โมเดลการแพร่ระบาดของมัลล์แวร์ โดย SMS/MMS ในโทรศัพท์มือถืออัจฉริยะ

SMS/MMS Smartphone Malware Propagation Models

ชูติวรรณ บุญอาชาทอง*[1] และ คงศักดิ์ บุญอาชาทอง[2]
[1]คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสวนดุสิต
[2]คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

Chutiwan Boonarchatong*[1] & Kongsak Boonarchatong[2]
[1]Faculty of Science and Technology, Suan Dusit University
[2]Faculty of Engineering, Kasetsart University

บทคัดย่อ

เนื่องจากความนิยมในการใช้โทรศัพท์มือถืออัจฉริยะเพิ่มจำนวนมากขึ้นอย่างรวดเร็ว ในขณะเดียวกันการคุมคามจากการโจมตีของมัลแวร์ก็เพิ่มขึ้นในทิศทางเดียวกัน วิธีการโจมตีที่สำคัญโดยการส่ง SMS/MMS อันจะทำให้เกิดความสูญเสียทรัพย์สินได้ โดยเฉพาะการทำธุรกรรมทางการเงิน ดังนั้นจึงได้มีการศึกษาวิเคราะห์แบบจำลองการโจมตีของมัลแวร์ โดยแบ่งออกเป็น 4 แบบจำลอง ประกอบด้วย 1) SEIR Model 2) Smartphone Social Network Model 3) Semi-Markov Process และ 4) The Social Relationship Graph ทั้งเครื่องปกติที่ไม่ติดตั้งโปรแกรมป้องกันไวรัส เครื่องที่ปกติที่ติดตั้งโปรแกรมป้องกันไวรัส และ เครื่องที่ไม่ติดตั้งโปรแกรมป้องกันไวรัสและติดมัลแวร์ จากการเปรียบเทียบทำให้เข้าใจถึงรูปแบบพฤติกรรมการแพร่ระบาด และพบวิธีการป้องกันการโจมตีจากมัลแวร์ โดยวิธีการป้องกันหลักๆ ประกอบด้วย 1) การติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ 2) ไม่เปิดอ่านและไม่ส่งต่อ SMS/MMS ที่มาจากผู้ที่ไม่รู้จักหรือเป็นข้อความแปลกๆ

คำสำคัญ : SMS มัลแวร์ โมเดลการแพร่ระบาด โทรศัพท์มือถืออัจฉริยะ

* ผู้ประสานงานหลัก (Corresponding Author)
e-mail: chutiwan_boo@dusit.ac.th

Abstract

The usage of smartphones has increased dramatically and the threats of malware attacks have risen in the same direction. SMS/MMS is widely used as a means to propagate malware to smartphones, leading to money lost in financial transactions. This study focused on the analysis of malware attacks models. The four models were: 1) SEIR Model, 2) Smartphone Social Network Model, 3) Semi-Markov Process, and 4) The Social Relationship Graph. They were organised in a different coherent network. The comparison of various smartphones in the three groups were as follows: 1) smartphone had no installed antivirus software, 2) smartphone had installed antivirus software, and 3) smartphone had malware inflection. The results show the understanding of propagation behavior and the prevention from malware attack. The main prevention methods were: 1) the installation of antivirus software, 2) not opening of forwarding SMS/MMS from unknown users or strange messages.

Keywords: SMS, Malware, Propagation model, Smartphone

บทนำ

การใช้งานโทรศัพท์มือถืออัจฉริยะมีหลากหลายวัตถุประสงค์ เช่น การหาข้อมูลจากอินเทอร์เน็ต การส่งข้อความสั้น (SMS) การส่งข้อความภาพเคลื่อนไหว (MMS) การส่งจดหมายอิเล็กทรอนิคส์ (email) การเล่นเกมทั้งออนไลน์และออฟไลน์ การใช้งานโปรแกรมประยุกต์ (Application Program) โดยเฉพาะอย่างยิ่งการทำธุรกรรมทางการเงินบนโทรศัพท์มือถือนั้นมีอัตราเพิ่มขึ้นอย่างต่อเนื่อง (Orcutt, 2014) อย่างไรก็ตาม วัตถุประสงค์หลักของการใช้งานโทรศัพท์มือถือเพื่อการสื่อสารด้วยวิธีการใช้เสียงพูดและการส่ง SMS/MMS ทำให้จำนวนผู้ใช้งานโทรศัพท์มือถืออัจฉริยะในโลกได้มีการเพิ่มขึ้นอย่างต่อเนื่องจาก 11.30 ล้านคน ในปี 2555 เป็น 2 ล้านล้านคน ในปี 2559 (eMarket staff, 2014) นอกจากนี้รายงานสถิติการใช้ SMS/MMS ในปี 2557 มีถึงร้อยละ 96 มาจากผู้ใช้โทรศัพท์มือถืออัจฉริยะ (Garcha, 2014) จะเห็นได้ว่าทุกวันนี้คนส่วนใหญ่ในโลกใช้ SMS/MMS กันอย่างแพร่หลายโดยเฉพาะในด้านธุรกิจ ซึ่งคนไทยใช้ SMS ในการทำธุรกรรมทางการเงินบนมือถือกันมากขึ้น เช่น การใช้ SMS เพื่อส่งรหัส OTP (One Time Pad) ของธนาคาร ถึงลูกค้าเพื่อยืนยันการทำธุรกรรมทางการเงินบนอินเทอร์เน็ต

