NFC เทคโนโลยีการเชื่อมต่ออุปกรณ์แบบไร้สายแห่งอนาคต จบ

วิชญ์คุทธ์ เมาะพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

โดยสรุปการใช้งาน เทคโนโลยี NFC มีอยู่ด้วยกัน 3 ลักษณะ ได้แก่

1. **ทำงานเป็น RFID Tag** ในอุปกรณ์โทรศัพท์มือถือ ในลักษณะนี้จะทำงานเสมือนเป็นบัตร Contactless ซึ่งนั่นหมายความว่าอุปกรณ์โทรศัพท์มือถือตามมาตรฐาน NFC จะเสมือนเป็นบัตรในรูปแบบใดก็ได้ตามมาตรฐาน ISO 14443 และ FeliCa ที่พบมากก็คือเป็น Contactless Smart Card เพื่อใช้ในการทำธุรกรรม โทรศัพท์มือถือที่มีเครื่องอ่าน NFC ฝังอยู่สามารถทำงานเป็น RFID tag ได้ ซึ่งต่างจากเครื่องอ่าน RFID ในปัจจุบันที่ทำหน้าที่เป็นเครื่องอ่านเพียงอย่างเดียว

การทำงานในลักษณะนี้ส่วนใหญ่จะใช้ใน Application ด้านการเงิน เช่น การจ่ายเงินชำระค่าผ่านทาง การจ่ายเงินตาม POS (Point of Sell) ต่างๆ เพียงแค่นำโทรศัพท์มือถือไปใกล้กับเครื่องอ่าน RFID ที่ติดตั้งไว้ที่จุดชำระเงิน ก็สามารถทาการชำระเงินได้ แทนการชำระเงินด้วยบัตร RFID หรือเงินสด นอกจากนั้นเราสามารถขยายการใช้งานอุปกรณ์ NFC ชิ้นเดียวเป็นบัตรหลายใบได้ เช่น เป็นบัตรเครดิต บัตรโดยสารรถ BTS MRT บัตรเงินสด บัตรสะสมแต้ม เป็นต้น ทำให้เมื่อ NFC เป็นที่นิยมและผู้ให้บริการบัตรต่างๆ ทำ Application สำหรับบริการของตนลงบนอุปกรณ์ เราอาจไม่ต้องพกบัตรมากมาย เช่น Visa อาจจะออก Application ที่สามารถแทน Visa Wave หลายบัญชีและให้เราเลือกบัญชีที่ต้องการใช้ได้จากโทรศัพท์มือถือ หรือ Sony อาจจะออก Application ที่ใช้จำลองบัตร FeliCa เพื่อที่เราสามารถเอาโทรศัพท์มือถือของเราไปลงทะเบียนกับ MRT เพื่อใช้แทนบัตรโดยสารได้ ซึ่งในโหมดนี้เราสามารถนำมาใช้กับระบบที่ใช้กันอยู่ในปัจจุบันได้ เราจึงจะได้ประโยชน์จาก NFC อย่างเห็นเป็นรูปธรรมที่สุด

ตัวอย่างการใช้มือถือทำงานเป็น RFID Tag

2. **ทำงานเป็นเครื่องอ่าน RFID** อุปกรณ์ เช่นโทรศัพท์มือถือที่มีเครื่องอ่าน NFC ฝังอยู่ สามารถทำงานเป็นเครื่องอ่าน RFID เมื่อต้องการอ่านข้อมูลจาก RFID Tag ในโหมดนี้อุปกรณ์ NFC สามารถทำตัวเสมือนเป็นเครื่องอ่านเขียน Contactless Smart Card (หรือบางครั้งเรียกว่า Tag) โดยจะสามารถอ่านข้อมูลจาก Tag ที่ติดอยู่ใน Smart poster หรือจุดให้บริการข้อมูล การประยุกต์ใช้งาน เช่น ทำการส่งเสริมการขายโดยแจกคูปองส่วนลดสำหรับ 50 คนแรกที่มาอ่านโฆษณาที่จุดให้บริการ ซึ่งการกำหนดจานวนแบบนี้ไม่สามารถทำได้โดยการใช้

