ถอดบทเรียนที่น่าสนใจจากภาคธนาคาร : แนวทางพัฒนาแอปพลิเคชันที่มีความมั่นคงปลอดภัยต่อ Digital ID

1. บทนำ

ในยุคที่การใช้ Digital ID ในการทำธุรกรรมอิเล็กทรอนิกส์บนอุปกรณ์ (เช่น สมาร์ตโฟน) กลายเป็นเรื่องปกติในชีวิตประจำวัน โดยเฉพาะการทำธุรกรรมทางการเงินในแอปพลิเคชันธนาคาร ซึ่งเป็นการทำธุรกรรมที่สำคัญและมีความอ่อนไหวต่อข้อมูลส่วนบุคคลและทรัพย์สิน

ที่ผ่านมา แอปพลิเคชันธนาคารมักเผชิญความเสี่ยงจากการที่ผู้ไม่หวังดีสามารถควบคุมอุปกรณ์ (device takeover) ของเหยื่อ แล้วใช้อุปกรณ์นั้นในการทำธุรกรรมผิดกฎหมายได้ ซึ่งถือเป็นภัยคุกคามร้ายแรงต่อความมั่นคงปลอดภัยของ Digital ID ภาคธนาคารจึงได้พัฒนามาตรการป้องกันภัยคุกคามต่าง ๆ เช่น การใช้ Library เสริมความปลอดภัย และการตรวจจับพฤติกรรมผิดปกติ ควบคู่กับการออกแบบแอปพลิเคชันธนาคารให้มีความปลอดภัยมากยิ่งขึ้น เพื่อปกป้องผู้ใช้บริการของตนเอง

2. แนวทางที่ภาคธนาคารใช้ในการพัฒนาแอปพลิเคชันที่มีความมั่นคงปลอดภัยต่อ Digital ID

ลักษณะของการโจมตีที่ผู้ไม่หวังดีมักใช้ในการโจมตีแอปพลิเคชันธนาคารคือการหลอกให้เหยื่อเปิด accessibility service ร่วมกับการโจมตีด้วย screen overlay ถึงแม้ว่า accessibility service จะถูกออกแบบมาเพื่อช่วยเหลือผู้พิการในการใช้งานสมาร์ตโฟน แต่ผู้ไม่หวังดีก็สามารถใช้ช่องทางนี้ในการโจมตี เช่น บันทึกการกดแป้นพิมพ์ (keylogging) หรือซ้อนหน้าจอปลอม (overlay) เพื่อขโมยข้อมูลของเหยื่อและข้อมูลในแอปพลิเคชันธนาคาร

ที่มา: "กลโกงมิจฉาชีพ หลอกติดตั้งแอปพลิเคชันดูดเงิน" https://www.tba.or.th/wp-content/uploads/pdf/TB-Cert_Presentation_16.10_ForPress_blur.pdf

จากการที่แอปพลิเคชันธนาคารมักตกเป็นเป้าหมายของการโจมตีเพื่อขโมยข้อมูลของผู้ใช้บริการและทำธุรกรรมโดยผิดกฎหมาย ภาคธนาคารจึงได้ออกแบบมาตรการรักษาความปลอดภัยและลดความเสี่ยงจากการถูกโจมตี ในรูปแบบที่หลากหลายดังนี้

2.1 การใช้ Library เสริมความปลอดภัยให้แก่แอปพลิเคชัน

การนำ library เสริมความปลอดภัย เช่น DexGuard (เวอร์ชันเชิงพาณิชย์ของ ProGuard) และ Appdome มาใช้ในการพัฒนาแอปพลิเคชันสามารถช่วยเพิ่มฟังก์ชันการตรวจจับและคุณสมบัติในการป้องกันการโจมตีได้หลากหลายรูปแบบ เช่น

- **Root/Jailbreak:** เป็นการตรวจจับว่าอุปกรณ์ที่กำลังใช้งานแอปพลิเคชัน ผ่านการดัดแปลงระบบปฏิบัติการเพื่อให้เจ้าของอุปกรณ์สามารถแก้ไขไฟล์ของระบบ หรือติดตั้งแอปพลิเคชันที่ถูกดัดแปลงหรือผิดกฎหมาย หรือไม่ [1] [3]
- **UI Protection:** เป็นการตรวจจับและป้องกันการแสดงหน้าจอที่ไม่ได้รับอนุญาตหรือเมื่อพบความพยายามที่ผิดปกติระหว่างการใช้งานแอปพลิเคชัน (Detect Overlay Attack) และแจ้งเตือนแก่ผู้ใช้งาน โดยแอปพลิเคชันจะแสดงหน้าจอ overlay สีดำ เพื่อป้องกันการบันทึกหน้าจอ การสะท้อนหน้าจอ (screen mirroring) และการจับภาพจากภายนอก [2]
- **Application Hardening:** เป็นการป้องกันการวิศวกรรมย้อนกลับ (reverse engineering) และการฉีดโค้ด (code injection) โดยใช้หลักการ Polymorphic Obfuscation ที่ทำให้โค้ดของแอปพลิเคชันถูกปกปิดเพื่อไม่ให้สามารถทำความเข้าใจได้ง่าย (obfuscation) และเปลี่ยนรูปแบบของโค้ดในทุกครั้งที่มีการ build แอปพลิเคชันใหม่ แม้โครงสร้างและการทำงานของแอปพลิเคชันจะเหมือนเดิม แต่โค้ดที่ถูกสร้างขึ้นจะมีรูปแบบแตกต่างกัน ทำให้ผู้ไม่หวังดีไม่สามารถนำความรู้หรือช่องโหว่จากแอปพลิเคชันเวอร์ชันก่อนหน้ามาใช้ในการโจมตีแอปพลิเคชันเวอร์ชันใหม่ได้ [4]

