11111111.00000000.00000000 |
| หมายเลขไอพีดั้งเดิม | 161 .200 .93 .1<br>10100001.11001000.01011101.00000001 |
| หมายเลขไอพีนิรนาม | 161 .200 .93 .1<br>10100001.11001000.01011101.00000001 |

รูปที่ 9 การปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวระดับที่ 1

ระดับความเป็นส่วนตัวระดับที่ 1 เหมาะกับประเภทของการวิเคราะห์และจัดการเครือข่ายในลักษณะที่ไม่สนใจหรือมองเห็นความเป็นส่วนตัวของหมายเลขไอพี เช่น การประมวลผลและสรุปผลค่าสถิติแบบเฉลี่ย หรือการสรุปผลลัพธ์แบบรายวัน รายเดือน และรายปี เป็นต้น ซึ่งจะได้นำเสนอรายละเอียดเพิ่มเติมต่อไปในอนาคต

**2. ระดับที่ 2 หรือ ระดับที่มีความเป็นส่วนตัวน้อย**

การปิดบังหมายเลขไอพีโดยการพิจารณาระดับความเป็นส่วนตัวระดับที่ 2 เป็นระดับที่ต้องการความเป็นส่วนตัวในระดับต่ำ โดยปิดบังหมายเลขไอพีในส่วนของกลุ่มเครือข่ายหรือกลุ่มบิตทางซ้ายที่แสดงถึงกลุ่มขององค์กรหรือหน่วยงานในเครือข่ายดังแสดงตามรูปที่ 10

| | |
|---|---|
| หมายเลขสับเน็ตมาส | 255 .255 .0 .0<br>11111111.11111111.00000000.00000000 |
| หมายเลขไอพีดั้งเดิม | 161 .200 .93 .1<br>10100001.11001000.01011101.00000001 |
| หมายเลขไอพีนิรนาม | xxx .xxx .93 .1<br>xxxxxxxx.xxxxxxxx.01011101.00000001 |

รูปที่ 10 การปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวระดับที่ 2

ระดับความเป็นส่วนตัวระดับที่ 2 เหมาะกับประเภทของการวิเคราะห์และจัดการเครือข่ายที่มีความสนใจหรือมองเห็นความเป็นส่วนตัวของหมายเลขไอพีในส่วนของกลุ่มเครือข่าย เช่น การเปรียบเทียบสถิติการเรียกใช้งานบริการต่าง ๆ ขององค์กรหรือหน่วยงานในเครือข่าย เป็นต้น ซึ่งประเภทของการวิเคราะห์และจัดการเครือข่ายประเภทอื่น ๆ จะได้นำเสนอรายละเอียดเพิ่มเติมต่อไปในอนาคต

**3. ระดับที่ 3 หรือ ระดับที่มีความเป็นส่วนตัวปานกลาง**

การปิดบังหมายเลขไอพีโดยการพิจารณาระดับความเป็นส่วนตัวระดับที่ 3 เป็นระดับที่ต้องการความเป็นส่วนตัวในระดับปานกลาง โดยปิดบังหมายเลขไอพีในส่วนของกลุ่มเจ้าบ้านหรือกลุ่มบิตทางขวาที่แสดงถึงหมายเลขตำแหน่งหรือจำนวนของเครื่องหรือจำนวนอุปกรณ์ปลายทางในเครือข่ายดังแสดงตามรูปที่ 11

| | |
|---|---|
| หมายเลขสับเน็ตมาส | 255 .255 .0 .0<br>11111111.11111111.00000000.00000000 |
| หมายเลขไอพีดั้งเดิม | 161 .200 .93 .1<br>10100001.11001000.01011101.00000001 |
| หมายเลขไอพีนิรนาม | 161 .200 .xxx .xxx<br>10100001.11001000.xxxxxxxx.xxxxxxxx |

