Suranaree J. Soc. Sci. Vol. 3 No. 1; June 2009 (99-112)

การวิเคราะห์ความปลอดภัยของโทรศัพท์เคลื่อนที่

A Security Analysis of Mobile Phones

วริญทร เจนชัย*, จิติมนต์ อั่งสกุล และธรา อั่งสกุล
Varinthorn Janchai*, Jitimon Angskun and Thara Angskun

สาขาวิชาเทคโนโลยีสารสนเทศ สำนักวิชาเทคโนโลยีสังคม มหาวิทยาลัยเทคโนโลยีสุรนารี

Abstract

Currently, mobile phones play an important role in the lives of Thai people. This can be seen from the numbers of mobile phone users among the Thai population which is up to 74%. However, most users do not know or unaware of the various threats that can access or damage their phones. This article presents a security analysis of mobile phone based on attacks via Bluetooth. It presents a basis for Bluetooth security (e.g., authentication and encryption), security tools and an evaluation of intrusion risks. Various mobile phones with different brand names and modules have been tested. The experimental results show that most mobile phones can be attacked where the impact of intrusion ranges from the stealing of a contact list to making calls from the victims' phones.

Keywords: Mobile phone security; Bluetooth attack; Security analysis

บทคัดย่อ

ในปัจจุบัน โทรศัพท์เคลื่อนที่ได้เข้ามามีบทบาทสำคัญในชีวิตประจำวันของคนไทย ดังจะเห็นได้จากจำนวนผู้ใช้โทรศัพท์เคลื่อนที่ในประเทศไทยมีสูงถึง 74% ของจำนวนประชากรทั้งประเทศ แต่อย่างไรก็ตาม ผู้ใช้ส่วนใหญ่ไม่ทราบหรือไม่ตระหนักถึงภัยคุกคามต่าง ๆ ซึ่งสามารถเข้าถึงหรือทำความเสียหายให้กับโทรศัพท์ได้ บทความนี้จึงได้นำเสนอ การวิเคราะห์ความปลอดภัยของโทรศัพท์เคลื่อนที่จากการโจมตีผ่านระบบบลูทูธ โดยนำเสนอความรู้พื้นฐานเกี่ยวกับระบบรักษาความปลอดภัยของบลูทูธ เช่น การระบุตัวตน และการเข้ารหัส เครื่องมือที่ใช้ในการรักษาความปลอดภัย และการประเมินการบุกรุก โดยใช้โทรศัพท์เคลื่อนที่หลากหลายยี่ห้อและมีฟังก์ชั่น

* *ผู้เขียนที่ให้การติดต่อ โทร. +66 4422 4336; โทรสาร +66 4422 4205*
E-mail address: varinth@sut.ac.th

การทำงานที่แตกต่างกันในการทดลอง ผลลัพธ์ของการทดลองแสดงให้เห็นว่า โทรศัพท์เคลื่อนที่ส่วนใหญ่สามารถถูกโจมตีได้ โดยที่ผลกระทบของการบุกรุกจะมีตั้งแต่การขโมยข้อมูลรายชื่อจนถึงการใช้โทรศัพท์ของเหยื่อในการโทรออกได้เลย

บทนำ

ในปัจจุบันเทคโนโลยีบลูทูธเริ่มเข้ามามีบทบาทสำคัญในวงการธุรกิจ และชีวิตประจำวันของคนเรามากขึ้น เพราะบลูทูธสามารถอำนวยความสะดวกให้กับเครื่องมือสื่อสาร และอุปกรณ์เทคโนโลยีต่าง ๆ ที่มีอุปกรณ์ต่อพ่วง โดยไม่จำเป็นต้องมีสายส่งสัญญาณระหว่างอุปกรณ์หลักกับอุปกรณ์ต่อพ่วงเหล่านั้น ทำให้การเคลื่อนย้าย หรือการใช้อุปกรณ์หลักและอุปกรณ์ต่อพ่วงมีความสะดวกรวดเร็วยิ่งขึ้น และทำให้เราสามารถใช้อุปกรณ์ต่อพ่วงกับอุปกรณ์หลักชนิดใดก็ได้ที่มีอุปกรณ์ส่งสัญญาณนั้นติดไว้ ดังนั้นในอนาคต เทคโนโลยีบลูทูธจึงมีแนวโน้มที่จะได้รับการพัฒนาให้มีประสิทธิภาพ และใช้งานได้กับอุปกรณ์ต่าง ๆ อย่างกว้างขวางมากขึ้น ทำให้มีความเป็นไปได้สูงมากที่เทคโนโลยีนี้จะเข้ามามีอิทธิพลต่อชีวิตประจำวันของทุกคนและต่อภาคธุรกิจ

