The 5th National Conference on Computing and Information Technology

NCCIT 2009

King Mongkut's University of Technology North Bangkok
May 22-23, 2009

ISBN : 978-974-19-3309-9

ระบบป้องกันผู้บุกรุกเครือข่ายอัตโนมัติโดยใช้อัลกอริทึมชิฟท์แมกซ์

Automatic network intrusion prevention system using shift max algorithms

ศุภกร ฤกษ์ดิถีพร, จตุพร สุจริตธรรม, สุรเดช บุญลือ

ภาควิชาวิทยาการคอมพิวเตอร์

คณะเทคโนโลยีสารสนเทศ วิทยาลัยนอร์ทกรุงเทพ

creativealone@hotmail.com, subzero_stjohn@hotmail.com, bosuradej@northbkk.ac.th

บทคัดย่อ

โครงงานวิจัยนี้ มีวัตถุประสงค์เพื่อพัฒนาระบบป้องกันผู้บุกรุกเครือข่ายอัตโนมัติ ลักษณะของกระบวนการทำงานแบ่งเป็น 2 ส่วนหลักๆ ส่วนงานแรกจะเป็นส่วนของการตรวจจับแพ็กเก็ตทั้งหมดที่ผ่านเข้ามายังเครื่องแม่ข่ายที่ติดตั้งระบบไว้แล้วนำข้อมูลที่ได้ไปวิเคราะห์รูปแบบการโจมตีด้วยอัลกอริทึม Shift Max และส่วนงานที่สองเป็นส่วนของการป้องกันการบุกรุกการปิดช่องทางที่ส่งผ่านข้อมูล ซึ่งทั้งสองส่วนนี้จะมีการแสดงผลทางเว็บเบสแอพพลิเคชัน ส่วนเครื่องมือที่ใช้ในการพัฒนาระบบนี้ ได้แก่ สนอร์ท, สนอร์ท-แซม, แอลแดบ และภาษาพีเอชพี หลังจากพัฒนาแล้วจะมีการทดสอบระบบด้วยวิธีการแบล็คบอคซ์ โดยใช้กลุ่มผู้เชี่ยวชาญทางด้านจัดการเครือข่ายคอมพิวเตอร์ ซึ่งจะประเมินหาค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐาน ผลการทดสอบพบว่าค่าเฉลี่ยของกลุ่มผู้เชี่ยวชาญอยู่ในระดับ 3.78 (SD = 0.37) ดังนั้นแสดงให้เห็นว่าระบบที่ได้พัฒนานี้มีคุณภาพในระดับดีสามารถนำไปใช้งานได้

คำสำคัญ: ป้องกันผู้บุกรุกเครือข่าย, อัลกอริทึมชิฟท์แมกซ์

Abstract

The project aims to develop of automatic network intrusion prevention system. The feature of the system is divided into two parts. Part one, to detect all incoming packets to the main network which the system is installed, then brings the data to analyze attack types with Shift Max Algorithm. Part two, to protect the intruders by protecting the penetrate entries that transmit the data. The both of the above ways will indicate via the web base application and the system tools are such as Snort, Snortsam, LDAP and PHP language. After the development, there will be a system test using a black box by the expert group of computer network managements. The evaluation showed that the mean of the expert group of computer network managements was 3.78 (SD = 0.37). The result is that the system has developed to a good quality.

Keyword: Network Intrusion, Shift Max Algorithm

1. ความสำคัญของปัญหา

ปัญหาการบุกรุกเครือข่ายคอมพิวเตอร์นั้นเป็นปัญหาสำคัญที่ต้องการการแก้ไขอย่างเร่งด่วน เนื่องจากรูปแบบการดำเนินชีวิตในปัจจุบันนั้น จำเป็นจะต้องพึ่งพาอาศัยเครือข่ายคอมพิวเตอร์เป็นอย่างมาก เพื่ออำนวยความสะดวกในการติดต่อสื่อสาร ทั้งในด้านการดำเนินธุรกิจ การทำงาน การใช้ชีวิตประจำวัน หรือเพื่อความบันเทิงในรูปแบบต่าง ๆ และมีแนวโน้มว่าจะยิ่งมีความจำเป็นเพิ่มมากขึ้นในอนาคต ซึ่งดูได้จากจำนวนผู้ใช้งานเครือข่ายที่เพิ่มมากขึ้นตลอดเวลา

