ความปลอดภัยของข้อมูลบนสมาร์ทโฟนแอนดรอยด์

Information Security on Android-Smartphone

ประมูล สุขสกาวผ่อง ศิรปัฐช์ บุญครอง
คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

บทคัดย่อ

ด้วยการเพิ่มของจำนวนผู้ใช้สมาร์ทโฟนมากขึ้นทำให้ต้องคำนึงถึงเรื่องความปลอดภัยมากขึ้น ระบบปฏิบัติการแอนดรอยด์จะมีสัดส่วนเพิ่มขึ้นของผู้ใช้มากที่สุด ทำให้ช่องโหว่เรื่องความปลอดภัยก็มีมากขึ้นตามไปด้วยและสมาร์ทโฟนในปัจจุบันมีประสิทธิภาพมากขึ้นความสามารถในการทำงานใกล้เคียงกับคอมพิวเตอร์ ทำให้ผู้โจมตีระบบคอมพิวเตอร์เดิมหันมาโจมตีสมาร์ทโฟนมากขึ้นโดยเฉพาะมัลแวร์(Malware) ในบทความนี้ได้นำเสนอกลไกการการทำงานของระบบรักษาความปลอดภัยของแอนดรอยด์รวมถึงช่องโหว่ด้านความปลอดภัย ได้ศึกษาถึงงานวิจัยด้านการพัฒนากลไกรักษาความปลอดภัยและงานวิจัยที่เกี่ยวข้อง พร้อมทั้งข้อเสนอแนะแนวทางสำหรับผู้ใช้งานให้ใช้สมาร์ทโฟนแอนดรอยด์ได้อย่างปลอดภัยและแนวทางสำหรับนักพัฒนาแอพพลิเคชั่น

คำสำคัญ : ความปลอดภัยของข้อมูล, แอนดรอยด์, มัลแวร์

Abstract

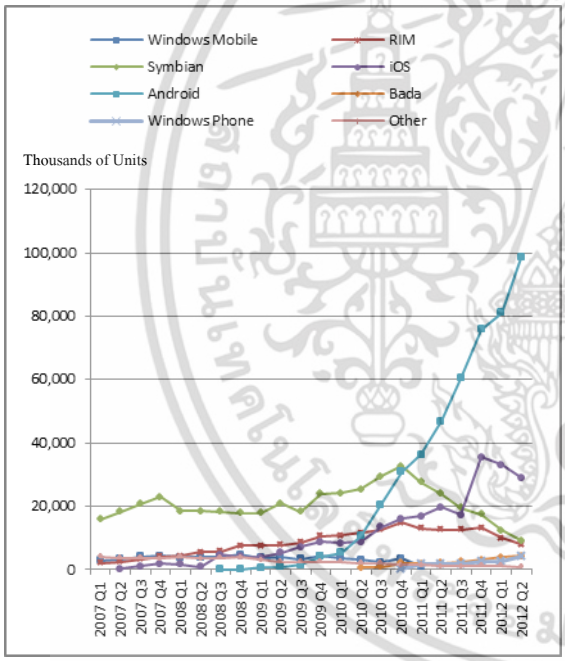
Since Android is the most popular smartphone platform, the volume of malware affecting Google's Android mobile operating system is also on the rise. Smartphones are becoming smaller, yet more powerful, with greater storage capacities. Traditional threats affecting computers such as malware now also affect these devices, leading to the need to protect data. This paper presents the current state of Android security mechanisms and their limitations. It also analyzes research on Android security and recommends the best practices for security.

