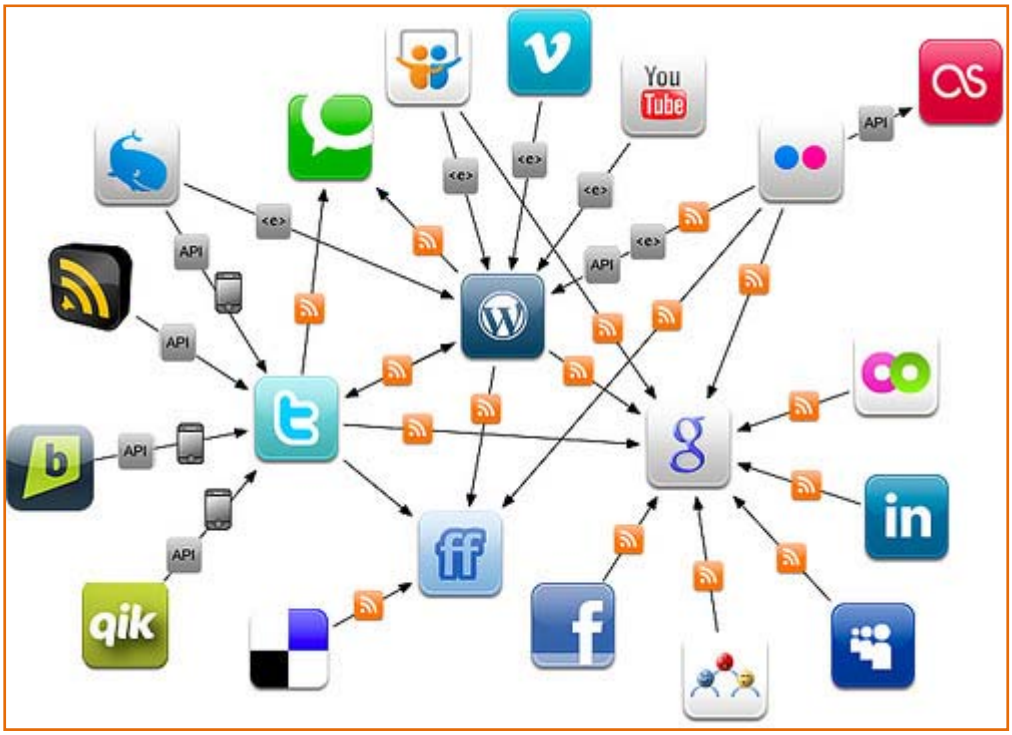
บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

เครือข่ายสังคมออนไลน์ (Online Social Networks) สามารถสนับสนุนให้ผู้ใช้มีส่วนสร้างเนื้อหาบนอินเทอร์เน็ต และ ผู้ใช้ยังเป็นผู้ร่วมกำหนดคุณค่าของเนื้อหา ทำให้สังคมพิจารณาได้ว่าเนื้อหาใดมีคุณภาพ รวมทั้งการให้ความสำคัญกับทัศนคติของคนที่มีต่อการเรียนรู้เรื่องราวต่างๆ มารวมกันให้เป็นองค์กรแห่งการเรียนรู้ (Learning Organization) ขนาดใหญ่ก่อให้เกิดการต่อยอดความรู้และความคิด นำมาซึ่งองค์ความรู้ (Knowledge) ทำให้เราเห็นปรากฏการณ์การเกิดชุมชนออนไลน์ ซึ่งกลายเป็นรูปแบบของสังคมประเภทหนึ่งที่อยู่ในโลกอินเทอร์เน็ตจริง ซึ่งแตกต่างจากเว็บ 1.0 (Web 1.0) จากรูปที่ 1.1 แสดงองค์ประกอบที่เชื่อมโยงกันของเครือข่ายสังคมออนไลน์แสดงถึงความสัมพันธ์และความเกี่ยวข้องของผู้ใช้บริการในลักษณะชุมชนออนไลน์ โดยผู้ใช้งานนิยมเป็นสมาชิกเครือข่ายสังคมออนไลน์หลากหลายชนิด ซึ่งผู้ใช้จะมีส่วนสร้างเนื้อหาของเว็บไซต์เครือข่ายสังคมออนไลน์นั้นๆ ด้วยตนเอง

จากความนิยมเครือข่ายสังคมออนไลน์ดังกล่าวข้างต้น ทำให้ผู้ใช้งานอินเทอร์เน็ตส่วนใหญ่มีความนิยมใช้เครือข่ายสังคมออนไลน์เช่น Twitter, Instagram และ Facebook ดังนั้นภัยอินเทอร์เน็ตสมัยใหม่จึงมุ่งไปยังกลุ่มผู้ใช้งานตามบ้านผ่านทางการเข้าเว็บไซต์เครือข่ายสังคมออนไลน์เหล่านั้น โดยพบการหลอกหลวงผ่านทางเว็บไซต์ยอดนิยมต่างๆ ด้วยเทคนิคการวิศวกรรมทางสังคม (Social Engineering) และภัยจากโปรแกรมมุ่งร้ายหรือโปรแกรมมัลแวร์ที่แพร่กระจายอยู่ที่เครือข่ายสังคมออนไลน์ เช่นมีโปรแกรมม้าโทรจันแพร่กระจายผ่านทางเว็บไซต์เครือข่ายสังคมออนไลน์ หรือผ่านทาง Instant Messaging เช่น MSN เป็นต้น