การพัฒนารูปแบบการให้บริการและโปรแกรมใหม่ ๆ เกิดขึ้นอย่างสม่ำเสมอ เทคโนโลยีด้านเครือข่ายได้รับการพัฒนาให้มีประสิทธิภาพและความเร็วสูงขึ้นเรื่อยๆ รวมทั้งการใช้งานเครือข่ายหรือการเข้าถึงเครือข่ายก็ได้รับการพัฒนาให้มีรูปแบบที่หลากหลายขึ้น แต่นั่นก็เท่ากับเปิดโอกาสให้ผู้บุกรุกมีช่องทางในการโจมตีเครือข่ายได้มากขึ้น การโจมตีสามารถทำได้เร็วขึ้นและความเสียหายที่เกิดจากการโจมตีก็รุนแรงขึ้น อีกทั้งยังทำให้การตรวจสอบและป้องกันการบุกรุกการโจมตีทำได้ยากขึ้นด้วย เพราะเมื่อปริมาณการใช้งานเครือข่ายสูงขึ้น ทำให้ข้อมูลที่

จะต้องตรวจสอบก็มีเพิ่มมากขึ้นด้วย และที่สำคัญก็คือ ไม่ใช่แค่เพียงระบบเครือข่ายเท่านั้นที่ได้รับการพัฒนา แต่วิธีการหรือรูปแบบการโจมตีผ่านเครือข่ายก็ได้รับการพัฒนาอยู่เสมอด้วยเช่นกัน [2]

ระบบตรวจจับหาการบุกรุกถูกนำมาใช้เพื่อเพิ่มสมรรถนะให้แก่ระบบรักษาความปลอดภัยและเพิ่มความต้านทานต่อการโจมตีภายนอกระบบ [1] โดยทำหน้าที่ค้นหาสัญญาณที่บ่งบอกถึงการบุกรุก บอกถึงการโจมตีที่เกิดขึ้น และบอกถึงกิจกรรมที่เป็นเครื่องหมายแสดงถึงการโจมตีร้ายแรง ระบบตรวจหาการบุกรุกที่ดีควรมีข้อผิดพลาดในการทำงานเพียงเล็กน้อย ตัวอย่างเช่น การแจ้งเตือนเกิดความเป็นจริง หรือการไม่แจ้งเตือนเมื่อถูกโจมตี ซึ่งปัจจัยภายนอกมีผลต่อการทำงานของระบบตรวจหาการบุกรุกเครือข่ายได้แก่ เทคนิคที่ใช้ในการตรวจหาและสภาพแวดล้อมของระบบตรวจหา เช่น ปริมาณการโจมตี ปริมาณข้อมูลในเครือข่าย จำนวนผู้ใช้งาน ความหลากหลายของการโจมตี เป็นต้น ซึ่งปัจจัยเหล่านี้อาจส่งผลกระทบให้ระบบการตรวจหาการบุกรุกที่เคยทำงานได้ดีในระบบหนึ่งประสบความล้มเหลวในการตรวจหาการบุกรุกในอีกระบบหนึ่ง ดังนั้นการเลือกใช้ระบบตรวจหาการบุกรุกที่มีประสิทธิภาพ จึงมีผลต่อความถูกต้องในการตรวจหาและช่วยให้ตรวจพบการบุกรุกก่อนที่ผู้บุกรุกจะโจมตีสำเร็จ

ระบบตรวจจับการบุกรุก เป็นเครื่องมือที่ใช้สำหรับตรวจจับความพยายามบุกรุกเครือข่าย โดยระบบจะแจ้งเตือนผู้ดูแลระบบเมื่อมีการบุกรุกหรือมีการพยายามที่จะบุกรุกเครือข่าย หน้าที่หลัก คือ แจ้งเตือนการเข้าใช้เครือข่ายที่ผิดปกติ โดยขึ้นอยู่กับสภาวะของระบบขณะนั้น และบางครั้งไม่สามารถตรวจจับการบุกรุกได้ เนื่องจากมีปัญหาเรื่องการทำงานกับสภาวะแวดล้อมสวิตช์ชิง (switching) เนื่องจาก Traffic ที่วิ่งบนเครือข่ายไม่ได้กระจายทั่วไปทำให้ยากต่อการตรวจจับ หรือในกรณีใช้แบบฐานข้อมูล (signature based IDS) รูปแบบต่าง ๆ ที่บุกรุกไม่ได้ทำการปรับปรุงอยู่เสมอ ทำให้ไม่สามารถตรวจจับการบุกรุกแบบใหม่ๆ ได้ และยังเจอกับเทคนิคใหม่ ๆ หรือ ซับซ้อนของแฮกเกอร์ โดยจะยิงแพ็กเก็ตแปลกๆ ที่มีการดัดแปลงส่วนหัว เพื่อทำการหลบเลี่ยงการทำงานของระบบตรวจจับการบุกรุก แต่โดยส่วนใหญ่แล้ว IDS ไม่ได้ทำการป้องกันการบุกรุกแบบทันที

