โพรโตคอลความมั่นคงปลอดภัยโดยใช้พร็อกซี่สนับสนุนคุณสมบัติความเป็นนิรนามของผู้ใช้สำหรับเครือข่ายสังคมเคลื่อนที่แบบอ้างอิงสถานที่

เอกลักษณ์ อิสระมโนรส[1] และ ศุภกร กังพิศดาร[2]

คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร

Emails: [1]boo10888@gmail.com, [2]supakorn@mut.ac.th

บทคัดย่อ

เครือข่ายสังคมเคลื่อนที่ (Mobile Social Networking) คือเครือข่ายสังคมที่สามารถเข้าถึงได้ผ่านทางอุปกรณ์สื่อสารไร้สาย แม้ว่าเครือข่ายดังกล่าวจะได้รับความนิยมสูงขึ้นในปัจจุบัน แต่ก็ยังมีปัญหาในหลายๆ ด้าน อย่างไรก็ตามงานวิจัยที่มีอยู่มุ่งเน้นไปที่การแก้ปัญหาของการละเมิดความเป็นส่วนตัวของผู้ใช้ โดยเฉพาะอย่างยิ่งการใช้งานผ่านโทรศัพท์มือถือที่สามารถระบุตำแหน่งได้ เพื่อแก้ไขปัญหาดังกล่าว งานวิจัยฉบับนี้นำเสนอโพรโตคอลสำหรับการเข้าใช้งานเครือข่ายสังคมเคลื่อนที่ที่สามารถซ่อนตัวตนที่แท้จริงของผู้ใช้ รวมทั้งไม่มีการบันทึกข้อมูลส่วนตัวของผู้ใช้ไว้ภายในระบบ นอกจากนี้ยังมีการกำหนดให้ระบบบันทึกหน้าเว็บเพจของผู้ใช้ที่ได้รับอนุญาตในการเผยแพร่แก่ผู้ใช้อื่นเพื่อเป็นการเพิ่มประสิทธิภาพของระบบอีกด้วย

คำสำคัญ— เครือข่ายสังคม; ความมั่นคงปลอดภัย; โพรโตคอลความมั่นคงปลอดภัย; ความมั่นคงปลอดภัยของเครือข่าย

1. บทนำ

ในปัจจุบันมีอุปกรณ์อิเล็กทรอนิกส์แบบพกพาที่รองรับการเชื่อมต่อแบบไร้สายจำนวนเพิ่มมากขึ้น เช่น คอมพิวเตอร์แลปท็อป (Laptop Computer) และพีดีเอ (Personal Digital Assistants หรือ PDA) เป็นต้น เนื่องจากแนวโน้มการใช้งานอุปกรณ์แบบพกพานั้นสามารถตอบสนองความต้องการและเพิ่มความสะดวกสบายให้แก่ผู้ใช้ และนอกจากอุปกรณ์ที่กล่าวถึงไปแล้วนั้น โทรศัพท์มือถือ (Mobile Device) ที่เชื่อมต่อกับเครือข่ายไร้สายได้ก็มีใช้ให้เห็นกันจำนวนมาก ตัวอย่างของเครือข่ายไร้สายได้แก่ Wi-Fi, CDMA หรือ GPRS/EDGE

การที่อุปกรณ์ดังกล่าวรองรับการเชื่อมต่อแบบไร้สายทำให้เกิดแอพพลิเคชั่น (Application) ใหม่ๆ ขึ้นมากมาย หนึ่งในแอพพลิเคชั่นที่เป็นที่นิยมคือ เครือข่ายสังคม (Social Networks) ซึ่งเป็นการสร้างสังคมเสมือนขึ้นบนอินเทอร์เน็ตผ่านทางเว็บไซท์ การที่เครือข่ายสังคมได้รับความนิยมอย่างสูงเนื่องจากผู้ใช้สามารถพูดคุย โพสต์ (Post) แลกเปลี่ยนความเห็นระหว่างกัน ส่งรูปภาพให้กัน ตัวอย่างของเครือข่ายสังคมได้แก่ Facebook [1] Hi5 [2] และ Twitter [3] เป็นต้น

เมื่อการเข้าถึงเครือข่ายสังคมบนอินเทอร์เน็ตได้รับความนิยมอย่างแพร่หลาย และสามารถเข้าถึงได้ง่ายมากขึ้นผ่านโทรศัพท์มือถือ ทำให้รูปแบบการใช้งานเครือข่ายสังคมในปัจจุบันเปลี่ยนไปเป็นแบบที่เรียกว่าเครือข่ายสังคมเคลื่อนที่ (Mobile Social Networking) [4] ด้วยคุณสมบัติเหล่านี้ เครือข่ายสังคมเคลื่อนที่จึงได้ถูกนำไปผสมผสานใช้ในธุรกิจการค้าการโฆษณา และการให้บริการต่างๆ เช่น บริการที่เกี่ยวกับตำแหน่งของผู้ใช้ (Location Based Service) หรือ บริการโฆษณาผ่านมือถือแบบอ้างอิงสถานที่ (Location Based Advertising) เป็นต้น

จากการที่ข้อมูลของผู้ใช้งานถูกนำเสนอผ่านเครือข่ายสังคมได้ง่าย รวดเร็วและมากขึ้นผ่านทางโทรศัพท์มือถือ ผู้ใช้งานอาจลืมคิดไปว่าข้อมูลส่วนตัวของผู้ใช้งานได้ถูกเปิดเผยง่ายมากขึ้นเช่นกัน นั่นยังไม่นับรวมถึงการพยายามเข้าถึงข้อมูลส่วนบุคคล จากบุคคลผู้ซึ่งไม่ได้รับอนุญาตให้เข้าถึงอีกด้วย

