การสืบสวนผู้ใช้บริการด้วยวิชวลไลเซชันไทม์แมชชีน สำหรับนิติวิทยาศาสตร์สำหรับเครือข่าย

User Investigations with Visualization Time Machine for Network Forensic

ณัฐโชติ พรหมฤทธิ์* และ อนิราช มิ่งขวัญ**

บทคัดย่อ

ข้อมูลจราจรทางคอมพิวเตอร์นับเป็นพยานหลักฐานสำคัญในการดำเนินคดีอันเป็นประโยชน์อย่างยิ่งต่อการสืบสวนสอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ ซึ่งในปัจจุบันยังไม่มีงานวิจัยที่สามารถใช้ประโยชน์จากข้อมูล Logs และ Network traffic เพื่อศึกษาและแสดงพฤติกรรมการใช้งานเครือข่าย และตรวจจับผู้ใช้งานที่มีการละเมิดนโยบายความปลอดภัย ผู้วิจัยจึงนำเสนอ Model เพื่อตรวจจับพฤติกรรมการใช้งานเครือข่ายโดยใช้เทคนิค Parallel coordinates ซึ่งแสดงความสัมพันธ์ด้วยตัวแปรต่างๆ ได้แก่ User, Source IP Address, Time, Destination IP Address, Destination service และ Domain name นอกจากนี้ผู้วิจัยได้นำเสนอเทคนิคการสืบสวนแบบ Timeline โดยทำการแสดงพฤติกรรมการใช้งานเครือข่ายเป็นช่วงเวลา ซึ่งแต่ละแถวของ Timeline จะแสดงข้อมูลการใช้งานเครือข่ายของผู้ใช้งานปกติ ผู้ต้องสงสัย และ Host ที่เกี่ยวข้องตามช่วงเวลาที่กำหนด

คำสำคัญ: นิติวิทยาศาสตร์สำหรับเครือข่าย การสร้างภาพข้อมูลจราจรทางคอมพิวเตอร์ Parallel coordinates

Abstract

A computer traffic is one of the important evidences in forensic science. It is useful for an investigation which seeking the criminals to punish. Recently, there is no research which takes the advantages from logs and the network traffic. To study and show the behavior of access the network including keeping an eye on the person who intends to infringe the network security policies, We proposed a model using Parallel coordinates which have a capability to present the relation by various parameters (User, Source IP Address, Time, Destination IP Address, Destination service and Domain name). In addition, the Timeline investigation was also proposed. Each row of the Timeline shows the behavior of access the network which is represented in term of general users, suspect users and involving hosts by time period.

Keyword: Network forensic, Network traffic visualization, Parallel coordinates

1. บทนำ

ในประเทศไทย ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) มีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งผู้ดูแลระบบเครือข่าย นักวิเคราะห์ และพนักงานเจ้าหน้าที่สามารถนำข้อมูลมาวิเคราะห์ และระบุตัวผู้ใช้บริการได้

การวิเคราะห์ข้อมูลจะต้องใช้เทคนิคทาง Network forensic [1], [2], [3], [4] ซึ่งในปัจจุบันยังไม่มีงานวิจัยที่สามารถใช้ประโยชน์จากข้อมูล Logs และ Network traffic เพื่อศึกษาและแสดงพฤติกรรมการใช้งานเครือข่าย และตรวจจับผู้ใช้งานที่มีการละเมิดนโยบายความปลอดภัยของเครือข่าย ผู้วิจัยจึงนำเสนอ UIV (User Investigations with

* *คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ*
** *คณะเทคโนโลยีและการจัดการอุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ*

Visualization Time Machine for Network Forensic) Model ซึ่งสามารถตรวจจับการใช้งานที่มีการละเมิดนโยบายความปลอดภัยของเครือข่าย และแสดงข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้งานปกติ ผู้ต้องสงสัย และ Host ที่เกี่ยวข้องในแบบ Visualization โดยรวบรวมข้อมูลจาก Logs และ Network traffic ในส่วนที่เหลือของบทความจะกล่าวถึงวรรณกรรมที่เกี่ยวข้อง, UIV Model, ประโยชน์ที่คาดว่าจะได้รับ, บทสรุป และงานที่จะทำในอนาคต

