Department of Computer Science; Faculty of Science,

Khon Kaen University

Course No: 322749

Course Name: Mobile and Wireless Networking Technology

Student Name/Last Name: นายมารุด คำภักดี

Student ID: 545020185-4

Submission Date: 02/26/2012

การสำรวจระบบตรวจจับการบุกรุกที่อยู่บนพื้นฐานของ Snort
Intrusion Detection System Base on Snort – A Survey

M. Khumphakdee
Department Of Computer Science,
Faculty of Science, Khon Kaen University
Khon Kaen, Thailand,
Marud-2011@live.kku.ac.th

C. So-In
Department Of Computer Science,
Faculty of Science, Khon Kaen University
Khon Kaen, Thailand,
chakso@kku.ac.th

บทคัดย่อ

การรักษาความปลอดภัยในเครือข่ายต้องเผชิญหน้ากับภัยคุกคามเป็นจำนวนมาก เช่น ไวรัส โทรจัน เวิร์ม การโจมตี การใช้ไฟวอล์ในเครือข่ายสามารถที่จะป้องกันภัยคุกคุกจากภายนอกได้เท่านั้น แต่ไม่สามารถที่จะป้องกันการโจมตีจากภายในเครือข่ายของตัวเองได้ ระบบตรวจจับการบุกรุก (Intrusion Detection System, IDS) เป็นระบบที่มีส่วนสำคัญในการรักษาความปลอดภัยในเครือข่ายและเป็นเครื่องมือที่ใช้คอยตรวจสอบกิจกรรมที่เกิดขึ้นในเครือข่าย ในปัจจุบันระบบตรวจจับการบุกรุกที่นิยมและได้รับความสนใจในการวิจัยคือ snort ซึ่งเป็นระบบตรวจจับการบุกรุกที่สามารถนำมาใช้งานได้ฟรี ไม่มีค่าใช้จ่าย นอกจากนั้นยังสามารถที่จะติดตั้งได้ทั้งบนระบบปฏิบัติการ windows และ Linux ลักษณะการทำงานของ snort จะทำงานในรูปแบบ real time ซึ่งจะทำหน้าที่คอยแจ้งเตือนให้ผู้ดูแลระบบทราบหากมีการบุกรุก โดยสามารถที่จะตรวจจับการบุกรุกจากภายนอกและภายในได้ ในงานวิจัยนี้จะเป็นการสำรวจเทคนิคต่างๆ ที่ได้นำมาใช้ในการวิจัยกับ snort ทั้งในส่วนของซอฟต์แวร์และฮาร์แวร์ และได้มีการเปรียบเทียบข้อแตกต่างของแต่ละเทคนิคที่นำมาใช้ รวมถึงข้อดีข้อเสียของแต่ละเทคนิค

Keywords: ระบบตรวจจับการบุกรุก, snort, ซอฟต์แวร์, ฮาร์ดแวร์

I. Introduction

เทคโนโลยีเครือข่ายการสื่อสารในปัจจุบันได้พัฒนาไปอย่างรวดเร็ว องค์กรหน่วยงานต่างๆ จำเป็นต้องมีเทคโนโลยีการรักษาความปลอดภัยสำหรับป้องกันภัยคุกคามที่จะเกิดขึ้นในองค์กร และในขณะที่อินเตอร์เน็ตก็มีการพัฒนาไปอย่างรวดเร็วพร้อมทั้งมีการใช้งานกันอย่างแพร่หลาย เนื่องจากทำให้มีความสะดวกในการสื่อสารและสามารถที่จะแลกเปลี่ยนข้อมูลกันได้อย่างรวดเร็ว สิ่งที่ต้องคำนึงถึงเป็นอย่างมากนั้นคือ ความปลอดภัย การพัฒนารูปแบบการโจมตี (Attack) ได้เกิดขึ้นทุกวัน โดยที่ผู้โจมตี (Hacker) นั้นสามารถที่จะโจมตีจากภายนอกหรือจะโจมตีจากภายในเครือข่ายได้ เป้าหมายที่ได้รับความเดือนร้อน เช่น ธนาคาร องค์กรหรือบริษัท แต่ในทุกวันนี้ภัยคุกคามไม่ได้มาจากอินเตอร์เน็ตเท่านั้น ระบบปฏิบัติการหรือซอฟต์แวร์ประยุกต์ก็เป็นอีกช่องทางที่ทำเกิดความไม่ปลอดภัย หรือแม้แต่โปรโตคอลที่ใช้ในการสื่อสารบนเครือข่ายอินเตอร์เน็ตก็มีส่วนทำให้ผู้โจมตี สามารถที่จะบุกรุกเข้ามาในเครือข่ายโดยไม่ได้รับอนุญาต การใช้ไฟวอล์ในองค์กรเพียงอย่างเดียวไม่สามารถที่จะป้องกันจากการโจมตีที่มีความหลากหลายประเภทได้

โดยในขณะนี้องค์กรต่างๆ ในทั่วทุกมุมโลกต่างมีความต้องการสำหรับการรักษาความปลอดภัยและหาความเหมาะสมของระบบการควบคุม เพื่อการตรวจสอบของพื้นที่และตรวจสอบการบุกรุกเป็นส่วนสำคัญของการรักษาความปลอดภัยคอมพิวเตอร์และในเครือข่าย เพื่อทำหน้าที่อย่างเหมาะสมต่อการป้องกันการโจมตี ขณะนี้รูปแบบการรักษาความปลอดภัยอาศัยอยู่ในระบบตรวจจับการบุกรุก เพื่อที่จะตรวจจับการบุกรุกที่เป็นกระบวนการของการระบุและการใช้งานที่ไม่ได้รับอนุญาต การใช้งานในทางที่ผิด และการละเมิดของระบบคอมพิวเตอร์ การกระทำที่ไม่ถูกต้องหรือเหมาะสม การตรวจจับการบุกรุกเป็นส่วนหนึ่งของมาตรการรักษาความปลอดภัยที่สอดคล้องกับเหตุการณ์ที่เกิดขึ้น รวมถึงภัยคุกคาม เหตุการณ์ที่เกิดขึ้น ความเสียหายของการเกิดขึ้น และการกู้คืน มาตรการรักษาความปลอดภัยรวมถึงการตรวจสอบ การป้องกัน การแก้ไข การหลอกลวง การทำให้ลดลง การโต้ตอบและการประเมินผล

ทุกระบบรวมไปถึงซอฟต์แวร์หรือฮาร์ดแวร์ เป็นผู้รับผิดชอบในการตรวจสอบกิจกรรมทั้งหมดที่มีอยู่ภายในระบบหรือในเครือข่ายเพื่อตรวจสอบกิจกรรมที่เป็นอันตราย และการรายงานไปยังระบบการจัดการระบบตรวจจับการบุกรุก (Intrusion detection systems, IDS) ด้วยจุดมุ่งหมายของระบบตรวจจับการบุกรุกเป็นการตรวจสอบโครงสร้างพื้นฐานเครือข่ายสำหรับการค้นหาพฤติกรรมที่ผิดปกติและในทางที่ผิดรวมทั้งเหตุการณ์ที่ไม่ปกติเป้าหมายดังกล่าวได้รับ

เนื่องจากไฟวอล์มีข้อจำกัดและในปัจจุบัน การโจมตีผ่านทางอินเตอร์เน็ตมีจำนวนเพิ่มมากขึ้น เช่น การโจมตีแบบ DoS เครื่องมือตรวจจับการบุกรุกจึงได้กลายเป็นเครื่องมือที่มีความสำคัญ สำหรับการตรวจสอบกิจกรรมที่เป็นอันตราย snort เป็นระบบตรวจจับการบุกรุกที่สามารถนำมาใช้งานได้ฟรี ลักษณะการทำงานของ snort จะทำการเปรียบเทียบการจราจร (Traffic) จากฐานข้อมูล ซึ่งฐานข้อมูลจะเก็บรูปแบบของการโจมตีหรือเรียกว่า signature ถ้าตรวจพบการจราจรที่ตรงกับ signature ก็จะทำการแจ้งเตือนให้ผู้ดูแลระบบทราบ

การตรวจจับการบุกรุกโดยใช้ snort ได้มีการวิจัยเป็นจำนวนมากเพื่อที่จะเอาชนะปัญหาและข้อจำกัดที่มีอยู่ใน snort และเพื่อที่จะออกแบบป้องกันจากการโจมตีทั้งภายนอกและภายในเครือข่าย สำหรับประเภทของระบบตรวจจับการบุกรุกจะกล่าวถึงในส่วนที่ 2 ส่วนที่ 3 ของการสำรวจจะกล่าวถึง snort ส่วนที่ 4 อธิบายเทคนิคต่างๆ ที่นำมาใช้กับ snort และมีการเปรียบเทียบเทคนิคต่างๆ ส่วนที่ 5 จะเป็นการสรุปของการสำรวจ และสุดท้ายในส่วนที่ 6 เป็นงานที่จะทำการสำรวจในอนาคต

II. Intrusion Detection System (IDS)

เครือข่ายที่ใช้ระบบตรวจจับการบุกรุก ทำหน้าที่ในการตรวจสอบการจราจรในเครือข่าย สามารถค้นหาตรวจจับแพ็กเก็ตการโจมตีแล้วทำการวิเคราะห์และแจ้งรายงานไปยังหน่วยงานกลาง เพื่อที่จะทำการสำรวจเพิ่มเติมที่จะระบุถึงรูปแบบของการโจมตี เซ็นเซอร์ตรวจจับการบุกรุกที่ได้ติดตั้งไว้ในเครือข่ายมีอยู่ 2 ประเภท คือ 1) เป็นการตรวจจับเหตุการณ์ที่ผิดปกติ (Anomaly-base Detection) 2) เป็นการตรวจจับการใช้งานในทางที่ผิด (misuse-base Detection)

A. การตรวจจับเหตุการณ์ที่ผิดปกติ (Anomaly-base Detection)

การตรวจจับการบุกรุกแบบ Anomaly-base Detection จะต้องแยกกิจกรรมการทำงานที่ปกติหรือกิจกรรมที่ยอมรับได้ออกและให้กิจกรรมที่เหลือ เป็นกิจกรรมผิดปกติ กิจกรรมที่ปกติซึ่งได้จากพฤติกรรมการทำงานของผู้ใช้ หรือการเชื่อมต่อเครือข่าย เป็นต้น ข้อมูลเหล่านี้จะถูกสร้างขึ้นจากประวัติการใช้งานและตัวตรวจจับการบุกรุกจะทำการเก็บข้อมูลเหตุการณ์ต่างๆ ไว้ แล้วใช้เกณฑ์ในการชี้วัดค่าทางสถิติ เพื่อเปรียบเทียบกับข้อมูลกิจกรรมที่ปกติที่มีอยู่ หากมีพฤติกรรมที่เบี่ยงเบนไปจากพฤติกรรมที่มีอยู่ถือว่า “ไม่ปกติ” จะถือว่าเป็นการโจมตี ข้อดีและข้อเสียของวิธี Anomaly-base Detection มีดังต่อไปนี้