2.2 การแจ้งเตือนเมื่อพบพฤติกรรมผิดปกติ

เป็นการตั้งค่าแอปพลิเคชันให้สามารถแจ้งเตือนผู้ใช้อุปกรณ์เมื่อตรวจพบพฤติกรรมผิดปกติได้ทันที เช่น การเปิด accessibility services หรือการ overlay หน้าจอโดยที่ไม่ได้รับอนุญาต โดยแอปพลิเคชัน

จะแจ้งเตือนผู้ใช้อุปกรณ์ผ่าน pop-up notification รวมทั้งอาจทำการปิดฟังก์ชันสำคัญของแอปพลิเคชันทันทีเพื่อป้องกันความเสียหาย

2.3 การจำกัดเวอร์ชันขั้นต่ำของระบบปฏิบัติการและ Security Patch

แอปพลิเคชันของธนาคารมีการกำหนดให้ทำงานได้บนอุปกรณ์ที่ใช้ระบบปฏิบัติการเวอร์ชันสูงกว่าหรือเท่ากับที่กำหนดไว้ และต้องได้รับการอัปเดต security patch อย่างสม่ำเสมอ การจำกัดความต้องการขั้นต่ำของแอปพลิเคชันนี้ช่วยลดความเสี่ยงจากการใช้ช่องโหว่ที่ถูกตรวจพบแล้วในระบบปฏิบัติการที่ล้าสมัย [5] [6] [7]

3. สรุป

บทเรียนจากภาคธนาคารแสดงให้เห็นว่า การรักษาความมั่นคงปลอดภัยของ Digital ID ไม่ใช่เพียงการป้องกันข้อมูลรั่วไหล แต่เป็นการรวบรวมมาตรการต่าง ๆ มาปรับใช้เพื่อสร้างความปลอดภัยในการให้บริการและป้องกันภัยคุกคาม มาตรการต่าง ๆ เช่น การตรวจสอบ accessibility การตรวจสอบการ overlay หน้าจอ และกการใช้ library เสริมความปลอดภัย ซึ่งเป็นตัวอย่างที่สามารถนำไปประยุกต์ใช้ได้ในการพัฒนาแอปพลิเคชันขององค์กรอื่น ๆ ตามความเหมาะสมของทรัพยากรและความจำเป็นขององค์กร

อ้างอิง

[1] J. Soelberg, “Mobile banking apps: A guide to mitigating fraud”, Accessed: Jun. 25, 2025. [Online]. Available: https://promon.io/security-news/mobile-banking-apps-fraud-prevention

[2] “How to Protect Mobile Apps from Overlay Attacks & Malware Using AI”, Appdome. Accessed: Jun. 25, 2025. [Online]. Available: https://www.appdome.com/how-to/account-takeover-prevention/account-protection/protect-android-apps-from-overlay-attacks-malware/

[3] “The Best Application Hardening Techniques”, PreEmptive In-App Protection. Accessed: Jun. 25, 2025. [Online]. Available: https://www.preemptive.com/blog/application-hardening-techniques/

[4] W. B. Guardsquare, “ProGuard vs. DexGuard: An Overview”, Accessed: Jun. 25, 2025. [Online]. Available: https://www.guardsquare.com/blog/dexguard-vs-proguard

[5] “System Requirements for Digital Banking”, Bank Forward. Accessed: Jun. 25, 2025. [Online]. Available: https://bankforward.com/learning-center/system-requirements-for-digital-banking/

[6] Carnegie Mellon University, “The Consequences of Not Updating Software - Information Security Office - Computing Services - Carnegie Mellon University”, Accessed: Jun. 25, 2025. [Online]. Available: https://www.cmu.edu/iso/news/2025/consequences-of-not-updating-software.html

[7] “Phones with outdated operating systems to lose mobile-banking access”, The Nation. Accessed: Jun. 25, 2025. [Online]. Available: https://www.nationthailand.com/business/30379684