ที่ผ่านมาได้มีงานวิจัยที่เสนอแนวทางการแก้ไขปัญหาความเป็นส่วนตัวของผู้ใช้ภายในเครือข่ายสังคมเคลื่อนที่ [4] Beach *et al.* [5] ได้เสนอเทคนิคของการซ่อนตัวตนของผู้ใช้ภายในเครือข่ายสังคมเคลื่อนที่ โดยจัดตั้งบุคคลที่สามเรียกว่า Identity Server (IS) เพื่อซ่อนข้อมูลตัวตนของผู้ใช้ โดยการออกไอดีนิรนาม (Anonymous ID) แทนข้อมูลระบุตัวตนของผู้ใช้ ด้วยวิธีการนี้ทำให้ผู้ใช้งานเครือข่ายสังคมเคลื่อนที่ ที่อยู่ภายในเครือข่ายไร้สายเดียวกันไม่ทราบตัวตนที่แท้จริงของผู้ใช้คนอื่น อย่างไรก็ตามพบว่าผู้ใช้ทุกคนต้องฝากข้อมูลที่เป็นความลับอันได้แก่ ยูสเซอร์เนม (Username) และพาสเวิร์ด (Password) ไว้กับ IS สิ่งนี้ทำให้ IS สามารถปลอมตัวเป็นผู้ใช้งานคนนั้นได้ นอกจากนี้ Beach *et al.* ได้อ้างว่าระบบที่นำเสนอสามารถซ่อนตัวตนของผู้ใช้เมื่อมีการร้องขอเข้าดูข้อมูลในโพรไฟล์ (Profile) โดยผู้ใช้คนอื่นผ่านทางบลูทูช (Bluetooth) อย่างไรก็ตามพบว่าการเชื่อมต่อด้วยบลูทูชเป็นการสื่อสารระยะใกล้ ที่แม้ผู้ใช้จะได้รับไอดีนิรนามแล้วก็ตาม ก็ยังสามารถค้นหาตัวตนที่แท้จริงของผู้ใช้ได้ง่ายโดยการค้นหาภายในบริเวณพื้นที่นั้น

งานวิจัยฉบับนี้จึงได้เสนอวิธีการแก้ไขปัญหาเรื่องความเป็นส่วนตัวของการใช้งานเครือข่ายสังคมเคลื่อนที่จากงานวิจัยที่มีอยู่ [5] โดยได้มีการปรับปรุงการทำงานของ IS ไม่ให้เก็บยูสเซอร์เนมและพาสเวิร์ดของผู้ใช้ รวมทั้งเพิ่มคุณสมบัติการบันทึก (Cache) เว็บเพจเครือข่ายสังคม

ของผู้ใช้ เพื่อให้การร้องขอและค้นหาข้อมูลของผู้ใช้ทำได้เร็วยิ่งขึ้น นอกจากนี้ยังปรับปรุงการสื่อสารภายในระบบให้มีการเข้ารหัสลับข้อมูลเพื่อความมั่นคงปลอดภัยของระบบ

โครงสร้างของบทความวิจัยฉบับนี้มีดังนี้ บทที่ 2 กล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้อง บทที่ 3 กล่าวถึงงานวิจัยที่นำเสนอ บทที่ 4 วิเคราะห์และอภิปรายผลการวิจัย บทที่ 5 สรุปผลการวิจัย

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 Mobile Computing

ในปัจจุบัน อุปกรณ์มือถือรองรับการเชื่อมต่ออินเทอร์เน็ตได้ตลอดเวลา และได้รับการสนับสนุนการพัฒนาอย่างเต็มที่สำหรับนักพัฒนาแอ็พพลิเคชั่น สิ่งนี้เป็นการเพิ่มขีดความสามารถให้กับผู้ใช้ มีแอพพลิเคชั่นที่รองรับการใช้งานผ่านอินเทอร์เน็ตมากมาย เช่น การสั่งจองร้านอาหาร การจองตั๋วภาพยนตร์ การค้นหาข้อมูลผ่านเซิร์ชเอนจิ้น (Search Engine) การนำทาง (Navigation) และ Online Social Networking (OSN) เป็นต้น

เมื่อไม่นานมานี้ได้มีการเพิ่มขึ้นอย่างมากกับการใช้งานอุปกรณ์มือถือ ทั้งโทรศัพท์ที่สามารถเข้าถึงอินเทอร์เน็ต, การสื่อสารแบบไร้สาย และการสนับสนุนการพัฒนาของโปรแกรมเสริมต่างๆ โดยส่วนมากจะเป็นไอโฟน (iPhone) และไอพอดทัช (iPod Touch) ในความเป็นจริง เป็นที่ยอมรับกันว่าแอบพลิเคชั่นทางด้านอินเทอร์เน็ต กับอุปกรณ์พกพาของบริษัทแอปเปิ้ล มีจำนวนมากถึง 2 ใน 3 ของข้อมูลการใช้งานเว็บเบราเซอร์ทางอุปกรณ์มือถือ [6] ในเดือนพฤษภาคมของปี ค.ศ. 2010 สิ่งซึ่งแสดงถึงการใช้งานจำนวนมากและเพิ่มขึ้นอย่างรวดเร็วในปัจจุบัน

2.2 เครือข่ายสังคม (Social Networking)

การเจริญเติบโตของเครือข่ายสังคม (Social Networking) ที่สูงขึ้นปีที่ผ่านมา โดยเฉพาะการใช้งานของ Facebook ได้กระจายทั่วโลกและทุกเพศทุกวัย ตามสถิติของเว็บไซท์ Facebook.com พบว่าเว็บไซท์นี้มีผู้ใช้งานมากกว่า 400 ล้านคน ซึ่งกว่า 200 ล้านเข้าสู่ระบบทุกวัน [7] ในการเปรียบเทียบสถิติการใช้งานอินเทอร์เน็ตทั่วโลกจาก comScore [8] สถิตินี้ได้บ่งบอกว่า เกือบ 1 ใน 10 ของผู้ใช้อินเทอร์เน็ตทั้งหมด เข้าสู่ Facebook เป็นประจำทุกวัน และผู้ที่เข้าสู่ระบบ Facebook มีขนาดสูงกว่าการใช้งานอินเทอร์เน็ตของประเทศใดประเทศหนึ่ง (จีนมีผู้ใช้อินเทอร์เน็ตสูงที่สุดด้วย 179,700,000 [8]) ตามสถิติ Facebook (เดือนมิถุนายน 2010) ขณะนี้มีมากกว่า 100 ล้านคนที่ใช้งาน Facebook ทางโทรศัพท์มือถือ [7] และผู้ใช้เหล่านั้นมีมากกว่า 50% ใช้งาน Facebook มากกว่าผู้ที่ไม่ใช้โทรศัพท์มือถือ