ดังนั้นทีมผู้วิจัยจึงมีแนวคิดในการพัฒนาระบบให้มีประสิทธิภาพสูงมากยิ่งขึ้น โดยคำนึงถึงความสามารถตรวจจับและหยุดการบุกรุกของผู้ที่ไม่ประสงค์ดีได้ทันที และจะมีการปรับปรุงฐานข้อมูลได้อัตโนมัติผ่านเซิร์ฟเวอร์ที่กลุ่มผู้วิจัยตั้งไว้อย่างสม่ำเสมอ ซึ่งฐานข้อมูลเหล่านี้จะทำงานภายใต้การจับคู่การคิดวิเคราะห์หลายแบบแผน (Multi-pattern string matching algorithm) ด้วยวิธี SMA (Shift Max Algorithm) ที่มีความสามารถสืบค้นได้รวดเร็วกว่าวิธีอื่นทั่วไป[8] และพบว่าเมื่อจำนวนแบบ (The pattern set number) ของการโจมตีมีเพิ่มขึ้นจะส่งผลกระทบต่อการทำงานของระบบเพียงเล็กน้อยเท่านั้น

2. วัตถุประสงค์

เพื่อพัฒนาระบบป้องกันผู้บุกรุกเครือข่ายอัตโนมัติโดยใช้การจับคู่การคิดวิเคราะห์หลายแบบแผน ด้วยอัลกอริทึม Shift Max ที่สามารถทำงานทั้งการตรวจจับและป้องกันผู้บุกรุกเครือข่ายในเวลาเดียวกัน อีกทั้งยังสามารถเพิ่มเติมกฎและเงื่อนไขการตรวจจับได้ในภายหลัง

3. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

3.1 ทฤษฎีทางด้านเครือข่ายคอมพิวเตอร์

3.1.1 ระบบตรวจจับการบุกรุก

(Intrusion Detection System: IDS)

เป็นส่วนหนึ่งของการรักษาความปลอดภัยบน เครือข่ายคอมพิวเตอร์ ซึ่งเป็นระบบที่ใช้ในการตรวจจับการใช้งาน และความพยายามในการใช้งานคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ซึ่งขัดกับข้อบังคับและเจตจำนงค์ของการใช้งาน ซึ่งส่งผลต่อความปลอดภัยของระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ 3 ประการ คือ การป้องกันข้อมูลจากผู้ที่ไม่ได้สิทธิในการเข้าถึง, การป้องกันไม่ให้ผู้ไม่มีสิทธิแก้ไขข้อมูล และการป้องกันไม่ให้ผู้ที่ไม่มีสิทธิทำข้อมูลเสียหายจนไม่สามารถให้บริการข้อมูลเหล่านั้น แบ่งเป็น

1) ระบบตรวจจับการบุกรุกในระดับเครือข่าย (Network-Based Intrusion Detection System) ทำการวิเคราะห์กิจกรรมต่างๆ ทีเกิดขึ้นบนระบบเครือข่ายคอมพิวเตอร์ว่าเป็น การบุกรุกหรือพยายามในการบุกรุก หรือไม่โดยการอาศัยค่าต่างๆ เช่น ปริมาณข้อมูลบนเครือข่ายลักษณะของ แพ็กเก็ต ที่ส่งมาใน

เครือข่าย การทำงานของระบบตรวจจับการบุกรุกในเครือข่าย มีลักษณะเป็นเรียลไทม์ เมื่อมีผู้บุกรุกเข้ามาจะสามารถรู้และร้องเตือน หรือกระทำเหตุการณ์ใดๆ ได้ทันที

2) ระบบตรวจจับการบุกรุกในระดับโฮสต์ (Host Based Intrusion Detection System) ระบบนี้จะทำงานอยู่บนเครื่องคอมพิวเตอร์แต่ละเครื่อง โดยตรวจสอบกิจกรรมที่เกิดขึ้นว่าเป็นกิจกรรมที่มีความพยายามในการบุกรุกหรือไม่ มีลักษณะเป็นเรียลไทม์ เช่นเดียวกันกับแบบแรก

3) ระบบค้นหาจุดอ่อน (Vulnerability Scanners) จะช่วยในการตรวจสอบระบบว่ามีความเสี่ยงต่อการบุกรุกมาแค่ไหน โดยจะทำหน้าที่ในการหาช่องโหว่ของระบบ แตกต่างจากเครือข่าย และ ระบบตรวจจับการบุกรุกเครือข่าย ตรงที่ไม่ได้ทำงานแบบเรียลไทม์แต่จะทำงานเป็นเวลาตามคำสั่ง

3.1.2 ระบบป้องกันการบุกรุก

(Intrusion Prevention System: IPS)

IPS = IDS+ Active Response หมายถึง IPS สามารถป้องกันการบุกรุกและหยุดการบุกรุกได้ทันท่วงที แบ่งออกเป็น 2 ช่วงอายุ (Generations) ดังต่อไปนี้