Keywords : Data security, Android, Malware

1. บทนำ

ด้วยความสามารถของโทรศัพท์มือถือที่เรียกว่าสมาร์ทโฟน (Smartphone) และแท็บเล็ต (Tablet) ที่เกือบเทียบเท่าได้กับคอมพิวเตอร์และมีผู้ใช้จำนวนมากจึงทำให้ผู้ที่เคยโจมตีเครือข่ายคอมพิวเตอร์เดิม ได้หันมาโจมตีอุปกรณ์สมาร์ทโฟนมากขึ้น และสมาร์ทโฟนใช้งานง่ายไม่จำเป็นต้องมีทักษะเหมือนการใช้คอมพิวเตอร์ [1] ทำให้มีผู้ใช้หลากหลาย ตั้งแต่เด็กจนถึงผู้สูงอายุก็สามารถ ใช้งานได้ จากสถิติจำนวนโทรศัพท์มือถือที่จดทะเบียนทั่วโลกประมาณเกือบ 7,000 ล้านเครื่องทั่วโลก และมีอัตราการเติบโตต่อเนื่องโดยเฉพาะสมาร์ทโฟน ส่วนการติดตั้งแอพพลิเคชั่นผู้ใช้งานจะเป็นผู้กำหนดเรื่องความปลอดภัยและความเป็นส่วนตัวด้วยตัวเอง [2] โดยเป็นผู้เลือกว่าจะยอมรับหรือไม่ยอมรับเงื่อนไขต่างๆ ในขั้นตอนการติดตั้งแอพพลิเคชั่น ซึ่งส่วนใหญ่จะเลือกยอมรับโดยไม่ได้อ่าน

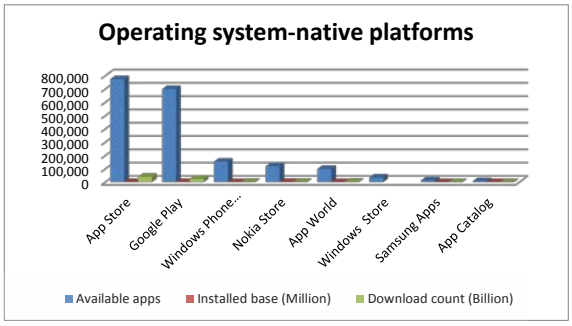
รายละเอียดข้อตกลง เพราะถ้าเลือกไม่ยอมรับก็จะติดตั้งแอพพลิเคชั่นไม่ได้ นอกจากนี้บางส่วน ยังติดตั้งแอพพลิเคชั่นจากร้านค้าครั้งละปริมาณมากๆ โดยไม่ได้เลือกเอง ซึ่งจะติดตั้งแอพพลิเคชั่นที่ไม่รู้จักมาด้วยซึ่งอาจจะเป็นแอพพลิเคชั่นที่แฝงโปรแกรมประเภทมัลแวร์ นอกจากนี้ยังมีการนำสมาร์ทโฟนมาใช้ในองค์กรหรือในบริษัทมากขึ้น เพื่อใช้งานอินเตอร์เน็ตและรับส่งอีเมล์ การเข้าใช้งานระบบเครือข่ายในองค์กรผ่านสมาร์ทโฟนทำให้ผู้บริหารด้านไอทีไม่สามารถควบคุมการติดตั้งในส่วนของแอพพลิเคชั่นต่างๆได้เหมือนกับควบคุมการติดตั้งบนเครื่องคอมพิวเตอร์ เพราะเครื่องสมาร์ทโฟนส่วนใหญ่จะเป็นเครื่องใช้ส่วนตัว ทำให้การควบคุมทำได้ยาก จึงมีความเสี่ยงที่จะเป็นช่องโหว่ให้แฮคเกอร์ (Hacker) เจาะเข้าระบบเครือข่ายขององค์กรได้



รูปที่ 1 ปริมาณยอดขายมือถือแยกตามระบบปฏิบัติการ [3]

2. แอพพลิเคชั่นบนแอนดรอยด์

จากรูปที่ 1 จะเห็นได้ว่าสมาร์ทโฟนในระบบปฏิบัติการแอนดรอยด์ (Android) มียอดขายที่สูงขึ้นอย่างก้าวกระโดด และระบบปฏิบัติการไอโอเอส (iOS) เป็นอันดับสอง ส่วนระบบปฏิบัติการวินโดวส์มีแนวโน้มที่จะอยู่ในอันดับสาม เนื่องจากจำนวนผู้ใช้เครื่องเดิมที่เป็นระบบปฏิบัติการวินโดวส์มีจำนวนมาก จึงคาดการณ์ได้ว่าจะทำให้ยอดของวินโดวส์สโตร์เติบโตขึ้นด้วย



รูปที่ 2 Apps from Operating system-native platforms [4]