รูปที่ 1.1 องค์ประกอบที่เชื่อมโยงกันของเครือข่ายสังคมออนไลน์
(ที่มา: www.fortinet.com, ออนไลน์, 2556)

จากการศึกษางานวิจัยจำนวนมาก พบว่าตลอดที่ผ่านมามีงานวิจัยส่วนหนึ่งที่ทำการศึกษาถึงลักษณะการใช้เครือข่าย (Network Behavior Analysis) โดยในปี 2002 C. Guang และคณะ [21] ได้ทำการพัฒนาตัวแบบ (Model) พฤติกรรมการใช้งานเครือข่าย โดยใช้การระบุกลุ่มของ IP ซึ่งผู้วิจัยได้ทำการสุ่มตัวอย่างเพื่อทดสอบทางสถิติ ในปี 2005 W. Ren และคณะ [111] ได้มีการศึกษาถึงการสอบกลับลักษณะการทำงานของเครือข่าย ทั้งในมุมมองด้านเทคนิคและมุมมองด้านกฎหมายเพื่อสร้างมาตรฐานของการสอบกลับลักษณะการทำงานของเครือข่ายขึ้น และในปี 2006 D. V.Klein [32] มีการศึกษาถึงผลกระทบของการถูกโจมตีในรูปแบบของอีเมล และนำเสนอแนวทางแก้ไขปัญหาพร้อมทั้งแนวทางต่อการเพิ่มระดับความมั่นคงปลอดภัยของเครือข่ายโดยการใช้คำสั่งการตรวจสอบ (Audit Scripts) เพื่อเฝ้าระวังระบบเครือข่าย

ในปี 2007 J. Timofte และคณะ [52] ได้นำเสนอการวิเคราะห์พฤติกรรมการใช้เครือข่ายเพื่อใช้ออกแบบระบบความมั่นคงปลอดภัยที่ระบุถึงรูปแบบข้อมูลจราจร (Traffics) ที่ผิดปกติ ส่วนในปี 2008 ได้มีงานวิจัยหลายชิ้นที่มุ่งเน้นในการวิเคราะห์รูปแบบข้อมูลจราจรในระบบเครือข่าย อาทิเช่น S. Kang และคณะ [90] งานวิจัยชิ้นนี้ได้เน้นทางด้านผลกระทบต่อองค์ประกอบของเครือข่ายโดยการสร้างระบบการสอบกลับ (Forensic System) ที่มีประสิทธิภาพ โดยทำการ

ในประเทศไทยได้มีการกำหนดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 [2] ขึ้นเพื่อสร้างความเข้าใจในตัวบทกฎหมายแก่ประชาชนและผู้เกี่ยวข้องใช้เป็นคู่มือแนวทางในการปฏิบัติตามกฎหมายปกป้องสิทธิ โดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งมีการกล่าวถึงลักษณะความผิดเกี่ยวกับคอมพิวเตอร์ประเภทต่างๆ ที่อาจนำภัยคุกคามอย่างอื่นแฝงมาด้วย เช่นไวรัส สปายแวร์ เป็นต้น จนส่งผลถึงขั้นทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานได้อีก โดยสามารถใช้เป็นเครื่องมือที่สำคัญในการกระทำความผิดทางคอมพิวเตอร์ต่อไป ดังนั้นเพื่อให้องค์กรสามารถใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่เหมาะสม หรือถูกคุกคามจากภัยต่างๆ ซึ่งจะช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน และบุคลากร จึงสมควรในการหาแนวทางเพื่อกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กรให้เหมาะสมที่สุด

เนื่องจากงานวิจัยได้ศึกษาถึงแนวทางการพัฒนาตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ ซึ่งการทำความเข้าใจกับภาพความเชื่อมโยงในเครือข่ายสังคมออนไลน์เป็นประโยชน์มากในการวิเคราะห์ และความเข้าใจในเครือข่ายสังคมออนไลน์ดังกล่าวสามารถนำไปสู่การดำเนินงานที่มีประสิทธิภาพของเครื่องมือในการสืบค้นผู้กระทำผิดปกติหรือมีพฤติกรรมการโจมตี การค้นหาเป้าหมายที่อาจจะได้รับผลกระทบจากการโจมตีนั้นๆ รวมทั้งการ

1.2 คำถามของการวิจัย

การวิจัยได้ศึกษาจากแนวคิดและผลการวิจัยต่างๆ เพื่อที่จะค้นหากลยุทธ์การติดตามภัยจากการใช้เครือข่ายสังคมออนไลน์โดยพัฒนาตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ ซึ่งมีคำถามในการวิจัย ดังนี้

1. เมื่อใช้เครือข่ายสังคมออนไลน์จะพบความผิดปกติและโอกาสการถูกโจมตีอย่างไร
2. การแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีลักษณะอย่างไร
3. การศึกษาความเชื่อมโยงในเครือข่ายสังคมออนไลน์สามารถใช้สืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงได้อย่างไร
4. การศึกษาความเชื่อมโยงในเครือข่ายสังคมออนไลน์สามารถทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ได้อย่างไร