1) ช่วงอายุที่1 การหยุดการบุกรุกทำได้โดยการส่งสัญญาณทีซีพี รีเซต จัดการกับ ทีซีพี เซสชั่น ที่ IPS คิดว่าเป็นการบุกรุกหรืออาจจะเข้าไปเปลี่ยนแปลงแก้ไข ข้อกำหนด (Rules Based) ในไฟร์วอลล์แบบอัตโนมัติ ซึ่งบางครั้งอาจเกิดความผิดพลาดได้

2) ช่วงอายุที่2 ได้มีการปรับปรุงให้เป็นลักษณะการวิเคราะห์เครือข่ายอย่างชาญฉลาด (Intelligent Network Element) ซึ่งสามารถรู้จักเทคนิคของพวกแฮกเกอร์ โดยมีการวิเคราะห์ไอพีแพ็กเก็ตทราฟฟิกอย่างละเอียด การนำเทคโนโลยีขั้นสูงในการวิเคราะห์ข้อมูล เช่น โครงข่ายประสาทเทียม และฟัซซี่ลอจิก ซึ่งจะทำให้ลดปัญหาความผิดพลาดในด้านบวก และ (Fault Positive) ความผิดพลาดในด้านลบ (Fault Negative) ลงได้อย่างมาก เนื่องจาก IPS ใช้หลักการเปรียบเทียบข้อมูลแปลกปลอมจากการปรับแต่งไอพีแพ็กเก็ตโดยใช้มาตรฐานอาร์เอฟซี (RFC) ของ ไออีทีเอฟ (IETF) ในการตัดสินใจ ทำให้ IPS บางรุ่น สามารถป้องกันการโจมตีแบบ DoS หรือ DDoS Attack ได้ด้วย

3.2 เทคนิคการตรวจจับการบุกรุก

3.2.1 สถาปัตยกรรมเครือข่ายความเร็วสูง

ปัจจุบัน network มีการพัฒนาหรือเคลื่อนที่ไปอย่างรวดเร็ว และ Ethernet เป็นอีกระบบหนึ่งที่ได้รับความนิยมมาก เนื่องจากสามารถที่จะดูแลและควบคุมได้ง่าย วิธีเข้าหรือขั้นตอนในการเข้าสู่ระบบ network-based intrusion detection นั้นมีความจำเป็นอย่างยิ่งที่จะต้องจัดการกับเครือข่ายที่เพิ่มขึ้น ซึ่งขณะนี้มี 2 วิธีหลักในการเพิ่มประสิทธิภาพการทำงานของ NIDSs [8]

1) วิธีแรกคือการพัฒนา (single detection engine) โดยการเพิ่มประสิทธิภาพของตัว detection algorithm หรือการใช้ dedicated operating platforms.

2) วิธีที่สองขึ้นอยู่กับ load-balancing devices ที่สามารถแยก hi-speed network traffic load จาก multiple intrusion detection engines

ในระบบเครือข่ายความเร็วสูง HPMonitor ใช้วิธีการที่สามารถวัดและคำนวณได้โดยตั้งอยู่บนพื้นฐานของ a load balancing device

ตามรูปที่ 1 ข้อมูลที่อยู่บน hi-speed network สามารถแบ่งแยกออกเป็นสายย่อยๆ แต่ละสายก็จะมีตัวเลขที่แตกต่างกัน กระจายตัว analyzer ออกเป็นตัวๆ แต่ละตัว จะรับผิดชอบเฉพาะ subset ของตัวเองเท่านั้น

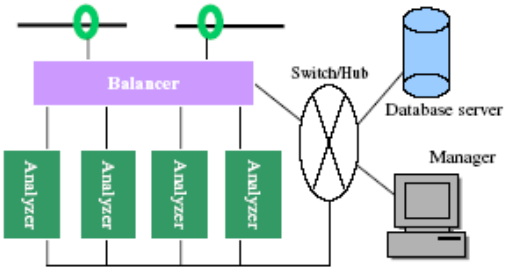


Figure 1 The architecture of HPMonitor.

รูปที่ 1 สถาปัตยกรรมของ HPMonitor

ซึ่งในหนึ่งระบบจะประกอบไปด้วย 4 อุปกรณ์ ดังนี้ balancer, analyzers, manager และ database

1) Balancer มีหน้าที่ในการเก็บ network packet และส่งผ่าน packet นี้ไปยัง analyzer ถัดไปซึ่งตัว balancer จะทำให้

ข้อมูลที่ได้ไหลไปรวมกันยัง multiple analyzer และลำเลียง load balancing ดังกล่าวผ่านตัว analyzer แต่ละตัว