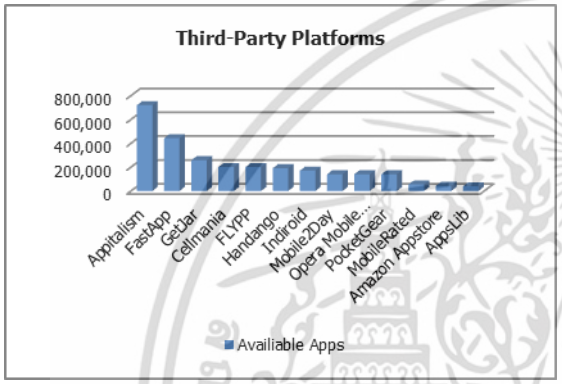
ส่วนโทรศัพท์มือถือรุ่นใหม่ๆ จะมีลักษณะการทำงานคล้ายกับเครื่องคอมพิวเตอร์ขนาดเล็กหรือที่เรียกว่าสมาร์ทโฟน และมีโปรแกรมที่ใช้งานอยู่บนสมาร์ทโฟนคือแอพพลิเคชั่นโปรแกรม หรือเรียกว่าแอพ (Apps) สถิติจำนวนแอพพลิเคชั่นบนสมาร์ทโฟน ที่มีอยู่สิ้นปี พ.ศ. 2555 ประมาณ 1,800,000 Apps จากผู้ผลิตมากกว่า 500,000 ราย นับเป็นปรากฏการณ์ที่เปลี่ยนโลกไปสู่ยุคของการใช้งานสมาร์ทโฟนอย่างแท้จริง แหล่งในการซื้อขายแอพพลิเคชั่นจะเรียกว่า แอพพลิเคชั่นสโตร์ (Application Store) โดยจะแยกเป็นสองประเภทคือ จากผู้ผลิตโดยตรง (Operating system-native platforms) ดังรูปที่ 2 และจากคนกลาง (Third-Party platforms)

2.1. ศูนย์จำหน่ายแอพพลิเคชั่นจากผู้ผลิต (Applications from Operating system-native platforms)

แหล่งในการซื้อขายหรือติดตั้งแอพพลิเคชั่นในสมาร์ทโฟน จะมีศูนย์จำหน่ายแอพพลิเคชั่นจากผู้ผลิตโดยตรง คือเป็นผู้ผลิตระบบปฏิบัติการโดยตรง ผู้ใช้งานเมื่อซื้อเครื่องแล้วต้องสมัครสมาชิกเพื่อติดตั้งแอพพลิเคชั่น เช่น แอพสโตร์ (App Store) ของบริษัทแอปเปิล และกูเกิลเพลย์ (Google Play) ของบริษัทกูเกิล จำนวนแอพพลิเคชั่นของแอนดรอยด์ในกูเกิลเพลย์เมื่อสิ้นปี พ.ศ. 2555 จะอยู่ที่ 700,000 กว่าแอพพลิเคชั่น ดังรูปที่ 2 และกำลังเพิ่มขึ้นอย่างต่อเนื่อง

2.2. ศูนย์จำหน่ายแอพพลิเคชั่นจากคนกลาง (Applications from Third-Party platforms)

นอกจากนี้ยังมีผู้ขายแอพพลิเคชั่นจากบริษัทอื่นๆ ที่ไม่ได้เป็นเจ้าของระบบปฏิบัติการหรือเจ้าของผลิตภันฑ์สามาร์ทโฟน แต่ก็สามารถเปิดสถานที่ให้มีการซื้อขายแอพพลิเคชั่นบนสามาร์ทโฟนได้ ดังภาพที่ 3 โดยส่วนใหญ่เป็นแอพพลิเคชั่น บนระบบปฏิบัติการแอนดรอยด์หรือรวมกับระบบปฏิบัติการอื่นด้วย เมื่อรวมกับจำนวนแอพพลิเคชั่นบนกูเกิลเพลย์แล้วแอพพลิเคชั่นแอนดรอยด์จะมีจำนวนมากที่สุด



รูปที่ 3 Apps from Third-Party platforms [4]