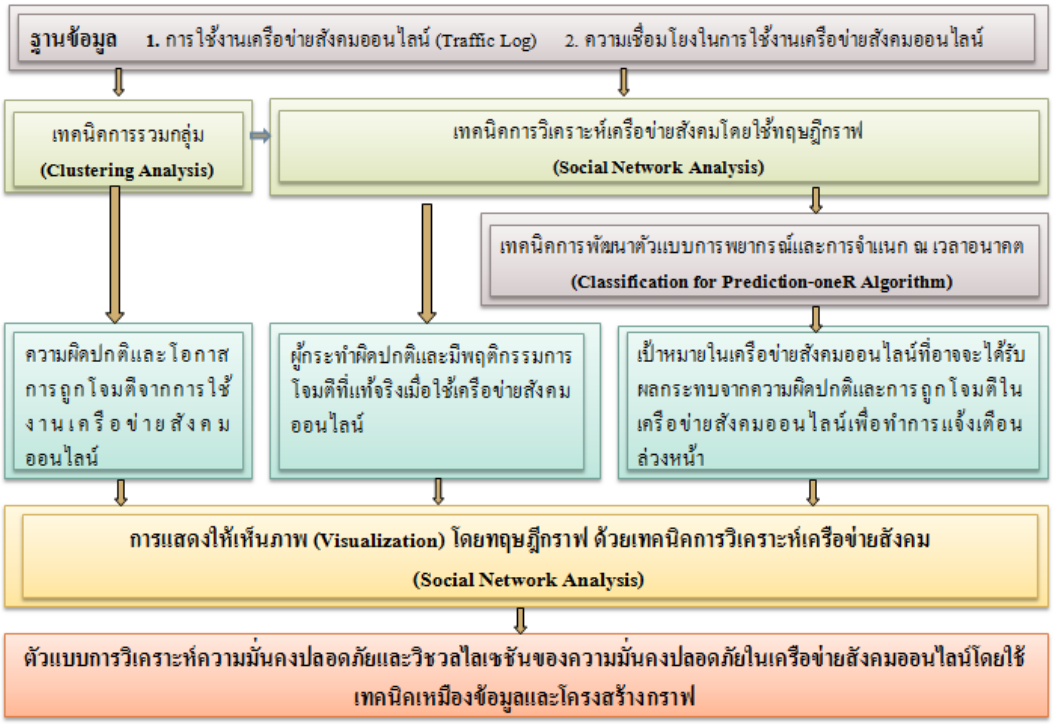
1.3 วัตถุประสงค์ของการวิจัย

ในการวิจัยครั้งนี้ ผู้วิจัยมีวัตถุประสงค์ ดังนี้

1. เพื่อทำการวิเคราะห์หาความผิดปกติและโอกาสการถูกโจมตีจากการใช้เครือข่ายสังคมออนไลน์
2. เพื่อศึกษารูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์
3. เพื่อพัฒนาตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟสำหรับรองรับการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริง
4. เพื่อพัฒนาตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้า

1.4 กรอบแนวคิดในการวิจัย

ผู้วิจัยได้กำหนดกรอบแนวคิดการวิจัย เป็นดังเสนอในรูปที่ 1.2



รูปที่ 1.2 กรอบแนวคิดการวิจัย

จากกรอบแนวคิดการวิจัยในรูปที่ 1.2 ผู้วิจัยได้ทำการศึกษาเอกสารและงานวิจัยที่เกี่ยวข้องเพื่อที่จะค้นหากลยุทธ์การติดตามภัยจากการใช้เครือข่ายสังคมออนไลน์จากตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ ดังต่อไปนี้

1. งานวิจัยอื่นๆ ที่เกี่ยวข้องในหัวข้อ ดังนี้
   1.1 การวิเคราะห์ความมั่นคงปลอดภัยในเครือข่ายคอมพิวเตอร์
   1.2 เทคนิคการวิเคราะห์ความมั่นคงปลอดภัยในเครือข่ายคอมพิวเตอร์
   1.3 เทคนิคการติดตามการแพร่กระจายข้อมูลข่าวสาร
   1.4 โครงสร้างกราฟ
   1.5 เทคนิคการทำให้เห็นภาพการวิเคราะห์ความมั่นคงปลอดภัยในเครือข่ายคอมพิวเตอร์

2. จากการวิเคราะห์ข้อดีและข้อจำกัดของงานวิจัยในแต่ละหมวดหมู่ที่ได้ทำการศึกษาดังกล่าว จะได้คุณลักษณะของงานวิจัยที่ควรพัฒนา จากนั้นทางผู้วิจัยและคณะ [73-78] ได้ทำการพัฒนางานวิจัยเพื่อประเมินผลการทดลองเบื้องต้น และเพื่อสร้างความเชื่อมโยงในกรอบแนวคิดการวิจัย

2.1 การศึกษาการแพร่กระจายไวรัสคอมพิวเตอร์ในเครือข่ายสังคม กรณีศึกษาศูนย์บริการโลหิตแห่งชาติ สภากาชาดไทย (Study of Computer Virus Distribution in Social Networks: A Case study of National Blood Centre, Thai Red Cross Society) เป็นการศึกษาถึงความเสี่ยงขององค์กรที่อนุญาตให้บุคลากรใช้งานเครือข่ายสังคมออนไลน์ด้วยสถิติวิเคราะห์ (Statistic Analysis)