2.3 เครือข่ายสังคมเคลื่อนที่ (Mobile Social Networking)

Mobile Social Networking (MSN) [4] เป็นเครือข่ายทางสังคมหรือกลุ่มบุคคลที่มีความสนใจในเรื่องเดียวกัน สนทนาและเชื่อมต่อกับบุคคลอื่น ผ่านทางอุปกรณ์พกพาจำพวกโทรศัพท์มือถือ หรือพีดีเอโฟน โดยแนวโน้มปัจจุบันสำหรับเครือข่ายสังคมออนไลน์นั้น เช่น Facebook, Hi5, Twitter หรืออื่นๆ จะนิยมเป็นอย่างมากในการใช้งานผ่านแอ็พลิเคชั่นบนโทรศัพท์มือถือ ที่ผู้ใช้งานจะสะดวกสบายมากขึ้น และสามารถที่จะใช้งานได้ทุกเวลาทุกสถานที่ ด้วยคุณสมบัติที่สามารถใช้งานได้ง่ายในทุกสถานที่ ทำให้เกิดการนำไปใช้ร่วมกับการให้บริการแบบอ้างอิงสถานที่ (Location Based Service หรือ LBS) ที่เป็นระบบให้บริการระบุตำแหน่งโทรศัพท์มือถือ เช่น GPS โดยนอกจากจะให้บริการระบุตำแหน่งแล้ว ยังสามารถนำ LBS ไปผนวกกับการให้บริการผ่านโทรศัพท์มือถือได้ เช่น Facebook ที่ใช้คุณสมบัตินี้ในการตรวจสอบสถานที่ต่างๆ [9] ร้านค้าปลีก ร้านอาหาร หรือ เป็นแอ็บพลิเคชั่นในการตามหาเพื่อน (Google Latitude [10]) หรือการให้บริการที่ผสมผสานระหว่างเครือข่ายสังคมและการระบุตำแหน่งสถานที่ (Four Square[11], Brightkite[12], Gowalla[13]) เป็นต้น

2.4 ปัญหาความมั่นคงปลอดภัยของเครือข่ายสังคมเคลื่อนที่

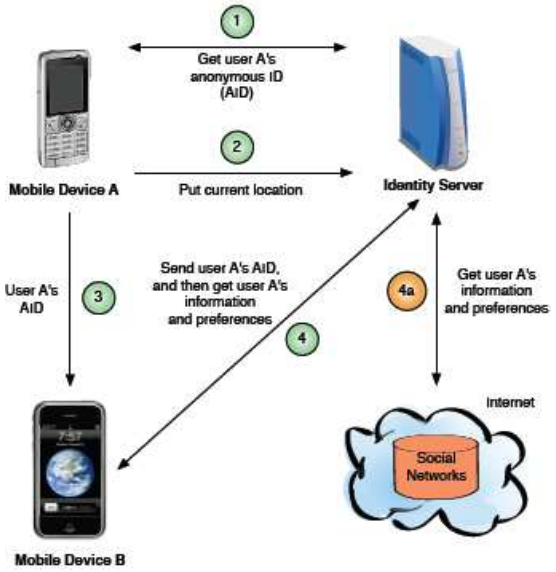
การใช้งานของ MSN ในปันจุบันต้องยอมรับว่ามีการใช้งานแพร่หลายอย่างมาก การที่ข้อมูลต่างๆของผู้ใช้มีการแลกเปลี่ยนกับผู้ใช้งานอื่นจำนวนมาก ทำให้ความเป็นส่วนตัวบนเว็บไซท์เครือข่ายสังคมน้อยลงไปทุกที แม้แต่ละเว็บไซท์จะมีคุณสมบัติบางประการที่ให้ความช่วยเหลือในการปกป้องข้อมูลส่วนบุคคล แต่ก็ยังมีความยุ่งยากและผู้ใช้งานก็ยังละเลยในเรื่องนี้ คุณสมบัติพื้นฐานหลายประการของเว็บไซท์เครือข่ายสังคมได้เปิดเผยข้อมูลส่วนบุคคลออกมามากมายอย่างที่ผู้ใช้งานคาดไม่ถึง เช่น การบอกตำแหน่ง tweet ของตนเองให้ผู้อื่นรู้ตำแหน่งของ GPS ซึ่งกรณีนี้เคยเกิดปัญหามาแล้ว [14] เนื่องจากมีผู้ใช้งานทำการโพสกิจกรรมที่ตนเองกำลังทำอยู่ ไปยังเว็บไซท์เครือข่ายสังคม คือกำลังจะออกไปดูคอนเสร์ต เพียงแค่ 13 นาทีเท่านั้น ผู้ใช้งานถูกโจรปล้นทรัพย์สินไปรวมมูลค่า 10,000 ดอลล่าห์ แต่ยังโชคดีที่สามารถจับโจรได้จากกล้องวงจรปิด ซึ่งผู้ใช้งานได้กล่าวว่าโจรคนนี้เป็นเพื่อนในเว็บไซท์เครือข่ายสังคม ได้ดักรอเวลาและเข้ามาขโมยทรัพย์สินทันทีที่ผู้ใช้งานออกไปข้างนอก ยังมีตัวอย่างอีกปัญหาหนึ่งที่พบคือการลงทะเบียน Facebook ผ่านทางโทรศัพท์มือถือ [15] โดย Facebook จะให้ทำการยืนยันด้วยเบอร์โทรศัพท์มือถือของผู้ลงทะเบียน นั่นเท่ากับว่าผู้ลงทะเบียนได้เปิดเผยข้อมูลเบอร์โทรศัพท์ไปโดยปริยาย ซึ่งอาจตามมาด้วยการนำข้อมูลเบอร์โทรศัพท์ไปใช้ในทางที่ไม่ดีก็เป็นได้ นี่ยังไม่ได้กล่าวถึงการเปิดเผยข้อมูลที่อยู่ อีเมล์ หรืออื่นๆ ด้วยการให้ข้อมูลเองจากผู้ใช้งาน จากตัวอย่างเหล่านี้แสดงให้เห็นว่าเรื่องความปลอดภัยของข้อมูลกับเครือข่ายสังคมเคลื่อนที่เป็นสิ่งที่สำคัญมากเพียงใด นี่ยังไม่รวมถึงเทคนิคการโจมตีแบบต่างๆ ที่มีอยู่บนระบบเครือข่าย เช่น การถูกดับจับข้อมูล (Eavesdropping), การปลอมตัวด้วย Social Network ID (Spoofing) และการนำ Social Network ID มาทำซ้ำเพื่อสวมรอย (Replay attack) [16]