2. วรรณกรรมที่เกี่ยวข้อง

เมื่อมีการกระทำความผิดบนเครือข่ายคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์นับเป็นพยานหลักฐานสำคัญในการดำเนินคดีอันเป็นประโยชน์อย่างยิ่งต่อการสืบสวนสอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ [5] ซึ่งจากพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ระบุว่าข้อมูลจราจรทางคอมพิวเตอร์สามารถใช้เป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมาย วิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ โดยในมาตรา 26 ผู้ให้บริการจะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับตั้งแต่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ [6]

การสืบสวนด้วย Network forensic จึงเป็นสิ่งสำคัญที่จะช่วยวิเคราะห์หาผู้ต้องสงสัยจากพยานหลักฐานที่มีการจัดเก็บ และตอบคำถามที่สำคัญ เช่น ใคร ทำอะไร ที่ไหน เมื่อไหร่ และอย่างไร โดยแสดงผลในแบบ Visualization [4], [7], [8], และ [9] ซึ่งแหล่งข้อมูลจราจรทางคอมพิวเตอร์ที่สำคัญที่มักนำมาใช้สำหรับ Network forensic ได้ เช่น 1) Intrusion Detection System software, 2) Security Event Management software, 3) Network Forensic Analysis Tool software, 4) Firewall, Router, Proxy Server and Remote Access Servers, 5) DHCP Server, 6) Packet Sniffers, 7) Network Monitoring และ 8) ISP Records [10] เป็นต้น

Maier และคณะ [11] ได้นำเสนอวิธีการรวบรวม และจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ จัดทำ Index สนับสนุนการค้นคืนผ่านทาง User interface และ Network connection interface ทำให้สามารถทำงานร่วมกับ Real-time Network Intrusion Detection System (NIDS) เพื่อสืบค้นข้อมูลจราจรทางคอมพิวเตอร์ในอดีตได้อย่างอัตโนมัติ ในขณะที่งานวิจัยของ Choi และคณะ [4] ได้นำเสนอวิธีการตรวจจับการบุกรุกโดยใช้เทคนิค Misuse detection และแสดงผลแบบ Visualization โดยทำการเปรียบเทียบ Flow data บนเครือข่ายกับ Attack signatures ซึ่งแสดงความสัมพันธ์ของ Flow ด้วยเทคนิค Parallel coordinates จากตัวแปร 4 ตัว คือ 1) Source IP Address, 2) Destination IP Address, 3) Destination port และ 4) ขนาดเฉลี่ยของ Packet ส่วนงานวิจัยของ Phan และคณะ [9] ได้นำเสนอเครื่องมือในการสืบสวนสำหรับทำการวิเคราะห์หาผู้ต้องสงสัยแบบ Timeline

งานวิจัยต่างๆ ได้มีการนำเสนอเทคนิค และวิธีการที่แตกต่าง โดยสามารถสรุปได้ดังตารางที่ 1

ตารางที่ 1 *คุณลักษณะของงานวิจัยที่เกี่ยวกับ Network forensic*

งานวิจัย	รวบรวม จัดเก็บ ข้อมูล	ตรวจจับ	สืบสวน	Visualization
FORWEB [1]		✓		
Source Attribution for NAT [2]		✓		
E-mail Forensic Analysis [3]		✓		✓
IDS Visualization [4]		✓		✓
HomeCentric Visualization [7]				✓
Flexible Interface [8]				✓
Timeline Visualization [9]			✓	✓
Time Machine [11]	✓			
UIV	✓	✓	✓	✓

จะเห็นได้ว่างานวิจัยเหล่านี้สามารถแก้ปัญหาทางด้าน Network forensic ในบางคุณลักษณะ ผู้วิจัยจึงนำเสนอ UIV Model ซึ่งสามารถรวบรวม จัดเก็บข้อมูล ตรวจจับผู้ต้องสงสัย สืบสวนเพื่อตอบคำถามที่สำคัญ เช่น ใคร ทำอะไร ที่ไหน เมื่อไหร่ และอย่างไรบนเครือข่ายคอมพิวเตอร์ และแสดงผลในแบบ Visualization โดยผู้วิจัยจะทำการศึกษาและนำเสนอการตรวจจับพฤติกรรมที่มีการละเมิดนโยบายความปลอดภัยของเครือข่ายด้วยเทคนิค In -> Out Parallel coordinates ซึ่งใช้ในการศึกษาพฤติกรรมของผู้ใช้บริการเครือข่ายที่มีการติดต่อสื่อสารกับเครือข่ายภายนอก โดยแสดงความสัมพันธ์ของ Flow ด้วยตัวแปร 6 ตัว ได้แก่ 1) User, 2) Source IP Address, 3) Time, 4) Destination IP