2.2 การวิเคราะห์ความผิดปกติและการถูกโจมตีในเครือข่ายสังคม (Social Networks Anomaly and Attack Patterns Analysis) เป็นการศึกษารูปแบบความผิดปกติและโอกาสการถูกโจมตีเมื่อมีการใช้งานเครือข่ายสังคมออนไลน์ด้วยเทคนิควิเคราะห์การรวมกลุ่ม (Cluster Analysis)

2.3 การวิเคราะห์ความผิดปกติและการถูกโจมตีในเครือข่ายสังคมด้วยการสร้างกฎความสัมพันธ์ (Social Networks Anomaly and Attack Patterns Analysis with Association Rules) เป็นการศึกษารูปแบบความผิดปกติและโอกาสการถูกโจมตีเมื่อมีการใช้งานเครือข่ายสังคมออนไลน์ด้วยเทคนิคการสร้างกฎความสัมพันธ์ (Association Rules)

2.4 การแสดงภาพวิชวลไลเซชันของการแพร่กระจายในเครือข่ายสังคม (Visualization of Information Diffusion in Social Networks) เป็นการศึกษารูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีของการใช้งานเครือข่ายสังคมออนไลน์ ด้วยเทคนิควิเคราะห์การรวมกลุ่ม (Cluster Analysis) และ การวิเคราะห์เครือข่ายสังคม (Social Network Analysis: SNA)

2.5 การทำนายความเชื่อมโยงในเครือข่ายสังคมด้วยเทคนิคการวิเคราะห์เครือข่ายสังคมและเทคนิคการเรียนรู้แบบมีผู้สอน (Links Prediction in Social Networks by Social Network Analysis and Supervised Learning) เป็นการศึกษาถึงเทคนิคการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงและเทคนิคการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ด้วยการวิเคราะห์เครือข่ายสังคม (Social Network Analysis: SNA) และเทคนิคการเรียนรู้แบบมีผู้สอน (Supervised Learning, Classification Analysis, J48, oneR, Naïve Bay)

2.6 การติดตามโหนดที่มีอิทธิพลต่อการเกิดความผิดปกติและการโจมตีในเครือข่ายสังคม (Tracking the Influencing Nodes of Anomaly and Attack Patterns in Social Networks) เป็น

1.5 สมมติฐานของการวิจัย

1. การศึกษาความเชื่อมโยงในเครือข่ายสังคมออนไลน์สามารถพัฒนาตัวแบบในการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีในเครือข่ายสังคมออนไลน์ที่มีความละเอียดถูกต้องอย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 %

2. การศึกษาความเชื่อมโยงในเครือข่ายสังคมออนไลน์สามารถพัฒนาตัวแบบในการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ที่มีความละเอียดถูกต้องอย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 %

3. สามารถประยุกต์ใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟเพื่อพัฒนาตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์ได้อย่างเหมาะสม

1.6 ขอบเขตการวิจัย

การศึกษาครั้งนี้ ได้ใช้ฐานข้อมูลความผิดปกติ (Anomaly) และการถูกโจมตี (Attack) ของการใช้เครือข่ายสังคมออนไลน์ขององค์กรที่ต้องการความมั่นคงปลอดภัยในระดับสูง เนื่องจากต้องป้องกันความเสี่ยงต่อข้อมูลและระบบสารสนเทศขององค์กรที่รองรับระบบงานทางด้านสุขภาพในระดับประเทศ (Public Health Sector in Thailand) จำนวน 2 ประเทศ ดังนี้

1. ข้อมูลของประเทศไทย ซึ่งประกอบไปด้วยสำนักงานใหญ่ที่กรุงเทพมหานคร 1 แห่ง สำหรับรองรับงานทางด้านสุขภาพของทั้ง 76 จังหวัดทั่วประเทศ

2. ข้อมูลของประเทศที่ร่วมทดสอบ ซึ่งประกอบด้วยสำนักงานใหญ่ที่เมืองหลวงของประเทศ 1 แห่งที่มีโครงการวิจัยร่วมกับประเทศไทยในประเด็นการปลูกถ่ายเซลล์ต้นกำเนิดเม็ดโลหิตสำหรับรองรับงานทางด้านสุขภาพของทั้งประเทศ

โดยผู้วิจัยวางแผนการเลือกตัวอย่างฐานข้อมูลความผิดปกติ (Anomaly) และการถูกโจมตี (Attack) ของการใช้เครือข่ายสังคมออนไลน์ซึ่งเป็น Traffic Log ด้วยหลักการของการเลือกตัวอย่างตามความน่าจะเป็น (Probability Sampling) ดังนี้

1. การเลือกตัวอย่างแบบกลุ่ม (Cluster Sampling)

การเลือกตัวอย่างแบบกลุ่ม (Cluster Sampling) เป็นการเลือกตัวอย่างที่ภายในแต่ละกลุ่มมีลักษณะที่สนใจทุกลักษณะ หรือมีลักษณะที่แตกต่างคละกัน ดังนั้นการเลือกตัวอย่างแบบกลุ่มจึงเป็นการเลือกตัวอย่างเพียงบางกลุ่มมาทำการศึกษาเท่านั้น โดยผู้วิจัยได้กำหนดกลุ่มย่อย (Cluster Factor) ตามเดือน