ข้อดี

- Anomaly-base Detection ดีกว่า signature-based เนื่องจากสามารถตรวจจับการโจมตีที่ไม่รู้จักได้
- Anomaly-base Detection สามารถรับข้อมูล signature ซึ่งใช้โดย misuse-base IDS ได้

ข้อเสีย

- Anomaly-base Detection โดยทั่วไปจะมีแจ้งเตือนที่ผิดพลาดจำนวนมาก เพราะพฤติกรรมของผู้ใช้และเครือข่ายไม่สามารถทราบล่วงหน้าได้ทุกอย่าง
- วิธีการของ Anomaly-base Detection จำเป็นต้องใช้การ training data ที่มีขนาดใหญ่ ซึ่งประกอบด้วยบันทึกเหตุการณ์ของระบบ เพื่อสร้างรายละเอียดพฤติกรรมที่ปกติ

B. Misuse -Based Detection

หลักการของการตรวจจับการบุกรุกด้วยแนวทาง Misuse-base Detection คือตัวตรวจจับการบุกรุกจะวิเคราะห์กิจกรรมของระบบ โดยการพิจารณาเหตุการณ์หรือชุดของเหตุการณ์ที่ตรงกับรูปแบบเหตุการณ์ที่ได้กำหนดไว้แล้วว่าเป็นการบุกรุก โดยจะอธิบายถึงการบุกรุกแบบต่างๆ ที่รู้จัก รูปแบบของเหตุการณ์การบุกรุกที่รู้จักเหล่านี้จะเรียกว่า ร่องรอยการบุกรุก (Signatures) ดังนั้นบางครั้งจึงเรียกแนวทาง Misused Detection ว่า Signature-based Detection แนวทางนี้จะใช้ข้อมูลความรู้เกี่ยวกับพฤติกรรมที่เป็นการบุกรุกหรือไม่ยอมรับ และค้นหาเพื่อตรวจจับพฤติกรรมเหล่านี้โดยตรง ซึ่งตรงกันข้ามกับAnomaly-base Detection ที่จะค้นหาเพื่อตรวจจับพฤติกรรมเหล่านี้ ข้อดีและข้อเสียของวิธี Misuse-base Detection มีดังต่อไปนี้

ข้อดี

- Misuse-base Detection มีประสิทธิภาพมากในการตรวจจับการโจมตีโดยไม่ส่งสัญญาณการเตือนผิดพลาด
- Misuse-base Detection สามารถตรวจจับเครื่องมือและเทคนิคที่ออกแบบมาเป็นพิเศษได้อย่างรวดเร็ว
- Misuse-base Detection ทำให้ผู้ดูแลระบบง่ายต่อการใช้เครื่องมือตรวจสอบเหตุการณ์ได้ง่าย แม้ไม่มีความชำนาญต่อการรักษาความปลอดภัย

ข้อเสีย

- Misuse-base Detection สามารถตรวจจับได้เฉพาะการโจมตีที่รู้จักเท่านั้น ด้วยเหตุนี้ระบบจะต้องมีการปรับปรุงการโจมตีที่ค้นพบใหม่ใน signatures
- Misuse-base Detection ถูกออกแบบมาเพื่อตรวจจับการโจมตีที่มีอยู่ในระบบ signature เท่านั้น เมื่อการโจมตีที่รู้จักมีการเปลี่ยนแปลงเพียงเล็กน้อย ตัวตรวจจับจะไม่สามารถตรวจจับได้

III. คุณสมบัติของ Snort

Martin Roesch พัฒนา Snort ในปี 1990 [1,2] ซึ่งถูกเขียนขึ้นด้วยภาษา C เพื่อที่จะตรวจจับการโจมตีในเครือข่าย Snort มีลักษณะเป็นแบบ signature-based และ open-source IDS ที่ทำงานได้อย่างรวดเร็ว จะทำการสร้างการส่งสัญญาณเตือนภัยให้ผู้ดูแลระบบทราบหากมีการใช้งานที่ผิด Snort ประกอบด้วย 4 องค์ประกอบต่อไปนี้

- Packetcapture/decode engine : Snort’s packet-capturing engine ใช้ libpcap packet-capturing library ทำหน้าที่รับข้อมูลจากส่วนที่เชื่อมกับระบบเครือข่าย แล้วทำการถอดรหัส (Decode) ข้อมูลเพื่อส่งต่อไปยังส่วนอื่นต่อไป แพ็กเก็ตที่วิ่งอยู่ในเครือข่ายจะถูกดักจับเข้าสู่ระบบตรวจจับผู้บุกรุกผ่านทางการทำงานส่วนนี้
- Preprocessor plug-ins : จำนวนแพ็กเก็ตถูกส่งผ่านจากการเตรียมประมวลผล ขั้นตอนนี้มีวัตถุประสงค์เพื่อตรวจสอบและการประมวลผลแพ็กเก็ตก่อนผ่านตัวตรวจสอบ ทุก preprocessor จะตรวจสอบแพ็กเก็ตสำหรับคุณลักษณะที่แตกต่างกันและทำการตัดสินใจที่จะส่งผ่านแพ็กเก็ตไปยังตัวตรวจสอบ โดยไม่ต้องทำการแก้ไข

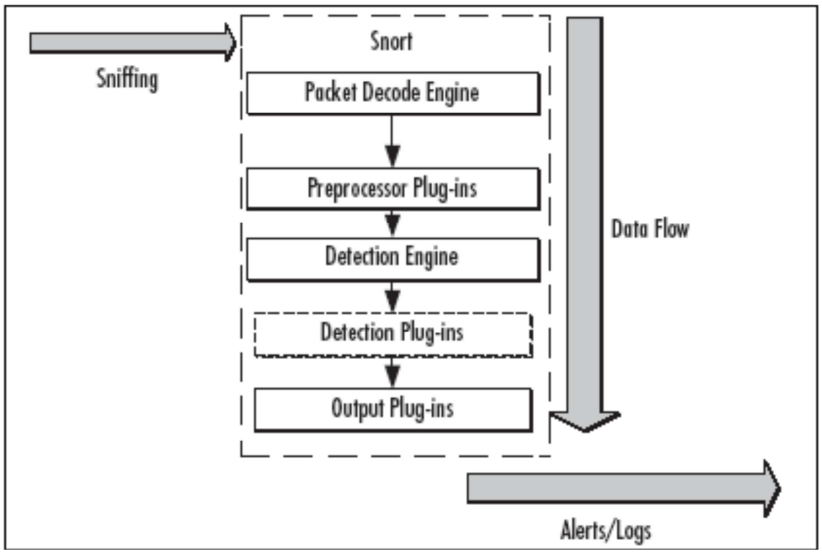
ปรับเปลี่ยนใดๆ และส่งไปยังตัวตรวจสอบหรือไม่ส่ง และสร้างการแจ้งเตือนสำหรับแพ็กเก็ต

- Detection engine : แพ็กเก็ตที่รับเข้ามาจากเครือข่าย หลังจากการทำงานจากสองส่วนแรก จะถูกเก็บเข้าสู่โครงสร้างข้อมูล (Data Structure) ซึ่งผ่านกระบวนการจัดโครงสร้าง การกลั่นกรอง และการถอดรหัส มาอยู่ในรูปแบบในส่วนของ Detection Engine โดยที่จะทำหน้าที่ตรวจจับพฤติกรรมการบุกรุกต่างๆ ที่ปรากฏอยู่ในแพ็กเก็ต ซึ่งในโปรแกรม Snort จะใช้วิธีการตรวจสอบแบบอ้างอิงกฎ (Rule-base)
- Output plug-ins : เป็น plug-ins ที่ทำหน้าที่ในการแสดงผลลัพธ์ เก็บบันทึกข้อมูลการบุกรุก และส่งสัญญาณการแจ้งเตือนที่ถูกสร้างจาก Detection engine, preprocessors หรือ ตัวถอดรหัส

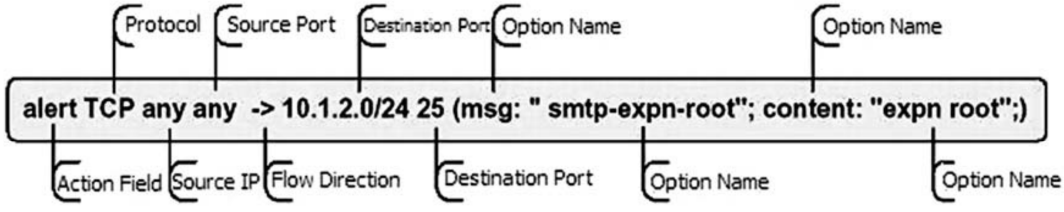
ภาพแสดงการประมวลผลของแพ็กเก็ต Snort [3] มีรายละเอียดดังรูปที่ 1

Snort เป็นระบบตรวจจับการบุกรุกในเครือข่ายที่อาศัยกฎ (rule-based network intrusion detection system, N-IDS) แต่ก็มีความยืดหยุ่นของภาษาที่ใช้กำหนดกฎ ที่ช่วยให้ทุกคนเปลี่ยนแปลงกฎที่มีอยู่หรือเพิ่มกฎใหม่ไปยัง IDS ทุกกฎประกอบด้วยสองส่วน ส่วนหัวของกฎ (header rule) และส่วนของตัวเลือก (rule option) ส่วนหัวของกฎมี 5 ส่วน ส่วนการกระทำของกฎ (rule action) (ถูกกระทำเมื่อมีการตรวจสอบการบุกรุก) แหล่งที่มาจากต้นทางไปยังปลายทางและข้อมูลปลายทาง (IP address ของต้นทางและปลายทาง และหมายเลข port ที่ขึ้นอยู่กับโปรโตคอล) และทิศทางของการจราจรรวมทั้งประเภทของโปรโตคอล (TCP, UDP หรือ ICMP)

Option ของกฎประกอบด้วยเงื่อนไขต่างๆ ที่จะช่วยให้การตัดสินใจว่าการดำเนินการดังกล่าวใช้งานที่ผิดหรือไม่ ตัวอย่างกฎของ Snort แสดงในรูปที่ 2 เขตข้อมูลแรกของทุกๆ กฎจะเป็นเขตข้อมูลการกระทำ เขตข้อมูลเหล่านี้สามารถมีค่าได้ดังต่อไปนี้ log การแจ้งเตือน การส่ง การตอบสนอง หรือไดนามิก เมื่อค่าข้อมูลที่เข้ามาตรงกับเกณฑ์ การกระทำจะถูกตอบสนอง การเลือกการกระทำในรูปที่ 2 เป็น “การแจ้งเตือน” สำหรับสถานะนี้ ถ้าข้อมูลตรงกับเกณฑ์ดังกล่าว การแจ้งเตือนจะถูกสร้างขึ้น เขตข้อมูลถัดไปเก็บข้อมูลโปรโตคอล ค่าเป็นไปได้ของเขตข้อมูลคือ TCP, UDP หรือ ICMP โปรโตคอลในตัวอย่างคือ TCP เขตข้อมูลที่สามและสี่เก็บแหล่งที่อยู่ต้นทาง ส่วนแรกหมายถึง IP address และส่วนที่สองเป็นหมายเลขพอร์ต ถ้าเขตข้อมูลมีค่าเป็น ‘‘any any” หมายถึงแพ็กเก็ตอาจจะมาจากทุก IP address และทุกพอร์ต TCP ในกรณีที่ค่าของโปรโตคอลเป็น ICMP จะไม่มีการใส่ค่าพอร์ต เขตข้อมูลนี้จะใช้งานสำหรับ TCP และ UDP เท่านั้น