การใช้งานที่เพิ่มขึ้นของทั้งเครื่องโทรศัพท์อัจฉริยะโดยฉพาะการส่งและรับ SMS/MMS ดังนั้น SMS/MMS จึงเป็นช่องทางหนึ่งที่ทำให้ไวรัสหรือมัลแวร์แพร่ระบาดเข้ามาในเครื่องโทรศัพท์อัจฉริยะนั้นได้ (Xia et al, 2008). นอกจากนี้มัลแวร์ยังทำความเสียหายให้กับเครื่องโทรศัพท์นั้นๆ ส่งผลให้โทรศัพท์ทำงาน

ช้าลง เพราะหน่วยความจำถูกใช้งานในการส่งข้อมูล SMS ไปยังโทรศัพท์อื่นๆ หน่วยความจำจึงเหลือน้อย อีกทั้งแบตตารี่ถูกใช้งานมากไปด้วย จึงพลังงานของแบตตารี่หมดเร็วกว่าที่ควรเป็น

ส่วนข้อมูลในเครื่องโทรศัพท์ เช่น เบอร์โทรศัพท์ต่างๆ รหัสลับที่ใช้ในการทำธุรกรรมทางการเงิน เป็นต้น ถูกลบทิ้ง หรือส่งต่อ ตลอดจนการทำให้ผู้ใช้งานโทรศัพท์นั้นต้องเสียค่าส่ง SMS/MMS จากการที่มัลแวร์เป็นผู้ส่งเองโดยอัตโนมัติ จึงเป็นแรงบันดาลใจให้มีการศึกษาถึงกระบวนการในการแพร่ระบาดของมัลแวร์ ทำให้เกิดเป็นองค์ความรู้ถึงวิธีการแพร่ระบาด การป้องกันและยังยั้งการแพร่ระบาดของมัลแวร์ สำหรับในบทความนี้จึงมุ่งเน้นศึกษาแบบจำลองการแพร่ระบาดของ SMS บนโทรศัพท์มือถือ โดยเลือกมาเฉพาะตั้งแต่ พ.ศ. 2553 จนถึงปัจจุบัน ทั้งนี้เพื่อให้เกิดเป็นประโยชน์ในวงการศึกษาต่อไป

มัลแวร์ในโทรศัพท์มือถืออัจฉริยะ

ในขณะที่โทรศัพท์มือถืออัจฉริยะที่มีจำนวนเพิ่มขึ้นนั้น ปริมาณการโจมตีของมัลแวร์ในโทรศัพท์มือถืออัจฉริยะก็เพิ่มขึ้นตามด้วยเช่นกัน รายงานจาก Kaspersky Lab พ.ศ. 2559 ซึ่งให้บริการผลิตภัณฑ์ด้านความปลอดภัยจากมัลแวร์ในโทรศัพท์มือถืออัจฉริยะ รายงานว่า เป้าหมายการโจมตีเพิ่มขึ้นเป็น 3 เท่า ใน พ.ศ. 2559 เมื่อเทียบกับ พ.ศ. 2558 โดยส่วนใหญ่จะเป็นมัลแวร์ ที่เรียกว่า แรนซัมแวร์ (Ransomware) โดยมีสิทธิ์การเข้าถึงอย่างไร้ขีดจำกัด ของ อุปกรณ์ ข้อมูล โดยเฉพาะข้อมูลทางการเงิน ที่บันทึกไว้โทรศัพท์มือถืออัจฉริยะ นอกจากนี้ มีมัลแวร์ที่แพร่ระบาดทาง SMS มีถึง 13 สายพันธุ์ในจำนวนมัลแวร์ในโทรศัพท์มือถืออัจฉริยะจำนวน 20 สายพันธุ์ (Virus News, 2016) คิดเป็นร้อยละ 60 จึงเป็นเหตุให้ต้องมีการควบคุมจำกัดการแพร่ระบาดของมัลแวร์โดย SMS

1. วิธีการโจมตีของมัลแวร์ โดยทาง SMS/MMS

การโจมตีของมัลแวร์ทำให้เกิดความเสียหายแก่เจ้าของโทรศัพท์ เช่น การใช้พลังงานในโทรศัพท์ที่เกินจริง การจ่ายค่าการส่ง SMS ที่มากกว่าการใช้งานจริง การถูกขโมยหรือการสูญเสียข้อมูลในโทรศัพท์ แต่การสูญเสียทางเศรษฐกิจเป็นปัญหาที่สำคัญที่สุด สำหรับในส่วนนี้ได้แบ่งชนิดการโจมตีของมัลแวร์โดย SMS ออกได้เป็น 4 ชนิด ดังนี้ (Seungyong et al., 2014)

1.1 การโจมตีที่ทำให้เสียค่าโทรศัพท์เล็กน้อย เกิดขึ้นจากการส่งเพื่อยืนยันตัวตนในการทำธุรกรรมการเงินโดยส่ง SMS เหตุการณ์นี้พบในประเทศเกาหลี ซึ่งนิยมการซื้อสินค้าด้วยการส่ง SMS ที่เรียกว่า Micro payment ทำให้มัลแวร์เข้าไปฝังตัวอยู่ในโทรศัพท์ และเข้าถึงส่วนที่เรียกว่า SMS content