Bar Code Tag ที่เป็นภาพแบบ 2 มิติ และยังสามารถทำ One-Touch Setup สำหรับ Wi-Fi และ Bluetooth คือ ช่วยในการจับคู่อุปกรณ์ NFC ที่มี Bluetooth หรือ Wi-Fi ในโหมด Ad-hoc เพียงแค่เอาอุปกรณ์มาแตะกันก็จะการจับคู่ให้อัตโนมัติสำหรับการใช้งานในลักษณะ Smart Poster เป็นต้น

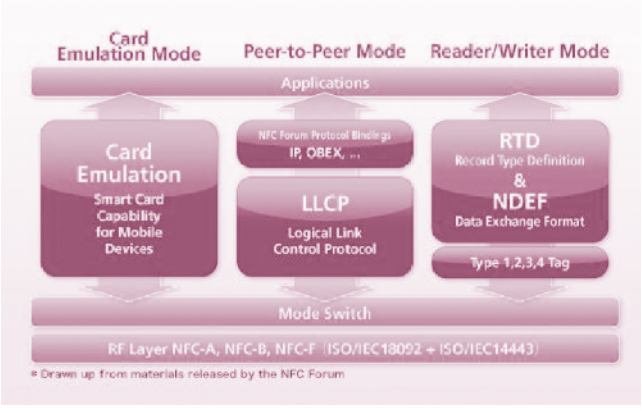
โดยที่โปสเตอร์จะมี RFID Sticker เมื่อต้องการอ่านข้อมูลจาก RFID Sticker เพียงแค่นำโทรศัพท์มือถือที่มีเครื่องอ่านไปอ่าน RFID Sticker บนโปสเตอร์ ข้อมูลในโปสเตอร์ก็จะปรากฏขึ้นมาบนโทรศัพท์มือถือ

Smart poster

3. **การสื่อสารในลักษณะ Peer to Peer (P2P)** เครื่องอ่าน NFC สองเครื่องสามารถที่จะติดต่อสื่อสารกันโดยตรงได้ โหมดนี้จะทำการแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์ NFC ด้วยกัน คล้ายกับการที่มือถือมี Bluetooth แล้วทำการแลกเปลี่ยนข้อมูลโดยการการจับคู่ (Pair) เครื่องเข้าด้วยกันแล้วแลกเปลี่ยนข้อมูล เช่น นามบัตร รูปถ่าย แฟ้มข้อมูลอื่นๆ แต่ว่าสำหรับ NFC แล้ว ไม่ต้องมีการจับคู่เหมือน Bluetooth เพียงแค่เลือกข้อมูลที่ต้องการแลกเปลี่ยนแล้วนำอุปกรณ์ NFC ที่รองรับโหมดนี้มาแตะหรือสัมผัสกัน ข้อมูลดังกล่าวก็จะถูกทำการถ่ายโอนกันระหว่างอุปกรณ์ เพราะรัศมีทำการของ NFC อยู่ในระดับน้อยกว่า 10 ซ.ม. ซึ่งต่างจาก Bluetooth ซึ่งออกแบบไว้ให้สื่อสารข้อมูลในระยะหลายเมตร การแลกเปลี่ยนข้อมูลทำได้ผ่านโปรโตคอล TCP/IP หรือ OBEX (เหมือนกับการแลกเปลี่ยนข้อมูลผ่าน Bluetooth หรือ IrDA)