3. ความปลอดภัยของแอพพลิเคชั่นแอนดรอยด์

จากรูปที่ 2 และ 3 จะเห็นได้ว่าแอพพลิเคชั่นของระบบปฏิบัติการแอนดรอยด์จะมีจำนวนมากที่สุดและมาจากหลายแหล่ง ทำให้เกิดช่องโหว่ในเรื่องความปลอดภัยในการใช้งาน เมื่อเทียบกับระบบปฏิบัติการอื่นๆ เช่น ระบบปฏิบัติการของแบล็กเบอร์รี่ โอเอส (Blackberry OS) เป็นระบบปิด มีการควบคุมการเข้ารหัสทั้งหมด การซื้อขายและติดตั้งแอพพลิเคชั่น ก็ต้องทำผ่านแอพสโตร์ของบริษัทเท่านั้น และเครื่องไอโฟน (iPhone) ของบริษัทแอปเปิล (Apple Inc.) ก็เป็นระบบปิดแต่ก็สามารถเปิดได้ แต่ระบบปฏิบัติการแอนดรอยด์ จะเป็นระบบเปิดทั้งหมด มีข้อพิจารณาดังนี้

3.1 แอนดรอย์เป็นระบบปฏิบัติการแบบโอเพ่นซอร์ส (Open Source) ที่หลายคนมีส่วนร่วมพัฒนาและเข้าถึงรหัสต้นฉบับ (Source Code) ต่างๆ ได้

3.2 เปิดให้ทุกคนมีสิทธิพัฒนาแอพพลิเคชั่นได้ (Open Developer)

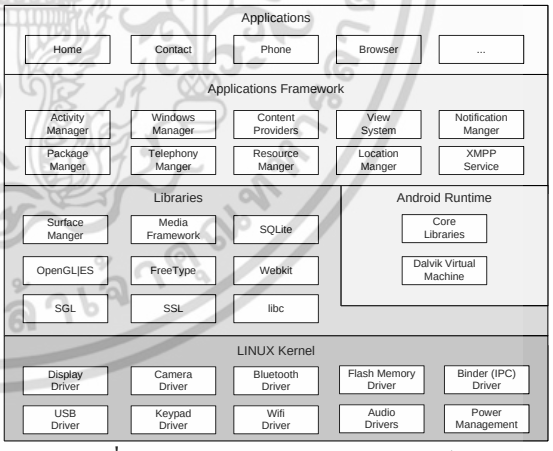
3.3 เปิดโอกาสให้บริษัทผลิตสมาร์ทโฟนต่างๆ ใช้ระบบปฏิบัติการแอนดรอยด์ได้ (Open Device)

3.4 เปิดโอกาสให้บริษัทอื่นๆ เปิดเซิร์ฟเวอร์สำหรับดาวน์โหลดแอพพลิเคชั่นได้ (Open Apps Store)

จากเหตุผลดังกล่าวข้างต้น จะเห็นได้ว่าระบบปฏิบัติการแอนดรอยด์มีความหลากหลายทั้งผู้ผลิต ผู้จัดจำหน่ายและผู้พัฒนาแอพพลิเคชั่น ดังนั้นจึงมีความจำเป็นที่ต้องพิจารณาเรื่องความปลอดภัยของข้อมูลกันมากขึ้น

4. กลไกการรักษาความปลอดภัยบนแอนดรอยด์

ระบบปฏิบัติการแอนดรอยด์เป็นโอเพนซอร์ส (Open Source) ที่พัฒนามาจากระบบปฏิบัติการลินุกซ์ (Linux) โครงสร้างเป็นชั้นๆ (Layer) ชั้นล่างสุดคือลินุกซ์คอร์เนล (Linux Kernel) เป็นส่วนที่เชื่อมต่อกับฮาร์ดแวร์ (Hardware) ชั้นต่อมาเป็นไลบารี่ (Library) ที่เขียนด้วยภาษาซี และมีส่วนที่เป็นรันไทม์ (Runtime) ประกอบไปด้วยดาลวิคเวอร์ชวลแมชชีน (Dalvik Virtual Machine) สำหรับการทำงานโปรแกรมคำสั่งต่างๆ และแอพพลิเคชั่นจะทำงานที่ชั้นบนสุด



รูปที่ 4 สถาปัตยกรรมของแอนดรอยด์ [5]

4.1 กลไกแซนบ็อก (Sandboxing Mechanism)