1.2 การโจมตี Premium-rate service โดยการทำให้ค่าโทรศัพท์เพิ่มขึ้นโดยที่เจ้าของโทรศัพท์ไม่รู้ตัว การโจมตีนี้พบได้ในประเทศรัฐเซียและประเทศจีน นอกจากนี้การขโมยข้อมูลโดยการส่ง SMS premium rate เพื่อติดตามพฤติกรรมการใช้งานของเจ้าของโทรศัพท์นั้นๆ โดยอัตราการส่ง SMS premium rate เพิ่มขึ้นจากร้อยละ 16 ในเดือนธันวาคม 2556 เป็นร้อยละ 18 ในเดือนธันวาคม 2557 (Eschelbeck, 2014)

1.3 การโจมตีโดยการส่ง SMS เป็นจำนวนมากจากเครื่องโทรศัพท์ที่ติดมัลแวร์ โดยการสุ่มส่งไปตามเบอร์โทรต่างๆ ที่บันทึกไว้ในโทรศัพท์ ส่งผลให้เจ้าของโทรศัพท์ต้องจ่ายค่า SMS เหล่านั้นเป็นราคาที่สูง

1.4 การโจมตีที่เครื่อง Server ของระบบเครือข่ายโทรศัพท์ (Distributed Denial-of-Service (DDoS)) จากนั้นมัลแวร์ที่มากับ SMS จะเข้ามาในโทรศัพท์แล้ว โทรศัพท์ที่ติดมัลแวร์นี้จะส่ง SMS จำนวนมาก เหมือนกับวิธีการของไวรัสซอมบี้ ที่มีจำนวนมากและทำงานพร้อมๆ กันโดยไม่หยุดพัก ทำให้เสียค่าบริการส่ง SMS จำนวนหลายครั้งและอาจจะเครื่องโทรศัพท์ชำรุด เสียหายเนื่องจากทำงานหนัก

2. ผลเสียจาก SMS มัลแวร์

มัลแวร์ที่มากับ SMS ทำให้เกิดผลกระทบทั้งตัวเครื่องโทรศัพท์ ซอฟต์แวร์โทรศัพท์หรือโปรแกรมประยุกต์ ข้อมูลส่วนตัวที่บันทึกไว้ในหน่วยความจำของโทรศัพท์ โดยเฉพาะอย่างยิ่ง การเสียค่าบริการส่ง SMS จำนวนหลายครั้ง สำหรับรายละเอียดของผลเสียดังกล่าว แยกได้เป็นประเด็นย่อยดังต่อไปนี้

2.1 การรั่วไหลพลังงาน มัลแวร์ที่ชื่อ RedBrowser ที่เขียนจากภาษาจาวา เป็นตระกูลเดียวกับโทรจัน ทำตัวเหมือนเป็น Browser และ ทำงานบน J2ME โดยโทรศัพท์ที่ติดมัลแวร์จะส่ง SMS โดยอัตโนมัติและต่อเนื่อง ทำให้โทรศัพท์เครื่องนั้นสูญเสียพลังงาน และยังทำให้ระบบของโทรศัพท์เสียหาย (Shabtai et al, 2012)

2.2 การสูญเสียค่าโทรศัพท์โดยไม่จำเป็น เนื่องจากโทรศัพท์ที่ติดมัลแวร์ชื่อ RedBrowser จะส่ง SMS ไปยังหมายเลขโทรศัพท์ที่ถูกกำหนดไว้ หลายๆ ครั้ง ทำให้เจ้าของโทรศัพท์ต้องเสียค่า SMS นั้นๆ

2.3 ข้อมูลส่วนตัวรั่วไหล หรือศูนย์หาย เนื่องจากมัลแวร์ที่ติดในโทรศัพท์จะเข้าถึงข้อมูลของเจ้าของเครื่องโทรศัพท์ และมัลแวร์จะส่งต่อหรือทำลายข้อความส่วนตัวเหล่านั้น (Sancheng et al., 2014)

2.4 การรบกวนเครือข่ายของโทรศัพท์ โดยโทรศัพท์ที่ติดมัลแวร์จะร่วมกันส่ง SMS ทำให้เครือข่ายของโทรศัพท์ถูกใช้งานสูง ส่งผลเสียให้การโทรเข้าและออกไม่ได้ (Deny of Service, DoS)

จากที่กล่าวมาจะเห็นถึงวิธีการโจมตีและผลกระทบที่เกิดขึ้น ในลำดับต่อไปจะได้กล่าวถึงโมลเดลการแพร่ระบาด ซึ่งเป็นการศึกษาและเรียนแบบพฤติกรรมของมัลแวร์ เนื่องจากการดักจับมัลแวร์ที่เกิดขึ้นจริงทำได้ยาก จึงต้องสร้างโมเดลเหตุการณ์การแพร่ระบาดขึ้นมา

โมเดลการแพร่ระบาด

โมเดลการแพร่ระบาดของมัลแวร์ได้มีการศึกษากันอย่างกว้างขวางมานาน สำหรับบทความนี้จะศึกษาเฉพาะในช่วง พ.ศ. 2553-2558 เพื่อเป็นข้อมูลที่ยังทันสมัย โดยโมเดลที่ใช้ศึกษาเปรียบเทียบประกอบด้วย SEIR Model, Smartphone Social Network Model, Semi-Markov Process and the Social Relationship Graph Model และ Two-Layer Malware Propagation Model โดยมีรายละเอียดดังนี้