รูปที่ 1 กระบวนขั้นตอนการทำงานของ Snort



รูปที่ 2 โครงสร้างกฎของ Snort

IV. implement for Snort techniques

สำหรับในส่วนนี้จะเป็นการสำรวจเทคนิคต่างๆ ที่นำมาปรับปรุงและพัฒนาให้กับระบบตรวจจับการบุกรุก snort IDS โดยได้แบ่งออกเป็น 4 ส่วนได้แก่ 1) เทคนิคการพัฒนาฮาร์ดแวร์และซอฟต์แวร์อัลกอริทึมรูปแบบการจับคู่ 2) เทคนิคการพัฒนา signature สำหรับ snort 3) เทคนิคการพัฒนา IDS และ IPS สำหรับ snort 4) เทคนิคการพัฒนาการแจ้งเตือนที่ผิดพลาดสำหรับ snort

A. Implement hardware and software pattern matching algorithm for Snort IDS techniques

ระบบตรวจจับการบุกรุกจะถือว่าเป็นองค์ประกอบที่สำคัญของมาตรการเพื่อป้องกันระบบคอมพิวเตอร์และจากการละเมิดเข้าสู่เครือข่ายโดยไม่ได้รับอนุญาต การบุกรุก การโจมตีและภัยคุกคามเพิ่มขึ้นอย่างรวดเร็วในเครือข่ายความเร็วสูงและปริมาณงานที่จะต้องตรวจสอบมีความจำเป็นต้องใช้เครือข่ายระบบการตรวจจับการบุกรุก (NIDS) ที่มีประสิทธิภาพสูงเช่นกัน เนื่องจากส่วนใหญ่ NIDSs จะต้องตรวจสอบจำนวนมากของรูปแบบการโจมตีที่รู้จักกันในทุกแพ็คเก็ต รูปแบบการจับคู่รูปกลายเป็นส่วนหนึ่งที่สำคัญที่สุดของ signature-based NIDSs ในส่วนของทรัพยากรการประมวลผลและหน่วยความจำ เพื่อสนับสนุนการแบ่งส่วนของการจราจรของเครือข่ายและตรวจจับการโจมตีที่กระจัดกระจาย

สำหรับในส่วนนี้จะเป็นการสำรวจรูปแบบการจับคู่ (pattern matching) ที่ได้นำมาปรับปรุงและช่วยเพิ่มประสิทธิภาพให้กับ snort ทั้งทางด้านของฮาร์ดแวร์และซอฟต์แวร์ โดยรูปแบบการจับคู่เป็นส่วนที่สำคัญของผลิตภัณฑ์ NIDS/NIPS [5] เช่น 3com, cisco IPS เป็นต้น โดยได้แบ่งรูปแบบการจับคู่ออกเป็น 3 ประเภทหลักๆ ดังต่อไปนี้

- ***Software-based:*** วิธีการซอฟต์แวร์ที่ใช้ยังวิธีการจะขึ้นอยู่กับโปรเซสเซอร์หรือหน่วยประมวลผลของเครือข่าย DFAs เป็นที่นิยมมากที่ใช้วิธีการขึ้นบนซอฟต์แวร์ เพราะจะต้องเปลี่ยนสถานะที่จะต้องทำให้การเข้าถึงหน่วยความจำที่มากที่สุด ดังนั้นมักจะต้องการอัตราเชื่อมโยงเครือข่ายในระดับสูง
- ***ASIC-based:*** ผู้จัดจำหน่ายอุปกรณ์เครือข่ายเชิงพาณิชย์ รวมทั้ง 3Com และ Cisco ได้จัดจำหน่าย NIDS ของตัวเอง ได้นำรูปแบบการจับคู่ ASICs นำไปใช้ภายใน NIDS การพัฒนา ASICs สำหรับ NIDS แต่มีข้อเสียต่างๆ มันต้องมีการลงทุนขนาดใหญ่และวงจรการพัฒนามีระยะนานและเมื่อที่ต้องการปรับปรุงทำได้ยาก
- ***FPGA-based:*** จำนวนของงานวิจัยที่สนับสนุนรูปแบบการจับคู่ FPGA-based ไม่เพียงแต่จะมีความสามารถให้การจับคู่ได้อย่างรวดเร็ว แต่ยังดำเนินการจับคู่ขนาน

สำหรับในงานวิจัย [5] ได้นำเสนอเทคนิควิธีการที่ใช้ในการตรวจสอบ deep packet ในการจับคู่ใหม่ เพื่อลดเวลาในการทำงานของการเข้าถึงหน่วยความจำในการจับคู่ โดยใช้ NFA ที่อยู่บนพื้นฐานของ BCAM แทน TCAM วิธีการนี้ไม่เพียงแต่เพิ่มความเร็วของสัญญาณนาฬิกาเท่านั้น แต่ที่สำคัญวิธีที่นำเสนอนี้ยังช่วยลดค่าใช้จ่ายและช่วยลดการทำงานของ SRAM ได้เป็นอย่างดี

Snort เป็นเครือข่ายระบบการบุกรุกที่มีการป้องกันการวิเคราะห์การจราจรแบบเวลาจริงและบันทึกแพ็คเก็ตเกี่ยวกับเครือข่าย IP ใช้กฎที่มีความยืดหยุ่น เพื่อดำเนินการวิเคราะห์การค้นหาและการจับคู่ของเนื้อหาโปรโตคอล และจะทำการตรวจสอบความหลากหลายของการโจมตี การเขียนกฎเพื่อใช้ในการตรวจจับการบุกรุก เพื่อที่จะป้องกันเครือข่ายจากการโจมตี ผู้ดูแลระบบต้องมีความรู้ความชำนาญในการสร้างกฎ Kadar and Girija [6] ได้ปรับปรุงโค้ดใน snort ด้วยอัลกอริทึมการจับคู่แบบ deterministic ในส่วนของ pcre regexp ด้วยอัลกอริทึม DFA-style ซึ่งทำให้ผู้ทำการเขียนกฎเพื่อตรวจสอบกฎใหม่และแน่ใจว่า IDS/IPS ของพวกเขาจะไม่ตกเป็นเหยื่อของการโจมตี อัลกอริทึมยังสามารถที่จะทำการตรวจสอบกฎที่ได้เขียนขึ้นที่อาจจะทำให้เป็นช่องโหว่ได้

ในงานงานวิจัยของ [7] ได้นำเสนอ fast software-based ที่ใช้อัลกอริทึมรูปแบบการจับคู่ที่จะช่วยลดจำนวนของเวลาในการดำเนินการรูปแบบการจับคู่ อัลกอริทึมจะแยกแพ็กเก็ตที่ปกติออกจากแพ็กเก็ตที่น่าสงสัย ใช้รูปแบบการค้นหาโดยได้ปรับปรุงอัลกอริทึมรูปแบบการจับคู่ Wu-Manber การกรอง exclusion-inclusion เป็นการปรับปรุงในส่วนของ Bloom filter จะประกอบไปด้วยรายการที่ตรงกันของ signature สำหรับแต่ละแพ็กเก็ตที่น่าส่งสัย อัลกอริทึมของ Wu-Manber ถูกนำเสนอโดยแนะนำโดย Udi Manber และ Sun Wu in 1994. จะเป็นส่วนขยายการแก้ปัญหาของอัลกอริทึม BM อัลกอริทึม WM ประกอบด้วยสองขั้นตอนคือขั้นตอนการเตรียมและการค้นหาข้อมูล ผลการทดสอบแสดงให้เห็นถึงความเร็วโดยเฉลี่ยเพิ่มขึ้น 3.4 เท่า 5.5 เท่าสำหรับการจราจรปกติและเวลาสำหรับการจราจร 1.6 กรณีที่เลวร้ายใช้หน่วยความจำเพิ่มขึ้นโดยอัลกอริทึมจำกัดที่ 0.11 %

การโจมตีได้รับการฝึกฝนและมีประสบการณ์ใช้วิธีการที่ฉลาดขึ้นเช่น กระจายตัวหลอกลวง IDS และทำการป้องกันตัวเองจากการถูกเปิดเผย สำหรับโครงสร้างข้อมูล CDAWG (Compact Direct Acyclic Word Graph) เป็นรุ่นที่ขนาดเล็กมากกว่าโครงสร้างข้อมูล DAWG ได้ถูกนำเสนอโดย [8] ผลการทดลองแสดงให้เห็นว่าอัลกอริทึมนี้ เร็วกว่าอัลกอริทึม Aho-Corasick 2.5 เท่า และดำเนินการศึกษาทดลองและการประเมินประสิทธิภาพการทำงานของอัลกอริทึมใหม่ บนเครื่องมือตรวจจับการบกรุก snort แนวคิดหลักของวิธีการเป็นการพัฒนรูปแบบการจับคู่ เพื่อสนับนุนของการกระจายตัวและการแบ่งส่วนของการจราจร ข้อดีของวิธีนี้คือมันหลีกเลี่ยงการรวมกลุ่มของแพ็กเก็ตที่รู้จักกันเพราะต้องใช้เวลาเพิ่มและข้อจำกัดของหน่วยความของการตรวจจับการโจมตี เช่น แพ็กเก็ตขนาดใหญ่และซ้อนทับกัน

งานวิจัยของ [9] ได้นำเสนอรูปแบบการจับคู่ NFA-base มีประสิทธิในหน่วยความจำในไบนารีที่สามารถเข้าถึง (BCAM) วิธีการนี้สามารถประมวลผลตัวอักษรหลายช่วงเวลา ไบนารีที่อยู่ในหน่วยความจำ (BCAM) วิธีการนี้สามารถ

ที่ประมวลผลได้หลายตัวอักษรแสดงให้เห็นว่าวิธีการนี้มีประสิทธิภาพเหนือกว่าวิธีการ CAM-base และที่ใช้ซอฟต์แวร์

การออกแบบนี้จะพัฒนาในแพลตฟอร์ม NetFPGA ซึ่งเป็นแพลตฟอร์มฮาร์ดแวร์ที่เหมาะสำหรับกับเครือข่ายความเร็วสูง รูปแบบระบบการจับคู่ขนานให้ throughput สูงขึ้น 4 Gbps