2.5 งานวิจัยที่เกี่ยวข้อง

เพื่อเป็นการแก้ไขปัญหาที่ได้อ้างถึงในหัวข้อ 2.4 นั้น Beach *et al.* [5] ได้นำเสนอการใช้ไอดีนิรนาม (Anonymous Identifier หรือ AID) และ Identity Server หรือ IS ในการแก้ไขปัญหาความเป็นส่วนตัวและความมั่นคงปลอดภัยแทนการใช้ไอดีของเครือข่ายสังคม (Social Networking ID) ในการสื่อสารโดยตรงระหว่างผู้ใช้และระบบ

ในการทำงานนั้น AID ซึ่งเป็นค่าสุ่ม (nonce) และถูกสร้างโดยเซิร์ฟเวอร์ที่เชื่อถือได้ (Identity Server หรือ IS) โดยก่อนที่โทรศัพท์มือถือจะประกาศให้โทรศัพท์มือถือเครื่องอื่นรู้ถึงการมีตัวตนอยู่นั้น จะต้องทำการติดต่อ IS อย่างปลอดภัย คือติดต่อผ่านเว็บเซอร์วิส (Web Service) ด้วยโพลโตคอลที่ถูกเข้ารหัส (HTTPS) เพื่อขอ AID จากนั้น IS จะทำการสร้าง AID ด้วยฟังก์ชั่นแฮช (Hash function) เช่น SHA-1 กับค่า Random Salt โดย IS จะสร้าง AID ใหม่ทุกครั้งที่ถูกร้องขอ และส่งกลับไปให้ผู้ใช้ A หลังจากนั้นผู้ใช้ A ก็จะแชร์ค่า AID กับโทรศัพท์มือถือของผู้ใช้อื่นในระยะของสัญญาณ ผ่านทาง Bluetooth AID Sharing Service หลังจากที่ผู้ใช้ B ค้นหาและพบ AID Sharing Service ของผู้ใช้ A แล้ว ผู้ใช้ B จะสร้างการเชื่อมต่อไปยังผู้ใช้ A เพื่อรับค่า AID ที่ถูกแชร์ไว้ หลังจากที่ผู้ใช้ B ได้รับ AID ผู้ใช้ A จะส่งการร้องขอ AID ค่าใหม่จาก IS ซึ่งทุกครั้งที่มีการร้องขอ AID ใหม่ IS จะบันทึกตำแหน่งของผู้ใช้ A และ AID ค่าใหม่นี้จะมีไว้กระจายให้กับผู้ใช้อื่นที่ต้องการเชื่อมต่อ AID Sharing Service กับผู้ใช้ A ต่อไป

หลังจากผู้ใช้ B ได้รับ AID ของผู้ใช้ A แล้วผู้ใช้ B ทำการค้นหาข้อมูลประวัติโดยย่อของเครือข่ายสังคม (Social Networking Profile) ที่สัมพันธ์กับ AID นี้บน IS โดยที่ผู้ใช้คนหนึ่งสามารถมี AID ได้มากกว่าหนึ่งค่า หมายถึงว่าผู้ใช้อื่นๆที่อยู่ใกล้สามารถรับข้อมูลเกี่ยวกับเครือข่ายสังคมของผู้ใช้ A ได้ และที่ IS เอง จะทำการตั้งค่าอายุของเวลา (Timeout) ของแต่ละ AID ไว้ที่ 30 วินาที เพื่อป้องกันรายการ AID ใน IS มีขนาดใหญ่เกินไปโดยขาดการควบคุม ดังรูปที่ 1



รูปที่ 1. Anonymous IDs และ Identity Server

การใช้ AID ของระบบนี้จะให้ความเป็นส่วนตัวกับโทรศัพท์มือถือ เนื่องจากโทรศัพท์มือถือจะใช้ AID ในการเชื่อมต่อ ทำให้บุคคลอื่นผู้ไม่หวังดีที่ต้องการจะดักจับข้อมูลเหล่านี้ ไม่สามารถหาความสัมพันธ์จาก AID และ Social Networking ID ได้

การลงทะเบียนของผู้ใช้ต่อ IS นั้น เริ่มต้นที่ผู้ใช้งานส่งข้อมูล IS User, IS Password และ Social Networking ID ให้แก่ IS โดย IS User นี้มีไว้เพื่อใช้ในการล็อกอิน (Login) เข้าสู่ IS จากนั้น IS ทำการบันทึกตำแหน่งของโทรศัพท์มือถือของผู้ใช้นั้นๆ ไว้ โดยที่เจ้าของ IS User จะมีสิทธิ์ทราบเพียงผู้เดียว หลังจากที่ IS ได้รับค่า Social Networking ID แล้ว IS ส่งการร้องขอข้อมูล Social Networking Profile ผ่านทาง Social Networking API ของเว็บไซท์เครือข่ายสังคมนั้นๆ [17, 18, 19] โดยที่ข้อมูลเหล่านี้จะเป็นข้อมูลที่ถูกแชร์ให้กับผู้ใช้อื่นๆ ที่อยู่ภายในระยะ 20 เมตร (ระยะการส่งข้อมูลของบลูทูธ)

การใช้ IS และ AID ของงานวิจัยนี้สามารถแก้ปัญหาการเปิดเผยข้อมูล Social Networking ID ของผู้ใช้ซึ่งถือเป็นข้อมูลส่วนตัวในระบบเครือข่ายสังคมได้ นอกจากนี้ยังพบว่าข้อมูลที่เป็นความลับของผู้ใช้อันได้แก่ ยูสเซอร์เนมและพาสเวิร์ดในการเข้าสู่เว็บไซท์เครือข่ายสังคม ถูกเก็บไว้ที่ IS สิ่งนี้ทำให้ IS สามารถปลอมตัวเป็นผู้ใช้ในการเชื่อมต่อกับเครือข่ายสังคมนั้นๆ ได้ ในความเป็นจริงแล้ว IS ควรจะทราบเพียงแค่ข้อมูลที่ผู้ใช้ต้องการเปิดเผยให้ IS ทราบเท่านั้น เนื่องจาก IS แท้จริงแล้วเป็นเพียงแค่บุคคลที่สาม และเป็นเพียงผู้ให้บริการที่ผู้ใช้ไม่จำเป็นต้องให้การเชื่อถือ หรือสามารถกล่าวอีกนัยหนึ่งว่า IS เป็นเพียงผู้อำนวยความสะดวกในการเชื่อมต่อกับเครือข่ายสังคมเท่านั้น

