การวิเคราะห์ความปลอดภัยการใช้งานแอพพลิเคชั่นธนาคารบนระบบแอนดรอยด์
FORENSIC ANALYSIS OF M-BANKING APPS ON ANDROID PLATFORMS

รัชฎา ชนะจิตต์ 5738689 ITCY/M

วท.ม. (ความมั่นคงไซเบอร์และการประกันสารสนเทศ)

คณะกรรมการที่ปรึกษาวิทยานิพนธ์: วันทนีย์ วิริยสิทธาวัฒน์, Ph.D., คิม-กวาง เรย์มอนด์ ชู, Ph.D.

บทคัดย่อ

เนื่องจากความก้าวหน้าทางเทคโนโลยี โทรศัพท์เคลื่อนที่ได้เข้ามามีบทบาทสำคัญในเชิงธุรกิจและการศึกษา ทำให้แอพพลิเคชั่นถูกพัฒนาขึ้นเพื่อรองรับการใช้งานผ่านทางโทรศัพท์ โดยแอพพลิเคชั่นธนาคารนั้นกำลังได้รับความนิยมและถูกใช้งานแพร่หลายมากขึ้น จากผลการวิจัยในเรื่องแนวโน้มการใช้จ่ายเงินผ่านโทรศัพท์ในปีที่ผ่านมาพบว่า ร้อยละ 69 ของผู้ใช้งานโทรศัพท์จาก 15 ประเทศทั่วโลกกำลังทำธุรกรรมการเงินกับทางธนาคารผ่านทางโทรศัพท์ เช่น การตรวจสอบยอดเงินในบัญชี การโอนเงินและการจ่ายบิล ซึ่งเซอร์วิสที่ทางธนาคารให้บริการผ่านทางโทรศัพท์นั้นถือเป็นการอำนวยความสะดวกให้กับผู้ใช้งานที่ไม่สามารถทำธุรกรรมผ่านทางสาขาของธนาคารได้ แต่อย่างไรก็ตามมาตรฐานความปลอดภัยในแอพพลิเคชั่นยังคงเป็นประเด็นที่สำคัญสำหรับผู้ใช้งานในการตัดสินใจที่จะทำธุรกรรมผ่านทางแอพพลิเคชั่น เนื่องด้วยแอพพลิเคชั่นที่ติดตั้งบนระบบปฏิบัติการที่ต่างกัน มีวิธีการจัดเก็บข้อมูลผู้ใช้งาน รวมถึงข้อมูลการทำธุรกรรมการเงินในหน่วยความจำภายในเครื่องที่แตกต่างกัน ทำให้เป็นโทรศัพท์กลายเป็นเป้าหมายในการโจมตีจากผู้ไม่หวังดีและมีความเป็นไปได้ที่ข้อมูลผู้ใช้งานจะถูกเข้าถึงผ่านการใช้งานแอพพลิเคชั่น ดังนั้นประสิทธิภาพของกลไกการรักษาความปลอดภัยของแอพพลิเคชั่นธนาคารจึงควรถูกประเมิน เพื่อสร้างความตระหนักความเสี่ยงด้านความปลอดภัยและความเป็นส่วนตัวให้กับผู้ใช้งานและผู้พัฒนาแอพพลิเคชั่นธนาคาร ในการวิจัยครั้งนี้ แอพพลิเคชั่นธนาคารที่ถูกพัฒนาบนแอนดรอยด์ ประกอบด้วย SCB EASY, Krungsri, K-Mobile Banking, Bualuang mBanking, MyMo, KTB netbank และ TMB Touch ถูกนำมาติดตั้งบนโทรศัพท์เคลื่อนที่ซัมซุงกาแล็กซี S4 ที่มีคุณสมบัติต่างกัน 2 เครื่อง และดำเนินการทำธุรกรรมการเงิน เช่น