ตารางที่ 1 เปรียบเทียบเทคนิคฮาร์ดแวร์และซอฟร์แวร์ pattern matching สำหรับ snort

Ref.	Algorithm	Hardware	Software	Throughput	Advantages	Disadvantages
[5]	BCAM	Yes	-	16 Gbps	Algorithm small	configurable hardware platform as FPGA
[6]	DFA-style	Yes	-	-	Can use analysis and test to check new rule	Complex
[7]	Bloom filter	-	Yes	-	Fast process and search	Use memory very
[8]	CDAWG	-	Yes	-	Avoids reassembly of packet	Extra time and memory limit
[9]	FPGA	Yes	-	Over 4 Gbps	High speed pattern matching	Complex

B. ***Implement signature for Snort techniques***

รูปแบบของ signature ใน snort [13] จะถูกเขียนแทนด้วยกฎ ซึ่งในกฎของ snort จะประกอบด้วย 2 ส่วนได้แก่ ส่วนหัว (rule header) และส่วนของตัวเลือก (rule option) โดยที่ส่วนหัวนั้นเป็นการระบุถึงพารามิเตอร์พื้นฐานของ signature เช่นการตรวจสอบโปรโตคอล (IP, UDP, TCP หรือ ICMP) ทิศทางของการสื่อสาร รวมทั้งต้นทางและปลายทาง IP addresses และหมายเลขพอร์ต ในส่วนของ rule option เป็นการระบุข้อจำกัดของ signature และใช้เป็นข้อกำหนดสำหรับการจับคู่

```
//rule header
    alert tcp any any -> 141.43.3.0/24 445 (
//header options
    tos: 1;
    flow: to_server, established;
//payload options
    content: "|FF|SMB%"; depth: 5; offset: 4;
    content: "&|00|"; within: 2; distance: 56;
    content: "|05|"; within: 1; distance: 2;
    content: "|0B|"; within: 1; distance: 1;
    byte_test: 1,&,1,0,relative;
    content: "|00|"; within: 1; distance: 21;
//actions
    msg: " Netbios access";
//rule ID
    sid: 2191;)
```

รูปที่ 3 ตัวอย่างของ signature snort [11]

สำหรับงานวิจัยที่ได้นำเสนอเทคนิค rapid malcode signature [10] ได้นำมาทดสอบการ Snort IDS ซึ่งจะเป็นการกำหนดให้ระบบตรวจจับการบุกรุกสามารถที่จะตรวจสอบ malcodes ใหม่ที่พวกเขาได้ออกแบบไว้ โดยได้สร้างไว้ใน signature ซึ่งมีลักษณะการทำงานเป็นแบบอัตโนมัติเมื่อมีการตรวจพบการบุกรุก และทำให้มีอัตราการแจ้งเตือนที่ผิดลดลง โดยที่ระบบจะทำเหมืองข้อมูลเลือก traffic ที่น่าส่งสัยจากการใช้กฎของ snort จากนั้นทำการแยกหมวดหมู่แพ็กเก็ตที่น่าสงสัยและไม่น่าสังสัย การจำแนกหมวดหมู่จะทำให้ช่วยลดปริมาณของ traffic ที่ต้องประมวลผลและยังช่วยลดการแจ้งเตือนที่ผิด เมื่อจำแนกการจราจรในระบบได้แล้วจำทำการวัดความถี่จาก payload จาก substring ที่น่าสงสัยและจะนำไปสร้าง signature ใหม่ซึ่งใช้วิธีการ sifting เพื่อกรอง traffic ที่ถูกต้องออกและแยก payload ที่ผิดปกติออกจาก traffic ที่มาจากแหล่งต่างๆ ซึ่งถือว่าเป็นเกณฑ์หลักในการสร้าง signature

ระบบส่วนใหญ่นั้นจะใช้การตรวจจับการบุกรุกด้วยวิธีการตรวจสอบความผิดปกติ (misuse detection) เพื่อการตรวจสอบความผิดปกติ จะทำการเปรียบเทียบข้อมูลที่กำหนดไว้ล่วงหน้า เช่น signature ซึ่งใน signature ถูกออกแบบจากการสังเกตและประสบการณ์และความเชี่ยวชาญ การพัฒนา signature จะมีความยาวนานเพื่อสำหรับสร้าง signature ใหม่ และอาจจะทำให้เกิดช่องโหว่ในระบบได้ ในงานวิจัยของ [11] ได้นำเสนอวิธีการสำหรับระบบ signature engineering ซึ่งอยู่บนพื้นฐานของการ re-use ที่มีอยู่ใน signature

signature engineering ได้รับการสนับสนุนโดยการออกแบบ re-using signature การตัดสินใจและ/หรือ fragments ที่มีอยู่ re-use ไม่เพียงแต่ช่วยลดกระบวนการวิศวกรรม signature แต่มันยังสามารถลดระยะการทดสอบและขั้นตอนการแก้ไขเป็นอย่างมาก นอกจากนั้น ขั้นตอน signature engineer จะช่วยประโยชน์จากการเข้ารหัสที่มีอยู่ใน signature แสดงให้เห็นถึงวิธีการทั่วไปที่สามารถใช้งานได้เพียงขั้นเดียวสำหรับ signatures มีองค์ประกอบของการวิเคราะห์ single-step signature ข้อกำหนดภาษาและระบุแปลงแนวคิดเหมาะสำหรับลายเซ็น signature วิธีการนี้ได้ถูกนำไปใช้กับ IDSs Snort

การนำซอฟต์แวร์โอเพนซอร์ (Open source) มาประยุกต์ร่วมกับ Snort ทำให้ระบบตรวจจับการบุกรุกมีประสิทธิภาพเพิ่มมากขึ้น หากระบบตรวจจับการบุกรุกสามารถที่สร้างกฎ เพื่อตรวจจับการโจมตีแบบอัตโนมัติได้ก็จะเป็นการแบ่งภาระของผู้ดูแลระบบได้เป็นอย่างมาก Honeyd เป็นซอฟต์แวร์โอเพนซอร์สที่มีนักวิจัยได้นำมาใช้งานร่วมกับ snort โดยที่ Homeyd สร้างขึ้นโดย Google

engineer Neils Provos มีคุณสมบัติหลายๆ ดังต่อไปนี้ 1) Honeyd มีความสามารถในการตรวจสอบหลายล้าน IP address สามารถที่จะทำงานในฟังก์ชันเหมือนกันพร้อมกันได้ 2) Honeyd มีกลไกที่สามารถหลอกผู้โจมตีได้ 3) Honeyd สามารถที่จะโต้ตอบกับแฮกเกอร์ได้ 4) Honeyd มีการทำงานที่สามารถควบคุมความปลอดภัยของระบบได้อย่างมีประสิทธิภาพ

ในงานวิจัยของ [12] เป็นระบบการสร้าง signature อัตโนมัติเมื่อมีการโจมตีเกิดขึ้น ได้นำเอา Honeyd ซึ่งเป็นซอฟต์แวร์เพนซอร์ส และคิดตั้ง Signature Generation System (SGS) เพื่อสร้าง signature การโจมตีสำหรับ snort อัตโนมัติ โดยที่ SGS จะทำการแยกแพ็กเก็ตที่ได้นำเข้าไปใน Honeyd และเปรียบเทียบกฎกับไลบารีกฎใน Snort หากพบกฎการบุกรุกที่เหมือนกันในไลบารีกฎ SGS จะทำการปรับปรุงกฎ ในทำนองเดียวกัน มันก็จะทำการปรับปรุงกฎของ snort ด้วย

ใน [13] เป็นการใช้เทคนิคแบบขนานสำหรับการปรับปรุงประสิทธิภาพของเครือข่ายระบบตรวจจับการบุกรุก signature โดยที่แต่ละเซ็นเซอร์ได้ถูกกำหนดด้วยกฎของ snort ทั้งหมด ได้มีการแบ่งพอร์ตให้แต่ละเซ็นเซอร์ การดำเนินการของพวกเขาใช้สถาปัตยกรรมแบบ real time ในเครือข่ายความเร็วสูง ข้อดีของระบบของพวกเขาที่ได้ออกแบบไว้มี 2 อย่างดังต่อไปนี้

- **สามารถปรับขยายได้ (Scalability) :** เครือข่ายความเร็วสูงต้องการประมวลผลข้อมูลด้วยความเร็ว และหากมีข้อมูลเป็นจำนวนมาก ความสามารถที่จะตรวจจับการบุกรุกจะลดลง เนื่องจากเซ็นเซอร์ไม่สามารถประมวลผลได้ทัน ดังนั้นจึงสามารถที่จะเพิ่มเซ็นเซอร์เข้าไปในเครือข่ายได้ เพื่อเพิ่มประสิทธิภาพในการตรวจจับ
- **ความคงทนต่อความเสียหาย (Fault tolerance) :** เมื่อเวลาเซ็นเซอร์ตัวใดตัวหนึ่งเสียหาย สามารถที่จะกำหนดให้ traffic ไปยังเซ็นเซอร์ตัว อื่นได้ เพื่อป้องกันกิจกรรมที่เป็นอันตราย

สำหรับการแบ่งพอร์ตให้กับเซ็นเซอร์ เพื่อทดสอบระบบตรวจจับการบุกรุกแบบขนาดของพวกเขา ได้แสดงตัวอย่างไว้ในตารางที่ 1

ตารางที่ 1 การแบ่งพอร์ตและกฎ

หมายเลขเซ็นเซอร์	ช่วงการแบ่งพอร์ต	การกำหนดพอร์ต
เซ็นเซอร์ 1 (Snort 1)	25,80,110,143,8080 (snortl) (SMTP, HTTP, POP3, IMAP4)	กฎทั้งหมดสำหรับพอร์ตปลายทางสอดคล้องกับเซ็นเซอร์ 1
เซ็นเซอร์ 2 (Snort 2)	21,22,23,53,3306 (Ftp, SSH, Telnet, DNS Server, MYSQL database system)	กฎทั้งหมดสำหรับพอร์ตปลายทางสอดคล้องกับเซ็นเซอร์ 2

ในปัจจุบันหนอน (worm) ได้เข้ามาคุกคามอินเตอร์เน็ตมากขึ้น และเป็นเรื่องยากที่จะแยกความหลากหลายของเวิร์มได้ทันทีด้วยวิธีการจับคู่ signature ความพยายามที่จะแยก signature worm จากการจราจรในอินเทอร์เน็ตได้รับการพัฒนาขึ้น แต่ประสิทธิภาพมีปัญหาที่ยังแก้ไม่ได้ โดยเฉพาะในเครือข่ายความเร็วสูง ในงานวิจัยของ [14] ได้นำเสนอวิธีการจัดกลุ่ม binary และมีการกำหนดนโยบายที่ต้องการที่จะปรับปรุงตัวกรองการจราจร ซึ่งสามารถลดการจราจรที่จะประมวลผล และปรับปรุงการจราจรให้มีความบริสุทธิ์มากขึ้น