3. งานวิจัยที่นำเสนอ

จากปัญหาของ Identity Server (IS) ที่เก็บข้อมูลส่วนตัวของผู้ที่ใช้ดังที่กล่าวไปแล้วในบทที่ 2 งานวิจัยนี้จึงได้นำเสนอแนวคิดการออกแบบโพรโตคอลที่สามารถรักษาความเป็นส่วนตัวของผู้ใช้ในการเข้าสู่เครือข่ายสังคมผ่านอุปกรณ์เคลื่อนที่ โดยที่มุ่งเน้นในการรักษาความคุณสมบัติความมั่นคงปลอดภัยที่จำเป็น ดังรายละเอียดด้านล่าง

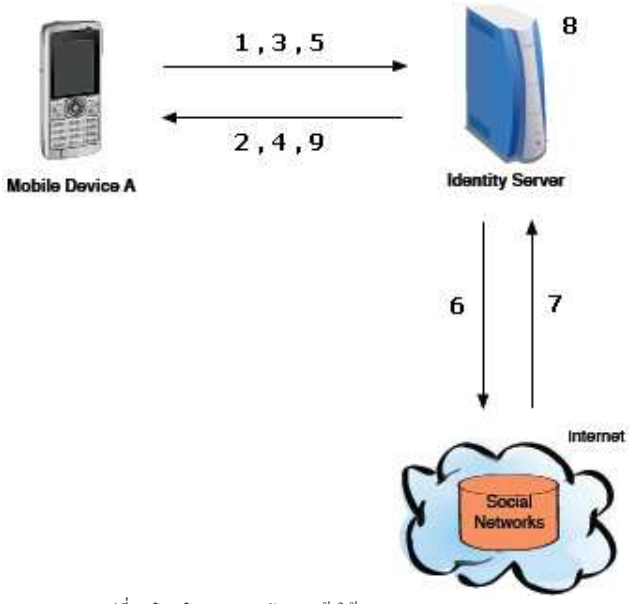
3.1. ภาพรวมของระบบ

ระบบที่นำเสนอประกอบด้วย

1) ผู้ใช้ โดยที่ผู้ใช้แต่ละคนสามารถเข้าถึงเครือข่ายสังคมได้ผ่านทางอุปกรณ์พกพาที่สามารถเชื่อมต่อกับเครือข่ายไร้สาย เช่น โทรศัพท์มือถือ เป็นต้น
2) Identity Server หรือ IS เป็นเซิร์ฟเวอร์ (Server) ที่ทำหน้าที่เป็นตัวกลางในการเชื่อมต่อแบบไร้สายเข้าสู่เครือข่ายสังคม ตัวอย่างของการเชื่อมต่อแบบไร้สายโดย IS ได้แก่ Wi-fi และ Bluetooth เป็นต้น

เพื่อเป็นการแก้ไขปัญหาของการเปิดเผยข้อมูลลับของผู้ใช้ [5] ในระบบนี้ IS ไม่มีการเก็บค่า Social Networking ID และพาสเวิร์ด โดยให้ผู้ใช้ล็อกอินเข้าสู่เว็บไซท์เครือข่ายสังคมด้วยตนเองผ่านทางโทรศัพท์มือถือ การที่โทรศัพท์มือถือสำรวจพบ AID Sharing Service และสามารถเข้าถึงข้อมูล Social Network Profile ของบุคคลอื่นได้โดยตรงนั้นอาจเป็นการเข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาตก็เป็นได้ ซึ่งงานวิจัยนี้ได้เห็นว่าปัญหาเรื่องความมั่นคงปลอดภัยของผู้ใช้งานเหล่านี้ เป็นสิ่งที่ไม่สามารถยอมรับได้ จึงหาแนวทางการแก้ไขปัญหาเหล่านี้ ดังแสดงรายละเอียดในหัวข้อถัดไป

3.2. รายละเอียดของงานวิจัยที่นำเสนอ



รูปที่ 2. โพรโตคอลสำหรับการเข้าใช้ Social Network Website

โพลโตคอลแรกที่ถูกนำเสนอขึ้นนี้ มีคุณสมบัติในการป้องกันการเปิดเผยของข้อมูลส่วนบุคคล ซึ่งอาจเกิดจากการโจมตีชนิดต่างๆ รวมไปถึงข้อมูล Social Network ID สำหรับผู้ที่เข้าใช้เครือข่ายสังคมบนอินเทอร์เน็ตผ่านโทรศัพท์มือถือ รายละเอียดของโพรโตคอลแสดงดังรูปที่ 2

1. A → IS : A ส่งการร้องขอ IS web login ไปยัง IS

2. IS → A : IS ตอบกลับพร้อมส่ง IS web login ไปยัง A

3. A → IS : A ทำการล็อกอินและส่งข้อมูลกลับด้วย {IS User, IS Password, Nonce, Timestamp} โดยค่าทั้งหมดจะผ่านฟังก์ชั่นแฮช (Hash function)

4. IS → A : เมื่อล็อกอินสำเร็จ IS จะส่งค่า AID และฟอร์มสำหรับการล็อกอินเข้าเว็บไซท์ Social Networking ไปยัง A

5. A → IS : A ล็อกอินและส่งข้อมูลกลับด้วย Social networking ID และ Social networking secret [17] เพื่อทำการร้องขอข้อมูล Social Networking Profile