อย่างไรก็ตามการสื่อสารระหว่างอุปกรณ์บลูทูธยังมีช่องโหว่และจุดอ่อนที่ทำให้ผู้ไม่ประสงค์ดีสามารถเข้ามาใช้อุปกรณ์ของผู้ที่เป็นเป้าหมายหรือเหยื่อได้ เช่น การขโมยข้อมูลในโทรศัพท์มือถือ การดักฟังโทรศัพท์ และใช้โทรศัพท์ของเหยื่อเพื่อเป็นตัวกลางในการทำสิ่งผิดกฎหมายอื่น ๆ ดั้งนั้น นอกจากการใช้ประโยชน์จากเทคโนโลยีที่มีอยู่แล้ว ผู้ใช้เทคโนโลยีจึงควรตระหนักถึงภัยคุกคามที่อาจเกิดขึ้นกับการนำเทคโนโลยีเหล่านั้นไปใช้ด้วย

ในบทความนี้ได้นำเสนอการวิเคราะห์ความปลอดภัยของโทรศัพท์เคลื่อนที่จากการโจมตีผ่านระบบบลูทูธ ซึ่งประกอบด้วย 6 ส่วนดังนี้ ส่วนที่ 1 คือ ความรู้พื้นฐานเกี่ยวกับบลูทูธ ได้แก่ การทำงานของบลูทูธ และระบบรักษาความปลอดภัยของบลูทูธในการยืนยันตัวตนและการเข้ารหัส ส่วนที่ 2 คือ ความเสี่ยงต่อการถูกโจมตีในการใช้เทคโนโลยีบลูทูธ ส่วนที่ 3 นำเสนอรูปแบบและเครื่องมือต่าง ๆ ที่ใช้ในการโจมตี ส่วนที่ 4 เป็นการทดสอบการโจมตีอุปกรณ์โทรศัพท์เคลื่อนที่ที่ติดตั้งบลูทูธ ส่วนถัดไปเป็นบทสรุป และส่วนสุดท้ายคือสิ่งที่ควรทำต่อไปในอนาคต

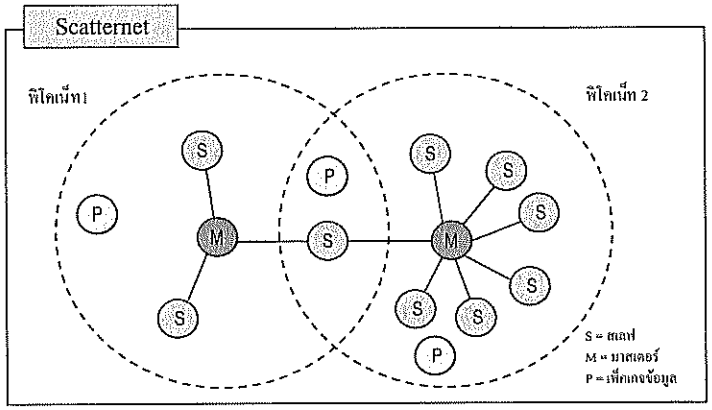
ความรู้พื้นฐานเกี่ยวกับบลูทูธ

การทำงานของบลูทูธ

เทคโนโลยีบลูทูธเป็นอุปกรณ์อิเล็กทรอนิกส์ที่ใช้สัญญาณความถี่วิทยุในการเชื่อมโยงสื่อสารสัญญาณไร้สายในระยะสั้นที่ไม่มีความซับซ้อนมากนัก และบลูทูธยังถูกออกแบบมาเพื่อใช้กับอุปกรณ์เคลื่อนที่ในการสื่อสารแลกเปลี่ยนข้อมูล เช่น ไฟล์ภาพ เสียง แอพพลิเคชั่นต่าง ๆ ซึ่งมีอัตราความเร็วในการส่งถ่ายข้อมูลอยู่ที่ 1 Mbps (1 เมกกะบิตต่อวินาที) แต่ในปัจจุบัน มีการพัฒนาเทคโนโลยีการส่งข้อมูลเป็นแบบ EDR (Enhanced Data Rate) คือระบบอิเล็กทรอนิกส์หรือคอมพิวเตอร์ที่ได้รับการปรับปรุงให้สามารถสื่อสารข้อมูลผ่านเครือข่ายได้เร็วขึ้น ทั้งนี้พัฒนาจากรุ่น 1.1 ที่ส่งข้อมูลด้วยอัตราความเร็ว 1 Mbps เป็นบลูทูธ 2.0+ EDR ส่งข้อมูลด้วยอัตราความเร็ว 3 Mbps และกำลังในการส่งสัญญาณของบลูทูธในโทรศัพท์เคลื่อนที่ มีกำลังในการส่ง 1 mW (เมกกะวัตต์) ส่งสัญญาณได้ในระยะสั้นประมาณ 0.1-10 เมตร