การป้อนข้อมูลการจราจรทั้งหมดเข้าสู่ระบบเครือข่าย และผลลัพธ์ที่ได้เป็นฐานข้อมูลของ signatures worm ซึ่งสามารถใช้ป้องกันที่อยู่บนพื้นฐานของเนื้อหา มีสามขั้นตอนหลักในการแยก signature ของเครือข่ายในวิธีการนี้คือ 1) ขั้นตอนการจัดกลุ่มข้อมูล โดยจะใช้การทำเหมืองแร่การจราจรวิเคราะห์ส่วนหัวของ IP ที่ใช้ในการระบุปริมาณการจราจรอย่างมีนัยสำคัญวิธีการจัดกลุ่มเลขฐานสองใช้ bloom filter ด้วยอัลกอริทึม BBF เพื่อเพิ่มประสิทธิภาพ 2) หลังจากที่จัดกลุ่ม ปริมาณการจราจรที่ไม่สำคัญจะถูกเก็บไว้ในพูลแพ็คเก็ตไม่มีอันตราย และปริมาณการจราจรที่สำคัญมีแยกโดยใช้การกระจายตัวที่เป็นที่น่าสงสัยหรือไม่สงสัย หลังจากนี้ ส่วนเล็ก ๆ ของแพ็กเก็ตที่จับจากเครือข่าย EDGE มีการวิเคราะห์ใน 3) แยก signatures ในขั้นตอนนี้จะให้ความสำคัญของอัลกอริทึมในการแยกตำแหน่งของ signature ให้มีในการแยก signature ที่ถูกต้องมากขึ้น เพื่อลดการแจ้งเตือนที่ผิด signature จะถูกตรวจสอบเพิ่มมากขึ้นที่ขึ้นอยู่กับพูลแพ็กเก็ตที่ไม่เป็นอันตรายก่อนที่จะเพิ่มเข้าไปยังฐานข้อมูล signature

สำหรับ [15] ได้นำเสนอวิธีการเพิ่มประสิทธิภาพของการจับคู่บิตที่จะทำให้เมื่อมีการบุกรุกเกิดขึ้น แต่ระบบนั้นไม่ทำการแจ้งเตือน (false negatives) โดยนำวิธีที่นำเสนอการแบ่งข้อมูลแบบขนาน

ระบบที่นำเสนอได้แบ่งข้อมูลแบบขนาดใหม่ประกอบด้วย array n ของโปรเซสเซอร์ การพัฒนามีนโยบายเหมือนกัน payload ของแพ็กเก็ตที่เดินทางมาถึงฝั่งตรงข้ามจะแบ่งออกไปแต่ละโปรเซสเซอร์ แต่ละหน่วยประมวลผลตรวจสอบเป็นเพียงส่วนเล็กๆ หรือ fragment ของ payload เดิม Fragments ถูกจัดคิวให้ประมวลผลที่มีการตรวจสอบสำหรับ signatures ดังนั้นการออกแบบระบบจะช่วยให้การประมวลผลเพื่อตรวจสอบ fragments ที่แตกต่างกันและประมวลผลพร้อมกันกับแพ็คเก็ตได้ โปรเซสเซอร์ 0 และ 1 สามารถตรวจสอบ fragments จากแพ็กเก็ตที่ 2 ขณะที่โปรเซสเซอร์ที่ 3 ตรวจสอบ fragments จากแพ็กเก็ตที่ 3 รูปแบบของการลำเลียงช่วยเพิ่มประสิทธิภาพในการทำงาน นอกจากนั้นวิธีการนี้ยังจะช่วยให้ป้องกันไม่ให้ทับซ้อนการไม่แจ้งเตือนเมื่อเกิดการโจมตี (false negatives)

การทดลองของระบบได้เทียบกับประสิทธิภาพการทำงานของอัลกอริทึมการค้นหาที่แตกต่างกัน (Wu-Manber และ Aho-Corasick) วิธีการที่นำเสนอการแบ่งข้อมูลแบบขนานใช้ (overlap และ match bit) และมาตรฐานข้อมูลแบบขนานโดยทั่วไปแล้ว Wu-Manber ช่วยให้การจับคู่ได้อย่างรวดเร็วและมีความต้องการหน่วยความจำขนาดเล็กน้อย ขณะที่ Aho-Corasick ช่วยให้เวลาค้นหาได้เร็วกว่า แต่ต้องใช้หน่วยความจำเพิ่มขึ้นในการจัดเก็บโครงสร้างข้อมูลที่จำเป็น ซึ่งทั้งสองอัลกอริทึมมีอยู่ในรุ่นปัจจุบันของ Snort

ตารางที่ 2 เปรียบเทียบเทคนิค IDS และ IPS สำหรับ snort

Ref.	System	Category	Type or Approach	Signature Detection	Signature Prevention	Anomaly Detection	Anomaly Prevention	Technique	Advantages	Disadvantages
[10]	IDS	NIDS	Automated Malcode Signature	Yes	No	No	No	Signature base	Automated generate signature	Not capable differentiate two nodes inside the network
[11]	IDS	NIDS	Signature Engineering re-use	Yes	No	No	No	Signature base	Automated re-use signature	Cannot detect anomaly behavior of intrusion novel
[12]	IDS	NIDS	Virtual Honeyports	Yes	No	No	No	Signature base	Automated generate signature for snort	High rate of Risk
[13]	IDS	NIDS	Parallel Technique	Yes	No	No	No	Signature base	Use for high-speed network	Every node have to rule same
[14]	IDS	NIDS	Mining Network Traffic	Yes	No	Yes	No	Signature base	Use for high-speed network	well trained analysis are required
[15]	IDS	NIDS	Distributed data parallel	Yes	No	No	No	Signature base and processor	No false negative	High cost

C. IDS and IPS for snort techniques

IDPS เป็นกระบวนการของการตรวจสอบเหตุการณ์ที่เกิดขึ้นในระบบคอมพิวเตอร์หรือในเครือข่ายคอมพิวเตอร์และวิเคราะห์สำหรับเหตุการณ์ที่จะเป็นการเป็นละเมิดหรือเป็นการคุกคามนโยบายของการรักษาความปลอดภัยคอมพิวเตอร์ การใช้งานที่ยอมรับได้ตามนโยบายหรือมาตรฐานการรักษาความปลอดภัย หรือพยายามที่จะหยุดเหตุการณ์ที่ได้ตรวจพบที่ผิดปกติ ในระบบ IDS และ IPS นั้นจะสามารถแยกออกได้เป็นสองอย่างดังต่อไปนี้

- **Host Based Intrusion Detection and Prevention System (HIDPS)** การรวมกันของระบบ IDS และ IPS ไว้ในเดียวแล้วจะเป็นการรู้จักของ Host-based Intrusion Detection และ Prevention System (HIDPS) โดยการทำงานเกี่ยวข้องกับการประมวลผลข้อมูลบนเครื่องคอมพิวเตอร์ตัวเอง เช่น บันทึกเหตุการณ์และ kernel logs HIDPS ยังสามารถตรวจสอบว่าโปรแกรมที่เข้าถึงทรัพยากรและอาจจะถูกตั้งค่าสถานะใหม่ได้ นอกจากนี้ยังสามารถที่จะตรวจสอบสถานะและการทำงานของระบบ ซึ่งเป็นพื้นฐานของเพื่อที่จะกรองความผิดปกติในระบบ HIDPS โดยปกติจะเก็บฐานข้อมูลเหตุการณ์ของระบบ และยังเก็บข้อมูลการทำงานที่ปกติรวมทั้งพฤติกรรมที่ผิดปกติเกิดขึ้นในระบบ ฐานข้อมูลมีข้อมูลที่สำคัญของระบบ HIDS เกี่ยวกับไฟล์ระบบ พฤติกรรมและเรื่องราวเหตุการณ์ต่างๆ ที่เกิดขึ้นเช่น แอตทริบิวต์ เวลาที่แก้ไข ขนาด เป็นต้น ถ้ามีพฤติกรรมน่าสงสัยหรือผิดปกติเกิดขึ้นแล้วมันจะสร้างระบบเตือนภัย และใช้เวลาบางส่วนเพื่อโต้ตอบกับการคุกคามหรือหากมีการตรวจพบการโจมตี
- **Network-Based Intrusion Detection and Prevention System (NIDPS)** การบุกรุกตรวจจับที่เป็น network-based ระบบจะใช้การวิเคราะห์แพ็กเก็ตในเครือข่าย Network-based Intrusion Detection และ Prevention System (NIDPS) ตรวจจับการจราจรในเครือข่ายขณะที่มัน

เดินทางไปยังโฮสต์ต่างๆ ในระบบเครือข่าย สามารถที่จะวิเคราะห์ได้โดยเฉพาะอย่างยิ่งสำหรับ signature หรือพฤติกรรมที่ผิดปกติหรือผิดปกติ เซ็นเซอร์ที่วางอยู่ในเครือข่ายได้ถูกออกแบบมาเพื่อที่จะตรวจสอบการจราจรในเครือข่าย ถ้ามีพฤติกรรมน่าสงสัยหรือผิดปกติเกิดขึ้นแล้วจะสร้างสัญญาณการแจ้งเตือน และข้อความไปยังระบบคอมพิวเตอร์ส่วนกลางหรือผู้ดูแลระบบ

ในงานวิจัยของ [16] นำเสนอวิธีการใหม่ในการกรองการจราจรของเครือข่ายที่เป็นอันตรายโดยการกำหนดค่า IPSec โดยอัตโนมัติ เมื่อตรวจพบการแจ้งเตือนที่เป็นอันตรายโดยทำงานร่วมกันระหว่าง Snort และ IPSec ซึ่งจะถูกติดตั้งอยู่ใน Windows 2000 Windows XP และ Windows Server 2003 ประการแรกผลการทดลองพิสูจน์วิธีการนี้สามารถที่จะป้องกันและควบคุมข้อมูลรวมทั้งหยุดแพ็คเก็ตที่เป็นอันตรายได้โดยไม่ต้องใช้ไฟร์วอลล์และแก้ไขเพิ่มเติมใดๆ ในระบบ Windows Kernel ขั้นตอนการทำงานขอระบบจะประกอบด้วยทั้งหมด 5 ขั้นตอน ดังต่อไปนี้

- เรียกใช้ cooperation module ทันทีเมื่อแพ็กเก็ตข้อมูลจะถูกจับคู่กับ cooperational rule
- สร้างและเริ่มจับเวลาที่สอดคล้องกันเพื่อควบคุมเวลาที่ถูกต้องของการกรอง IP
- สร้างและติดตั้งตัวกรอง IP ใหม่ ไปที่กฎ cooperational พารามิเตอร์ตัวกรองอาจจะเป็น IP ต้นทางและ IP ปลายทาง port ทิศทางขาเข้าหรือขาออก
- เพิ่มการกรอง IP ใหม่ลงไปในรายการกรอง
- ลบตัวกรอง IP ที่สอดคล้องกันจากรายการกรอง IP เมื่อเวลาที่ตั้งไว้หมด