2. การเลือกตัวอย่างสุ่มแบบง่าย (Simple Random Sampling)

เป็นการเลือกตัวอย่างที่ให้แต่ละหน่วยในประชากรมีโอกาสถูกเลือกเท่าๆกันในแต่ละครั้งของการเลือก โดยผู้วิจัยได้ทำการเลือกตัวอย่างแบบง่ายจากการเลือกตัวอย่างแบบกลุ่มได้เดือนเมษายน และธันวาคม

เนื่องจากงานวิจัยนี้ได้ทำการศึกษาตั้งแต่พฤศจิกายน 2554-2556 จึงทำการเลือกตัวอย่าง โดยกำหนดขอบเขตการสุ่มตัวอย่างฐานข้อมูลความผิดปกติ (Anomaly) และการถูกโจมตี (Attack) ของการใช้เครือข่ายสังคมออนไลน์ของ 2 ประเทศ คือ ประเทศไทย และประเทศที่เข้าร่วมทดสอบ ในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556

ทั้งนี้ การค้นหากลยุทธ์การติดตามภัยจากการใช้เครือข่ายสังคมออนไลน์จากตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์ เพื่อทำความเข้าใจกับภาพความเชื่อมโยงในเครือข่ายสังคมออนไลน์ที่เป็นประโยชน์มากในการวิเคราะห์และความเข้าใจในเครือข่ายสังคมออนไลน์ดังกล่าว สามารถนำไปสู่การดำเนินงานที่มีประสิทธิภาพของเครื่องมือในการสืบค้นผู้กระทำผิดปกติหรือมีพฤติกรรมการโจมตี การค้นหาเป้าหมายที่อาจจะได้รับผลกระทบจากการโจมตีนั้นๆ รวมทั้งการระบุกลุ่มที่ซ่อนอยู่หรือการหาสมาชิกที่หายไปของกลุ่ม ฯลฯ ในเครือข่ายสังคมออนไลน์ ซึ่งเป็นปัญหาที่พบบ่อยที่สุดในการรักษาความมั่นคงปลอดภัยและการสอบสวนทางอาญา

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1.7.1 ประโยชน์ทางวิชาการ

1. เผยแพร่ตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์ เพื่อใช้ในเชิงป้องกันเพื่อสร้างความมั่นคงปลอดภัยจากการใช้งานเครือข่ายสังคมออนไลน์

2. เผยแพร่ความรู้ถึงความเสี่ยงในการใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบความผิดปกติและโอกาสการถูกโจมตีในการใช้งานเครือข่ายสังคมออนไลน์ โดยอธิบายถึงรูปแบบของความผิดปกติและการถูกโจมตี และรูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์

3. มีตัวแบบในการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์ และตัวแบบของการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้า

1.7.2 ประโยชน์ต่อสังคม

1. สร้างนโยบายและแนวปฏิบัติขององค์กรที่ต้องการความมั่นคงปลอดภัยในระดับสูง เนื่องจากต้องป้องกันความเสี่ยงต่อข้อมูลและระบบสารสนเทศขององค์กร

2. มีกลยุทธ์การติดตามภัยจากการใช้เครือข่ายสังคมออนไลน์ซึ่งสามารถทำให้ทราบถึงเหตุการณ์ปัจจุบัน และทำนายหาความเชื่อมโยงในเครือข่ายสังคมออนไลน์

1.7.3 ประโยชน์ต่อองค์กร

1. องค์กรได้รับความเชื่อถือไว้วางใจจากหน่วยงานอื่นๆ ด้านความมั่นคงปลอดภัย

2. สามารถทำหนังสือเวียนหรือรายงานเพื่อแจ้งให้ผู้ใช้และเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ ได้รับทราบเกี่ยวกับประเภทของเหตุการณ์ด้านความมั่นคงปลอดภัย ได้แก่

2.1 การกระทำที่ขัดต่อ พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

2.2 การกระทำที่ขัดต่อความมั่นคงของชาติ

2.3 การใช้ทรัพยากรสารสนเทศขององค์กรผิดวัตถุประสงค์

1.8 นิยามศัพท์

1. เครือข่ายสังคมออนไลน์ (Online Social Networks)

เครือข่ายสังคมออนไลน์ เป็นปรากฏการณ์ของการเชื่อมต่อระหว่างบุคคลในโลกอินเทอร์เน็ต และ ยังหมายรวมถึง การเชื่อมต่อระหว่างเครือข่ายกับเครือข่ายสังคมออนไลน์ เข้าด้วยกัน เป็นการเน้นไปที่การสร้างชุมชนออนไลน์ซึ่งผู้คนสามารถที่จะแลกเปลี่ยน แบ่งปันตามผลประโยชน์ กิจกรรม หรือความสนใจเฉพาะเรื่อง ซึ่งอาศัยระบบพื้นฐานของเว็บไซต์ที่ทำให้มีการโต้ตอบกันระหว่างผู้คน

2. การวิเคราะห์ความมั่นคงปลอดภัย (Security Analytic)