ในการติดต่อสื่อสารระหว่างอุปกรณ์เพื่อแลกเปลี่ยนข้อมูลนั้นใช้ช่วงความถี่ที่ 2.4000 – 2.4835 GHz (Bluetooth SIG, 2001) โดยมีระยะการทำงานในช่วง 0.1-100 เมตร ขึ้นอยู่กับชนิดของตัวส่งสัญญาณและผู้ให้บริการในการเชื่อมต่อ ในรูปที่ 1 แสดงเครือข่ายการติดต่อสื่อสารระหว่างอุปกรณ์ โดยการติดต่อสื่อสารในการทำงานร่วมกันของอุปกรณ์นั้นจะยอมให้มีการเชื่อมต่ออุปกรณ์ในการติดต่อสื่อสารกันได้สูงสุดถึง 8 อุปกรณ์พร้อมกัน เรียกว่าพิโคเน็ท (Piconet) (Vainio, 2000; Persso, J., and Smeets, B., 2000) โดยพิโคเน็ทนั้นประกอบด้วยอุปกรณ์ที่แสดงตัวเป็นมาสเตอร์ (Master) และ อุปกรณ์ต่อพ่วงแสดงตัวเป็น สเลฟ (Slave)

อุปกรณ์มาสเตอร์ทำหน้าที่ในการกำหนดรูปแบบความถี่ในการส่งสัญญาณ ซึ่งเป็นตัวเริ่มต้นในการสื่อสาร ขณะที่อุปกรณ์ต่อพ่วงที่เป็นสเลฟจะสามารถส่งสัญญาณได้ทั้งแบบจุดต่อจุด (Point-to-point) เมื่อมีอุปกรณ์บลูทูธเพียงแค่ 2 ตัว หรือแบบจุดต่อหลายจุด (Point-to-multipoint) เมื่อมีอุปกรณ์บลูทูธมากกว่า 2 ตัว นอกจากนี้อุปกรณ์ที่เป็นสเลฟที่เชื่อมต่ออยู่ในแต่ละพิโคเน็ทยังสามารถเชื่อมต่อกับอุปกรณ์อื่นที่อยู่ต่าง พิโคเน็ทกันได้ ซึ่งทำให้เกิดการทำงานเหลื่อมทับกัน ดังนั้นการเชื่อมต่ออุปกรณ์กันนั้นจึงจำเป็นต้องคำนึงถึงการเกิดคลื่นรบกวนของแต่ละอุปกรณ์ด้วย โดยจะเรียกการทำงานของพิโคเน็ทที่มีการทำงานเหลื่อมทับกันแต่ปราศจากการรบกวนของแต่ละอุปกรณ์ว่า สแกตเตอร์เน็ต (Scatternet) (Persso, J., and Smeets, B., 2000)



รูปที่ 1 แสดงเครือข่ายการติดต่อสื่อสารระหว่างอุปกรณ์

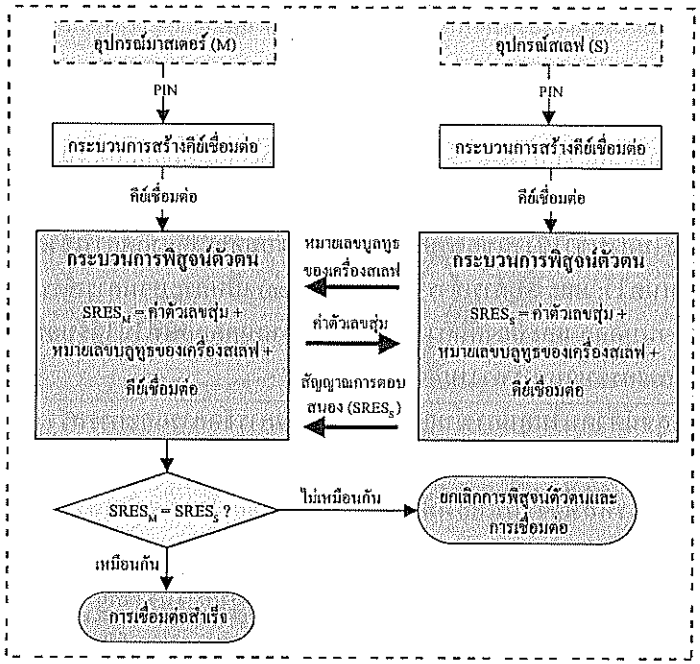
การส่งสัญญาณคลื่นวิทยุในการติดต่อสื่อสารกันของบลูทูธจะใช้การกระโดดเปลี่ยนความถี่ (Frequency hop) โดยทำการแบ่งช่องสัญญาณในช่วงความถี่ระหว่าง 2.400 – 2.4835 GHz ออกเป็น 79 ช่องสัญญาณ และจะใช้ช่องสัญญาณที่แบ่งนี้ในการส่งข้อมูลสลับช่องไปมา 1,600 ครั้งต่อ 1 วินาที เช่น มีการใช้ช่องที่ 1 ช่องที่ 2 จนไปถึงช่องที่ 79 แล้ววนซ้ำมาช่องที่ 1 อีกครั้ง จนครบ 1,600 ครั้ง โดยที่ไม่จำเป็นต้องเรียงตามหมายเลขช่อง และระบบมีความสามารถในการเลือกเปลี่ยนความถี่ที่ใช้ในการติดต่อเองอัตโนมัติ