2) Analyzer มีหน้าที่ในการตัดสินใจในกรณีที่เกิดมีการรบกวนเกิดขึ้นในระบบ ซึ่ง analyzer จะรับ packet มาจาก balancer output ที่เกิดจาก analyzer จะส่งสัญญาณเตือนหากมีการรบกวนเกิดขึ้นในระบบรวมไปถึงการรายงานผลที่เกิดขึ้นจากการรบกวนดังกล่าวด้วย ซึ่ง analyzer นั้นจะส่งข้อมูลที่ได้ไปยัง manager หรือส่งไปยัง database

3) Manager สามารถทำให้ user ดูภาพรวมของระบบและยังสามารถควบคุมพฤติกรรมสภาวการณ์ในระบบได้ด้วย

4) Database เป็นที่เก็บข้อมูลทุกครั้งที่มีการเตือนเมื่อมีเรื่องรบกวนเกิดขึ้น ตัว parameter ต่างๆ ซึ่งสามารถจะรื้อหรือกู้คืนได้ในภายหลัง

3.2.2 การจับคู่การคิดวิเคราะห์หลายแบบแผน

(Multi-pattern string matching algorithm)

กลไกในการป้องกันของ Analyzer ใน HPMonitor นั้นขึ้นอยู่กับ string matching ดังนั้นประสิทธิภาพของตัว string matching algorithm นั้นจึงมีความสำคัญอย่างยิ่งต่อการทำงานของระบบ ดังนั้น Wenbao Jiang และคณะ[8] จึงได้ทำการออกแบบ string matching algorithm ขึ้นมาใหม่ เรียกว่า SMA (Shift Max Algorithm) หลักการของวิธีนี้เป็นการนำข้อดีของ BM algorithm มาใช้และขยายผล

SMA algorithm จะทำการเปรียบเทียบรูปแบบใน matching window จากขวาไปซ้ายและเพิ่มความยาวของ suffix ในขณะเดียวกันก็ต้องมีการเปรียบเทียบรูปแบบใน prefix tree จากขวาไปซ้ายด้วยเช่นกัน ดังนั้นจึงต้องมีการตีค่าย้อนกลับตัว prefix ซึ่งหลักการย้อนกลับกำหนดให้ ถ้า $p = x_1, x_2, ..., x_k$ แล้ว $p' = x_k, x_{k-1}, ..., x_1$ แล้วกำหนดให้ prefix ทั้งหมดใน pattern นั้นกลายย้อนกับมาเป็น suffix ของ pattern นั้นแทน จะได้เป็น prefix ของ pattern set p กลายมาเป็น suffix ของ pattern set p' ทำให้สามารถ match (เทียบ) กับ text window $\{y_i, y_{i+1}, ..., y_{i+m-1}\}^r$, $\{y_{i+m-1}, y_{i+m-2}, ., y_i\}$ สวนทางกับ suffix tree เพื่อที่จะได้หา suffix v ที่ยาวที่สุด (longest suffix)

Algorithm นี้ประกอบไปด้วย 2 ส่วน ในส่วนแรกคือ suffix tree ที่สร้างมาจากค่าย้อนกลับของตัว pattern set p' เพื่อให้การสืบค้น text เป็นไปอย่างรวดเร็วตัว automaton set จึงเปรียบเสมือนตัวแทนของ suffix tree ในส่วนที่ 2 text string นำมาประยุกต์เพื่อใช้กับ suffix automaton ในทุกๆ matching window ตัว suffix automaton จะเป็นเป็น suffix ที่ยาวที่สุด (longest suffix) v ของ text window string และ $shift = m - |v|$ สัญญาณของ automaton นั้นไม่ว่าอย่างไรก็ตามสามารถตรวจเจอ และเทียบลงได้กับ pattern นั้นๆ

ในระบบสุ่ม หลายครั้งที่ลอง match หรือเทียบตัว sub string v, ดังนั้น $|v|$ ค่าที่ออกมาจึงน้อยโดยปกติซึ่งเป็น long shift ค่าของ shift จะถูกกระทบโดย ค่า M_{min} ซึ่งมีค่าความยาวของ pattern ที่สั้นที่สุด ค่าของ shift ไม่สามารถจะมากไปกว่า M_{min} ได้ ถ้าไม่อย่างนั้นแล้วอาจจะทำให้เกิดการผิดพลาดเกิดขึ้น