ในปัจจุบันได้มีวิธีการรวม snort และไฟร์วอลล์ให้มีการทำงานร่วมกัน ซึ่งทำการปรับขยายขีดความสามารถของ snort ทำให้ snort นั้นมีความสามารถและตอบสนองการใช้งานได้ดีขึ้น โดยให้ snort ทำงานในโหมดอินไลน์ โดยที่ [17] ได้นำเสนอเทคนิค support vector machine (SVM) เข้ามาทำงานร่วมกับ snort ให้ทำงานร่วมกับ firewall เพื่อให้ตรวจจับการบุกรุกได้อย่างรวดเร็ว โดยมีการพิจารณาในการเพิ่มประสิทธิระบบป้องกันบุกรุกสองอย่างคือ 1) IPS นั้นจะต้องนำไปใช้ในโหมดอินไลน์ และมีการปรับปรุงบางอย่างใน snort 2) วิธีการที่จะทำให้ snort และกฎของ iptable เพื่อกรองในไฟร์วอลล์

สำหรับการออกแบบของเครือข่ายระบบป้องกันการบุกรุกที่ขึ้นอยู่กับ Snort-inline และไฟร์วอลล์ Netfilter ของ iptablesโดยการตั้งค่าเริ่มต้นของ Snort จะทำการตรวจจับแพ็กเก็ตโดยใช้ libpcap หลังจากติดตั้งการทำงานของ Snort แล้วในแบบอินไลน์ผ่านสคริปต์ rc.firewall เพื่อเปลี่ยนวิธีการใช้ iptables และกำหนดค่าไฟร์วอลล์ ใช้กฎไฟร์วอลล์กำหนดค่า iptables หากใช้ libipq ใน iptables เพื่อจับแพ็กเก็ต จำเป็นที่จะต้องเรียกใช้ comman: configure--enable-iptables

Snort จะใช้ libipq ผ่านซ็อกเก็ต netlink รับแพ็กเก็ตจาก QUEUE ของเคอร์เนล Netfilter จากนั้นจับคู่กฎ ทำการตรวจสอบโดยใช้รูปแบบการจับคู่และการตรวจสอบของสถานะ ถ้าแพ็กเก็ตตรงกับกฎบางอย่าง นั้นคือ Snort ได้ค้นพบการโจมตี แล้วใช้ฟังก์ชั่นของ ipCLset_verdict ในไลบารี libipq สื่อสารกับ Netfilter ผ่านอินเตอร์เฟซ netlink เพื่อที่จะยกเลิกแพ็กเก็ต ข้อมูลการแจ้งเตือนและรูปแบบของ log ถ้าการจับคู่ล้มเหลว Netfilter จัดการภายใต้ rc.firewall และ iptables ที่ได้กำหนดค่าไว้ในกฎไฟร์วอลล์ กระบวนการดังกล่าวจะถูกแสดงใน

งานวิจัยใน [18] ได้นำเสนอระบบป้องการบุกรุกเพื่อป้องกันการโจมตีจากภัยคุกคาม โดยการออกแบบระบบจะใช้ Snort เป็น IDS ทำงานร่วมกับเร้าเตอร์ จุดมุ่งหมายของงานวิจัยนี้มีการออกแบบระบบป้องกันการบุกรุกที่ไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม เพียงแต่นำเร้าเตอร์และเครื่องคอมพิวเตอร์ที่มีในเครือข่ายมาทำงานร่วมกัน ซึ่งระบบนั้นสามารถที่จะเป็นได้ทั้งระบบตรวจจับการบุกรุก (IDS) และระบบป้องกันการบุกรุก (IPS) ลักษณะการทำงานของระบบโดยการสร้างกฎในซิสโก้ ACL สำหรับในการแจ้งเตือนนั้นจะใช้ snort หน้าที่หลักของเร้าเตอร์คือการป้องกันการบุกรุกที่อาจจะเกิดขึ้นในเครือข่าย เมื่อมีการแจ้งเตือนเกิดขึ้นจะถูกบันทึกลงในฐานข้อมูลและจากนั้นจะมีการกำหนดค่าใหม่ลงในกฎของซิสโก้ ACL

สำหรับในงานวิจัยข้อดีและข้อเสียบางอย่าง ข้อดีคือระบบสามารถที่จะทำงานได้ในหลากหลายแพลตฟอร์ม ในการกำหนดค่าต่างๆ ให้กับระบบง่ายและไม่เสียค่าใช้จ่ายสำหรับการดำเนินงานใดๆ เนื่องจากใช้เราเตอร์และคอมพิวเตอร์ที่มีอยู่แล้วในเครือข่าย และไม่จำเป็นต้องมีบุคคลที่มีความรู้เฉพาะทางในการดูแล ข้อเสียคือระบบอาจจะไม่เหมาะสำหรับเครือข่ายที่ใช้ DHCP และการโจมตีที่อยู่ในรูปแบบแพ็คเก็ตเดียวสามารถที่จะบุกรุกเครือข่ายได้

รูปแบบของการโจมตีมีการกระจายอยู่ในเครือข่าย และทำให้การตรวจสอบการบุกรุกทำได้ยาก ในการตรวจจับการบุกรุกจึงจำเป็นที่จะต้องมีส่วนของการทำงานร่วมกันหลายองค์ประกอบ เพื่อตรวจจับการบุกรุกที่มีความแตกต่างกัน ใน [19] ได้นำวิธีการทำเหมืองข้อมูล (Data mining) เข้ามาทำงานร่วมกัน snort ให้เป็นระบบป้องการบุกรุกที่มีประสิทธิภาพ สำหรับการออกแบบระบบนำเครื่องมือ See5 สำหรับ Window XP มาพัฒนาระบบป้องการบุกรุกในเครือข่ายโดยใช้เทคนิคการจัดกลุ่มข้อมูลที่ปกติและไม่ปกติที่ได้จาก traffic ในเครือข่ายร่วมกับเครื่องมือการทำเหมืองข้อมูล See5 สามารถที่จะวิเคราะห์ฐานข้อมูล Snort และตารางการระบุ IP จึงทำให้ถึงวิธีการในการตรวจสอบและป้องกันข้อบกพร่องด้านความปลอดภัยในเครือข่ายปัจจุบันได้ และรวมถึงระบบคอมพิวเตอร์ความผิดปกติที่อาจรวมถึงการโจมตีหลากหลายรูปแบบที่มีอยู่ในเครือข่าย เอาท์พุทจำแนกโดย See5 ในรูปแบบของต้นไม้ตัดสินใจ (decision trees) หรือชุดของ ifthen rules ซึ่งทำให้เข้าใจง่ายกว่ารูปแบบเครือข่ายประสาทเทียม

ภายในระบบนอกจากจะนำระบบตรวจับการบุกรุก snort และการทำเหมืองข้อมูลด้วย see5 โดยมีการจัดหมวดหมู่แล้ว ระบบยังสามารถที่จะรับรู้กิจกรรมของการจราจรในเครือข่ายที่น่าสงสัย โดยมีการจำแนกข้อมูลพฤติกรรมของผู้ใช้ที่เป็นปกติและพฤติกรรมที่ไม่ปกติ และระบบยังเป็นระบบป้องการบุกรุกแบบอัตโนมัติที่สามารถตั้งกฎไฟร์วอลล์เพื่อป้องกันกิจกรรมที่เป็นอันตราย

การควบคุมการใช้งานอินเตรอร์เน็ตโดยมีการกำหนดนโยบายควบคุมการใช้งานเป็นอีกวิธีหนึ่งที่จะทำให้สามารถป้องกันการบุกรุกได้ แต่นโยบายที่ได้กำหนดยังไม่ยืดหยุ่นเพียงพอสำหรับรูปแบบการโจมตีที่มีความหลากหลาย ใน [20] ได้มีการนำเสนอการจัดการควบคุมการใช้งานที่อยู่บนพื้นฐานของการกำหนดนโยบาย (policy-base) และใช้กลไกการควบคุมการรักษาความปลอดภัยของระบบสารสนเทศขององค์กร วิธีการนี้จะขึ้นอยู่กับการปรับค่าแบบไดนามิกของมาตรการรักษาความปลอดภัย โดยการปรับค่าแบบไดนามิกระหว่าง snort signature-base IDPS และ anomaly-based *FireCollaborator* IDS

ประสิทธิภาพของวิธีการปรับแบบไดนามิกนี้นอกจากจะทำให้ลดค่าใช้ในองค์กรแล้ว ยังสามารถที่จะตรวจจับการบุกรุกที่ไม่รู้จักได้อีกด้วย การปรับค่าของ *FireCollaborator* IDS ในระบบทำให้สามารถที่จะตรวจหาการโจมตีแบบ DDos ได้อย่างรวดเร็ว นอกจากนั้นยังมีคุณสมบัติเป็นทั้ง IDS และ IPS อีกด้วย แต่ระบบนี้ก็ยังมีข้อเสียเนื่องจากระบบต้องมีการปรับค่าของ windows size ใน *FireCollaborator* IDS ทำให้มีการแจ้งเตือนที่ผิดพลาดบ่อย ในทางกลับกันการแจ้งเตือนจะเพิ่มขึ้นหรือลดลงจะขึ้นอยู่กับการวิเคราะห์การจราจรในเครือข่ายของผู้ดูแลระบบ

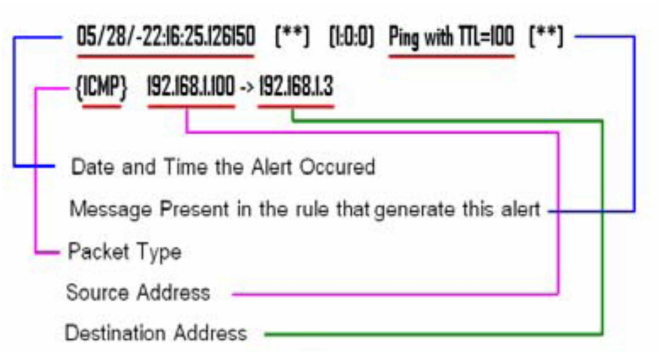
ตารางที่ 3 เปรียบเทียบเทคนิค IDS และ IPS สำหรับ snort

Ref.	System	Category	Type or Approach	Signature Detection	Signature Prevention	Anomaly Detection	Anomaly Prevention	Technique	Advantages	Disadvantages
[16]	IDS and IDPS	NIDPS	cooperation IPsec and firewall	Yes	Yes	No	No	Signature base	Automated to malicious attacks	Use to windows OS only
[17]	IDS and IDPS	NIDPS	SVM	Yes	Yes	No	No	Signature base	Automated to malicious attacks	Unable to detect attack unknown
[18]	IDS and IDPS	HIDPS and NIDPS	ACL generation	Yes	Yes	No	No	Signature base	Multi-platform use	Can not for use DHCP network
[19]	IDS and IDPS	NIDPS	Data mining fusion	Yes	Yes	No	No	Signature base	Automatic Generate rule into firewall	well trained analysis are required
[20]	IDS and IDPS	NIDPS	Application approach	Yes	Yes	Yes	Yes	Signature base and anomaly base	Small cost	High rate of false positive