Address, 5) Destination service และ 6) Domain name และเทคนิค Out -> In Parallel coordinates ซึ่งใช้ในการศึกษาพฤติกรรมของ Domain name ที่มีการติดต่อสื่อสารกับเครือข่ายภายใน โดยแสดงความสัมพันธ์ของ Flow ด้วยตัวแปร 5 ตัว ได้แก่ 1) Domain name, 2) Source IP Address, 3) Time, 4) Destination IP Address และ 5) Destination service ซึ่งผู้วิจัยคาดว่าการศึกษาในมิติของเวลาจะสามารถบ่งชี้ถึงพฤติกรรมการใช้งานเครือข่าย จึงกำหนดให้ Time เป็นตัวแปรหนึ่งใน Parallel coordinates และนำเสนอเทคนิคการสืบสวนแบบ Timeline ซึ่งสามารถแสดงข้อมูลการใช้งานเครือข่ายของผู้ใช้บริการและ Host ที่เกี่ยวข้องในช่วงเวลาที่กำหนด โดยผู้วิเคราะห์สามารถศึกษาและเปรียบเทียบลักษณะการใช้งานเครือข่ายจาก Timeline ที่สนใจ

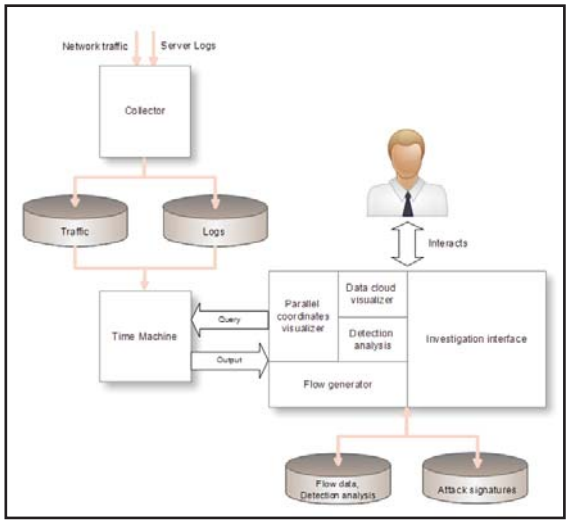
3. UIV Model

เนื้อหาในส่วนนี้จะอธิบายแนวคิดการตรวจจับผู้ต้องสงสัยและการสืบสวนโดยแสดงผลในแบบ Visualization ซึ่ง UIV model ประกอบด้วย

Collector ทำหน้าที่รวบรวม Network traffic บนเครือข่ายและ Logs จาก Server Logs

Time Machine ทำหน้าที่ดึงข้อมูล Traffic และ Logs ตามช่วงเวลาที่ระบุ

Flow generator ทำหน้าที่สร้าง Flow ของ data จากข้อมูล Network traffic และ Logs ด้วยเทคนิค Parallel coordinates



ภาพที่ 1 *UIV model*

Detection analysis ทำหน้าที่วิเคราะห์พฤติกรรมการละเมิดนโยบายความปลอดภัยของเครือข่ายจาก Flow data และ Attack signatures

Parallel coordinates visualizer แสดง Flow data ในรูปแบบกราฟิกด้วยเทคนิค Parallel coordinates

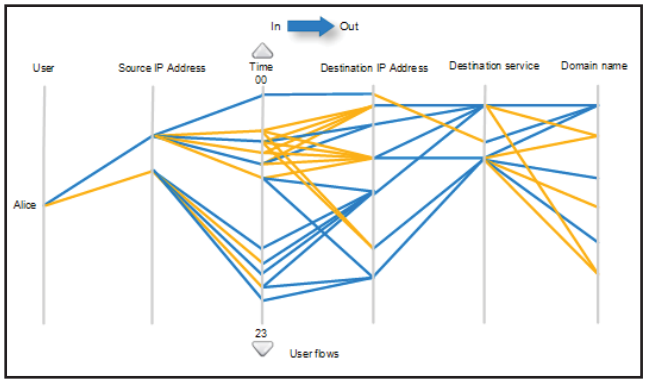
Data cloud visualizer แสดงผลการตรวจจับด้วย Data cloud