3.3 งานวิจัยที่เกี่ยวข้อง

Top Layer networks [7] ได้เสนอ IDS load-balancing device เพื่อช่วยในการเก็บหรือรักษา application level sessions (application ระดับต่างๆ) ซึ่งการทำงานของ network (network traffic) จะถูกกระจายหรือทำให้แยกออกจากกันตาม session (กลุ่ม) แล้วถูกส่งไปที่ตัว intrusion detection sensors อื่น ถึงแม้ว่าหลักการของ Top layer network จะได้ผลและสอดคล้องกับการจัดการระบบการขนส่ง/เดินทางในเครือข่ายได้เป็นอย่างดีทั้งในเรื่องประเภทและแหล่งที่มาแต่ก็ยังขาดกลไกในการขับเคลื่อนตัว load balancing อยู่ Kruegel [6] เสนอรูปแบบการสร้าง partition เพื่อนำไปสู่การวิเคราะห์ความปลอดภัยในระบบเครือข่ายซึ่งจะรองรับ in-depth และแสดงสภาวะการทำงานของ intrusion detection บน high-speed links รูปแบบนี้ศูนย์กลางจะอยู่ที่ ตัว slicing mechanism ซึ่งจะทำหน้าที่ในการแยกข้อมูลต่างๆ ออกเป็น subset ย่อย แต่อย่างไรก็ตามวิธีของ Kruegel นั้นก็ยังมีโครงสร้างที่ซับซ้อนเกินไป

BM algorithm [4] นับได้ว่าเป็น algorithm ที่มีชื่อเสียงเป็นอย่างมากเพื่อที่จะทำให้ specific pattern string สามารถเข้าไปใน string text ได้ BM algorithm กฎ Heuristic rule (การแก้ปัญหาที่ไม่มีกฎหรือรูปแบบที่ตายตัวแน่นอน) คือการที่มองข้ามข้อเปรียบเทียบอื่นๆ แล้วตรวจสอบ pattern string ใน text จาก ซ้ายไปขวา ใน matching window ตัวtext และ the pattern string จะวางเป็นแนวเส้นตรง ซึ่ง Character comparison (ลักษณะเปรียบเทียบ) จะสร้างจากขวาไปซ้าย โดย

เริ่มจากตอนท้ายของ pattern BM ถือได้ว่าเป็นหนึ่ง algorithm ในจำนวน algorithm อื่นๆ ที่มีประสิทธิภาพในการค้นหา single pattern string ใน text และใช้โดย snort ได้อย่างดีและมีประสิทธิภาพ อย่างไรก็ตามการทำงานของ BM ก็ยังไม่เร็วพอในกรณีที่เป็น Multi-pattern เนื่องจาก BM ต้องการค้นหาแยกเป็นแต่ละ pattern ไป โดยกำหนดให้จำนวนครั้งในการค้นหาเป็น O(kn) โดยให้ k เป็นจำนวน pattern

Aho และ Corasick [3]ได้คิดค้นและออกแบบ multi-patterns string matching algorithm ที่สามารถจะสอบเหตุการณ์และจำนวนของ pattern ที่เกิดขึ้นใน text ได้โดย algorithm แรกกำหนด ให้ multi-pattern เป็นการตัวสร้างหรือตัวบอก finite state-matching automaton และ ใช้ automaton เพียงตัวเดียวในการค้นหา the text และหา pattern อื่นที่อยู่ใน text ด้วย ด้วย Algorithm ของ AC นี้ความซับซ้อนอยู่ที่ O(n) เนื่องจากใน AC algorithm ได้มีการป้อน the character ลงไปใน text หลายๆ ครั้ง ทำให้ไม่สามารถจะมองข้ามตัวเปรียบเทียบตัวอื่นๆ ไปได้เลยดังนั้นในทางปฏิบัติ AC algorithm ยังไม่นับว่าเป็น algorithm ที่ดีที่สุด

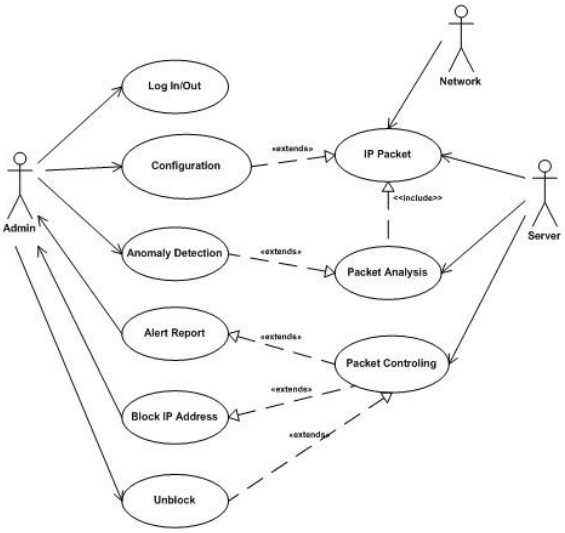
ส่วน CW algorithm [5] ขั้นตอนแรกคือการสร้าง searching tree โดยอาศัย the pattern set จากนั้นก็คล้ายของ BM algorithm คือ CW จะเข้าไปใน text และ ค้นหา the pattern โดยใช้ searching tree หรืออีกทางหนึ่งจะเรียกว่า CW algorithm เป็นการนำ BM algorithm มาขยายผลนั่นเอง โดยกำหนดให้ความซับซ้อนของเวลา (time complexity) เท่ากับ O(n) ซึ่งทำให้สามารถมองข้างตัวเปรียบเทียบตัวอื่นที่ไม่เกี่ยวข้องออกไปได้ แต่ยังมีปัญหาเวลาที่ จำนวน pattern เพิ่มขึ้น ในกรณี multi-pattern มีความเป็นไปได้ที่จะเกิดการ mismatch เกิดขึ้นเนื่องจาก pattern มีขนาดเล็ก โดยเฉพาะอย่างยิ่งถ้า pattern มีการเพิ่มจำนวนมากเกิน CW algorithm ยังใช้งานได้ไม่ดีเท่ากับ AC algorithm