D. Implement false alert for snort technique

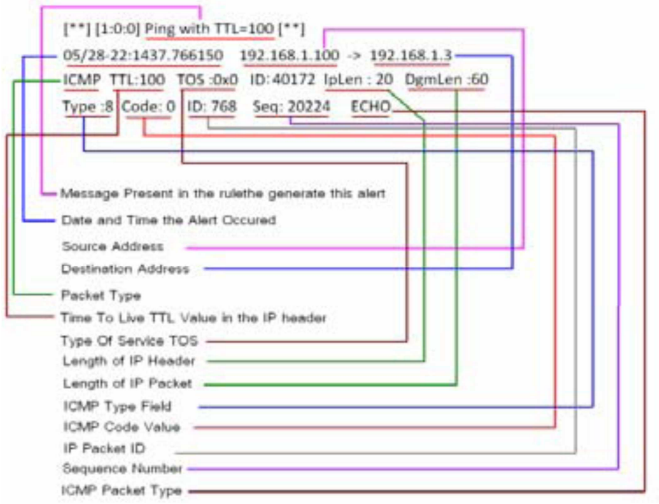
ในขณะที่การพัฒนาอินเตอร์เป็นไปอย่างรวดเร็วและการพัฒนาความเร็วของอินเตอร์มีความเร็วเพิ่มมากขึ้น ระบบตรวจจับการบุกรุกจึงเป็นระบบที่มีความสำคัญในการตรวจจับหาการโจมตีและภัยคุกคามในเครือข่าย ในการพัฒนาระบบตรวจจับการบุกให้มีความรวดเร็วในการตรวจจับ และจะทำให้ระบบตรวจจับการบุกรุกสร้างการแจ้งเตือนผิด (false alert) ให้น้อยลงด้วย นอกจากนี้ระบบยังต้องสามารถที่จะเรียนรู้รูปแบบของการโจมตีแบบใหม่ได้ด้วย ปัญหาที่ทำให้ snort ยังมีข้อบอกบกพร่องและยังส่งสัญญาณแจ้งเตือนผิดพลาด [18] ซึ่งอาจจะมีสาเหตุมาจาก 1) การวางตำแหน่งของ Snort IDS 2) นโยบายขององค์ที่ช่วยให้กิจกรรมที่ทำให้เกิดสัญญาณเตือน IDS 3) องค์กรขาดความความเอาใจใส่ต่อระบบ IDS

เมื่อ IDS จับแพ็คเก็ตที่ติดไวรัสจะสร้างการแจ้งเตือน ที่สอดคล้องกับ snort l สำหรับการแจ้งเตือนสามารถแจ้งเตือนด้วยสองคือโหมดรวดเร็ว (fast mode) และการแจ้งเตือนโหมดเต็มรูปแบบ (full mode) โหมดการแจ้งเตือนแบบรวดเร็วมีองค์ประกอบด้วย time stamp, alert message, IP address ต้นทาง และ IP address ปลายทาง แสดงในรูปที่ 3



รูปที่ 4 โหมดการแจ้งเตือนแบบรวดเร็ว

โหมดแจ้งเตือนเต็มรูปแบบมีส่วนประกอบด้วย เช่น ความยาวของ IP header และความยาวของ IP packet ความแตกต่างระหว่างสองโหมดคือโหมดแสดงข้อความการแจ้งเตือนแบบเต็ม และส่วนหัวของแพ็กเก็ต ในขณะที่การแจ้งเตือนโหมดรวดเร็วจะแสดงเฉพาะข้อความแจ้งเตือนดังแสดงในรูปที่ 4



รูปที่ 5 โหมดการแจ้งเตือนแบบเต็ม

Neural network ได้ถูกนำเสนอโดย [21] เพื่อนำมาแก้ปัญหาของการแจ้งที่ผิด (false alert) ที่เกิดขึ้นกับ snort IDS ภายในระบบได้นำ Multilayer Perceptron (MLP) ด้วยอัลกอริทึม Back-Propagation ใช้ในการจำแนกการโจมตีและเรียนรู้รูปแบบของการโจมที่ไม่รู้จักได้ โดยการทดสอบระบบนั้น สามารถตรวจจับการโจมตีแบบ Dos และแบบ Probe ได้อย่างถูกต้อง แต่สำหรับการโจมตีแบบ U2R นั้นระบบยังมีความบกพร่องอยู่บ้าง

จากปัญหาของ snort ที่มีการแจ้งเตือนที่ผิดพลาดเป็นจำนวนมาก [22] ได้นำวิธีการแก้ปัญหาโดยใช้ระบบเครือข่ายประสาทเทียม neuro-fuzzy ช่วยให้แก้ปัญหาที่เกิดขึ้นจาก false negatives, false positives ได้เลือก NEFCLASS และ JRip เป็นตัวแยกแยะข้อมูลที่ปกติสำหรับ snort กรอบงานที่ได้นำเสนอขึ้นอยู่บนพื้นฐานของเทคนิคปัญญาประดิษฐ์

ในระบบเครือข่ายอินเตอร์เน็ตความน่าเชื่อในการให้บริการเป็นสิ่งจำเป็นและมีรูปแบบของการโจมตีแบบการกระจายปฏิเสธให้บริการ (Distributed denial of service, DDos) [23] ได้นำเสนอการทดสอบระบบตรวจจับการบุกรุกที่มีขนาดใหญ่ที่ขึ้นอยู่กับสถาปัตยกรรมแบบ P2P ในวิธีการใหม่แต่ละIDS จำมีหน้าที่กำกับดูแลเครือข่ายย่อย แต่ละ IDSs เป็น peer ในระบบ peer to peer เป้าหมายเพื่อการทำงานร่วมกัน แต่ละระบบการตรวจสอบแบ่งการแจ้งเตือนให้ IDS อื่น ๆ ข้อมูลที่เกี่ยวกับการจราจรที่น่าสงสัยที่ตรวจพบในเครือข่ายย่อย ไฟล์กำหนดค่าเริ่มต้นนั้นจะมีการสร้างการแจ้งเตือนเป็นจำนวนมากต่อวัน (ขึ้นอยู่กับเครือข่าย) โดยเฉพาะอย่างยิ่งกับข้อความ ICMP และแพ็กเก็ต reassembly ที่เกี่ยวข้องหมดเวลา เพื่อ preprocessor Snort stream4 อย่างไรก็ตาม การแจ้งเตือนบางอย่างเกิดขึ้นบ่อยครั้งสำหรับเหตุการณ์เดียวกันในช่วงเวลาสั้นๆ ของเวลาในไฟล์กฎ Snort การจัดการกระบวนการของการแจ้งเตือนการแลกเปลี่ยนข้อมูลระหว่างเซ็นเซอร์นั้น ใช้วิธีการของ distributed hash table (DHT)

ในเครือข่ายที่ใช้ระบบตรวจจับการบุกรุก (IDS) ที่อยู่บนฐานของ signature snort เพียงอย่างเดียว รูปแบบของการโจมตีนั้นจะถูกบันทึกไว้ในฐานข้อมูลหรือที่เรียกว่า signature แต่ก็มีข้อจำกัดของ snort จะรู้จักแต่การโจมตีที่บันทึกไว้ในฐานข้อมูลเท่านั้น ส่วนระบบเครือข่ายที่ใช้การตรวจจับความผิดปกติ (anomaly base) ระบบมีข้อจำกัดอยู่ที่มีการแจ้งเตือนที่ผิดเป็นจำนวนมาก

ใน [24] จึงได้แก้ไขปัญหาของระบบที่ใช้ signature base และ anomaly base โดยการออกแบบระบบให้มีการแจ้งเตือนที่ผิดพลาดให้น้อยลง ด้วยวิธีการนำข้อดีและข้อเสียของแต่ละระบบมารวมกัน และได้เพิ่มเทคนิคเอนโทรปีเข้าไว้ในระบบเพื่อจัดลำดับความสำคัญของการโจมตีและจัดลำดับความสำคัญของการแจ้งเตือน ซึ่งทำให้ช่วยลดการแจ้งเตือนที่ผิดพลาดได้เป็นจำนวนมาก

การแก้ไขปัญาการแจ้งเตือนที่ผิดพลาดได้ถูกนำเสนออีกครั้งในงานวิจัยของ [25] เป็นวิธีการสร้างภาพ (visualization) ของการแจ้งเตือนข้อมูล IDS ช่วยให้ผู้บริหารเครือข่ายสามารถทำความเข้าใจโครงสร้างของเครือข่ายปัจจุบันได้ ขั้นตอนของการตรวจสอบและตอบสนองความพยายามในการบุกรุก ซึ่งมีประกอบด้วยสามองค์ประกอบหลักอยู่ 3 อย่างคือ 1) ระบบที่สามารถที่จะทำแผนภาพของโครงสร้างเครือข่าย ที่ช่วยให้ผู้ใช้สามารถเรียกดูกลุ่มการแจ้งเตือนได้อย่าง่าย 2) ความสามารถในการจัดกลุ่มของการแจ้งเตือนที่มีความคล้ายคลึงกัน 3) แสดงภาพและทำนายการโจมตีแบบหลายขั้นตอน

การสร้างภาพ (visualization) การบุกรุกของเราและระบบตรวจจับการบุกรุกหลายขั้นซึ่งขึ้นอยู่กับการแจ้งเตือนที่สร้างโดย Snort ด้วยสี่ขั้นตอนของการแจ้งเตือน Snort การจัดกลุ่มและการสร้างกฎความสัมพันธ์ รายละเอียดพฤติกรรมของผู้โจมตีและสุดท้ายการพยากรณ์ การสร้างภาพและการโจมตีหลายขั้น ผู้ดูแลระบบสามารถดูภาพรวมของการจราจรบนเครือข่ายได้อย่างรวดเร็ว และสามารถที่จะดูจำนวนการแจ้งเตือนแต่ละโหนด เมื่อพวกเขาถูกสร้างขึ้นและรายชื่อโดยละเอียดของแต่ละแจ้งเตือน กระบวนการของการวิเคราะห์การแจ้งเตือนถูกสร้างขึ้นโดยใช้รูปแบบการ flocking เพื่อจัดกลุ่มการแจ้งเตือน ข้อมูลเทคนิคการทำเหมืองแร่ (data mining) เพื่อหาการโจมตีหลายขั้นเป็นขั้นตอนที่สำคัญ

ของระบบ ระบบตรวจจับการบุกรุกาขึ้นอยู่กับการแจ้งเตือนที่สร้างโดย Snort และกฎระเบียบที่สร้างความสัมพันธ์ขึ้นโดยอัลกอริทึม Apriori