Investigation interface แสดงการใช้งานเครือข่ายแบบ Timeline

จากภาพที่ 1. Collector จะรวบรวม Traffic และ Logs ลง Database เพื่อเป็นข้อมูลสำหรับการตรวจจับพฤติกรรมที่มีการละเมิดนโยบายความปลอดภัยของเครือข่ายใน Phase 1 : Detection of suspect และทำการสืบสวนใน Phase 2 : Investigation โดย Flow generator จะสร้าง Flow data ด้วยเทคนิค Parallel coordinates จาก Traffic และ Logs ซึ่งทำการดึงข้อมูลตามช่วงเวลาที่ระบุด้วย Time Machine และแสดงผล Flow data แบบ Parallel coordinates ด้วย Parallel coordinates visualizer ในขณะที่ Detection analysis จะนำ Flow data และ Attack signatures มาวิเคราะห์พฤติกรรมที่มีการละเมิดนโยบายความปลอดภัยของเครือข่าย และแสดงผลลัพธ์ด้วย Data cloud visualizer นอกจากนี้ผู้ดูแลระบบเครือข่าย นักวิเคราะห์ และพนักงานเจ้าหน้าที่สามารถสืบสวนเพิ่มเติมด้วย Investigation interface

3.1 Detection of suspect phase

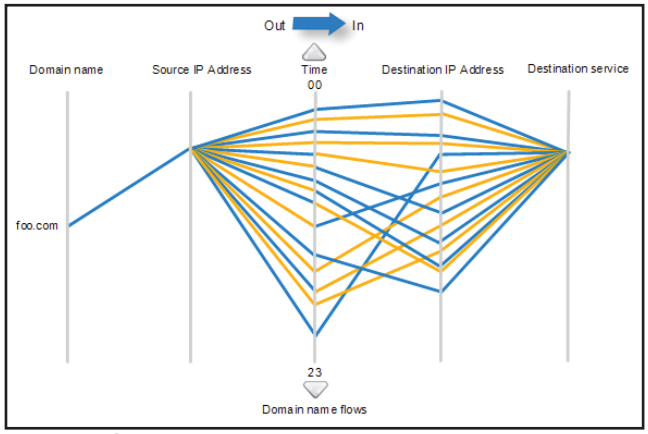
จะศึกษา Flow data ของผู้ใช้บริการ เพื่อตรวจจับพฤติกรรมที่มีการละเมิดนโยบายความปลอดภัยของเครือข่ายด้วยเทคนิค In -> Out Parallel coordinates ดังภาพที่ 2



ภาพที่ 2 *Phase 1 In -> Out Parallel coordinates*

และศึกษา Flowdata ของ Domain name ต่างๆ ที่มีการติดต่อสื่อสารกับเครือข่ายภายในเพื่อตรวจจับพฤติกรรมที่มีการละเมิดนโยบายความปลอดภัยของเครือข่ายด้วย

เทคนิค Out -> In Parallelcoordinates ดังภาพที่ 3



ภาพที่ 3 *Phase 1 Out -> In Parallel coordinates*

จากภาพที่ 2 แสดง Flow data ของ Alice ซึ่งใช้ Host ทั้งหมด 2 Host ทำการติดต่อสื่อสารกับเครือข่ายภายนอกภายในเวลา 1 วัน โดย Alice จะใช้งานแต่ละ Host ในช่วงเวลาที่ต่างกัน แต่ละช่วงเวลา Alice มีการติดต่อสื่อสารกับ Host ปลายทางที่อยู่ใน Domain name ต่างๆ เพื่อเรียกใช้ Services โดยแต่ละคู่ของ coordinates จะสามารถบอกความสัมพันธ์ของ ตัวแปรแบบ Many-to-Many ยกเว้น User กับ Source IP Address เช่น Time กับ Destination IP Address ซึ่งอธิบายได้ว่าแต่ละช่วงเวลา Alice มีการติดต่อสื่อสารกับ Host ปลายทางหลาย Host และแต่ละ Host ปลายทางถูกติดต่อสื่อสารในหลายช่วงเวลา

จากภาพที่ 3 แสดง Flow data แบบ Out -> In Parallel coordinates ซึ่ง Host หนึ่งใน Domain name “foo.com” มีการทำ Host scan มายังเครือข่ายภายในเวลา 24 ชั่วโมง