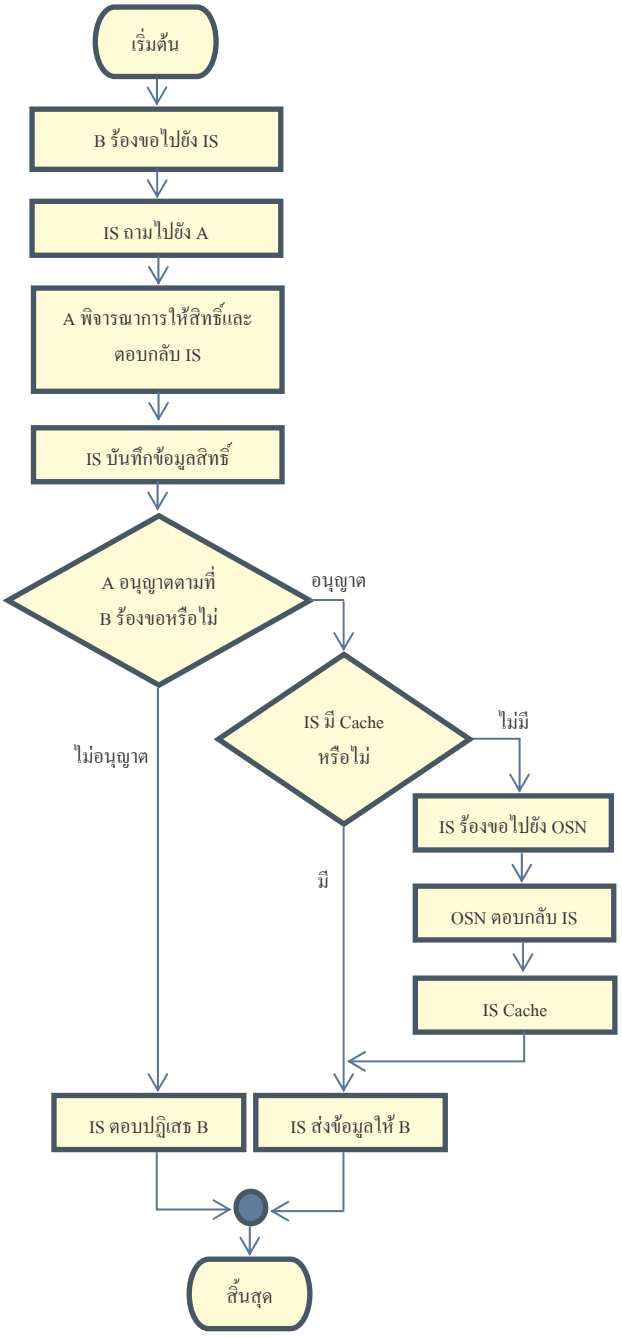
6. IS → OSN: IS ทำการส่งต่อข้อมูล Social networking ID และ Social networking secret ผ่าน Social Networking API [17, 18, 19] ไปยัง OSN

7. OSN → IS: OSN ทำการส่งข้อมูล Social Networking Profile ของ A กลับไปยัง IS

8. IS : IS เก็บข้อมูล Social Networking Profile ของ A เอาไว้เพื่อให้ผู้ใช้คนอื่นสามารถเปิดดูข้อมูลโดยย่อของ A ได้ อย่างไรก็ตาม การอนุญาตให้ผู้ใช้คนใดเปิดดูข้อมูลของ A ได้นั้นจะต้องได้รับการอนุญาตจาก A ก่อน รายละเอียดของโพรโตคอลดังกล่าวแสดงในหัวข้อที่ 3.3

9. IS → A : IS ส่งข้อมูล Social Networking Profile ของ A ไปยัง A

3.3 โพรโตคอลการให้สิทธิ์ผู้ใช้ในการเข้าถึงข้อมูลเครือข่ายสังคม



รูปที่ 3. โพรโตคอลการให้สิทธิ์สำหรับ MSN

จุดประสงค์ของโพรโตคอลนี้ คือ เพื่อเพิ่มคุณสมบัติให้กับ IS ในการบันทึก (Caching) และจำแนกชนิดของรายการข้อมูลบนเว็บไซท์ที่เคยถูกเรียกใช้งานมาแล้ว เช่น รายการข้อมูลประวัติโดยย่อ, รายการรูปภาพ, รายการเพื่อน หรือส่วนอื่นๆ เป็นต้น โดยหากมีผู้ใช้งานอื่นต้องการเข้าถึงข้อมูลส่วนบุคคลเหล่านี้จะต้องทำการขออนุญาตเจ้าของข้อมูล ว่าสามารถยอมให้เข้าถึงกลุ่มข้อมูลใดได้บ้าง โดยขั้นตอนทั้งหมดนี้จะมี IS เป็นตัวกลางในการเก็บบันทึกสิทธิ์ที่อนุญาต รวมถึงข้อมูลทั้งหมดจะถูก

เข้ารหัสลับด้วยโพรโตคอลที่ปลอดภัย (HTTPS) รายละเอียดผังงานของโพรโตคอลแสดงดังรูปที่ 3 และสามารถอธิบายได้ดังนี้

1. B → IS : B ส่งการร้องขอไปยัง IS เพื่อขอเข้าถึงข้อมูล Social Networking ของ A
2. IS → A : IS ส่งคำถามหา A ว่า อนุญาตให้เปิดเผยข้อมูลใดบ้างกับ B
3. A → IS : A เลือกรายการข้อมูลที่อนุญาต และส่งกลับข้อมูลไปยัง IS
4. IS : IS บันทึกและปรับปรุงข้อมูลสิทธิ์ของผู้ใช้งาน
   กรณีที่1: ถ้าผู้ใช้ A ไม่อนุญาตให้ผู้ใช้ B เข้าถึงข้อมูล
5. IS → B : IS ตอบปฏิเสธการเข้าถึงข้อมูลไปยัง B
   กรณีที่2: ถ้าผู้ใช้ A อนุญาต และ IS มีข้อมูล Cache
6. IS → B : IS ส่งข้อมูลตามที่ร้องขอไปยัง B
   กรณีที่3: ถ้าผู้ใช้ A อนุญาต แต่ IS ไม่มีข้อมูลใน Cache
7. IS → OSN: IS ส่งการร้องขอข้อมูลไปยัง OSN
8. OSN → IS: OSN ตอบกลับมายัง IS
9. IS : IS ทำการเก็บข้อมูล (Caching)
10. IS → B : IS ส่งข้อมูลตามที่ร้องขอไปยัง B