นอกจากแลกเปลี่ยนข้อมูลแล้วยังสามารถใช้ทำการ synchronize ข้อมูลกับอุปกรณ์อื่นๆ ได้ด้วย ตัวอย่างเช่น โทรศัพท์มือถือสองเครื่องที่มีฟังก์ชัน NFC สามารถที่จะส่งข้อมูลให้แก่กันได้โดยตรง เพียงนำโทรศัพท์ทั้งสองเครื่อง เข้ามาใกล้กันในระยะที่เครื่องอ่านที่อยู่ในโทรศัพท์ทั้งสองสามารถอ่านกันได้ ก็สามารถที่จะส่งข้อมูลถึงกันได้โดยไม่จำเป็นต้องอาศัยเครือข่ายของโทรศัพท์มือถือ ไม่ว่าจะเป็น GPRS หรือ EDGE เป็นต้น

ตัวอย่างการสื่อสารในลักษณะ Peer to Peer (P2P)



ภาพการเปรียบเทียบ NFC ทั้ง 3 โหมด

ถึงแม้ว่าเทคโนโลยี NFC จะได้รับการกล่าวถึงเป็นอย่างมากในปัจจุบัน แต่อุปกรณ์โทรศัพท์มือถือที่รองรับเทคโนโลยี NFC ยังมีอยู่อย่างจำกัด ดังนั้น ในช่วงการเปลี่ยนผ่านจึงมีการพัฒนาเทคโนโลยีต่างๆ ขึ้นมาเพื่อรองรับกับเทคโนโลยี NFC ที่กำลังจะเกิดขึ้น ตัวอย่าง เช่น เทคโนโลยี SIM Card และเสาอากาศ เป็นการต่อเสาอากาศเพิ่มจาก SIM Card ของโทรศัพท์มือถือ ซึ่งได้แก่ SIM pass, N-Flex เป็นต้น โดยใช้ RFID ที่คลื่นความถี่ 13.56 Mhz เทคโนโลยีนี้มีการใช้อย่างแพร่หลายในประเทศจีน

ความเสี่ยงในการใช้ NFC

ถึงแม้ว่าข้อมูลที่ NFC สามารถรับส่งได้นั้นจะทำได้ในปริมาณไม่มากและระยะทางในการทำงานนั้นมีจำกัด แต่ก็เป็นข้อมูลที่ค่อนข้างมีความสำคัญโดยเฉพาะอย่างยิ่งข้อมูลการทำธุรกรรมด้านการเงิน รวมทั้งตัวเทคโนโลยีเองยังมีช่องโหว่ด้านความมั่นคงปลอดภัยที่อาจทำให้ผู้ไม่หวังดีสามารถใช้เป็นช่องทางเข้ามาโจมตีผู้ใช้งานได้ ซึ่งสาเหตุหลักๆ ของภัยคุกคามที่เกี่ยวข้องกับ NFC นั้นเกิดจากรูปแบบการทำงานที่จะเน้นความรวดเร็วในการติดต่อสื่อสารเป็นหลัก จึงอาจทำให้ไม่มีการยืนยันตัวตนที่ดีและเพียงพอ นอกจากนี้ยังพบว่าในปัจจุบัน NFC ยังไม่มีการเข้ารหัสลับข้อมูลที่รับส่งในการทำงานระดับฮาร์ดแวร์ ส่งผลให้เกิดปัญหาภัยคุกคาม อาทิ

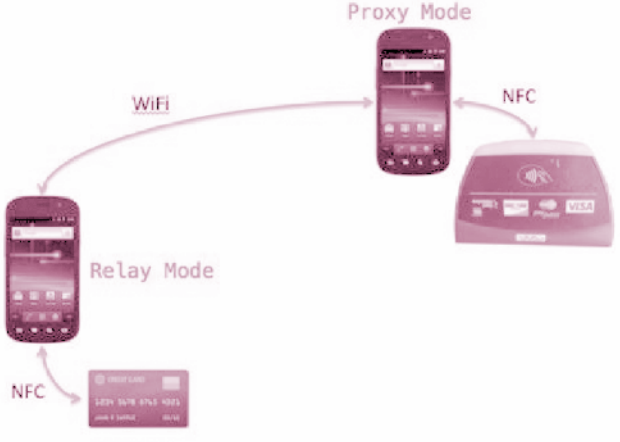
➲ **การดักรับข้อมูล (Eavesdropping)** ผู้ไม่หวังดีจะดักข้อมูลที่มีการรับ-ส่งระหว่างอุปกรณ์ NFC กับเครื่องอ่าน โดยนำอุปกรณ์