รูปที่ 11 การปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวระดับที่ 3

ระดับความเป็นส่วนตัวระดับที่ 3 เหมาะกับประเภทของการวิเคราะห์และจัดการเครือข่ายที่มีความสนใจหรือมองเห็นความเป็นส่วนตัวของหมายเลขไอพีในส่วนของกลุ่มเจ้าบ้าน เช่น การนับจำนวนเครื่องและอุปกรณ์ที่เปิดใช้งานในเครือข่าย หรือการประมวลผลการทำงานของกลุ่มองค์กรหรือหน่วยงานย่อยใด ๆ ภายในเครือข่าย เป็นต้น ซึ่งประเภทของการวิเคราะห์และจัดการเครือข่ายประเภทอื่น ๆ จะได้นำเสนอรายละเอียดเพิ่มเติมต่อไปในอนาคต

**4. ระดับที่ 4 หรือ ระดับที่มีความเป็นส่วนตัวมาก**

การปิดบังหมายเลขไอพีโดยการพิจารณาระดับความเป็นส่วนตัวระดับที่ 4 เป็นระดับที่ต้องการความเป็นส่วนตัวในระดับสูง โดยปิดบังหมายเลขไอพีทั้งในส่วนของกลุ่มเครือข่ายและกลุ่มเจ้าบ้าน ซึ่งลักษณะการปิดบังจะเกี่ยวเนื่องกันทั้งสองส่วนโดยอาจจะปิดบังในทุกตำแหน่งบิตทั้ง 32 บิต หรืออาจปิดบังเพียงบางตำแหน่งบิตก็ได้ ดังแสดงตามรูปที่ 12

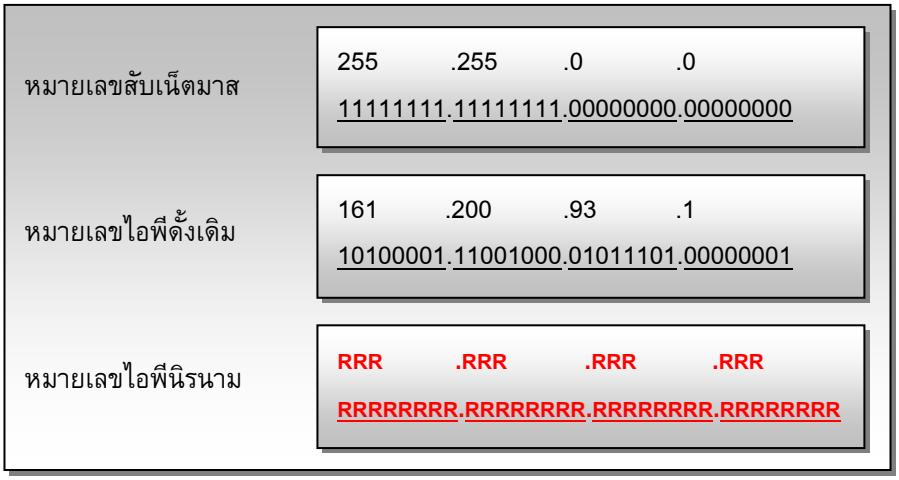
| | |
|---|---|
| หมายเลขสับเน็ตมาส | 255 .255 .0 .0<br>11111111.11111111.00000000.00000000 |
| หมายเลขไอพีดั้งเดิม | 161 .200 .93 .1<br>10100001.11001000.01011101.00000001 |
| หมายเลขไอพีนิรนาม | xxx .xxx .xxx .xxx<br>xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx |

รูปที่ 12 การปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวระดับที่ 4

ระดับความเป็นส่วนตัวระดับที่ 4 เหมาะกับประเภทของการวิเคราะห์และจัดการเครือข่ายที่มีความสนใจหรือมองเห็นความเป็นส่วนตัวของหมายเลขไอพีทั้งในส่วนของกลุ่มเครือข่ายและกลุ่มเจ้าบ้าน เช่น การตรวจหาและค้นหาผู้บุกรุกในเครือข่าย การตรวจตราและติดตามผู้ใช้ในเครือข่ายเพื่อวิเคราะห์พฤติกรรมบางอย่าง การค้นหาสิ่งแปลกปลอมเช่นไวรัสและหนอนอินเตอร์เน็ตที่เข้ามาในเครือข่าย เป็นต้น ซึ่งประเภทของการวิเคราะห์และจัดการเครือข่ายประเภทอื่น ๆ จะได้นำเสนอรายละเอียดเพิ่มเติมต่อไปในอนาคต

**5. ระดับที่ 5 หรือ ระดับที่มีความเป็นส่วนตัวมากที่สุด**

การปิดบังหมายเลขไอพีโดยการพิจารณาระดับความเป็นส่วนตัวระดับที่ 5 เป็นระดับที่ต้องการความเป็นส่วนตัวในระดับสูงสุด โดยปิดบังหมายเลขไอพีทั้งในส่วนของกลุ่มเครือข่ายและกลุ่มเจ้าบ้านแบบสุ่มค่า (Random) หรือไม่คงไว้ซึ่งค่าของกลุ่มเครือข่าย ดังนั้นหมายเลขไอพีนิรนามในระดับนี้จะไม่มีคุณสมบัติเหมือนกับหมายเลขไอพีดั้งเดิมและยากต่อการแปลงย้อนกลับมาเป็นหมายเลขไอพีดังเดิม ดังแสดงตามรูปที่ 13




รูปที่ 13 การปิดบังหมายเลขไอพีตามระดับความเป็นส่วนตัวระดับที่ 5

ระดับความเป็นส่วนตัวระดับที่ 5 เหมาะกับประเภทของการวิเคราะห์และจัดการเครือข่ายที่ต้องการความเป็นส่วนตัวอย่างยิ่ง เช่น การแสดงผลและรายงานผลออกสู่สาธารณะหรือ การส่งผลลัพธ์ที่ได้จากการประมวลผลไปยังบุคคลอื่นนอกเหนือจากกลุ่มของผู้ดูแลระบบเครือข่าย เป็นต้น ซึ่งรายละเอียดต่าง ๆ จะได้นำเสนอเพิ่มเติมต่อไปในอนาคต

**5.4 วิธีการปิดบังหมายเลขไอพีที่เหมาะสมกับระดับความเป็นส่วนตัว**

วิธีการปิดบังหมายเลขไอพีของระดับความเป็นส่วนตัวระดับต่าง ๆ จะพิจารณาและเลือกอัลกอริทึมที่เหมาะสม ซึ่งในระดับความเป็นส่วนตัวทั้ง 5 ระดับ สามารถมีอัลกอริทึมในการปิดบังหมายเลขไอพีได้มากกว่า 1 วิธีและในขณะเดียวกันอัลกอริทึมในการปิดบังวิธีหนึ่ง ๆ ก็สามารถใช้ได้กับระดับความเป็นส่วนตัวได้มากกว่า 1 ระดับเช่นกัน โดยได้เลือกและจำแนกอัลกอริทึมในการปิดบังหมายเลขไอพีซึ่งประกอบไปด้วยรูปแบบการปิดบังดังต่อไปนี้

**1. การปิดบังโดยการจับคู่แบบหนึ่งต่อหนึ่ง (One-to-One Mapping Anonymization)** ซึ่งประกอบไปด้วยอัลกอริทึมดังต่อไปนี้

**1.1 ฟังก์ชันทางเดียว (Trapdoor Function)** เป็นฟังก์ชันทางเดียวที่ยากในการแปลงย้อนกลับ เช่น อาร์เอสเอ (RSA) และเอ็มดี 5 เอ็กซ์ (MD5X) เป็นต้น