ผู้วิจัยจะเลือกใช้เทคนิค Anomaly detection และ Misuse detection ทำการตรวจจับพฤติกรรมที่มีการละเมิดนโยบายความปลอดภัยของเครือข่ายจาก Flow data ดังต่อไปนี้

Anomaly detection ทำการเรียนรู้ Flow data ของผู้ใช้และ Flow data ของ Domain name ที่ปกติ และตรวจจับ Flow data ที่ผิดปกติ

Misuse detection ทำการศึกษา Signatures หรือ Pattern ที่เป็นการบุกรุก หรือละเมิดนโยบายความปลอดภัยของเครือข่าย โดยตรวจจับ Flow data ของผู้ใช้และ Flow data ของ Domain name ที่ตรงตาม Attack signatures ที่กำหนด

ดังนั้นการใช้เทคนิค In -> Out Parallel coordinates และ Out -> In Parallel coordinates ดังภาพที่ 2 และ 3 นอกจากจะทำให้ผู้ดูแลระบบเครือข่าย นักวิเคราะห์ และพนักงานเจ้าหน้าที่สามารถศึกษาพฤติกรรมการใช้งานเครือข่ายแล้ว ผู้ดูแลระบบเครือข่าย นักวิเคราะห์ และพนักงานเจ้าหน้าที่ยังสามารถทราบถึงพฤติกรรมที่น่าสงสัยด้วยเทคนิค Anomaly detection และ Misuse detection และแสดงผลการตรวจจับผ่าน Visualization ด้วย Data cloud ดังภาพที่ 4

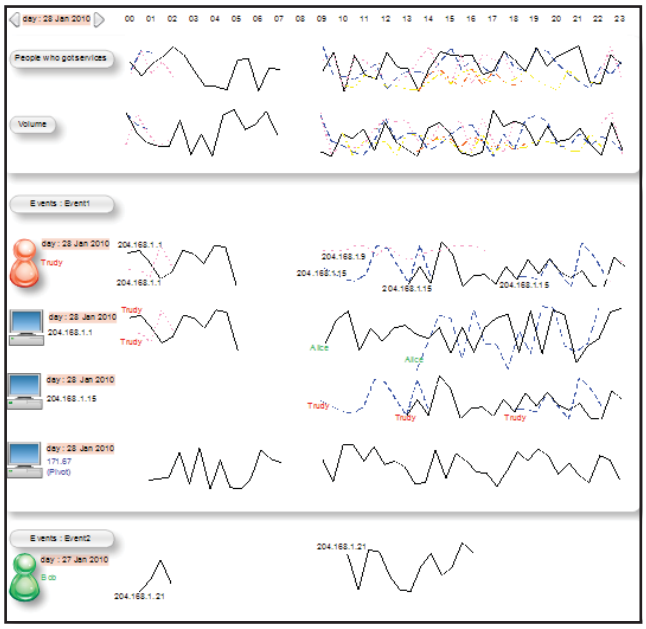
ภาพที่ 4 *Phase 1 Data cloud (User name)*

Data cloud จะแสดงชื่อผู้ใช้งานและ Domain name โดยขนาดตัวอักษรจะแสดงถึงจำนวนของ Traffic ที่มีการติดต่อสื่อสาร สีแดง แดงส้ม และส้ม จะแสดงถึงระดับความน่าสงสัยของผู้ใช้และ Domain name จากมากไปน้อย สีเขียวแสดงถึงชื่อผู้ใช้และ Domain name ที่มีพฤติกรรมปกติ ซึ่งจะเป็นข้อมูลที่เป็นประโยชน์ในการสืบสวนใน Investigation phase ต่อไป

3.2 Investigation phase

จะนำเสนอเทคนิคการสืบสวน โดยแสดงข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้งานปกติ ผู้ต้องสงสัย และ Host ที่เกี่ยวข้อง ได้แก่ 1) ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่ายซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย แสดงด้วยเส้นกราฟสีเขียว 2) ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail server) แสดงด้วยเส้นกราฟสีน้ำเงิน 3) ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล แสดงด้วยเส้นกราฟสีชมพู 4) ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ แสดงด้วยเส้นกราฟสีดำ 5) ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet) แสดงด้วยเส้นกราฟสีส้ม และ 6) ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ Instance Messaging (IM) เป็นต้น แสดงด้วยเส้นกราฟสีเหลือง [5]