4. วิเคราะห์และอภิปราย

งานวิจัยฉบับนี้เชื่อว่า วิธีดังกล่าวจะสามารถช่วยทำให้การใช้งานเครือข่ายสังคมเคลื่อนที่กับระบบ Location-based service ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น ทั้งในด้านของความเป็นส่วนตัวและความมั่นคงปลอดภัย ทั้งในด้านของประสิทธิภาพทางการใช้งาน รวมไปถึงความยืดหยุ่นและความเข้ากันได้ในเครือข่ายสังคมเคลื่อนที่

4.1. ความเป็นส่วนตัวของผู้ใช้ (User Privacy) และความมั่นคงปลอดภัย

จากระบบเดิม ร่วมกับโพลโตคอลที่งานวิจัยฉบับนี้ได้ออกแบบมานั้น ได้นำเสนอให้มีการใช้ค่า AID ในการติดต่อสื่อสารภายในระบบเครือข่ายแทน ทำให้ค่า Social Network ID ซึ่งถือเป็นข้อมูลส่วนบุคคลไม่ถูกเปิดเผยออกไป โดยหากมีผู้ที่พยายามปลอมตัว (Spoofing) ด้วย Social Network ID หรือ พยายามนำข้อมูล Social Network ID มาทำซ้ำเพื่อขโมยความเป็นส่วนตัว (Replay attack) ผู้ที่ประสงค์ร้ายจะได้รับค่า AID ไปแทน และเนื่องจากระบบมีการติดต่อสื่อสารด้วยโพลโตคอลที่ถูกเข้ารหัส (HTTPS) ทำให้สามารถป้องกันการถูกดักจับข้อมูล (Eavesdropping) ได้

และจากระบบเดิมที่ผู้ใช้งานจะต้องให้ค่า Social Network ID กับ Identity Server (IS) ตั้งแต่ขั้นตอนการลงทะเบียน เพื่อใช้ในการหาความสัมพันธ์กับค่า AID และนอกจากนั้น IS ยังใช้ค่า Social Network ID ดึงข้อมูลประวัติโดยย่อ (Profile) ผ่าน Social Network API มาเก็บไว้บน IS ทำให้ระบบรู้ข้อมูลส่วนบุคคลของผู้ใช้งานมากเกินความจำเป็น แต่ด้วยการนำโพลโตคอลของงานวิจัยฉบับนี้เข้ามาใช้ ทำให้ระบบไม่จำเป็นต้องใช้ค่า Social Networking ID ในการหาความสัมพันธ์กับ AID อีกต่อไป เนื่องจากสามารถใช้ค่าอื่นทดแทนได้ เช่น ค่า IS User ในการระบุความสัมพันธ์แทน เพราะฉะนั้นโอกาสของการที่จะหาความสัมพันธ์ไปยัง Social Network ID นั้น จะหลุดจากข้อจำกัดของระบบเดิมไป รวมไปถึงผู้ใช้งานยังสามารถที่จะปกป้องข้อมูลส่วนบุคคลของตนเองได้ระดับหนึ่ง โดยหากมีการร้องขอข้อมูล Social Networking Profile จากโทรศัพท์มือถือเครื่องอื่น IS จะนำข้อมูลการร้องขอนั้น ไปถามเพื่อขออนุญาตเจ้าของข้อมูลเสียก่อน และเจ้าของข้อมูลนั้นสามารถเลือกได้ว่าจะอนุญาตให้เข้าถึงข้อมูลใดบ้างในเครือข่ายสังคม ก่อนที่ IS จะส่งข้อมูลหน้าเว็บเพจของเครือข่ายสังคมตามที่ถูกอนุญาตกลับไปให้ผู้ที่ร้องขอ

4.2. การวิเคราะห์ประสิทธิภาพ

ด้วยคุณสมบัติที่มากขึ้นของ Identity Server (IS) ทำให้ระบบสามารถเก็บบันทึก (Caching) หน้าเว็บเพจที่เคยถูกเข้าถึงได้ในฐานข้อมูล โดยผู้ใช้งานสามารถกำหนดกลุ่มเว็บเพจที่ต้องการอนุญาตให้กับผู้ที่ต้องการเข้าถึงข้อมูลได้ด้วยตนเอง ว่าในแต่ละคนจะอนุญาตให้เข้าถึงหน้ากลุ่มเว็บเพจส่วนตัวใดได้บ้าง ซึ่งถือเป็นการเพิ่มประสิทธิภาพและหลุดจากข้อจำกัดเดิมของระบบ ที่ยอมให้ผู้ใช้งานในระบบบุคคลอื่นๆสามารถเข้าถึงข้อมูลเครือข่ายสังคมของผู้ใช้งานได้โดยไม่มีมาตรการป้องกันใดทั้งสิ้น

ที่อุปกรณ์โทรศัพท์มือถือนั้น จะใช้งานผ่านทางเว็บเบราเซอร์ควบคู่ไปกับการใช้งาน Java Applet ในการล็อกอินเข้าสู่เครือข่ายสังคม ซึ่งเครื่องมือเหล่านี้ส่วนใหญ่รองรับกับโทรศัพท์มือถือในปัจจุบันอยู่แล้ว

ในส่วนของระบบเครือข่าย ระบบนี้สามารถใช้งานได้ทั้งกับเครือข่าย Bluetooth หรือ Wi-Fi ก็ได้ โดยหากเป็นเครือข่าย Bluetooth นั้นอาจจะได้ระยะทางที่ใกล้กว่า และการทำงานของ Bluetooth AID Sharing Service อาจทำให้ประสิทธิภาพการทำงานของโทรศัพท์มือถือลดน้อยลง หากเป็นการทำงานผ่านเครือข่าย Wi-Fi นั้น จะได้ระยะทางที่ไกลขึ้น ความกว้างของช่องสัญญาณ Bandwidth เพิ่มมากขึ้น โดยส่วนของ AID Sharing Service สามารถย้ายไปทำงานที่ฝั่งของ Identity Server ได้ ส่งผลให้โทรศัพท์มือถือที่มีคุณภาพไม่สูงมาก ก็ยังสามารถใช้งานระบบนี้ได้