ระบบรักษาความปลอดภัยของบลูทูธ

อุปกรณ์บลูทูธสามารถกำหนดระดับในการรักษาความปลอดภัยที่แตกต่างกันได้ 3 รูปแบบ ดังนี้ รูปแบบที่ 1 เรียกว่า ระดับที่ไม่มีความปลอดภัย (Non-secure) โดยจะยอมให้อุปกรณ์อื่นสามารถเชื่อมต่อได้; รูปแบบที่ 2 เรียกว่า ระดับการรักษาความปลอดภัยในการให้บริการ (Service-level security) โดยใช้หลักการในการตรวจสอบสิทธิ์การใช้งานของอุปกรณ์ที่เข้ามาเชื่อมต่อเพื่อจำกัดการเข้าถึงข้อมูลและบริการ ซึ่งการรักษาความปลอดภัยจะเกิดขึ้นภายหลังจากการเชื่อมต่อ และยินยอมให้มีการประมวลผลโปรแกรมอื่นๆได้เมื่อมีการใช้งานหลายๆ โปรแกรม; และรูปแบบที่ 3 เรียกว่า ระดับการรักษาความปลอดภัยในการเชื่อมต่อ (Link-level security) โดยจะเกิดขึ้นก่อนการเชื่อมต่ออุปกรณ์ และมีการควบคุมความปลอดภัยโดยใช้ทั้งหลักการพิสูจน์ตัวตน และการเข้ารหัสข้อมูล (Bluetooth SIG, 2001)

ระบบการรักษาความปลอดภัยของบลูทูธจะมีการควบคุมความมั่นคงปลอดภัยในการใช้งาน 3 ลักษณะคือ 1) การพิสูจน์ตัวตน (Authentication) เพื่อยืนยันความถูกต้องว่าเป็นบุคคลที่เข้ามาร้องขอในการเชื่อมต่อจริง; 2) การตรวจสอบสิทธิ์ (Authorization) เป็นการกำหนดสิทธิ์ในการเข้าใช้งานของอุปกรณ์ที่เข้ามาเชื่อมต่อเพื่อจำกัดการเข้าถึงข้อมูลและบริการที่กำหนดไว้; และ 3) การเข้ารหัส (Encryption) เป็นกระบวนการเข้ารหัสข้อมูลให้เป็นข้อมูลส่วนบุคคล และป้องกันการเข้าถึงข้อมูลจากบุคคลอื่นที่ไม่ได้รับอนุญาติ โดยมีรายละเอียดการกระบวนการทำงานดังนี้

การพิสูจน์ตัวตนในอุปกรณ์บลูทูธใช้กระบวนการจัดการและการสร้างคีย์ที่เรียกว่าคีย์เชื่อมต่อ (Link keys) เมื่อผู้ใช้ต้องการเชื่อมต่ออุปกรณ์บลูทูธเพื่อให้ใช้งานร่วมกันได้นั้น ผู้ใช้จะต้องป้อนรหัสที่ตั้งขึ้นมาเองเพื่อสร้างการเชื่อมต่อ โดยเรียกรหัสที่ผู้ใช้ตั้งขึ้นมาว่าหมายเลข PIN (Personal Identification Numbers) และอุปกรณ์บลูทูธที่ต้องการเชื่อมต่อกันนั้นต้องป้อนหมายเลข PIN ที่ตรงกันทั้งสองด้าน ซึ่งระบบการสร้างคีย์จะนำเอาหมายเลข PIN ไปใช้ในกระบวนการสร้างคีย์เชื่อมต่อ (Link-key-generation function) หลังจากได้คีย์เชื่อมต่อแล้ว ระบบจะนำคีย์เชื่อมต่อเข้าสู่กระบวนการพิสูจน์ตัวตน (Authentication function) เพื่อตรวจสอบว่าคีย์เชื่อมต่อที่ได้มาตรงกันหรือไม่ โดยอุปกรณ์ที่เป็นสเลฟจะส่งหมายเลขบลูทูธของเครื่อง (Bluetooth device address) มายังอุปกรณ์ที่ทำหน้าที่เป็นมาสเตอร์ และอุปกรณ์ที่ทำหน้าที่เป็น มาสเตอร์จะส่งค่าตัวเลขที่สุ่มได้ (Random number) กลับไปยังเครื่องที่เป็นสเลฟ ภายใต้ระยะความกว้างหรือความถี่ของช่องสัญญาณที่ตรงกัน จากนั้นทั้งสองฝั่งจะทำการสร้างสัญญาณการตอบสนอง (Signed response: SRES) โดยใช้หมายเลขบลูทูธของเครื่องสเลฟ (Bluetooth device address) ค่าตัวเลขที่สุ่มได้ (Random number) และคีย์เชื่อมต่อ (Link key) จากนั้นเครื่องสเลฟจะส่ง SRES กลับมายังอุปกรณ์ที่เป็นมาสเตอร์ และอุปกรณ์ที่ทำหน้าที่เป็นมาสเตอร์จะทำการตรวจสอบว่าอุปกรณ์ทั้งคู่มี SRES เหมือนกันหรือไม่ (Kitsos, P., Sklavos, N., Papadomanolakis, K., and Koufopavlou, O., 2003) ซึ่งหากอุปกรณ์ทั้งคู่มี SRES ที่เหมือนกัน กระบวนการพิสูจน์ตัวตนก็เสร็จสมบูรณ์สามารถเชื่อมต่อได้สำเร็จ แต่หากไม่เหมือนกันกระบวนการพิสูจน์ตัวตนและการเชื่อมต่อก็จะถูกยกเลิกไป กระบวนการทำงานแสดงในรูปที่ 2