การกระทำความผิดซึ่งกระทบกับหลักพื้นฐานด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ที่ได้รับการวิเคราะห์ความมั่นคงปลอดภัย จะครอบคลุมประเด็นเหล่านี้

a) ความลับของข้อมูล (Confidentiality)
b) ความถูกต้องสมบูรณ์ของข้อมูล (Integrity)
c) การมีอยู่ของข้อมุล (Availability)
d) ผู้ใช้มีตัวตนจริง (Authentication)
e) ผู้ใช้มีสิทธิ์ในการจัดทำอะไรบ้าง (Authorization)
f) ผู้ใช้ไม่สามารถปฏิเสธการกระทำ (Non repudiation)

ทั้งนี้การตรวจสอบระบบสารสนเทศต้องพิจารณาเรื่องของการควบคุม (Control) ว่าได้มีการกำหนดไว้อย่างถูกต้อง แบ่งการควบคุมออกเป็น 3 ประเด็น ดังนี้

a) การควบคุมแบบป้องกันล่วงหน้า (Preventive Control)
b) การควบคุมแบบค้นหาประวัติเหตุการณ์ที่เกิดขึ้น (Detective Control)
c) การควบคุมแบบแก้ไขปัญหาจากเหตุการณ์ที่เกิดขึ้น (Corrective Control)

3. ความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Anomaly and Attack Patterns in Online Social Networks) ได้แก่ การที่ผู้ใช้ได้รับผลกระทบต่างๆที่เกิดจากการใช้งานเครือข่ายสังคมออนไลน์ที่ Firewall สามารถดักจับและแปลผลออกมาว่าเป็นความผิดปกติ ได้แก่

a) ภัยมัลแวร์ และ เทคนิควิศวกรรมสังคม (Malware with Social Engineering Technique Attack)
b) ภัยสแปมเมล์ (Spam Mail Attack)

c) ภัยจากการใช้โปรแกรมประเภท IM และ P2P โดยไม่ระวังอย่างเพียงพอ (IM and P2P Attack)

d) ภัยกับดักหลอกลวงผ่านทางอิเล็คโทรนิกส์เมล์ และ การโจมตีผู้เล่นเกมส์ออนไลน์ (Phishing, Pharming และ Gold Farming Attack)

e) ภัยการโจมตีระบบด้วยวิธี DoS หรือ DDoS (Denial of Services and Distributed Denial of Services Attack)

f) ภัยการโจมตี Web Server และ Web Application (Web Server and Web Application Attack)

g) ภัยเครือข่ายหุ่นยนต์ (Botnets Attack)

h) ภัยแฝงแอบซ่อนเร้น (Rootkits Attack)

4. โครงสร้างข้อมูลแบบกราฟ

a) นิยามกราฟ

กราฟ (Graph) เป็นโครงสร้างข้อมูลแบบไม่ใช่เชิงเส้นอีกชนิดหนึ่ง กราฟเป็นโครงสร้างข้อมูลที่มีการนำไปใช้ในงานที่เกี่ยวข้องกับการแก้ปัญหาที่ค่อนข้างซับซ้อน เช่น การวางข่ายงานคอมพิวเตอร์ การวิเคราะห์เส้นทางวิกฤติ และปัญหาเส้นทางที่สั้นที่สุด เป็นต้น

กราฟ เป็นโครงสร้างที่นำมาใช้เพื่อแสดงความสัมพันธ์ระหว่างวัตถุ โดยแทนวัตถุด้วยเวอร์เท็กซ์ (Vertex) หรือโหนด (Node) และเชื่อมโยงความสัมพันธ์ด้วยเอดจ์ (Edge) สามารถเขียนในรูปของสัญลักษณ์ได้เป็น $G = (V, E)$ โดยที่

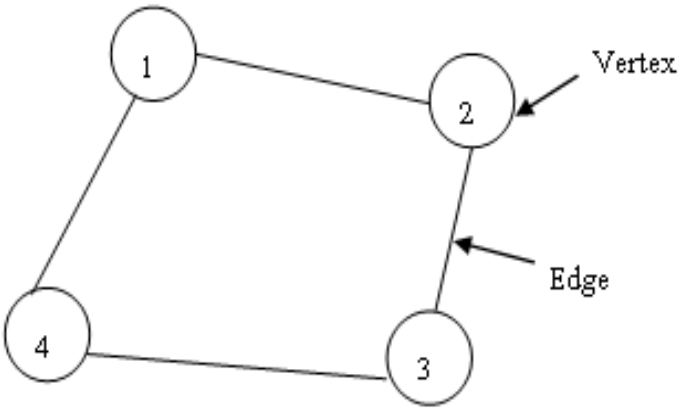
$V(G)$ คือ เซตของเวอร์เทกซ์ที่ไม่ใช่เซตว่าง และมีจำนวนจำกัด

$E(G)$ คือ เซตของเอดจ์ ซึ่งเขียนด้วยคู่ของเวอร์เท็กซ์

จากรูปที่ 1.3 สามารถอธิบายถึง $V(G)$ และ $E(G)$ ดังนี้

$V(G) = \{1, 2, 3, 4\}$

$E(G) = \{(1, 2), (1, 4), (2, 3), (3, 4)\}$



รูปที่ 1.3 ตัวอย่างโครงสร้างข้อมูลแบบกราฟ

b) โหนด (Node)

บุคคลในเครือข่ายสังคมออนไลน์ หรือคือเวอร์เท็กซ์ (Vertex) ในโครงสร้างกราฟ

c) ความเชื่อมโยง (Link)