ดักรับข้อมูลมาครอบไว้ที่ด้านสัมผัสของเครื่องอ่าน ซึ่งวิธีการโจมตีลักษณะนี้จะคล้ายๆ กับการทำ Skimming ตู้ ATM ที่มีผู้ไม่หวังดีนำอุปกรณ์มาครอบเครื่องอ่านบัตรหรือครอบแป้นพิมพ์ไว้เพื่อดักข้อมูล

➲ **การแก้ไขข้อมูล/การทำให้ข้อมูลเสียหาย** (Data Manipulation/Data Corruption)

ผู้ไม่หวังดีดักรับข้อมูลแล้วแก้ไขข้อมูลระหว่างทาง ซึ่งอาจเป็นการแก้ไขข้อมูลทางการเงิน หรือเปลี่ยนข้อมูลที่มรการรับ-ส่งให้เกิดความผิดพลาด เพื่อไม่ให้ผู้ใช้สามารถใช้บริการนั้นได้ตามปกติ (Denial of Service)

➲ **Relay Attack** เป็นการโจมตีในลักษณะ Man-in-the-Middle ผู้ไม่หวังดีจะหลอกให้เครื่องของผู้ใช้ส่งข้อมูลมาที่ตัวเองก่อนแล้วค่อยส่งข้อมูลนั้นต่อไปให้กับเครื่องอ่าน NFC อีกทีหนึ่งและเมื่อได้รับข้อมูลจากเครื่องอ่าน NFC ก็จะส่งกลับไปให้เหยื่อ จุดประสงค์ของการโจมตีในลักษณะนี้คือเพื่อการขโมยข้อมูล ตัวอย่างซอฟต์แวร์ที่สามารถใช้ในการโจมตีในลักษณะนี้ได้ เช่น NFCProxy



ตัวอย่างการโจมตีแบบ Replay Attack

➲ **ชุดคำสั่งไม่พึงประสงค์** (Malicious code)

อุปกรณ์ที่ใช้บริการธุรกรรมผ่านระบบ NFC จะต้องมีการเก็บข้อมูลที่เกี่ยวข้องกับการทำธุรกรรมไว้ในตัวเครื่องด้วย เช่น หมายเลขบัตรเครดิต เป็นต้น ซึ่งหากอุปกรณ์ดังกล่าวติดมัลแวร์ที่ถูกสร้างขึ้นมาเพื่อขโมยข้อมูล ก็อาจถูกขโมยเงิน หรือถูกขโมยข้อมูลสำคัญไปได้ นอกจากนี้อาจมีการใส่ชุดคำสั่งที่เป็นอันตรายไว้ใน NFC Tag เพื่อให้เครื่องที่เข้ามาอ่านข้อมูลประมวลผลคำสั่งที่เป็นอันตราย เช่น การใส่คำสั่งที่ใช้ในการทำ Factory Reset โทรศัพท์มือถือไว้ใน NFC เป็นต้น

➲ **เครื่องหาย หรือถูกขโมย** หากเป็นโทรศัพท์มือถือที่มีข้อมูลทางการเงินอยู่ก็อาจถูกขโมยหรือสูญเสียข้อมูลสำคัญได้ แต่หากเป็นโทรศัพท์มือถือที่ใช้แทนบัตรผ่านประตู ก็อาจทำให้ผู้ไม่หวังดีเข้าถึงสถานที่หวงห้ามได้