1. SEIR Model

YuanYuan et al. (2010) ได้สร้างโมเดลชื่อ Susceptible-Exposed-Infected-Recovered (SEIR) ซึ่งเป็นโมเดลสำหรับ SMS/MMS และ การแพร่แบบไฮบริด การสร้างอยู่บนพื้นฐานแนวคิดในการป้องกันมัลแวร์จากผู้ใช้โทรศัพท์ ในโมเดลนี้ใช้ค่าพารามิเตอร์ของ การกลายพันธุ์ของมัลแวร์ การป้องกัน SMS/MMS ในโครงข่าย และค่าเฉลี่ยของดีกรีในแต่ละโหนดของการแพร่ระบาดของมัลแวร์ในโครงข่ายบลูทูธ โมเดลนี้ใช้สมการหลัก 8 สมการ สำหรับผลการทดลอง พบว่า มัลแวร์ในโทรศัพท์มือถือมีความเร็วในการแพร่ระบาดแบบไฮบริด เร็วกว่า วิธีการแพร่ระบาดแบบเดิมที่เป็นโหนดเดี่ยว

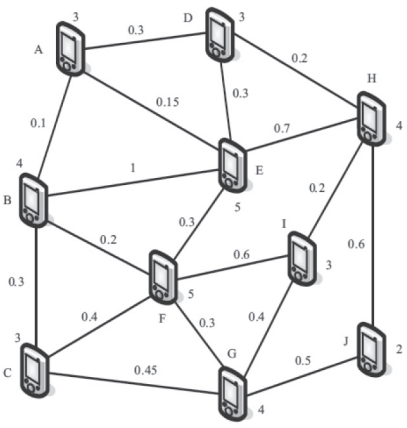
YuanYuan et al. (2010) ยังได้เสนอการป้องกันมัลแวร์ในโทรศัพท์ โดยมีพื้นฐานแนวคิดความรู้ มาจาก SEIR Model ดังนี้

1) ซอฟต์แวร์สำหรับป้องกันไวรัส สามารถช่วยควบคุมความเร็วและขอบข่ายในการแพร่ระบาดได้ ดังนั้นผู้ที่ใช้โทรศัพท์มือถือต้องติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เหมาะสมกับการใช้งาน ชนิดของโทรศัพท์และราคา

2) ผู้ใช้งานโทรศัพท์ควรหลีกเหลี่ยงพื้นที่ที่มีการส่ง SMS/MMS อย่างหนาแน่น

2. Smartphone Social Network Model

Sancheng et al. (2013) ได้ออกแบบการแพร่ระบาดของมัลแวร์โดยใช้โทรศัพท์มือถือมาเชื่อมต่อกันเป็นโครงข่าย เพื่อประเมินการแพร่ระบาดของมัลแวร์โดย SMS/MMS ในการทดลองใช้โทรศัพท์มือถือจำนวน 10 เครื่อง โดยใช้ความสัมพันธ์แบบกราฟ SMS/MMS ถูกส่งจากโทรศัพท์เครื่องหนึ่งที่ติดมัลแวร์ไปยังอีกเครื่องหนึ่งหรือเรียกว่าอีกโหนดหนึ่ง เมื่อเวลาผ่านไปพบว่า จำนวนของโทรศัพท์ที่ติดมัลแวร์มีเพิ่มขึ้นและจำนวนครั้งในการส่ง SMS ต่อเครื่องก็มากขึ้นด้วย ดังนั้น มัลแวร์สามารถแพร่ระบาดได้โดย SMS/MMS และระยะเวลาส่งผลต่อการแพร่ระบาด



ภาพที่ 1 จำนวนครั้งใน 1 สัปดาห์ และเส้นทางการส่ง SMS/MMS เป็นเครือข่ายแบบกราฟ
ที่มา: Sancheng et al., (2013)

3. Semi-Markov Process and the Social Relationship Graph Model

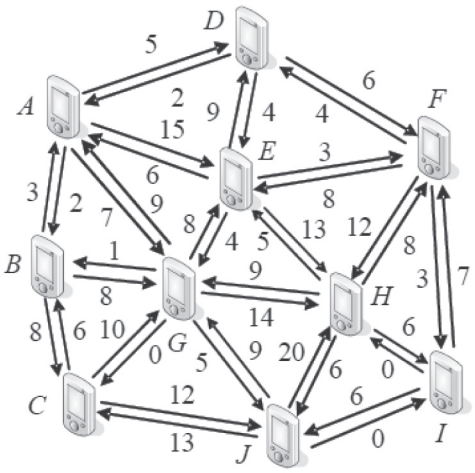
Peng et al. (2014) ได้นำเสนอ โมเดลกลไกคุณลักษณะการแพร่ระบาดของเวิร์ม ใน SMS/MMS โดยกลไกของโมเดลนี้มีแนวคิดมาจาก Semi-Markow Process และ กราฟความสัมพันธ์ทางสังคม โมเดลนี้ใช้โทรศัพท์เป็นโหนด ซึ่งคล้ายกับโมเดลที่กล่าวมาข้างต้น ต่างกันที่โมเดลนี้ความสัมพันธ์ของแต่ละโหนดเป็น กราฟเครือข่ายทางสังคม โดยแต่ละโหนดมีการแพร่ระบาดของมัลแวร์ และมีการส่ง SMS/MMS แบบไดนามิกซ์