กลไกนี้จะให้แต่ละแอพพลิเคชั่นแยกเป็นอิสระจากกันป้องกัน [10] ไม่ให้แอพพลิเคชั่นเข้าถึงส่วนอื่นๆ ของระบบปฏิบัติการ หรือเข้าถึงแอพพลิเคชันซึ่งกันและกัน มีพื้นที่จัดเก็บข้อมูลแยกส่วนกันและมีโปรเซส (Process) เป็นของตัวเอง การติดตั้งจะมีเลขที่ลำดับเฉพาะที่

ไม่ซ้ำกัน (UID : Unique user ID) ทำให้ป้องกันการลงแอพพลิเคชั่นซ้ำในเครื่องเดียวกัน ถ้าต้องการใช้โปรเซสหรือข้ออนุญาตระหว่างโปรเซสร่วมกัน ก็ต้องทำผ่านทาง *sharedUserID* ทำให้ต้องใช้ UID ร่วมกัน

4.2 กลไกการอนุญาตแอพพลิเคชั่น (Application Permission Mechanism)

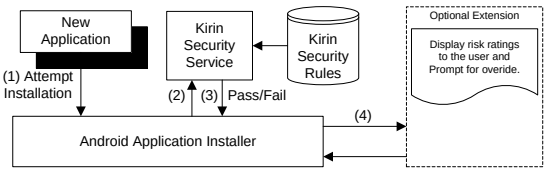
จะใช้ *Package Manager* ในการกำหนดสิทธิหรือการอนุญาตว่าแอพพลิเคชั่นจะสามารถทำอะไรได้บ้าง การกำหนดสิทธิจะทำเพียงครั้งเดียวในขั้นตอนการติดตั้ง โดยแอพพลิเคชั่นสามารถขอสิทธิการใช้ เช่น การเข้าอินเตอร์เน็ต (INTERNET) ส่งข้อความ (WRITE_SMS) หรือใช้กล้องถ่ายรูป (CAMERA) ซึ่งจะเป็นข้อความหรือข้อตกลงถามผู้ใช้งานให้เป็นคนตัดสินใจว่าจะอนุญาตหรือไม่ ถ้าไม่อนุญาตทั้งหมดตามที่ขอก็จะไม่ติดตั้งเลย (*all-or-nothing*) เมื่อติดตั้งไปแล้ว ผู้ใช้งานจะไม่สามารถไปยกเลิกหรือเปลี่ยนแปลง การกำหนดสิทธิได้ภายหลัง

5. กลไกรักษาความปลอดภัยของข้อมูลบนสมาร์ทโฟนแอนดรอยด์

5.1 ด้านกลไกการรักษาความปลอดภัยของข้อมูล

ในเรื่องกลไกการรักษาความปลอดภัยมีการทำวิจัยกันมากเพราะกลไกที่มีอยู่เดิมมีช่องโหว่ โดยเฉพาะกลไกการอนุญาตให้ให้ผู้ใช้งานเป็นคนตัดสินใจว่าจะอนุญาตให้แอพพลิเคชั่นจะมีสิทธิเข้าถึงอะไรหรือทำอะไรได้บ้างในขั้นตอนการติดตั้งเท่านั้น ถ้าไม่อนุญาติทั้งหมดตามที่แอพพลิเคชั่นร้องขอ ก็จะยกเลิกการติดตั้งทั้งหมด เช่นการติดตั้งแอพพลิเคชั่นเครือข่ายสังคมออนไลน์ในระหว่างการติดตั้งมีการร้องขออนุญาตให้ใช้อินเตอร์เน็ตด้วย หากมีการอนุญาตในขณะติดตั้งแล้ว แอพพลิเคชั่นก็สามารถเปิดบราวเซอร์อินเตอร์เน็ตได้ ทำให้ผู้ใช้อาจเผลอคลิกเข้าเวบที่เชื่อมโยงจากแอพพลิเคชั่นได้

คิริน (kirin) William Enck [6] เป็นกลไกแรกๆที่มีการพูดถึงการทำวิจัยเรื่องกลไกการรักษาความปลอดภัย โดยมีการแก้ไขกลไกในส่วนขั้นตอนการติดตั้ง ให้มีการตรวจสอบความปลอดภัยก่อนการติดตั้ง



รูปที่ 5 กลไกการรักษาความปลอดภัยของคิริน [6]