ความสัมพันธ์ของบุคคลในเครือข่ายสังคมออนไลน์มีการติดต่อกับบุคคลอื่นในเครือข่ายสังคมออนไลน์ หรือคือเอดจ์ (Edge) ในโครงสร้างกราฟ

5. ดีกรี (Degree)

จำนวนเส้นความสัมพันธ์ที่เข้าและออกของโหนดแต่ละโหนด แบ่งเป็น โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) และ โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes)

a) โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes)

In-degree แสดงจำนวนเส้นเชื่อมที่เข้ามายังโหนดนั้นๆ โดยในเครือข่ายสังคมออนไลน์ โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) หมายถึงบุคคลในเครือข่ายสังคมออนไลน์ที่มีการติดต่อกับบุคคลอื่นในเครือข่ายสังคมออนไลน์ ซึ่งเป็นบุคคลที่เป็นศูนย์กลางของการรับข้อมูลข่าวสารหรือผลการกระทำผิดปกติและการโจมตีในเครือข่ายสังคมออนไลน์

b) โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes)

Out-degree แสดงจำนวนเส้นเชื่อมที่ออกจากโหนดนั้นไป โดยในเครือข่ายสังคมออนไลน์ โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) หมายถึงบุคคลในเครือข่ายสังคมออนไลน์ที่มีการติดต่อกับบุคคลอื่นในเครือข่ายสังคมออนไลน์ ซึ่งเป็นบุคคลที่เป็น

6. โหนดที่มีอิทธิพล (Influencing Nodes)

บุคคลในเครือข่ายสังคมออนไลน์ที่มีการติดต่อกับบุคคลอื่นในเครือข่ายสังคมออนไลน์ ซึ่งเป็นบุคคลที่เป็นศูนย์กลางของการรับหรือการกระจายข้อมูลข่าวสารในเครือข่ายสังคมออนไลน์ โดยโหนดที่มีอิทธิพลดังกล่าวมีพฤติกรรมของการแพร่กระจายความผิดปกติและการโจมตีบุคคลอื่นในเครือข่ายสังคมออนไลน์

7. โหนดที่ได้รับอิทธิพล (Attacked Nodes)

บุคคลในเครือข่ายสังคมออนไลน์ที่ได้รับผลกระทบของการติดต่อกับโหนดที่มีอิทธิพลในเครือข่ายสังคมออนไลน์ ทำให้ได้รับผลการกระทำผิดปกติและการโจมตีจากโหนดที่มีอิทธิพล (Influencing Nodes)

8. โหนดที่มีความใกล้ชิด (Closeness Nodes)

บุคคลในเครือข่ายสังคมออนไลน์ที่มีการติดต่อใกล้ชิดกับบุคคลที่เป็นศูนย์กลางของการการรับข้อมูลข่าวสารหรือผลการกระทำผิดปกติและการโจมตีในเครือข่ายสังคมออนไลน์ หรือบุคคลในเครือข่ายสังคมออนไลน์ที่มีการติดต่อใกล้ชิดกับบุคคลที่เป็นศูนย์กลางของการ**การ**กระจายข้อมูลข่าวสารหรือผลการกระทำผิดปกติและการโจมตีในเครือข่ายสังคมออนไลน์

9. โหนดเชื่อมโยงเครือข่าย (Betweenness Nodes)

บุคคลในเครือข่ายสังคมออนไลน์ที่มีการติดต่อกับบุคคลอื่นในเครือข่ายสังคมออนไลน์หลายกลุ่ม ทำหน้าที่เป็นผู้เชื่อมโยงระหว่างเครือข่ายสังคมออนไลน์แต่ละกลุ่มในการรับหรือการกระจายข้อมูลข่าวสารหรือผลการกระทำผิดปกติและการโจมตีในเครือข่ายสังคมออนไลน์

10. ฐานข้อมูลความผิดปกติและการถูกโจมตีของการใช้เครือข่ายสังคมออนไลน์ (Anomaly and Attack)

ข้อมูลการใช้งานระบบคอมพิวเตอร์จาก Log File ของการใช้งานเครือข่ายสังคมออนไลน์ในอินเทอร์เน็ต ที่มีลักษณะการกระทำผิดหรือการโจมตีบุคคลอื่นโดยผิดหลักของพระราชบัญญัติการกระทำผิดทางคอมพิวเตอร์ จากการใช้งานเครือข่ายสังคมออนไลน์ ซึ่ง Firewall สามารถตรวจจับความผิดปกติดังกล่าว และแสดงความผิดปกติและการโจมตีเป็นหมายเลขความผิดปกติ (Attack ID) ที่กำหนดโดย Firewall นั้น

11. ผังสังคมมิติ (Sociogram)