**1.2 ฟังก์ชันแฮช (Hash Function)** เช่น เอ็มดี 5 (MD5) และเอสเอชเอ-1 (SHA-1) เป็นต้น

**1.3 การเข้ารหัส (Encryption)** เช่น โบลว์ฟิช (Blowfish) และซีซ่า (Caesar) เป็นต้น

**2. การปิดบังโดยคงไว้ซึ่งความหมายของกลุ่มเครือข่าย (Prefix-Preserving Anonymization)** ประกอบไปด้วยอัลกอริทึมดังต่อไปนี้

**2.1 ทีซีพีดีไพรว์ (Tcpdpriv)** เป็นการปิดบังหมายเลขไอพีแบบหนึ่งต่อหนึ่งแต่ยังคงไว้ซึ่งความหมายของกลุ่มเครือข่าย

**2.2 คริปโตแพน (Crypto-PAn)** เป็นการปิดบังหมายเลขไอพีโดยใช้หลักการทางด้านวิทยาการเข้ารหัสลับ

**3. การปิดบังโดยพิจารณาระดับการเข้าถึงหลายชั้น (Multiple Access Levels Anonymization)** เป็นการปิดบังหมายเลขไอพีโดยใช้กุญแจในการเข้าถึงข้อมูลตามระดับที่แตกต่างกัน

จากวิธีการและอัลกอริทึมในการปิดบังหมายเลขไอพีทั้งหมดนี้ จะถูกนำมาพิจารณาเพื่อนำไปใช้ในการปิดบังหมายเลขไอพีในระดับความเป็นส่วนตัวระดับต่าง ๆ อย่างเหมาะสมต่อไปในอนาคต

### 5.5 การวัดและทดสอบประสิทธิภาพการทำงาน

ในการวัดและทดสอบประสิทธิภาพการทำงานของแบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัวมีประเด็นที่สนใจดังนี้

**1. ประสิทธิภาพของความถูกต้องในการประมวลผล** ซึ่งจะต้องสามารถทำงานได้ถูกต้องเหมือนกับแบบแผนการปิดบังหมายเลขไอพีแบบอื่น ๆ และให้ผลการทำงานที่ไม่ด้อยไปกว่าการทำงานแบบอื่น ๆ โดยจะทำการเลือกประเภทของการวิเคราะห์และจัดการเครือข่ายบางประเภทขึ้นมาทำการทดสอบและเปรียบเทียบ

**2. ประสิทธิภาพของเวลาการทำงาน** ทำการวัดค่าเวลาในการทำงานและเวลาการประมวลผลเปรียบเทียบกับวิธีการปิดบังวิธีอื่น ๆ ซึ่งจะต้องใช้เวลาน้อยหรือเท่ากับเวลาการทำงานของการปิดบังวิธีอื่น ๆ หรือไม่เช่นนั้น เวลาการทำงานที่ใช้ในการปิดบังหมายเลขไอพีวิธีนี้จะต้องอยู่ในขอบเขตที่ยอมรับได้

**3. ประสิทธิภาพของความเป็นส่วนตัว** ทำการเปรียบเทียบค่าหรือขอบเขตของความเป็นส่วนตัวที่ปรากฏในแบบแผนหรือวิธีการปิดบังหมายเลขไอพีแบบต่าง ๆ กับแบบแผนการปิดบังวิธีนี้

**4. ประสิทธิภาพการทำงานโดยรวม** ซึ่งจะวัดประสิทธิภาพการทำงานทั้งหมดโดยเปรียบเทียบลักษณะการปิดบังหมายเลขไอพีในแต่ละแบบกับการปิดบังหมายเลขไอพีวิธีนี้ เพื่อให้ได้ประสิทธิภาพการทำงานที่ดีและเหมาะกับสภาพความเป็นจริงของระบบเครือข่ายที่มีปริมาณข้อมูลมหาศาล

ทั้งนี้อาจจะมีการพิจารณาประเด็นอื่น ๆ เพิ่มเติมและอาจปรับเปลี่ยนปัจจัยต่าง ๆ ในการวัดและทดสอบประสิทธิภาพการทำงานต่อไปได้ในอนาคต