4.3. ความเข้ากันได้ในเครือข่ายสังคมเคลื่อนที่ทั่วไป

การเชื่อมต่อไปยังเว็บไซท์เครือข่ายสังคมนั้นเป็นหน้าที่ของ Identity Server (IS) โดยจะเชื่อมต่อผ่าน Social Network API ทำให้ไม่จำเป็นต้องแก้ไขเปลี่ยนแปลงสิ่งใดเพิ่มสำหรับทางฝั่งของเว็บไซท์เครือข่ายสังคม สำหรับความหยืดหยุ่นในการเพิ่มหรือลด Social Networking API นั้น ในปัจจุบันเว็บไซท์เครือข่ายสังคมหลายๆเว็บไซท์มีการพัฒนา API ของตนเองขึ้นมา เช่น Facebook ได้พัฒนา Facebook API [17] ขึ้นมา ทาง Twitter ได้พัฒนา Twitter API [18] ขึ้นมา และทางบริษัท Google ก็มีความพยายามที่จะพัฒนา OpenSocial API [19] ขึ้นมาเช่นเดียวกัน ที่สามารถใช้ได้กับเว็บไซท์เครือข่ายสังคมอื่นทั่วๆไปหลายเว็บไซท์ ซึ่ง API เหล่านี้สามารถนำมาใช้ร่วมกับ Identity Server (IS) ได้

5. บทสรุป

ในเวลานี้เครือข่ายสังคมออนไลน์ได้รับความนิยมสูงมาก อย่างไรก็ตามการใช้งานไม่ว่าจะเป็นในส่วนของผู้ใช้งานหรือส่วนของแอ็บพลิเคชั่นก็ตามจะต้องมีการปกปิดข้อมูลส่วนตัวของผู้ใช้งาน ต้องสามารถยืนยันตัวบุคคลได้ รวมไปถึงต้องมีมาตรการในการควบคุมดูแลรักษาความมั่นคงปลอดภัยของผู้ใช้งานอีกด้วย แต่ถึงอย่างไรก็ตามแม้ว่างานวิจัยฉบับนี้จะมีมาตรการในการจัดการเรื่องความมั่นคงปลอดภัย แต่ในความเป็นจริงข้อมูลต่างๆของผู้ใช้งานที่อยู่บนอินเทอร์เน็ต เช่น เพลงที่ชื่นชอบ, ภาพยนตร์ที่ชื่นชอบ , กีฬาที่ชื่นชอบ เป็นต้น ข้อมูลเหล่านี้สามารถที่จะนำมาทำสถิติ เพื่อค้นหาย้อนกลับถึงข้อมูลส่วนบุคคลที่เป็นจริงก็ได้ หรือการที่เพื่อนในเครือข่ายสังคมที่มีสิทธิ์ในการเข้าถึงข้อมูลส่วนบุคคล เช่น รูปภาพ ได้ทำสำเนา (copy) ข้อมูลและบันทึกเก็บลงในหน่วยเก็บความจำส่วนตัว สิ่งเหล่านี้ก็เป็นอีกสาเหตุหนึ่งที่ทำให้ข้อมูลส่วนบุคคลรั่วไหล (Privacy Leakage) ได้เช่นกัน

ผลงานที่จะนำเสนอต่อไปในอนาคต จะเป็นการสร้างระบบโดยอ้างอิงจากงานวิจัยฉบับนี้ เพื่อพิสูจน์และประเมินในเรื่องของประสิทธิภาพและราคา โดยการพิสูจน์นั้นจะแสดงถึงการจัดการด้านความเป็นส่วนตัวและความมั่นคงปลอดภัยตามที่ถูกระบุโดยงานวิจัยฉบับนี้ ว่าสามารถแก้ไขปัญหา และทำงานได้อย่างมีประสิทธิภาพ

เอกสารอ้างอิง

[1] Facebook. “Facebook”. www.facebook.com.

[2] Hi5. “Hi5”. www.hi5.com.

[3] Twitter. “Twitter”. www.twitter.com.

[4] WIKIPEDIA The Free Encyclopedia. “Mobile Social Network”. http://en.wikipedia.org/wiki/Mobile_social_network. 2010.

[5] Aaron Beach, Mike Gartrell, and Richard Han. “Solutions to Security and Privacy Issues in Mobile Social Networking”. 2009.

[6] NETMARKETSHARE. “Mobile browsing by platform market share”. http://marketshare.hitslink.com/mobile-phones.aspx.

[7] Facebook. “Facebook Statistics”. http://www.facebook.com/press/info.php?statistics. 2010.

[8] ComScore. “Comscore”. http://www.comscore.com/Press_Events.

[9] Mashable Social Media. “Facebook Adding Location Features This Month”. http://mashable.com/2010/05/06/facebook-location. 2010.

[10] WIKIPEDIA The Free Encyclopedia. “Google Latitude”. http://en.wikipedia.org/wiki/Google_Latitude. 2010.

[11] WIKIPEDIA The Free Encyclopedia. “Foursqaure”. http://en.wikipedia.org/wiki/Foursquare_(social_networking). 2010.

[12] WIKIPEDIA The Free Encyclopedia. “Brightkite”. http://en.wikipedia.org/wiki/Brightkite. 2010.

[13] WIKIPEDIA The Free Encyclopedia. “Gowalla”. http://en.wikipedia.org/wiki/Gowalla. 2010.

[14] NEWS CHANNEL8. “Facebook Status Updates Linked to Burglaries”. http://www.news8.net/news/stories/0310/719489.html. 2010.

[15] ACIS PROFESSIONAL CENTER. “ภัยจากการใช้งานโปรแกรมประเภท "Social Networks" โดยไม่ระมัดระวัง”. http://www.acisonline.net/article/?p=15. 2010.

[16] Fabian Schneider, Anja Feldmann, Balachander Krishnamurthy, Walter Willinger. “Understanding Online Social Network Usage from a Network Perspective”. 2009.

[17] Facebook Developers. “Facebook API”. http://developers.facebook.com/docs. 2010.

[18] Twitter. “Twitter API”. http://apiwiki.twitter.com.

[19] WIKIPEDIA The Free Encyclopedia. “OpenSocial API”. http://en.wikipedia.org/wiki/OpenSocial. 2010.