โดยกลไกการรักษาความปลอดภัยจะกระทำในขั้นตอนการติดตั้งแอพพลิเคชั่น โดยในระหว่างการติดตั้งจะตรวจสอบข้อมูลด้านความปลอดภัยเทียบกับฐานข้อมูล หากเห็นว่ามีอันตรายต่อความปลอดภัย ก็จะแจ้งให้ผู้ติดตั้งได้ทราบและยกเลิกการติดตั้งไป แต่ก็ยังมีจุดอ่อนตรงที่การจะทราบว่าแอพพลิเคชั่นไหนที่ไม่ปลอดภัยต้องอ้างอิงกับฐานข้อมูล ซึ่งอาจจะไม่ทันสมัย และมีการตรวจสอบเฉพาะขั้นตอนการติดตั้งเท่านั้น

สแกนดรอยด์ (SCanDroid) Adam P. Fuchs [7] เป็นกลไกที่ตรวจสอบการทำงานของแอพพลิเคชั่นว่ามีการเรียกใช้ข้อมูลหรือส่วนประกอบอะไรบ้างหรือมีการร้องขออนุญาตอะไรบ้าง แต่ก็ยังมีข้อเสียคือการตรวจสอบต้องอาศัยฐานข้อมูลเดิมและกระทำในขั้นตอนการติดตั้งเท่านั้น

Hammad Banuri [8] ได้ศึกษารูปแบบในการทำงานของแอพพลิเคชั่นว่ามีพฤติกรรม (behavior) ในการทำงานของแอพพลิเคชั่นว่ามีการไปใช้สิทธิหรือมีลักษณะที่เป็นภัยคุกคามที่เป็นอันตรายหรือไม่ โดยมีการกำหนดเป็นโครงสร้าง Security Enhanced Android Framework (SEAF) และใช้ตรวจสอบการทำงานของแอพพลิเคชั่นในช่วงการทำงาน แต่ข้อเสียคือหากนำไปใช้งานจริงต้องทดสอบว่าไปรบกวนการทำงานของระบบหรือไม่ หรืออาจทำให้บางแอพพลิเคชั่นไม่สามารถทำงานได้

5.2 ด้านความปลอดภัยของข้อมูลบน SSL

Sascha Fahl [9] ได้ศึกษาถึงความปลอดภัยของการรับส่งข้อมูลผ่านโปรโตคอล SSL/TLS โดยได้ทำการสร้างเครื่องมือที่เรียกว่า MalloDroid ในการตรวจสอบการทำงานของ SSL/TLS จากแอพพลิเคชั่นที่ดาวโหลดมาจากกูเกิลเพลย์ (Google Play) ประมาณ 13,500 แอพ ซึ่งก็พบว่ามีจำนวนหนึ่งที่มีการใช้ SSL ไม่ถูกต้องประมาณ 100 กว่าแอพพลิเคชั่น มีการใช้ SSL ที่ไม่ถูกต้อง จากการกำหนดใบอนุญาตด้านความปลอดภัย (CAs : Certificate

Authorities) โดยที่ไม่มีการระบุเฉพาะเจาะจงของแหล่งใบอนุญาตด้านความปลอดภัย

5.3 งานวิจัยด้านพฤติกรรมผู้บริโภค

การที่ระบบปฏิบัติการให้สิทธิผู้บริโภคเป็นคนตัดสินใจเองในเรื่องความปลอดภัยและสิทธิต่างๆ ทำให้เกิดคำถามตามมาว่าผู้บริโภคได้ตระหนักถึงภัยคุกคามที่จะตามมาหรือเปล่า Alexios Mylonas [2] ได้ทำการวิจัยเชิงสำรวจถึงความตระหนักในเรื่องความปลอดภัยในการใช้สมาร์ทโฟนของผู้บริโภค โดยทำการสำรวจ จากผู้ใช้แอพพลิเคชั่นที่ดาวโหลดแอพพลิเคชั่นจากผู้ผลิตโดยตรง เช่น แอพสโตร์ กูเกิลเพลย์ เพื่อเปรียบเทียบว่า ผู้ใช้งานได้ระวังเรื่องความปลอดภัยของข้อมูลหรือไม่ พบว่าส่วนใหญ่จะเชื่อถือว่าได้ดาวโหลดแอพพลิเคชั่นจากแหล่งที่มีความน่าเชื่อถือแล้ว จึงไม่ได้ระมัดระวังเรื่องความปลอดภัยของข้อมูล และไม่มีติดตั้งโปรแกรมป้องกันไวรัสเหมือนกับการใช้งานเครื่องคอมพิวเตอร์