รูปที่ 2 แสดงกระบวนการพิสูจน์ตัวตน

การตรวจสอบสิทธิ์เป็นการกำหนดสิทธิ์ในการเข้าใช้งานของอุปกรณ์ที่เข้ามาทำการเชื่อมต่อเพื่อจำกัดการเข้าถึงข้อมูลและบริการ กระบวนการตรวจสอบสิทธิ์ขึ้นอยู่กับกระบวนการพิสูจน์ตัวตน เนื่องจากการกำหนดสิทธิ์การเข้าใช้งานนั้นต้องตรวจสอบได้ว่าเป็นอุปกรณ์ที่ได้รับการยินยอมให้เชื่อมต่อจากเจ้าของเครื่องจริงและยินยอมให้ใช้งานในระดับใดได้บ้าง ดังนั้น ระดับในการกำหนดสิทธิ์การใช้งานจึงมีอยู่ 3 รูปแบบ ได้แก่ 1) ระดับที่เชื่อถือได้ (Trusted) เมื่อการเชื่อมต่อของอุปกรณ์ A กับอุปกรณ์ B อยู่ในระดับที่เชื่อถือได้ การเข้าถึงข้อมูลจะสามารถทำได้โดยไม่มีเงื่อนไข; 2) ระดับที่เชื่อถือไม่ได้ (Untrusted) เมื่อการเชื่อมต่อของอุปกรณ์ A กับอุปกรณ์ B อยู่ในระดับที่เชื่อถือไม่ได้ การเข้าถึงข้อมูลจะถูกจำกัดตามระดับความปลอดภัยที่กำหนดไว้; 3) ระดับที่ไม่รู้จัก (Unknown) เมื่อการเชื่อมต่อของอุปกรณ์ A กับอุปกรณ์ B อยู่ในระดับที่ไม่รู้จัก อุปกรณ์ที่เชื่อมต่อจะไม่สามารถเข้าถึงข้อมูลใดๆได้

การเข้ารหัส (Encryption) เป็นกระบวนการเข้ารหัสข้อมูลเพื่อป้องกันการเข้าถึงข้อมูลจากบุคคลอื่นที่ไม่ได้รับอนุญาติ ซึ่งผู้รับข้อมูลที่แท้จริงเท่านั้นที่จะสามารถทำการถอดรหัสข้อมูลออกมาได้ ซึ่งคีย์ที่ใช้ในการเข้ารหัสของอุปกรณ์บลูทูธขึ้นอยู่กับคีย์เชื่อมต่อที่ถูกสร้างขึ้นขณะเชื่อมต่ออุปกรณ์ เนื่องจากจะนำคีย์เชื่อมต่อมาใช้ในการสร้างคีย์ในการเข้ารหัสโดยผู้ส่งและผู้รับจะมีคีย์ลับที่ใช้ในการเข้ารหัสและถอดรหัสกันได้

ความเสี่ยงต่อการถูกโจมตี

โดยทั่วไป ความเสี่ยงในการถูกโจมตีของโทรศัพท์เคลื่อนที่ซึ่งใช้ระบบบลูทูธ จะมีสาเหตุมาจากจุดอ่อนหรือช่องโหว่ของระบบรักษาความปลอดภัยของบลูทูธเอง ซึ่งในส่วนนี้จะสรุปจุดอ่อนของบลูทูธซึ่งพบในปัจจุบัน ดังนี้