จาค็อบ โมเรโน (Jacob Moreno) เป็นผู้พัฒนาผังสังคมมิติ (Sociogram) ขึ้นเป็นคน

a) ลูกศรชี้ออกจากโหนด หมายถึงมุ่งไปพึ่งพาผู้อื่นในประเด็นนั้นๆ และลูกศรชี้เข้า

b) จำนวนและความหลากหลาย บ่งบอกถึงศักยภาพและความมีบทบาทเชื่อมโยงกับ

c) ผังสังคมมิติแสดงเห็นว่า ปัจเจกทุกคนในชุมชนหนึ่งๆนั้น จะมีทุนศักยภาพอยู่ใน

d) ทุกคนมีบทบาทในความเป็นผู้นำและผู้ตาม รวมทั้งต่างก็พึ่งพากันในแง่มุมที่

e) ในประเด็นต่างๆนั้น หากผู้ใดหรือโหนดใกมีลูกศรวิ่งเข้าหามาก ก็ทำให้วิเคราะห์

f) ผู้ที่มีลูกศรชี้เข้าและชี้ออกหลากหลายสี ก็แสดงถึงมีโครงสร้างและการปฏิสัมพันธ์

g) Key Leader หรือผู้นำหลัก ได้แก่ผู้ที่มีลูกศรวิ่งเข้าหามากที่สุด

12. Egocentric Network

เครือข่ายที่มีจุดศูนย์กลางอยู่ที่โหนดเดียว เครือข่ายแบบนี้จะสนใจความสัมพันธ์ระหว่างโหนดหนึ่งกับอีกโหนดหนึ่งเป็นคู่ๆ

13. Minimum Spanning Tree ของ Prim's Algorithm
เป็นอัลกอริทึมในทฤษฎีบทเกียวกับกราฟ โดยจะทำการหา Minimum Spanning

สมมติว่า $G = (V, E)$ คือกราฟแบบต่อเนื่อง ซึ่งแต่ละเส้นเชื่อมมีค่า Cost ประจำอยู่ Spanning Tree ของ G คือทรีอิสระที่เชื่อมต่อทุกๆ Vertices ใน V คือ Spanning Tree คือ ผลรวมของ Cost ของเส้นเชื่อมในทรีนั้น และในตอนนี้เราจะหาค่า Spanning Tree ที่มีค่าต่ำสุด

14. All-Pair Shortest Path ของ Floyd-Warshall Algorithm
เป็นขั้นตอนวิธีการวิเคราะห์กราฟเพื่อที่จะหาระยะทางของเส่นทางสั้นสุดในกราฟที่

1.9 สรุป

ในบทที่ 1 ได้นำเสนอถึง สภาพปัญหาของการใช้งานเครือข่ายสังคมออนไลน์ และความผิดปกติและโอกาสการถูกโจมตีในการใช้งานเครือข่ายสังคมออนไลน์ โดยผู้วิจัยได้นำเสนอถึงแนวทางในการพัฒนาตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ ในประเด็นดังนี้

1. เพื่อทำการวิเคราะห์หาความผิดปกติและโอกาสการถูกโจมตีจากการใช้เครือข่ายสังคมออนไลน์

2. เพื่อศึกษารูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์

3. เพื่อพัฒนาตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟสำหรับรองรับการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริง

4. เพื่อพัฒนาตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้า

ประโยชน์หลักที่คาดว่าจะได้รับจากงานวิจัยคือการพัฒนาตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ เป็นผลให้ข้อมูลและสารสนเทศขององค์กรสามารถได้รับการป้องกันและสร้างความมั่นคงปลอดภัยทั้งในด้านความลับ (Confidentiality) ความคงสภาพความถูกต้อง (Integrity) และความพร้อมใช้ (Availabllity) รวมทั้งองค์กรสามารถสร้างนโยบายและแนวปฏิบัติขององค์กร เพื่อป้องกันความเสี่ยงต่อข้อมูลและระบบสารสนเทศขององค์กรที่รองรับระบบงานทางด้านสุขภาพในระดับประเทศ (Public Health Sector in Thailand) ให้มีความมั่นคงปลอดภัยในระดับสูง

ประโยชน์ในด้านวิชาการ เนื่องจากผู้วิจัยได้ศึกษาแนวคิด ทฤษฎีงานวิจัย และได้สรุปรวบรวมไว้ในงานวิจัยชิ้นนี้ จึงเชื่อได้ว่าเป็นประโยชน์ต่อผู้อื่นได้ในอนาคต เพื่อที่จะค้นหากลยุทธ์การติดตามภัยจากการใช้เครือข่ายสังคมออนไลน์จากตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ สามารถทำให้ทราบถึงเหตุการณ์ปัจจุบัน และสามารถใช้ความเชื่อมโยงในเครือข่ายสังคมออนไลน์เพื่อพัฒนาตัวแบบในการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์ รวมทั้งพัฒนาตัวแบบในการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้า ซึ่งเป็นประโยชน์มากในการวิเคราะห์ และความเข้าใจในเครือข่ายสังคมออนไลน์ดังกล่าว สามารถนำไปสู่การดำเนินงานที่มีประสิทธิภาพของเครื่องมือในการสืบค้นผู้กระทำผิดปกติหรือมีพฤติกรรมการโจมตี การค้นหาเป้าหมายที่อาจจะได้รับผลกระทบจากการโจมตีนั้นๆ รวมทั้งการระบุกลุ่มที่ซ่อนอยู่หรือการหาสมาชิกที่หายไปของกลุ่มฯลฯ ในเครือข่ายสังคมออนไลน์ ซึ่งเป็นปัญหาที่พบบ่อยที่สุดในการรักษาความมั่นคงปลอดภัยและการสอบสวนทางอาญา