6. ข้อแนะนำความปลอดภัยสำหรับแอพพลิเคชั่นบนสมาร์ทโฟน

ข้อแนะนำเพื่อความปลอดภัยของแอพพลิเคชั่นบนสมาร์ทโฟนโดย Andrew Hoog [11] จะประกอบไปด้วยหลายส่วนคือ แอพพลิเคชั่นตัวเครื่อง และผู้พัฒนาแอพพลิเคชั่น นอกจากนี้ยังสามารถใช้ตัวกลางที่คอยตรวจสอบความปลอดภัยของแอพพลิเคชั่นได้

6.1 ตัวเครื่อง

สำหรับการใช้งานโทรศัพท์มือถือที่เป็นสมาร์ทโฟนให้ปลอดภัยควรปฏิบัติดังนี้

1. อัพเดทซอฟต์แวร์สม่ำเสมอ
2. ปิดการใช้งานอื่นที่ไม่จำเป็น เช่น บลูทูธ (Bluetooth)
3. เปิดระบบป้อนรหัสผ่านในการเข้าใช้งาน
4. อย่าเข้าลิ้งค์หรือเวบที่เราไม่แน่ใจ
5. เลือกติดตั้งแอพพลิเคชั่นที่น่าเชื่อถือได้
6. ลบข้อมูลก่อนจะขายหรือยกเลิกการใช้

6.2 เลือกใช้คนกลางในการตรวจสอบแอพพลิเคชั่น

การตรวจสอบว่าแอพพลิเคชั่นไหนปลอดภัยสำหรับผู้ใช้เป็นเรื่องยุ่งยาก แต่ปัจจุบัน ก็มีบริษัทที่ทำการตรวจสอบแอพพลิเคชั่นบนมือถือว่าปลอดภัยหรือไม่เช่น AppWatchdog [12] จะทำการตรวจสอบดังนี้

1. มีการเก็บพลาสเวิร์ดที่มีการเข้ารหัสข้อมูลหรือไม่
2. มีการเก็บชื่อผู้ใช้ที่มีการเข้ารหัสหรือไม่
3. มีการเก็บข้อมูลที่มีความปลอดภัยหรือไม่
4. มีการเก็บข้อมูลบัตรเครดิตหรือไม่

6.3 ข้อแนะนำสำหรับผู้พัฒนาแอพพลิเคชั่น

ข้อแนะนำเพื่อความปลอดภัยสำหรับผู้พัฒนาแอพพลิเคชั่น (Developer) บนสมาร์ทโฟนโดย Andrew Hoog [11] มีดังนี้

1. User names ควรเก็บชื่อผู้ใช้เป็นความลับหรือมีการเข้ารหัสก่อนจัดเก็บ และการนำมาแสดงผลคือปิดบังข้อมูลไว้บางส่วน เช่น ใช้เครื่องหมาย * แทนอักขระบางตัวก่อนนำไปแสดงผล
2. Passwords ควรเก็บรหัสผู้ใช้เป็นความลับหรือมีการเข้ารหัสก่อนจัดเก็บ
3. Credit card data ไม่ควรเก็บข้อมูลบัตรเครดิตไว้ทั้งหมดและมีการเข้ารหัสข้อมูลก่อนจัดเก็บ การนำมาแสดงผลคือปิดบังข้อมูลไว้บางส่วนเช่น ใช้เครื่องหมาย*แทนอักขระบางตัวก่อนนำไปแสดงผลบนหน้าจอ
4. Sensitive application data ข้อมูลอื่นๆ ที่สำคัญควรมีการเข้ารหัสก่อนจัดเก็บ

7. สรุป

ความปลอดภัยของข้อมูลการใช้แอพพลิเคชั่นบนสมาร์ทโฟนแอนดรอยด์นับวันต้องยิ่งให้ความสำคัญมากขึ้นเพราะจำนวนมัลแวร์ที่เพิ่มขึ้นอย่างมากตามจำนวนแอพพลิเคชั่น และจากการวิจัยเชิงสำรวจก็ชี้ให้เห็นว่าผู้ใช้ส่วนใหญ่ยังไม่ได้ให้ความสำคัญในเรื่องความปลอดภัยของข้อมูลมากนักและการที่ผู้ใช้งานยังขาดความใส่ใจเรื่อง