ผลจากการทดลอง พบว่า

1) จำนวนโหนดหรือโทรศัพท์ จำนวนผู้ใช้งาน จำนวนการตอบโต้ มีผลทางตรงกับอัตราเร็ว และขอบเขตในการแพร่ระบาดของมัลแวร์

2) เมื่อมัลแวร์มีการแพร่ระบาดรุนแรง ส่งผลต่อของเขตของการแพร่ระบาดกว้างขึ้น

3) โมเดลนี้ช่วยให้คาดการณ์หลักการแพร่ระบาดของมัลแวร์ และการแพร่ระบาดอย่างหยุดไม่ได้ ได้ดีกว่า SEIR โมเดล



ภาพที่ 2 ข้อมูลการส่ง SMS/MMS ใน 1 สัปดาห์ ของโทรศัพท์ 10 เครื่อง ที่ติดมัลแวร์และมีเส้นทางการส่งแบบกราฟเครือข่ายสังคม
ที่มา: Peng et al. (2014)

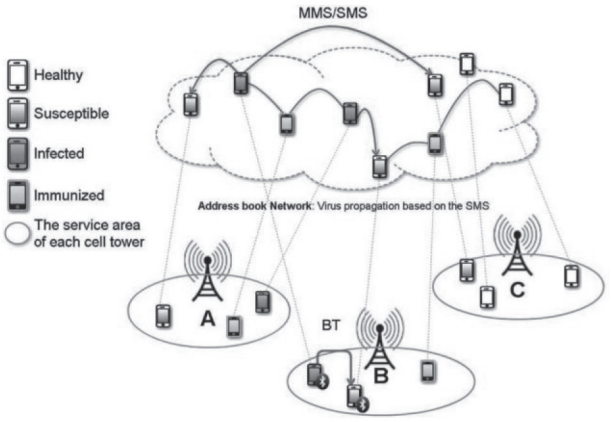
4. Two-Layer Malware Propagation Model

Chao & Jiming (2013) นำเสนอโมเดลสองชั้น ในการส่ง SMS/MMS ของโทรศัพท์ผ่านบลูทูธ เพื่อศึกษาการแพร่ระบาดของมัลแวร์ โดยโมเดลชั้นที่ 1 วางโทรศัพท์ไว้ชั้น 1 ส่วนโมเดลชั้นที่ 2 วางโทรศัพท์ไว้ชั้นบนของอาคาร จากรูปที่ 3 เป็นการจัดวางโทรศัพท์ในอาคาร โดยแบ่งเป็น 3 กลุ่มด้วยกัน A, B และ C ในแต่ละกลุ่ม ประกอบด้วยโทรศัพท์ที่ติดมัลแวร์ โทรศัพท์ที่มีโปรแกรมป้องกันไวรัส โทรศัพท์ที่ไม่ติดมัลแวร์ โดยกำหนดให้โทรศัพท์แต่ละเครื่องติดต่อกันเป็นเครือข่ายสังคม จากผลการทดลองสรุปได้ว่า

1) การแพร่ระบาดของมัลแวร์เป็นไปอย่างอัตโนมัติ เมื่อกดอ่าน SMS/MMS ที่ติดมัลแวร์ ทำให้โทรศัพท์เครื่องนั้นติดมัลแวร์ด้วย และโทรศัพท์ที่ติดมัลแวร์นั้นจะส่ง SMS/MMS ที่มีมัลแวร์ไปยังรายชื่อและเบอร์โทรศัพท์ที่บันทึกไว้ในเครื่อง โดยจะส่งแบบอัตโนมัติ

2) โทรศัพท์ที่ติดมัลแวร์จะส่ง SMS/MMS ที่มีไวรัสไปยังโทรศัพท์เป้าหมายเพียงครั้งเดียวไม่มีการส่งซ้ำในเบอร์เดียวกัน

3) โทรศัพท์ที่มีโปรแกรมป้องกันไวรัส เมื่อติดมัลแวร์หลังจากเปิดอ่าน SMS/MMS แต่โทรศัพท์นั้นจะไม่ส่งต่อ SMS/MMS ที่ติดมัลแวร์ไปยังเครื่องอื่นๆ



ภาพที่ 3 การวางโทรศัพท์มือถือในโมเดลเครือข่าย 2 ชั้น
ที่มา: Chao & Jiming (2013)

เมื่อนำโมเดลการแพร่ระบาดทั้งสี่โมเดลมาเปรียบเทียบกัน ในส่วนของข้อดีและข้อด้อย แสดงไว้ในตารางที่ 1 ดังนี้

ตารางที่ 1 การเปรียบเทียบในแต่ละโมเดล

Model	ข้อดี	ข้อด้อย
SEIR Model (YuanYuan et al., 2010)	1) เป็นต้นแบบโมเดลการแพร่ระบาดของมัลแวร์ในโทรศัพท์มือถือ ซึ่งนักวิจัยได้ใช้นำไปการพัฒนาต่อ 2) มีการอภิปรายถึงการการกลายพันธุ์ของมัลแวร์ 3) ใช้ระยะทางของโหนดโทรศัพท์ การใช้โปรแกรม anti-virus และ การ patch ในสมการ	1) ขาดการปัจจัยพฤติกรรมการใช้งานของผู้ใช้โทรศัพท์มือถือ
Smartphone Social Network Model (Sancheng et al., 2013)	1) โมเดลทำให้รู้ถึงลักษณะการแพร่ระบาดโดย SMS/MMS แบบไดนามิก ซึ่งใช้ในการสร้างโมเดลด้วยกราฟความสัมพันธ์ทางสังคม 2) แสดงให้เห็นถึงผลที่มาจากปัจจัยการต้านทานการแพร่ระบาดของมัลแวร์ที่ต่างกัน 3) ให้ประสิทธิภาพการแพร่ระบาดน้อยกว่า SEIR Model	1) ขาดการเปรียบเทียบกับรูปแบบกราฟอื่นๆ 2) ขาดการพิจารณาด้านพฤติกรรมการใช้งานของเจ้าของโทรศัพท์มือถือ 3) ขาดวิธีการป้องกันการแพร่ระบาด