- การร้องขอและการโต้ตอบคีย์ของบลูทูธอ่อนแอ เนื่องจากในส่วนนี้อาจใช้เพียงตัวเลขคงที่ ซึ่งเป็นการลดความเข้มแข็งในการยืนยันตัวตน
- การร้องขอและโต้ตอบคีย์ของบลูทูธใช้ได้ง่าย ซึ่งการร้องขอของบลูทูธจะเป็นแบบทางเดียวในการยืนยันตัวตนทำให้เป็นจุดอ่อนในการถูกโจมตีได้ง่าย
- คีย์ที่ใช้ในการเข้ารหัสมีความอ่อนแอ เนื่องจากคีย์ที่ใช้ในการเข้ารหัสข้อมูลของอุปกรณ์ที่เป็นมาสเตอร์เพื่อส่งข้อมูลไปยังอุปกรณ์ที่เป็นสเลฟที่อยู่ในพิโคเน็ตเดียวกันนั้นเป็นคีย์ตัวเดียวกัน ทำให้ผู้บุกรุกสามารถใช้คีย์เดียวกันนี้โจมตีอุปกรณ์ทั้งหมดที่อยู่ในพิโคเน็ตเดียวกันได้
- คีย์หลักจะถูกแชร์ขณะเชื่อมต่อบลูทูธ ซึ่งทำให้คีย์นี้แพร่กระจายบนเครือข่ายและง่ายต่อการถูกบุกรุก
- ขั้นตอนวิธีในการเข้ารหัสเป็นแบบทางเดียวและยอมให้ยืนยันตัวตนซ้ำได้จากคีย์เดิม
- หมายเลข PIN (Personal Identification Number) ที่สั้นเกินไป แม้ว่าบลูทูธจะยอมให้ผู้ใช้ตั้งค่า PIN ได้ถึง 16 อักขระ แต่ผู้ใช้ส่วนใหญ่จะตั้งเพียง 4-6 อักขระเท่านั้น ซึ่งง่ายแก่การคาดเดา (Potter, B., 2003)

รูปแบบและเครื่องมือที่ใช้ในการโจมตี

จากการศึกษาของ Solon, AJ., Callaghan, MJ., Harkin, J., และ McGinnity, TM. (2006) และงานของ Dell, P., และ Ghori, K. S-H. (2008) พบว่ามีรูปแบบของการโจมตี ลักษณะการโจมตี วิธีการโจมตี และเครื่องมือที่ใช้ในการโจมตีต่าง ๆ แสดงดังตารางที่ 1

ตารางที่ 1 รูปแบบการโจมตีผ่านระบบบลูทูธ

รูปแบบการโจมตี	ลักษณะการโจมตี	วิธีการโจมตี	เครื่องมือที่ใช้
BlueSnarfing (Information Theft)	เป็นการโจมตีทั่วไปในการขโมยข้อมูลส่วนตัว ผ่านอุปกรณ์บลูทูธ โดยเฉพาะกับโทรศัพท์มือถือเพื่อคัดลอกสมุดโทรศัพท์ รายการโทรเข้า-ออก อ่านข้อความที่อยู่ในโทรศัพท์ รวมทั้งหมายเลขเครื่องของโทรศัพท์ (IMEI)	ทำงานโดยการเชื่อมต่อกับโปรโตคอล OBEX	Bloover ใช้ได้กับโทรศัพท์ที่รองรับ J2ME HeloMoto ใช้ได้กับโทรศัพท์ Motorola V Series
Denial of service	เป็นการปฏิเสธการร้องขอในการเชื่อมต่อ โดยการขัดขวางไม่ให้สามารถใช้งานอุปกรณ์ได้ เช่น BlueSmack ที่สามารถซ่อนไม่ให้สัญญาณของอุปกรณ์บลูทูธทำงานได้	ทำงานผ่านเลเยอร์ L2CAP	BlueSmack
BlueJacking	เป็นการส่งข้อความเชื้อเชิญหรือนามบัตรที่ผู้รับไม่ได้ต้องการหรือไม่มีการร้องขอ ไปยังอุปกรณ์เป้าหมาย ขณะที่ยังไม่มีการเชื่อมต่อคีย์ โดยไม่ได้ทำลายข้อมูลใดๆ ในเครื่อง อาจใช้เพื่อประโยชน์ในการประชาสัมพันธ์ข่าวสาร หรือหากนำไปใช้ในทางที่ผิด เช่น การส่งข้อความหลอกลวง แกล้ง หรือสร้างความรำคาญแก่ผู้รับและเปิดช่องทางในการโจมตีรูปแบบอื่นๆ	ทำงานโดยการเชื่อมต่อกับโปรโตคอล OBEX	BlueJacking
BluePrint	เป็นการค้นหาและแสดงรายละเอียดข้อมูลเกี่ยวกับผู้ผลิต รุ่น หมายเลขประจำเครื่อง (Bluetooth device address) ของอุปกรณ์ บลูทูธที่มีการเปิดใช้งานอยู่ ซึ่งแต่ละเครื่องจะมีลักษณะแตกต่างกัน เพื่อสร้างรูปแบบจำลองและที่อยู่ให้เป็นแบบเดียวกับอุปกรณ์บลูทูธที่ต้องการจู่โจม ซึ่งจะสามารถ	-	BlueStumbler RedFang BluePrint