ความปลอดภัยของข้อมูลจึงเป็นช่องโหว่ให้แฮคเกอร์ใช้ในการโจมตีและมีรูปแบบหลากหลายมากขึ้น เช่น การส่งข้อความหลอกลวงหรือการโจมตีโดยใช้เทคนิคทางจิตวิทยาสังคม (Social Engineering) ก็เป็นรูปแบบหนึ่งของการหลอกลวงให้ผู้ใช้งานหลงเชื่อ การวิจัยด้านพฤติกรรมของผู้บริโภคเพื่อให้ทราบถึงการใช้งานและความเข้าใจถึงเรื่องความปลอดภัยในการใช้สมาร์ทโฟนเพียงใด จะเป็นแนวทางในการปรับเปลี่ยนพฤติกรรมการใช้งานหรือให้ความรู้แก่ผู้ใช้ทั่วไปให้ใช้สมาร์ทโฟนได้อย่างปลอดภัย

ปัญหาเรื่องความปลอดภัยของข้อมูลส่วนหนึ่งมาจากกลไกการรักษาความปลอดภัยของระบบปฏิบัติการแอนดรอยด์แบบเดิมที่มีช่องโหว่ เพราะมีการตรวจสอบเฉพาะตอนติดตั้งเท่านั้นแต่แอพพลิเคชั่นที่เป็นมัลแวร์สามารถซ่อนการตรวจจับและทำงานภายหลังได้ ทำให้มีการทำวิจัยด้านไกการรักษาความปลอดภัยด้วยวิธีการใหม่ๆมากขึ้น บางวิธีการก็เหมือนกับการทำงานของโปรแกรมป้องกันไวรัสบนคอมพิวเตอร์ นอกจากนี้ผู้ผลิตแอพพลิเคชั่นก็ต้องคำนึงถึงขั้นตอน และวิธีการต่างๆที่ใช้ในการสร้างแอพพลิเคชั่นให้มีความปลอดภัยต่อการใช้งาน

8. เอกสารอ้างอิง

[1] Chris Rose, “Smart Phone, Dumb Security,”. Review of Business Information Systems, Vol.16, 2012.

[2] Alexios Mylonas, Anastasia Kastania and Dimitris Gritzalis, “Delegate the smartphone user? Security awareness in smartphone platforms,” Computers & Security,. Greece, November, 2012.

[3] http://en.wikipedia.org/wiki/Smartphone

[4] http://en.wikipedia.org/wiki/List_of_mobile_software_distribution_platforms

[5] http://developer.android.com

[6] William Enck, Machigar Ongtang, and Patrick McDaniel, “On lightweight mobile phone application certification,” in Proceedings of the 16th ACM conference on Computer and Communications Security, ACM, 2009.

[7] Adam Fuchs, Avik Chaudhuri, and Jeffrey Foster, "SCanDroid: Automated Security Certification of Android Applications," University of Maryland, College Park.

[8] Hammad Banuri, Masoom Alam, Shahryar Khan, Jawad Manzoor, Bahar Ali, Yasar Khan, Mohsin Yasee, Mir Nauman Tahir and Tamleek Ali, Quratulain Alam and Xinwen Zhang, “An Android runtime security policy enforcement framework,” Pers Ubiquit Comput, Vol. 16, 2012.

[9] Sascha Fahl, Marian Harbach, Thomas Muders, Lars Baumgärtner, Bernd Freisleben and Matthew Smith, “Why Eve and Mallory Love Android:An Analysis of Android SSL (In)Security,” ACM, 2012.

[10] Sohail Khan, Mohammad Nauman, Abu Talib Othman and Shahrulniza Musa, “How Secure is your Smartphone: An Analysis of Smartphone Security Mechanisms,” Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). Malaysia, June, 2012.

[11] Andrew Hoog, “Android Forensics: Investigation, Analysis and Mobile Security for Google Android,” Syngress, 2011

[12] https://viaforensics.com/resources/reports/mobile-app-security-study/