4. วิธีการดำเนินการ

ทีมผู้วิจัยได้ทำการพัฒนาระบบงานอย่างมีขั้นตอนเพื่อให้มีลำดับงานที่ชัดเจนและเป็นไปอย่างมีประสิทธิภาพ โดยมีวิธีการดำเนินงานดังต่อไปนี้

4.4.1 การออกแบบระบบ

ใช้การวิเคราะห์และออกแบบระบบเชิงวัตถุ โดยใช้โปรแกรม Microsoft Visio 2003 เป็นเครื่องมือช่วยพัฒนา ซึ่งภาพรวมของระบบสามารถแสดงได้ดังภาพที่ 2 ข้างล่างต่อไปนี้



ภาพที่ 2 Use Case Diagram

4.4.2 การพัฒนาซอฟต์แวร์ระบบงาน

การพัฒนาโปรแกรมจะใช้ภาษา PHP ในการทำเว็บเบสแอพพลิเคชั่นเพื่อใช้สำหรับติดต่อกับผู้ใช้ และเชื่อมต่อกับโปรแกรมสนอร์ทที่นำมาใช้ในการดักจับแพ็กเก็ต รวมทั้งโปรแกรมสนอร์ทแซม และแอลแคบที่ใช้ระงับ IP Address

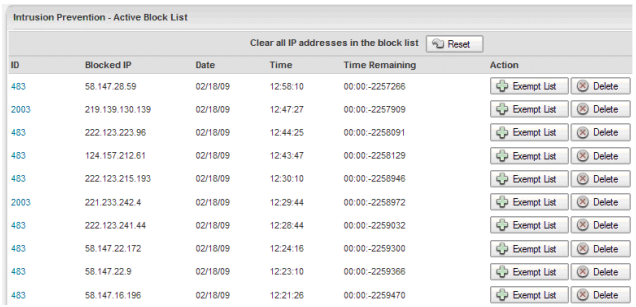
4.4.3 การทดสอบระบบงาน

การทดสอบระบบงานใช้วิธีการแบล็กบอกซ์ ซึ่งจะทำการประเมินคุณภาพของระบบจำนวน 6 ด้าน โดยผู้เชี่ยวชาญด้านระบบเครือข่ายคอมพิวเตอร์ โดยมีเกณฑ์การยอมรับประสิทธิภาพของระบบต้องมีค่าเฉลี่ยตั้งแต่ระดับ 4 ขึ้นไปจากเกณฑ์การประเมิน 5 ระดับ

5. ผลของการดำเนินงาน

5.1 ส่วนการตั้งค่าของระบบ

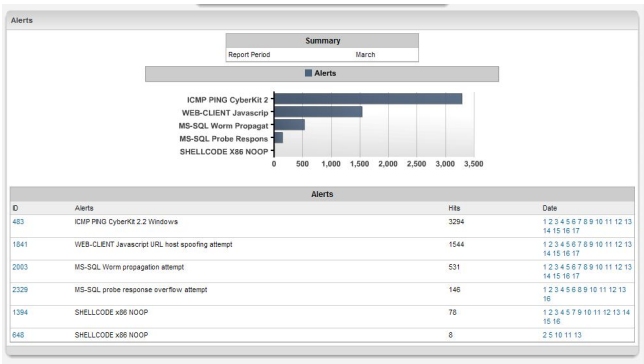
การตั้งค่าที่สามารถกระทำได้ของส่วนงานนี้ จะมีตั้งแต่การตั้งค่าของหมายเลข IP ที่เครื่องแม่ข่าย, การตั้งค่าของระบบตรวจจับผู้บุกรุก และการตั้งค่าของระบบป้องกันผู้บุกรุก ซึ่งสามารถแสดงดังตัวอย่างในภาพที่ 3 ข้างล่างต่อไปนี้



ภาพที่ 3 แสดงส่วนของการตั้งค่าการป้องกันผู้บุกรุก

5.1 ส่วนการออกรายงานของระบบ

การออกรายงานที่สามารถกระทำได้ของส่วนงานนี้ จะมีตั้งแต่ รายงานการตรวจจับผู้บุกรุก และรายงานการป้องกันผู้บุกรุก ซึ่งสามารถแสดงดังตัวอย่างในภาพที่ 4 ข้างล่างต่อไปนี้