การตรวจสอบยอดเงินในบัญชี, การโอนเงิน, การตั้งค่าเตือน, การค้นหาสาขาธนาคาร และการจ่ายบิล โดยงานวิจัยนี้เป็นงานค้นคว้าชิ้นแรกที่นำเสนอการจัดลำดับการวิเคราะห์ข้อมูลเชิงนิติคอมพิวเตอร์บนแอพพลิเคชั่นธนาคาร โดยมุ่งเน้นในส่วนการจัดเก็บหลักฐานทางดิจิทัลและการวิเคราะห์ข้อมูลของการใช้งานแอพพลิเคชั่นจากมุมมองของผู้ใช้งาน ผ่านทางการการสร้างอิมเมจทางกายกายภาพของหน่วยความจำทั้งหมดภายในเครื่องด้วยเทคนิคคำสั่ง DD และ JTAG จากนั้นใช้ซอฟท์แวร์ในการทำดิจิทัลฟอเรนสิกส์ที่ได้รับการยอมรับในระดับสากลในการวิเคราะห์อิมเมจ เพื่อค้นหาข้อมูลที่จัดเก็บอยู่ในเครื่องและ/หรือข้อมูลที่เหลืออยู่หลังจากผู้ใช้งานปิดการใช้งานแอพพลิเคชั่น และสามารถระบุธุรกรรมการเงินที่ผู้ใช้งานได้ดำเนินการเสร็จสิ้น นอกจากนี้แอพพลิเคชั่นโค้ดถูกวิเคราะห์ตามฟังก์ชั่นการทำงานและกลไกความปลอดภัย เพื่อค้นหาข้อมูลผู้ใช้งานที่อาจถูกฝังอยู่ภายในโค้ด รวมถึงรีคอมไพล์แอพพลิเคชั่นเพื่อแก้ไขโค้ดในส่วนของการตรวจสอบใบรับรอง แอพพลิเคชั่นที่ผ่านการรีคอมไพล์ถูกเซ็นด้วยใบรับรองที่สร้างขึ้นมาโดยเฉพาะและติดตั้งลงบนเครื่อง จากผลการทดลองจะเห็นได้ว่าโดยส่วนใหญ่พบข้อมูลผู้ใช้งานถูกจัดเก็บในส่วนของพาธทิชั่นข้อมูลผู้ใช้ เช่น พบข้อมูลเบอร์โทรศัพท์ วันเกิด รหัสผ่าน หมายเลขบัตรประชาชน และหมายเลขบัตรเครดิต ซึ่งข้อมูลเหล่านี้สามารถถูกนำไปใช้ก่ออาชญากรทางไซเบอร์ ปลอมแปลงเป็นเจ้าของบัญชีเพื่อทำธุรกรรมทางการเงินโดยปราศจากการแจ้งเตือนไปยังเจ้าของบัญชี แอพพลิเคชั่นบางส่วนมีโมดูลความปลอดภัย เช่น การเข้ารหัสข้อมูล การทำ SSL pinning แต่ไม่ถูกใช้งานโดยตัวแอพพลิเคชั่นทำให้สามารถเทราบถึงข้อมูลผู้ใช้งานในรูปแบบไม่เข้ารหัสข้อมูล แต่อย่างไรก็ตามจากการประเมินความปลอดภัยบนแอพพลิเคชั่นธนาคารพบว่า มาตรฐานความปลอดภัยเบื้องต้นได้รับการติดตั้งอยู่ในแอพพลิเคชั่นธนาคาร ทั้งนี้เพื่อยกระดับมาตรฐานความปลอดภัยของแอพพลิเคชั่นบนโทรศัพท์ ผู้พัฒนาแอพพลิเคชั่นควรคำนึงถึงข้อกำหนดด้านความปลอดภัยในขณะที่วางแผนพัฒนาแอพพลิเคชั่น ก่อนที่จะปล่อยแอพพลิเคชั่นนั้นให้ผู้ใช้งานดาวน์โหลด

98 หน้า