Model	ข้อดี	ข้อด้อย
Semi-Markov Process and The Social Relationship Graph Model (Peng et al., 2014)	1) วิธีเซมิมาคอฟช่วยในการทำนายการแพร่ระบาดของมัลแวร์ได้ดี 2) โมเดลนี้สามารถทำนายการแพร่ระบาดขั้นหยุดไม่ได้ดีกว่าโมเดลของ SEIR 3) มีการทดลองใช้ทั้งสองโมเดล ทำให้เกิดการเปรียบเทียบในสิ่งแวดล้อม ปัจจัยเดียวกัน 4) รองรับการแพร่ระบาดแบบไดนามิก	1) ขาดรายละเอียดที่ใช้สนับสนุนตัวอย่าง 2) ขาดการทดลองกับข้อมูลขนาดใหญ่เพื่อวิเคราะห์หาคำตอบ
Two-Layer Malware Propagation Model (Chao & Jiming, 2013)	1) ใช้พฤติกรรมของผู้ใช้งานมาเป็นปัจจัยในการสร้างโมเดล เช่น การแจ้งเตือนเรื่องการแพร่ระบาดของมัลแวร์ ทำให้ผู้ใช้โทรศัพท์มือถือมีความระวังในการป้องกันการแพร่ระบาดของมัลแวร์ 2) มีเรื่องความปลอดภัย โดยใช้โปรแกรมป้องกันไวรัส ในการสร้างโมเดล เช่น โทรศัพท์มือถือที่มีโปรแกรมป้องกันไวรัสกับที่ไม่มีโปรแกรมป้องกันไวรัส ทำให้การแพร่ระบาดของมัลแวร์ต่างกัน	1) ขาดเรื่องการเปลี่ยนแปลงพฤติกรรมของผู้ใช้งานแบบไดนามิกส์

SEIR Model เป็นโมเดลต้นแบบของโมเดลการแพร่ระบาดของ SMS มัลแวร์ โดยโมเดลอื่นๆ มีปัจจัยที่เหมือนและต่างกัน อยู่ในสมการของแต่ละโมเดล เช่นลักษณะทางกายภาพของ Smartphone Social Network Model และ Semi-Markov Process and The Social Relationship Graph Model มีการจัดวางของโทรศัพท์ในรูปกราฟเป็นครือข่ายทางสังคมที่เหมือนกัน และ Two-Layer Malware Propagation Model ที่วางโทรศัพท์มือถือไว้การวางบนอาคารสองชั้น ซึ่งแตกต่างจากโมเดลอื่นๆ ในจากการจัดวางโทรศัพท์ที่ต่างกันทำให้ความรวดเร็วของการแพร่ระบาดต่างกัน นอกจากนั้นการใช้โทรศัพท์ที่ติดตั้งโปรแกรมป้องกันไวรัส เช่น ใน Two-Layer Malware Propagation Model ทำให้การแพร่ระบาดของมัลแวร์ไม่รุนแรงเท่ากับโมเดลที่โทรศัพท์ไม่ได้ติดตั้งโปรแกรมป้องกันไวรัส จะเห็นได้ว่าแต่ละโมเดลมีทั้งข้อดีและข้อด้อยที่เหมือนและต่างกันดังจะได้กล่าวต่อไปในบทอภิปรายผล

อภิปรายผล

จากการศึกษาเรื่อง “โมเดลการแพร่ระบาดของมัลล์แวร์ โดย SMS/MMS ในโทรศัพท์มือถืออัจฉริยะ” ผู้วิจัยได้ศึกษาแนวคิด วิเคราะห์ ทฤษฎี และงานวิจัยที่เกี่ยวข้อง ที่เป็นไปตามวัตถุประสงค์ กล่าวคือ เพื่อศึกษาโมเดลการแพร่ระบาด การวิเคราะห์หาแนวทางการป้องกันและยับยั้งการแพร่ระบาด ทำให้เกิดเป็นองค์ความรู้สำหรับในการศึกษาต่อไป การวิจัยนี้มุ่งเน้นวรรณกรรมเกี่ยวข้องกับโมเดลการแพร่ระบาดของมัลแวร์ ตั้งแต่ พ.ศ. 2553 เป็นต้นมา เพื่อให้เป็นโมเดลที่ยังทันสมัย ในการศึกษาเปรียบเทียบมีจำนวน 4 โมเดล ประกอบด้วย 1) Smartphone Social Network Model 2) SEIR Model 3) Two-Layer Malware Propagation Model และ 4) Semi-Markov Process and the Social Relationship Graph Model จากการศึกษาวิธีการสร้างและผลลัพท์ที่ได้ทำให้พบว่า แต่ละโมเดลมีการออกแบบโดยใช้ปัจจัยที่ต่างกัน อย่างไรก็ตามทุกโมเดลมีจุดมุ่งหมายเดียวกัน คือให้เข้าถึงวิธีการแพร่ระบาด อันจะนำไปสู่การป้องกันการแพร่ระบาดด้วยวิธีต่างๆ