ภาพที่ 4 แสดงรายงานในส่วนตรวจจับผู้บุกรุกเมื่อมีการตั้งค่า

5.3 การประเมินหาประสิทธิภาพของระบบโดยผู้เชี่ยวชาญ

เมื่อได้นำระบบไปประเมินโดยผู้เชี่ยวชาญด้านระบบเครือข่ายคอมพิวเตอร์ จำนวน 5 คน สามารถสรุปผลการประเมินแต่ละด้าน ได้ดังตารางที่ 1 ข้างล่างต่อไปนี้

ตารางที่ 1 การประเมินประสิทธิภาพโดยผู้เชี่ยวชาญ

รายการประเมิน	$\bar{x}$	SD	ระดับ
1. ผลการประเมินด้านความสามารถในการทำงาน	3.80	0.31	ดี
2. ผลการประเมินด้านความต้องการของผู้ใช้	3.83	0.26	ดี
3. ผลการประเมินด้านการใช้งานของโปรแกรม	3.86	0.25	ดี
4. ผลการประเมินด้านผลลัพธ์ที่ได้จากโปรแกรม	3.88	0.22	ดี
5. ผลการประเมินด้านความปลอดภัย	3.67	0.58	ดี
6. ด้านคู่มือการใช้งานและการติดตั้งระบบ	3.67	0.58	ดี
สรุปประเมินประสิทธิภาพโดยผู้เชี่ยวชาญ	3.78	0.37	ดี

6. บทสรุป

งานวิจัยนี้ได้พัฒนาระบบที่มีความสามารถในการตรวจจับผู้บุกรุก โดยใช้อัลกอริทึม Shift Max ในการคิดวิเคราะห์หลายแบบแผนของการโจมตี รวมทั้งยังสามารถป้องกันผู้บุกรุกได้โดยการไปสั่ง Block IP ตามเงื่อนไขที่กำหนด นอกจากนั้นยังสามารถแสดงรายงานของระบบต่างๆ ได้ อาทิเช่น การแสดงรายงานในส่วนของการตรวจจับผู้บุกรุก การแสดงรายงานในส่วนของการป้องกันผู้บุกรุก เป็นต้น ซึ่งเมื่อมีการนำระบบนี้ไปใช้ในองค์กรใดก็ตาม องค์กรนั้นจะมีความปลอดภัยที่สูงขึ้น

7. กิตติกรรมประกาศ

ขอขอบพระคุณ นายเอกพล กรรณสูต และคณะ จากบริษัท แปซิฟิค อินเตอร์เน็ต (ประเทศไทย) ที่ให้ความอนุเคราะห์ในการให้คำปรึกษา, การเก็บข้อมูล รวมทั้งประเมินผลการทดสอบระบบงาน

8.บรรณานุกรม

[1] กาญจนา ศิลาวราเวทย์. “การเปรียบเทียบโปรแกรมตรวจหาการบุกรุกเครือข่ายระหว่างโปรแกรมสนอร์ทและเรียลซีเคียวภายใต้ปัจจัยการโจมตี”. กรุงเทพ: จุฬาลงกรณ์มหาวิทยาลัย, 2545.

[2] มหคม อร่ามเสรีวงศ์. “การออกแบบและพัฒนาระบบป้องกันการบุกรุกเครือข่ายโดยอัตโนมัติโดยใช้เครือข่ายแอ็กทีฟ เพื่อรับมือการโจมตีจากเครือข่ายภายในที่ถูก ผู้บุกรุกยึดครอง”. กรุงเทพ: จุฬาลงกรณ์มหาวิทยาลัย, 2548.

[3] Aho A, Corasick M. “Efficient string matching: an aid to bibliographic search”. Commun ACM, 1975;18:333e40.

[4] Boyer RS, Moore JS. “A fast string searching algorithm” Commun ACM 1977;20(10):762e72.

[5] Commentz-Walter. “A string matching algorithm fast on average.In: Maurer HA”, editor. Proceedings 6th International Colloquium on Automata, Languages and Programming,Lecture Notes in Computer Science, vol. 71. Berlin: Springer;1979. p. 118e32.

[6] Kruegel Christopher,Valeur Fredrik, et al. Stateful “intrusion detection for high-speed networks” Santa Barbara: Reliable Software Group, University of California; Nov. 2001.

[7] Toplayer Networks. IDS Balancer, <http://www.toplayer.com/content/products/intrusion_detection/ids_balancer.jspO; Jan. 2004.

[8] Wenbao Jiang, Hua Song, Yiqi Dai. “Real-time intrusion detection for high-speed networks” Computers & Security, 2005. 24, 287e294.