แนวทางป้องกัน

เนื่องจากระบบการทำงานของ NFC นั้น ถูกออกแบบมาเพื่อให้สามารถแลกเปลี่ยนข้อมูลได้อย่างรวดเร็ว จึงไม่ได้มีการตรวจสอบหรือยืนยันตัวบุคคลที่ซับซ้อนมากนัก ดังนั้น การทำให้ระบบมีความมั่นคงปลอดภัยจึงเป็นหน้าที่ของผู้พัฒนาเทคโนโลยีที่ต้องมีการตรวจสอบ หรือเข้ารหัสลับข้อมูลเพิ่มเติม เพื่อป้องกันไม่ให้ผู้ไม่หวังดีดักรับหรือแก้ไขข้อมูลระหว่างทาง ซึ่งสำหรับผู้ใช้งานควรตระหนักอยู่เสมอว่าระบบที่ใช้งานอยู่อาจยังไม่มีการรักษาความมั่นคงปลอดภัยที่ดีพอ หรืออาจมีผู้ไม่หวังดีเข้ามาดัดแปลงระบบเพื่อให้ทำงานผิดปกติ ซึ่งอาจทำได้โดยการตรวจสอบเครื่องอ่าน NFC ว่ามีอุปกรณ์แปลกปลอมติดตั้งอยู่หรือเปล่า ไม่ควรนำอุปกรณ์ไปแตะเข้ากับ NFC Tag ที่น่าสงสัย รวมถึงระมัดระวังในการเก็บข้อมูลสำคัญไว้ในเครื่องและควรกำหนดรหัสผ่านสำหรับการใช้งานโทรศัพท์มือถือ เพื่อป้องกันผู้ไม่หวังดีนำข้อมูลไปใช้ในกรณีที่ทำโทรศัพท์มือถือสูญหาย

สำหรับองค์การ หรือหน่วยงานที่ต้องการหรือมีแนวคิดที่จะนำเทคโนโลยี NFC มาประยุกต์ใช้โดยเริ่มจากการทดแทนบัตรผ่านในการเข้าออกสำนักงาน อาจต้องพิจารณาถึงความเสี่ยงที่อาจจะเกิดขึ้น เนื่องจากเทคโนโลยีดังกล่าวยังคงมีจุดอ่อนบางประการ ซึ่งหากประเมินแล้วพบว่ามีความเสี่ยงก็ยังไม่ควรนำมาใช้ในพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยสูง

ข้อมูลอ้างอิง

"แนวโน้มการใช้โมบายแอพพลิเคชั่น (Usages Trend of Mobile Application)" สุชาดา พลาชัยภิรมย์ศิล มหาวิทยาลัยกรุงเทพ

"Payment เกิดใหม่ เมื่อแถบแม่เหล็ก-สมาร์ทการ์ดไม่ใช่คำตอบสุดท้าย" ภูสิทธิ์ รัตน์ปิยะสุนทร

"NFC (Near field communication)" ภัทราพร จงบุญทรัพย์,ภาณุพงศ์ โตเต็ม,เกตุนภัส พลอำนวยเดช

Ortiz, C. Enrique (2006-06). "An Introduction to Near-Field Communication and the Contactless Communication

http://mobiledista.com/

https://thaicert.or.th

http://www.bot.or.th/Thai/PaymentSystems ธนาคารแห่งประเทศไทย ระบบการชำระเงิน

http://www.addictivetips.com/hardware/what-is-nfc-how-it-works-what-are-its-practical-applications/

http://www.nfc-forum.org/aboutnfc/nfc_in_action/

http://news.softpedia.com/news/NFC-Could-Change-the-Future-of-Communications-126078.shtml

http://www.nearfieldcommunication.org/nfc-security-risks.html

http://electronics.howstuffworks.com/how-secure-is-nfc-tech.htm

http://www.sciencedirect.com/