## 6. ขอบเขตการวิจัย

6.1 หมายเลขไอพีดั้งเดิมที่นำมาทำการปิดบังในงานวิจัยเรื่องนี้ใช้หมายเลขไอพีรุ่นที่ 4 ขนาด 32 บิต โดยกระบวนการทดลองและการทำงานต่าง ๆ ในการปิดบังหมายเลขไอพีจะอยู่บนระบบไอพีรุ่นที่ 4

6.2 งานวิจัยเรื่องนี้มีการศึกษาข้อมูลของรูปแบบและวิธีการปิดบังหมายเลขไอพีในซอฟต์แวร์สำเร็จรูปและเครื่องมือดูแลระบบเครือข่ายโดยจะพิจารณาเลือกซอฟต์แวร์ที่ได้รับความนิยมเช่น เอ็มอาร์ทีจี นาทิออส และออปเมเนเจอร์ เป็นต้น

6.3 แบบแผนการปิดบังหมายเลขไอพีครอบคลุมระดับความเป็นส่วนตัวดังต่อไปนี้

1. *ระดับความจำเป็นในความเป็นส่วนตัว (Privacy Need Levels)* ซึ่งพิจารณาในด้านของผู้ดูแลระบบเครือข่ายในการเลือกและจัดระดับความจำเป็นให้กับข้อมูลที่ประกอบไปด้วยหมายเลขไอพี โดยพิจารณาว่ามีความจำเป็นมากน้อยเพียงใดในการปิดบัง

2. *ระดับความต้องการในความเป็นส่วนตัว (Privacy Requirement Levels)* ซึ่งพิจารณาในด้านการใช้งานของผู้ใช้ในระบบเครือข่าย โดยแบ่งหน้าที่และประเภทของการวิเคราะห์และจัดการเครือข่ายเพื่อพิจารณาว่าการทำงานแต่ละประเภทมีความต้องการที่จะปิดบังหมายเลขไอพีมากน้อยเพียงใดเพื่อไม่ให้เป็นการละเมิดความเป็นส่วนตัวของผู้ใช้งานระบบเครือข่าย

6.4 แบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัวเป็นแนวทางและหลักการให้กับขอบเขตการทำงานดังต่อไปนี้

1. *การวิเคราะห์เครือข่าย (Network Analysis)* เช่น การวิเคราะห์การจราจร การตรวจตราการจราจร การตรวจจับผู้บุกรุก เป็นต้น โดยเป็นการสำเนาข้อมูลจากเครือข่ายขึ้นมาวิเคราะห์และเก็บไว้ในฐานข้อมูลซึ่งไม่ใช่การกระทำแบบทันกาล (Real Time)

2. *การจัดการเครือข่าย (Network Management)* เช่น การใช้งานและการให้บริการในเครือข่าย การแสดงข้อมูลสรุปของเครือข่ายในรูปแบบของข้อความ กราฟ ตาราง และแผนที่เครือข่าย เป็นต้น

6.5 หมายเลขไอพีนิรนามที่ได้จากขั้นตอนของการปิดบังหมายเลขไอพี ไม่สามารถนำเอาไปใช้งานได้จริงในการสื่อสารและรับส่งข้อมูลในระแบบเครือข่าย แต่จะเป็นประโยชน์แก่นักวิจัยและนักวิเคราะห์ระบบเครือข่ายได้เท่านั้น

6.6 อัลกอริทึมที่เลือกมาใช้ในการปิดบังหมายเลขไอพี อาจได้มาจากอัลกอริทึมที่มีการนำเสนอในงานวิจัยต่าง ๆ หรืออาจมาจากการคิดและพิจารณาเลือกอัลกอริทึมอื่น ๆ ที่เหมาะสม