รูปแบบการโจมตี	ลักษณะการโจมตี	วิธีการโจมตี	เครื่องมือที่ใช้
	ช่วยให้การโจมตีในลักษณะอื่นๆทำได้ง่ายขึ้นในภายหลัง		
BlueBugging	ผู้บุกรุกจะสร้างหมายเลขการเชื่อมต่อไปยังอุปกรณ์ของเป้าหมาย โดยไม่มีการยืนยันตัวตน โดยการส่งคำสั่งไปยังอุปกรณ์บลูทูธ เช่น สั่งให้เปิดโทรศัพท์ของเป้าหมายแล้วโทรไปที่เครื่องของผู้บุกรุกเพื่อดักฟังการสนทนา นอกจากนี้แล้วผู้บุกรุกยังสามารถที่จะตั้งการส่งต่อการเรียกเข้า (Call Forwarding) ให้ทุกการเรียกที่เข้ามาที่เครื่องของเป้าหมายส่งต่อไปยังเครื่องของผู้บุกรุกได้ โดยที่เป้าหมายไม่รู้ตัว	เชื่อมต่อผ่านเลเยอร์ L2CAP และ base band โดยใช้คำสั่ง AT-command	Gnokii
BlueTracking	เนื่องจากอุปกรณ์บลูทูธทุกชิ้นมีคีย์เฉพาะตัว คล้าย ๆ กับที่การ์ดเครือข่าย (Network Card) มีหมายเลขประจำเครื่องคอมพิวเตอร์ (MAC Address) ดังนั้นจึงสามารถที่จะล็อกหมายเลข (ID) ของอุปกรณ์บลูทูธชิ้นนั้น และติดตามดูการเคลื่อนไหวของเจ้าของอุปกรณ์บลูทูธนั้นได้	ทำงานผ่าน Bluetooth address (BDADDR)	-

การทดสอบการโจมตี

สภาพแวดล้อมในการทดสอบ

ในการทดสอบระบบรักษาความปลอดภัยของโทรศัพท์เคลื่อนที่ผ่านการโจมตีระบบบลูทูธนี้ จะใช้โทรศัพท์เคลื่อนที่รุ่น Nokia 6681 ที่ติดตั้งระบบบลูทูธ ในการโจมตีโทรศัพท์เคลื่อนที่รุ่นอื่น ๆ ที่เปิดใช้งานระบบบลูทูธ ซึ่งในการทดสอบนี้จะทดลองโจมตีโทรศัพท์เคลื่อนที่ 10 รุ่น ได้แก่ Nokia 6300, Nokia 5300, Nokia 6120, Nokia N72, Nokia N73, Nokia 7610, Sony Ericson w550i, Sony Ericson k750, Sumsung D900 และ Sumsung E690 ซึ่งการทดสอบนี้จะใช้การโจมตี 2 รูปแบบ คือ BlueJacking และ BlueSnarfing โดยแต่ละรูปแบบจะมีลักษณะของการโจมตี และขั้นตอนในการทดลองที่แตกต่างกัน ดังนี้

รูปแบบที่ 1 : BlueJacking เป็นการส่งข้อความเชื้อเชิญหรือนามบัตรที่ผู้รับไม่ได้ต้องการหรือไม่มีการร้องขอ ไปยังอุปกรณ์เป้าหมายขณะที่ยังไม่มีการเชื่อมต่อคีย์ โดยไม่ได้ทำลายข้อมูลใด ๆ ในเครื่อง อาจใช้เพื่อประโยชน์ในการประชาสัมพันธ์ข่าวสาร หรือหากนำไปใช้ในทางที่ผิดเช่น การส่งข้อความหลอกลวง แกล้ง หรือสร้างความรำคาญแก่ผู้รับและเปิดช่องทางในการโจมตีรูปแบบอื่น ๆ โดยสามารถส่งข้อความได้ในระยะใกล้ผ่านทางการเชื่อมต่อบลูทูธ โดยเหตุผลที่เลือกรูปแบบนี้ เนื่องจากเป็นวิธีการที่สามารถดาวน์โหลดโปรแกรมและใช้งานได้ง่าย ซึ่งการส่งข้อความถึงเครื่องเป้าหมายโดยไม่ต้องมีการเชื่อมต่อคีย์ถือเป็นอันตรายอย่างยิ่งหากข้อมูลถูกส่งเข้าโทรศัพท์โดยไม่ได้รับการยินยอมจากเจ้าของเครื่อง ซึ่งมีขั้นตอนการทดลองคือ