Smartphone Social Network Model และ Semi-Markov Process and the Social Relationship Graph Model มีการวางรูปแบบโทรศัพท์ที่คล้ายกัน โดยวางเป็นเครือข่ายทางสังคมแบบกราฟ ต่างกันที่สมการที่ใช้ในการทดลอง สำหรับ Smartphone Social Network Model ใช้ศึกษาการแพร่ระบาดโดย SMS/MMS แบบไดนามิก ส่วน Semi-Markov Process and the Social Relationship Graph Model เป็นโมเดลที่มีประสิทธิภาพกว่าโมเดล ในตระกูลของ SEIR Model อย่างไรก็ตามทั้งโมเดลของ Smartphone Social Network และ Semi-Markov Process and the Social Relationship Graph นี้ไม่ได้นำพฤติกรรมผู้ใช้งานเป็นตัวแปรของสมการในการสร้างโมเดล

ส่วน SEIR Model เป็นโมเดลที่นักพัฒนาใช้เป็นพื้นฐานในการคิดค้นโมเดลใหม่ๆ ซึ่งสมการที่ใช้ในโมเดล SEIR ใช้ระยะทางระหว่างโทรศัพท์ การกลายพันธุ์ของมัลแวร์มาวิเคราะห์ การใช้โปรแกรม anti-virus และการ patch ในสมการ แต่ไม่ได้นำพฤติกรรมผู้บริโภคบรรจุไว้ในสมการ

ในส่วนของ Two-Layer Malware Propagation Model มีการนำเอาพฤติกรรมการใช้งานของผู้บริโภค ความปลอดภัยในการใช้งาน โดยใช้โปรแกรม anti-virus ของผู้ใช้งาน มาวิเคราะห์ในสมการ นอกจากนี้เป็นโมเดลที่คำนึงถึงชีวิตคนเมืองที่ออกแบบให้มีการใช้งานในอาคารที่ต่างชั้นกัน ทำให้ได้แนวคิดทฤษฎีใหม่ในการออกแบบสมการ

เมื่อนำโมเดลทั้งสี่โมเดลมาวิเคราะห์ถึงวิธีการป้องกันการแพร่ระบาดของมัลแวร์ในโทรศัพท์มือถือจากการส่ง SMS/MMS แบ่งเป็นประเด็นวิธีการป้องกันได้ดังนี้

1) โปรแกรมป้องกันไวรัส เป็นเครื่องมือที่มีประโยชน์ในการควบคุมการแพร่ระบาดของมัลแวร์ให้อยู่ในขอบเขตจำกัด ดังนั้นผู้ใช้งานโทรศัพท์มือถือต้องตระหนักถึงการติดตั้งโปรแกรมป้องกันไวรัสและมีการอัพเดทโปรแกรมอยู่เสมอๆ นอกจากนี้การเลือกโปรแกรมให้เหมาะสมกับการใช้งานและเครื่องโทรศัพท์มือถือ ทำให้การป้องกันมัลแวร์หรือไวรัสมีประสิทธิภาพสูงสุด

2) ผู้ใช้งานโทรศัพท์มือถือควรหลีกเลี่ยงพื้นที่ที่มีเครือข่ายของ SMS/MMS หนาแน่น อย่างไรก็ตามวิธีนี้ทางปฏิบัติทำได้ยาก

3) การแจ้งเตือนและการติดตามข่าว เรื่องการระบาดของมัลแวร์ ช่วยลดการแพร่ระบาดได้

4) พฤติกรรมการใช้งานเป็นปัจจัยหนึ่งที่ทำให้มีการแพร่ระบาดของมัลแวร์ เช่น การไม่ส่งต่อ SMS/MMS ที่มีให้กดเข้าไปในหน้าเว็บหรือลิงค์ ที่มาจากผู้ไม่รู้จัก

จากที่กล่าวมา ทั้งสี่โมเดลมีพื้นฐานมาจากสมการและปัจจัยประกอบทั้งที่แตกต่างกันและเหมือนกัน ทำให้เกิดเป็นโมเดลที่ต่างๆ กัน ทุกโมเดลมีทั้งข้อดีและข้อด้อย จะเห็นได้ว่าการได้ศึกษาถึงการแพร่ระบาดของมัลแวร์ ทำให้เกิดเป็นองค์ความรู้ใหม่ในการรู้เท่าทัน การป้องกัน และการกำจัด ตลอดจนแนวทางการศึกษาเพิ่มเติมโดยการสร้างโมเดลใหม่ในการศึกษาการป้องกันการแพร่ระบาดของมัลแวร์สายพันธุ์ใหม่ๆ ในโทรศัพท์มือถืออัจฉริยะจากการส่ง SMS/MMS อีกทั้งการแพร่ระบาดผ่านโปรแกรมประยุค สำหรับการสนทนาต่างๆ ซึ่งกำลังเป็นที่นิยมในปัจจุบัน เช่น ไลน์ และ เฟสบุคเมสเซ็นเจอร์ เป็นต้น นอกจากนี้ยังแนวทางการศึกษาต่อไปอีกอาทิ การสร้างโมเดลโดยการจัดกลุ่มแบ่งตามพฤติกรรมผู้ใช้งาน ว่ากลุ่มใดมีความเสี่ยงที่ทำให้มัลแวร์แพร่ระบาดในโทรศัพท์มือถือ ในการจัดกลุ่มใช้เทคนิคต้นไม้ตัดสินใจ (Decision Tree) หรือ เคมีนส์ (k-means Cluster) ตามที่ Surasit (2015) ได้กล่าวไว้ เพื่อศึกษาความสัมพันธ์ระหว่างกลุ่มพฤติกรรมผู้ใช้งานโทรศัพท์มือกับการแพร่ระบาดของมัลแวร์