6.7 การวัดและทดสอบประสิทธิภาพการทำงานของแบบแผนการปิดบังหมายเลขไอพีจะกระทำกับระบบเครือข่ายจริง โดยอาจเลือกระบบหรือรูปแบบของข้อมูลที่เหมาะสมในการทดสอบต่อไป เช่น การทดสอบกับระบบพร๊อกซี (Proxy) เป็นต้น และการทดสอบทั้งหมดจะรวมไปถึงการทดสอบของกรณีการแปลงย้อนกลับของหมายเลขไอพีด้วย

6.8 การพัฒนาระบบการทำงานทั้งหมดจะกระทำภายใต้ระบบปฏิบัติการยูนิกส์ (UNIX) และใช้ภาษาซีในกระบวนการพัฒนา

## 7. ขั้นตอนการวิจัย

7.1 ศึกษาข้อมูลเอกสารและงานวิจัยที่เกี่ยวข้องกับหัวข้อของการปิดบังหมายเลขไอพี และศึกษาประเด็นของความเป็นส่วนตัว

7.2 ศึกษาลักษณะการทำงานของซอฟต์แวร์สำเร็จรูปต่าง ๆ ที่นิยมใช้ในการวิเคราะห์และจัดการเครือข่ายในปัจจุบัน และศึกษาการประยุกต์ใช้งานของการปิดบังหมายเลขไอพีในเครือข่ายตัวอย่าง

7.3 วิเคราะห์หลักการของการปิดบังหมายเลขไอพี และวิเคราะห์ถึงระดับความเป็นส่วนตัวในประเภทและลักษณะต่าง ๆ ของการวิเคราะห์และจัดการเครือข่าย

7.4 ออกแบบโครงสร้างแบบแผนการปิดบังหมายเลขไอพีโดยใช้ระดับความเป็นส่วนตัวในการจัดกลุ่มและจัดระดับของการปิดบัง

7.5 สร้างและบูรณาการแบบแผนการปิดบังหมายเลขไอพีด้วยระดับความเป็นส่วนตัว เพื่อให้เหมาะสมกับการวิเคราะห์และจัดการเครือข่าย

7.6 ทดสอบและตรวจสอบการทำงานและประสิทธิภาพของแบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว

7.7 ปรับปรุงแบบแผนการปิดบังหมายเลขไอพีบนพื้นฐานของระดับความเป็นส่วนตัว

7.8 สรุปผลการวิจัยและตีพิมพ์ผลการวิจัย

7.9 เรียบเรียงและจัดทำวิทยานิพนธ์

ตารางที่ 2 ลำดับขั้นตอนการวิจัยและการดำเนินการของวิทยานิพนธ์ส่วนที่ 1

| เดือน / ปี<br>สัปดาห์<br>ขั้นตอนการพัฒนา | มีนาคม 2550 | | | | เมษายน 2550 | | | | พฤษภาคม 2550 | | | | มิถุนายน 2550 | | | | กรกฎาคม 2550 | | | | สิงหาคม 2550 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 7.1 | ■ | ■ | ■ | ■ | | | | | | | | | | | | | | | | | | | | |
| 7.2 | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | | | | | | | | | | | | | |
| 7.3 | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | | | | | | | | | | | |
| 7.4 | | | | | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | | | |
| 7.5 | | | | | | | | | | | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ |

ตารางที่ 3 ลำดับขั้นตอนการวิจัยและการดำเนินการของวิทยานิพนธ์ส่วนที่ 2

| เดือน / ปี<br>สัปดาห์<br>ขั้นตอนการพัฒนา | กันยายน 2550 | | | | ตุลาคม 2550 | | | | พฤศจิกายน 2550 | | | | ธันวาคม 2550 | | | | มกราคม 2551 | | | | กุมภาพันธ์ 2551 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 7.5 | ■ | ■ | ■ | ■ | | | | | | | | | | | | | | | | | | | | |
| 7.6 | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | | | | | | | | | | | | | | | |
| 7.7 | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | | | | | | | | | | | |
| 7.8 | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | | | |
| 7.9 | | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |

## 8. ประโยชน์ที่จะได้รับ

8.1 ได้แบบแผนการปิดบังหมายเลขไอพีในการระบุถึงระดับความเป็นส่วนตัวเพื่อใช้วิเคราะห์และจัดการเครือข่ายได้

8.2 สามารถจัดกลุ่มประเภทของการวิเคราะห์และจัดการเครือข่ายที่เหมาะสมกับระดับความเป็นส่วนตัว โดยเลือกอัลกอริทึมในการปิดบังหมายเลขไอพีที่เหมาะสมต่อการวิเคราะห์และจัดการเครือข่ายในประเภทต่าง ๆ ได้

8.3 สามารถรักษาความเป็นส่วนตัวของข้อมูลส่วนบุคคลต่อการนำไปวิเคราะห์และจัดการเครือข่ายได้

8.4 ทำให้ระบบการทำงานในการวิเคราะห์และจัดการเครือข่ายสามารถทำงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

8.5 เป็นแนวทางให้กับผู้ดูแลระบบเครือข่ายที่จะทำการวิเคราะห์และจัดการเครือข่ายในหน่วยงานหรือองค์กรต่าง ๆ ได้สนใจและคำนึงถึงความเป็นส่วนตัวของข้อมูลส่วนบุคคลมากยิ่งขึ้น

8.6 สามารถนำหลักการของแบบแผนการปิดบังหมายเลขไอพีไปประยุกต์ใช้ในงานด้านอื่น ๆ ได้อย่างเหมาะสม

8.7 สามารถสร้างความน่าเชื่อถือและความมั่นใจให้กับทุกฝ่ายในองค์กรหนึ่ง ๆ ว่าจะไม่ละเมิดหรือก้าวก่ายข้อมูลส่วนบุคคลเหล่านี้ในกระบวนการวิเคราะห์และประมวลผล

## 9. รายการอ้างอิง


[1] ภาณุพันธ์ สุวรรณมาตร์, การวิเคราะห์สถิติการใช้งานอินเตอร์เน็ตในระบบเครือข่ายระดับสถาบันอุดมศึกษา, วิทยานิพนธ์ระดับมหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย, 2541.

[2] วงศ์ยศ เกิดศรี, ระบบบริหารจัดการเครือข่ายส่วนการดูแลเครือข่าย, โครงงานวิจัยระดับปริญญาตรี, มหาวิทยาลัยสงขลานครินทร์, 2548.

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

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

[5] F. Potorti, Tcpdpriv, Available: http://fly.isti.cnr.it/software/tcpdpriv/, February 2004.

[6] G. Minshall, Tcpdpriv Command Manual, July 1996.

[7] 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.

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

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

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

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

[12] OpManager, Available: http://manageengine.adventnet.com/products/opmanager/, Access date: March 21, 2007.

[13] Q. Zhang and X. Li, An IP Address Anonymization Scheme with Multiple Access Levels, Springer-Verlag Berlin Heidelberg, International Conference on Information Networking (ICOIN), 2006.

[14] R. Smith, IP Address: Your Internet Identity, Available: http://www.ntia.doc.gov/ntiahome/privacy /files/smith.htm, 1997.

[15] Wikipedia, Multi Router Traffic Grapher, Available: http://en.wikipedia.org/wiki/MRTG, Access date: March 21, 2007.

[16] Wikipedia, Paessler Router Traffic Grapher, Available: http://en.wikipedia.org/wiki/PRTG, Access date: March 21, 2007.

[17] Wikipedia, Nagios, Available: http://en.wikipedia.org/wiki/Nagios, Access date: March 21, 2007.

[18] Wikipedia, IP Address, Available: http://en.wikipedia.org/wiki/IP_Address, Access date: March 21, 2007.