ตารางที่ 4 เปรียบเทียบเทคนิคt false alert สำหรับ snort

Ref.	System	Category	Type or Approach	Signature Detection	Anomaly Detection	False Negative	False Positive	Technique	Advantages	Disadvantages
[21]	IDS	NIDS	MPL Neural Network	Yes	No	Yes	No	Signature base	Detect known and un known attack	well trained analysis are required
[22]	IDS	NIDS	Neuro-Fuzzy	Yes	No	Yes	Yes	Signature base	Less False Positive and False negative	Cannot detect anomaly behavior of intrusion novel
[23]	IDS	HIDS	Peer to Peer	Yes	No	Yes	No	Signature base and	reliable trusted and efficient	Cannot detect anomaly behavior of intrusion novel
[24]	IDS	NIDS	Alert Ranking Entropy	Yes	Yes	Yes	No	Signature base anomaly base	Can detect anomaly behavior of intrusion	well trained analysis are required
[25]	IDS	NIDS	Data mining Apriori Algorithm	Yes	No	Yes	No	Signature base	Visualization	Cannot detect anomaly behavior of intrusion novel

V. Conclusion

ในปัจจุบันระบบตรวจจับการบุกรุกได้รับดำเนินการวิจัยเป็นอย่างมาก ซึ่งเป็นผลมาจากความเร็วของอินเตอร์เน็ตได้เพิ่มขึ้น ดังนั้นการรักษาความปลอดภัยในเครือข่ายขององค์จึงต้องมีการพัฒนา เพื่อให้รอดพ้นจากภัยคุกคามและการโจมตี ซึ่งรูปแบบของการโจมตีมีการพัฒนาไปอย่างรวดเร็ว ในการพัฒนาระบบตรวจจับการบุกรุก (Intrusion detection system, IDS) ด้วย Snort โดยที่ snort เป็นซอฟต์แวร์ฟรี (Open) และนำมาพัฒนาในระบบ windows และ Linux

การพัฒนาระบบตรวจจับการบุกรุกส่วนใหญ่จะขึ้นอยู่บนพื้นฐานของการตรวจจับความผิดปกติ (anomaly-base) และการตรวจจับเหตุการณ์ที่ผิดปกติ (misuse base) แต่ละระบบก็มีข้อดีและข้อเสียที่แตกต่างกัน การตรวจจับความผิดปกติมีข้อเสียอยู่ที่ระบบจะมีการแจ้งเตือนที่ผิดพลาดเป็นจำนวนมาก และต้องมีการวิเคราะห์การบุกรุกสำหรับกิจกรรมที่เกิดขึ้นในเครือข่าย ในส่วนระบบการตรวจจับเหตุกการณ์ที่ผิดปกติจะมีข้อเสียคือ ระบบไม่สามารถที่จะตรวจจับการโจมตีที่รู้จักได้ จากการสำรวจในงานวิจัยที่ได้นำทั้งสองวิธีนี้รวมเข้าได้กันเพื่อแก้ไขปัญหาของแต่ละวิธี ทำให้ระบบตรวจจับการบุกรุกมีประสิทธิภาพเพิ่มมากขึ้น นอกจากนี้ในส่วนของฮาร์ดแวร์ยังได้นำ snort ไปพัฒนาเพื่อวัดประสิทธิภาพในรูปแบบของอัลกอริทึมรูปแบบการจับคู่ (Pattern matching) เพื่อให้สามารถรองรับการจราจร (traffic) ในเครือข่าย ที่มีความเร็วเพิ่มในปัจจุบัน

Snort นอกจากจะเป็นระบบตรวจจับการบุกรุกแล้วในงานวิจัยยังได้ snort นำมาปรับปรุงประสิทธิภาพให้เป็นระบบป้องกันการบุกรุก (Intrusion Prevention System) ด้วยการนำเทคนิคต่างๆ เช่น การทำเหมืองข้อมูล (Data mining) ระบบเครือข่ายประสาทเทียม (Neuron Network) และ Support vector machine (SVM) นอกจากนั้นระบบที่นำแต่ละเทคนิคมาพัฒนาร่วมกับ snort นั้นยังสามารถที่จะนำไปใช้ร่วมกับอุปกรณ์ป้องกันการบุกรุก เช่น ไฟร์วอลล์ (Firewall) หรือเราเตอร์ อย่างไรก็ตามแต่ปัญหาของ snort ก็ยังได้รับการแก้ไขด้วยการพัฒนาในส่วนของ signature แต่อย่างไรก็ตามปัญหาที่เกิดขึ้นกับ snort ก็ยังเกิดขึ้นอีก เมื่อระบบตรวจจับการบุกรุกในเครือข่ายส่งสัญญาการแจ้งเตือนที่

ผิดพลาด (false positive) เป็นจำนวนมาก และบางระบบมีการโจมตีเกิดขึ้นแต่ระบบตรวจจับการบุกรุกไม่ส่งสัญญานแจ้งเตือน (false negative) ปัญหานี้ก็ได้มีงานวิจัยเพื่อลดปัญหาเช่นกัน

VI. Future Work

ในอนาคตเราจะทำการสำรวจเทคนิคต่างๆ ที่นำมาพัฒนาปรับปรุงประสิทธิภาพให้ snort ดียิ่งขึ้น เช่น ระบบตรวจจับการบุกรุกแบบไฮบริด (Hybrid Intrusion Detection System) ระบบตรวจจับการบุกรุกแบบขนาน (Parallel Intrusion Detection System) เป็นต้น

Reference

[1] Zhimin Zhou, Chen Zhongwen, Zhou Tiecheng and Guan Xiaohui, "The study on network intrusion detection system of Snort," in Proc. 2nd International Conference on Networking and Digital Society (ICNDS), 2010, vol.2, no., pp.194-196.

[2] M. Ali Aydın, A. Halim Zaim and K. Gokhan Ceylan, "A hybrid intrusion detection system design for computer network security", Computers and Electrical Engineering 35,2009,p.517–526.

[3] K. Salah and A. Kahtani, "Improving snort performance under linux," Communications, IET , vol.3, no.12, pp.1883-1895,2009.

[4] S.O Al-Mamory, A. Hamid, A. Abdul-Razak and Z. Falah, "String matching enhancement for snort IDS," in Proc. 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), 2010, vol., no., pp.1020-1023.

[5] Yan Sun, V.C. Valgenti, and Min Sik Kim, "NFA-Based Pattern Matching for Deep Packet Inspection," Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN), 2011 , vol., no., pp.1-6.

[6] K. Namjoshi and G. Narlikar, "Robust and Fast Pattern Matching for Intrusion Detection," INFOCOM, 2010 Proceedings IEEE , vol., no., pp.1-9, 14-19 March 2010

[7] M. Aldwairi and D. Alansari, "Exscind: Fast pattern matching for intrusion detection using exclusion and inclusion filters," in Proc. 7th International Conference on Next Generation Web Services Practices (NWeSP), 2011 , vol., no., pp.24-30.

[8] S. Anithakumari and D. Chithraprasad, "An Efficient Pattern Matching Algorithm for Intrusion Detection Systems," Advance Computing Conference, 2009. IACC 2009. IEEE International , vol., no., pp.223-227.

[9] Jing Yu, Bo Yang, Ruiyuan Sun and Zhenxiang Chen; , "FPGA-Based Parallel Pattern Matching Algorithm for Network Intrusion Detection System," International Conference on Multimedia Information Networking and Security, 2009. MINES '09., vol.2, no., pp.458-461, 18-20 Nov. 2009.

[10] H. Rajabi, M.N. Marsono and A. Monemi, "A framework for automated malcode signatures generation," IEEE Student Conference on Research and Development (SCOReD), 2010, vol., no., pp.72-76.

[11] S. Schmerl, H. Koenig, U. Flegel, M. Meier and R. Rietz, "Systematic Signature Engineering by Re-use of Snort Signatures," Computer Security Applications Conference, 2008. ACSAC 2008. Annual , vol., no., pp.23-32.

[12] Xinyu Tang, "The Generation of Attack Signatures Based on Virtual Honeypots," International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), 2010, vol., no., pp.435-439.

[13] F.I. Shiri, B. Shanmugam and N.B. Idris, "A parallel technique for improving the performance of signature-based network intrusion detection system," in Proc. 3rd IEEE International Conference on Communication Software and Networks (ICCSN), 2011, vol., no., pp.692-696

[14] Hao Tu, Zhitang Li and Bin Liu, "Mining Network Traffic for Worm Signature Extraction," in Proc. Fifth International Conference on Fuzzy Systems and Knowledge Discovery, 2008. FSKD '08., vol.4, no., pp.327-331.

[15] Christopher V. Kopek, Errin W. Fulp and Patrick S.Wheeler, "Distributed Data Parallel Techniques for Content-Matching Intrusion Detection Systems," Military Communications IEEE Conference, 2007. MILCOM 2007, vol., no., pp.1-7.

[16] Jiqiang Zhai and Yining Xie, "Researh on Network Intrusion Prevention System Based on Snort," in Proc. *6th International Forum on Strategic Technology (IFOST), 2011*, vol.2, no., pp.1133-1136.

[17] Hui Li and Dihua Liu, "Research on intelligent intrusion prevention system based on Snort," in Proc. *International Conference on Computer Mechatronics, Control and Electronic Engineering (CMCE), 2010*, vol.1, no., pp.251-253.

[18] M. Naveed, S. un Nihar and M. Inayatullah Babar, "Network intrusion prevention by configuring ACLs on the routers, based on snort IDS alerts," in Proc. *6th International Conference on Emerging Technologies (ICET), 2010*, vol., no., pp.234-239, 18-19 Oct. 2010

[19] M. Beheshti, J. Han, K. Kowalski, J. Ortiz, J. Tomelden, and D. Alvillar, "Packet information collection and transformation for network intrusion detection and prevention," in Proc. *International Symposium on Telecommunications, 2008. IST 2008.*, vol., no., pp.42-48.

[20] K. Alsubhi, I. Aib, J. Francois and R. Boutaba, "Policy-Based Security Configuration Management, Application to Intrusion Detection and Prevention," in Proc. *IEEE International Conference on Communications, 2009. ICC '09.*, vol., no., pp.1-6.

[21] P. Barapatre, N.Z. Tarapore, S.G. Pukale and M.L. Dhore, "Training MLP neural network to reduce false alerts in IDS," in Proc. International Conference on Computing, Communication and Networking, 2008. ICCCn 2008., vol., no., pp.1-7.

[22] M. Naveed, S. un Nihar, and M. Inayatullah Babar, "Network intrusion prevention by configuring ACLs on the routers, based on snort IDS alerts," in Proc. 6th International Conference on Emerging Technologies (ICET), 2010, vol., no., pp.234-239.

[23] R. Khatoun, G.Doyen, D. Gaiti, R. Saad, and A. Serhrouchni, "Decentralized Alerts Correlation Approach for DDoS Intrusion Detection," New Technologies, Mobility and Security, 2008. NTMS '08. , vol., no., pp.1-5.

[24] S. Kumar and R.C. Joshi, "Design and implementation of IDS using Snort, Entropy and alert ranking system," Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on , vol., no., pp.264-268.

[25] W. Li Yang; Gasior, R. Katipally and Xiaohui Cui, "Alerts Analysis and Visualization in Network-based Intrusion Detection Systems," Social Computing (SocialCom), 2010 IEEE Second International Conference on , vol., no., pp.785-790.