สำหรับข้อจำกัด ในการสร้างโมเดลทั้งสี่แบบนั้น กล่าวได้ดังนี้ ในการทดลองใช้โทรศัพท์ไม่ได้ระบุถึงเครือข่ายที่ให้บริการโทรศัพท์มือถือว่า เครือข่ายนั้นๆ ได้ติดตั้งโปรแกรมป้องกันหรือตรวจจับ SMS มัลแวร์ ไว้หรือไม่ นอกจากนี้โทรศัพท์มือถืออัจฉริยะที่ใช้ในโมเดลจะใช้ประมาณ 10-20 เครื่อง เนื่องจากโทรศัพท์มีราคาสูงและตัวเครื่องโทรศัพท์อาจจะเสียหายได้หลังจากเสร็จการทดลอง อีกทั้งอุปกรณ์เครือข่ายที่ให้บริการสัญญาณโทรศัพท์มือถือมีราคาสูงเช่นกัน ทำให้ในการสร้างโมเดลมีต้นทุนสูง การทดลองจึงจำกัดอยู่ในหน่วยงานหรือสถาบันที่มีงบประมาณสูง

References

Chao, G. & Jiming, L. (2013). Modeling and Restraining Smartphone Virus Propagation. *Smartphone Computing, IEEE Transactions on,* 12(3), 529-541.

eMarketer staff. (2014). *2 Billion Consumers Worldwide to Get Smart (phones) by 2016.* Retrived March 18, 2016, from eMarkwter website, http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694

Eschelbeck, G. (2014). *Security Threat Report 2014, in Smarter, Shadier, Stealthier Malware. 2014,* SOPHOS.

Garcha, I. (2014). *UPDATED: SMS Marketing Statistics 2014.* Retrieved July 14, 2015, from Digitalmarketingmagazine website, http://digitalmarketingmagazine.co.uk/mobile-digital-marketing/7-key-statistics-for-sms-marketing/558

Orcutt, M. (2014). *Malware on the Move.* Retrieved July 14, 2015, from MIT Technology Review, https://www.technologyreview.com/s/528306/malware-on-the-move/

Peng, S., Wu, M., Wang, G. & Yu, S. (2014). Propagation model of smartphone worms based on semi-Markov process and social relationship graph. *Computers & Security,* 44(0), 92-103.

Sancheng, P., Guojun, W. & Shui, Y. (2013). *Modeling Malware Propagation in Smartphone Social Networks.* 12th IEEE International Conference on 2013, Melbourne, 196–201.

Sancheng, P., Shui, Y. & Aimin, Y. (2014). Smartphone Malware and Its Propagation Modeling: A Survey. *Communications Surveys & Tutorials IEEE,* 16(2), 925-941.

Seungyong, Y., Jeongnyeo, K. & Hyunsook, C. (2014). *Detection of SMS smartphone malware. in Electronics, Information and Communications (ICEIC).* International Conference on 2014. Kota Kinabalu, 1-2.

Shabtai, A., Kanonov, U., Elovici, Y., Glezer, C. & Weiss, Y. (2012). "Andromaly": a behavioral malware detection framework for android devices. *Journal of Intelligent Information Systems,* 38(1), 161-190.

Surasit, S. (2015). Comparative Efficiency of Classification Data by ID3 with Different Discretization Techniques. *SDU Research Journal Humanities and Social Sciences,* 8(3), 29-46.

Virus News. (2016). *The Volume of New Mobile Malware Tripled in 2015.* Retrieved March 18 2016, from kaspersky website, http://www.kaspersky.com

Xia, W., Li, Z-H., Chen, Z-Q. & Yuan, Z-Z. (2008). *Commwarrior worm propagation model for smart phone networks. The Journal of China Universities of Posts and Telecommunications,* 15(2), 60-66.

YuanYuan, F., Kangfeng, Z. & Yixian, Y. (2010). *Epidemic Model of Smartphone Virus for Hybrid Spread Mode with Preventive Immunity and Mutation. in Wireless Communications Networking and Smartphone Computing (WiCOM).* 6th International Conference on. 2010. Chengdu, 1-5.

คณะผู้เขียน

อาจารย์ชูติวรรณ บุญอาชาทอง

อาจารย์ประจำคณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสวนดุสิต

295 ถนนราชสีมา เขตดุสิต กรุงเทพมหานคร 10300

email: chutiwan_boo@dusit.ac.th

นายคงศักดิ์ บุญอาชาทอง

นิสิตคณะวิศวรกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

แขวงลาดยาว เขตรจตุจักร กรุงเทพมหานคร 10900

email: kongsakb@yahoo.com