ดังภาพที่ 5



ภาพที่ 5 *Phase 2 Investigation*

ภาพที่ 5 แสดงข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งจัดกลุ่มข้อมูลเป็น 6 ประเภท โดยแต่ละแถวเรียกว่า Timeline แสดงเป็นกราฟระยะเวลาตั้งแต่ 00 – 23 น. ประกอบด้วย 2 Timeline หลัก คือ 1.People who got services แสดงจำนวนผู้ใช้งานในเครือข่าย และ 2.Volume แสดงจำนวนของ Traffic ถัดมาจะเป็น Timeline ของผู้ใช้งานปกติ (แสดงด้วยสัญลักษณ์สีเขียว) หรือผู้ใช้งานที่มีพฤติกรรมที่น่าสงสัย (แสดงระดับความน่าสงสัยของผู้ใช้จากมากไปน้อยด้วยสัญลักษณ์สีแดง แดงส้ม และส้ม) หรือ Host ที่ใช้, Timeline ที่เกี่ยวข้องกันจะอยู่ในกลุ่มเดียวกันซึ่งตั้งชื่อเป็น Event1 และ Event2 ซึ่ง Event1 ประกอบด้วย 4 Timeline ได้แก่

1) Timeline ของ Trudy เป็นผู้ใช้งานที่มีพฤติกรรมที่น่าสงสัย มีการใช้บริการ Web, File transfer และ e-mail จาก Host ทั้งหมด 3 Host โดยในช่วงเวลา 00 – 05 น. Trudy ทำการติดต่อสื่อสารจาก Host ที่มี IP Address เป็น 204.168.1.1 ในช่วงเวลา 09 – 23 น. Trudy ทำการการติดต่อสื่อสารจาก Host ที่มี IP Address เป็น 204.168.1.15 และในช่วงเวลา 09 – 16.30 น. Trudy มีการโอนแฟ้มข้อมูลจาก Host ที่มี IP Address เป็น 204.168.1.9 เป็นจำนวนมาก ซึ่งในบางเครือข่ายอาจจะมีนโยบายจำกัดจำนวนการโอนแฟ้มข้อมูลในช่วงเวลาดังกล่าว

2) Timeline ของ Host 204.168.1.1 มีการใช้บริการ Web, File transfer และ e-mail โดยในช่วงเวลา 00 – 05 น. Host 204.168.1.1 ถูกใช้งานโดย Trudy และในช่วงเวลา 09 – 23 น. Host 204.168.1.1 ถูกใช้งานโดย Alice

3) Timeline ของ Host 204.168.1.15 มีการใช้บริการ Web, File transfer และ e-mail โดยในช่วงเวลา 09 – 23 น. Host 204.168.1.15 ถูกใช้งานโดย Trudy

4. Timeline ของเครือข่าย 171.67 ซึ่งเป็นเครือข่ายปลายทาง ทำการส่งข้อมูลกลับมายัง Trudy สำหรับ Event2 จะแสดง Timeline ของ Bob ซึ่งเป็นผู้ใช้ปกติ มีการใช้บริการ Web โดยในช่วงเวลา 00 – 02 น. และ 10 – 16 น. Bob ทำการติดต่อสื่อสารจาก Host ที่มี IP Address เป็น 204.168.1.21

4. ประโยชน์ที่คาดว่าจะได้รับ

1) สามารถตรวจจับพฤติกรรมการละเมิดนโยบายความปลอดภัยของเครือข่ายได้โดยแสดงผลการตรวจจับด้วย Data cloud ซึ่งสามารถบอกถึงจำนวนของ Traffic ที่มีการติดต่อสื่อสาร และระดับความน่าสงสัยของผู้ใช้และ Domain name ในขณะที่ผู้วิเคราะห์สามารถศึกษาพฤติกรรมการใช้งานเครือข่ายจาก Flow data ในรูปแบบกราฟิกด้วยเทคนิค Parallel coordinates

2) ง่ายในการสืบสวนผู้กระทำความผิดและผู้ใช้งานที่มีการละเมิดนโยบายความปลอดภัยของเครือข่าย และแก้ไขปัญหาเกี่ยวกับเครือข่าย ด้วยเทคนิค Timeline ซึ่งสามารถตอบคำถาม เช่น ใครเป็นผู้ต้องสงสัย ใครเป็นผู้ใช้ปกติ ใช้ Host ใด ทำการติดสื่อสื่อสารด้วย Traffic ประเภทใด ในช่วงเวลาไหน และมีลักษณะของ Traffic เป็นอย่างไร

5. บทสรุปและงานที่จะทำในอนาคต

งานวิจัยนี้ทำการศึกษาพฤติกรรมของผู้ใช้บริการเครือข่ายและ Domain name จาก Flow data โดยใช้เทคนิค Parallel coordinates แบบ In -> Out Parallel coordinates และ Out -> In Parallel coordinates ซึ่งผู้วิจัยคาดว่าการศึกษาในมิติของเวลาจะสามารถบ่งชี้ถึงพฤติกรรมการใช้งานเครือข่าย จึงกำหนดให้ Time เป็นหนึ่งในตัวแปร นอกจากนี้ได้นำเสนอการตรวจจับพฤติกรรมที่น่าสงสัยของผู้ใช้บริการและ Domain name ซึ่งละเมิดนโยบายความปลอดภัยของเครือข่ายจาก Flow data โดยแสดงด้วย Visualization

แบบอัตโนมัติ และนำเสนอเทคนิคการสืบสวน สอบสวน แบบ Timeline ซึ่งสามารถแสดงพฤติกรรมของผู้ใช้งานปกติ ผู้ต้องสงสัย และ Host ที่เกี่ยวข้อง

ในอนาคตผู้วิจัยจะพัฒนาและทดสอบประสิทธิภาพด้วย Data sets และใช้งานบนสถานที่จริง พร้อมทั้งศึกษา Flow data เพื่อตรวจจับพฤติกรรมการใช้งานที่มีการละเมิดนโยบายความปลอดภัยของเครือข่าย ด้วยเทคนิค Anomaly detection และ Misuse detection และทำ Usability test กับระบบ Interface แบบ Visualization

6. เอกสารอ้างอิง

[1] John Haggerty, David Llewellyn-Jones, and Mark Taylor, "FORWEB: File Fingerprinting for Automated Network," *e-Forensics 2008*, January 21 - 23, 2008.

[2] M.I. Cohen, "Source attribution for network address translated forensic captures," *digital investigation 5*, pp. 138 - 145, 2009.

[3] Rachid Hadjidj, Mourad Debbabi, Hakim Lounis, and Farkhund Iqbal, "Towards an integrated e-mail forensic analysis framework," *digital investigation 5*, pp. 124 – 137, 2009.

[4] Hyunsang Choi, Heejo Lee, and Hyogon Kim, "Fast detection and visualization of network attacks on parallel coordinates," *computers & security 28,* pp. 276 – 288, 2009.

[5] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, *ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550*, [ออนไลน์], [สืบค้นวันที่ 21 ธันวาคม 2552], จาก http://www.mict.go.th/download/law/TrafficData.pdf

[6] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, *พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*, [ออนไลน์], [สืบค้นวันที่ 21 ธันวาคม 2552], จาก http://www.mict.go.th/download/law/20070618_CC_Final.pdf

[7] Robert Ball, Glenn A. Fink, and Chris North, "HomeCentric Visualization of Network Traffic for Security Administration," *VizSEC/DMSEC'04*, pp. 55 – 64, October 29, 2004.

[8] Adam Perer and Ben Shneiderman, "Systematic Yet Flexible Discovery: Guiding Domain Experts through Exploratory Data Analysis," *IUI'08*, pp. 109 – 118, January 13-16, 2008.

[9] Doantam Phan, Andreas Paepcke, and Terry Winograd, "Progressive Multiples for Communication-Minded Visualization," *Graphics Interface Conference 2007*, pp. 225 – 232, May 28-30, 2007.

[10] Karen Kent, Suzanne Chevalier, Tim Grance, and Hung Dang, "Guide to Integrating Forensic Techniques into Incident Response", *National Institute of Standards and Technology Special Publication* 800-86, August 2006.

[11] Gregor Maier, Robin Sommer, Holger Dreger, and Anja Feldmann, Vern Paxson, and Fabian Schneider, "Enriching Network Security Analysis with Time Travel," *SIGCOMM*'08, pp. 183 – 194, August 17 – 22, 2008.