(1) ดาวน์โหลดโปรแกรม EasyJackv2.jar และติดตั้งลงในโทรศัพท์ Nokia 6681
(2) ค้นหาสัญญาณบลูทูธที่เปิดใช้งานอยู่ โดยเลือกที่เมนู Device Search
(3) เลือกเครื่องเป้าหมายที่ต้องการส่งข้อความ
(4) โทรศัพท์ Nokia 6681 ของผู้บุกรุกจะเข้าสู่โหมดการพิมพ์ข้อความตามรูปแบบของโปรแกรมที่ดาวน์โหลดมา ผู้บุกรุกสามารถพิมพ์ข้อความที่ต้องการส่งได้
(5) ผู้บุกรุกทำการส่งข้อความ โดยข้อความจะปรากฏบนเครื่องเป้าหมาย และให้ผู้รับเลือกว่าจะรับหรือไม่รับข้อความ
(6) ถ้าเครื่องเป้าหมายเลือกรับ ข้อความจะถูกส่งเข้าไปยังเครื่องเป้าหมายทันที โดยไม่ต้องเชื่อมต่อคีย์ แต่ถ้าเครื่องเป้าหมายปฏิเสธ การส่งข้อความจะล้มเหลวและรายงานผลการส่งมายังเครื่องของผู้บุกรุก

รูปแบบที่ 2 : BlueSnarfing เป็นการโจมตีทั่วไปเพื่อขโมยข้อมูลส่วนตัว เช่น การคัดลอกสมุดโทรศัพท์หรือปฏิทินเวลา การอ่านข้อความ การสั่งเปิดหรือปิดโทรศัพท์ การ**สั่งเปิดเพลง การสั่งล็อคโทรศัพท์ การอ่านรายการที่ทำการติดต่อ** การเปลี่ยนแปลงแก้ไขข้อมูลส่วนตัว เป็นต้น โดยเหตุผลที่เลือกรูปแบบนี้ เนื่องจากเป็นวิธีการที่ได้รับความนิยมแพร่หลายและสามารถดาวน์โหลดโปรแกรมได้ง่าย อีกทั้งยังมีวิธีในการโจมตีเพื่อขโมยข้อมูลส่วนตัวในโทรศัพท์เคลื่อนที่ได้หลากหลายรูปแบบ ซึ่งมีขั้นตอนการทดลอง ดังนี้

(1) ดาวน์โหลดโปรแกรม Super Bluetooth Hack v1.08 และติดตั้งลงในโทรศัพท์ Nokia 6681
(2) เปลี่ยนภาษาจากภาษาสโลวัก เป็นภาษาอังกฤษ โดยเมื่อเริ่มเปิดโปรแกรมจะพบตัวเลือกเมนู "Nastavenia" (แปลว่า "การตั้งค่า") ให้เลือกที่ "Jazyk" (แปลว่า "ภาษา") ถัดมาเลือกภาษา "English" และสุดท้ายเลือกที่ "Späť" (แปลว่า "ตกลง") เสร็จเรียบร้อยแล้วโปรแกรมการทำงานของโทรศัพท์จะเป็นภาษาอังกฤษ

(3) เชื่อมต่อสัญญาณบลูทูธ โดยเลือกที่ Connect จะแสดงรายการที่ตรวจพบ และถัดมาเลือกเครื่องเป้าหมายที่ต้องการเชื่อมต่อ เสร็จเรียบร้อยแล้วระบบจะแจ้งให้เครื่องเป้าหมายทราบและให้เลือกการยอมรับหรือไม่ยอมรับการเชื่อมต่อ
(4) ถ้าเครื่องเป้าหมายเลือกยอมรับ ระบบจะให้ตั้งค่าคีย์ที่ใช้ในการเชื่อมต่อ และทำการใส่ค่าคีย์ที่ใช้ในการเชื่อมต่อที่ตรงกัน เพื่อทำการเชื่อมต่อ
(5) การเชื่อมต่อสามารถใช้งานได้แล้ว จากนั้นผู้บุกรุกจะสามารถเข้าไปทำรายการต่าง ๆ ของเครื่องเป้าหมายได้ตามต้องการ

ผลการทดสอบและการวิจารณ์ผล

จากการจำลองสภาพแวดล้อมเพื่อทดสอบการโจมตีทั้งสองรูปแบบ ผลการทดสอบจะแสดงดังตารางที่ 2 ซึ่งมีรายละเอียดของการทดสอบในแต่ละรูปแบบดังนี้

รูปแบบที่ 1 การทดสอบการโจมตีแบบ BlueJacking พบว่าเครื่องมาสเตอร์สามารถส่งข้อความไปยังเครื่องเป้าหมายได้ในทุกเครื่องที่ติดตั้งอุปกรณ์บลูทูธและเปิดใช้งานอยู่ ซึ่งการส่งข้อความจะเป็นไปในลักษณะที่ผิดกฎหมายหรือไม่ ขึ้นอยู่กับข้อความที่ส่งว่าสร้างความรำคาญแก่ผู้รับหรือไม่

รูปแบบที่ 2 การทดสอบการโจมตีแบบ BlueSnarfing จะเปรียบเทียบการเชื่อมต่อจากเครื่องผู้บุกรุกคือ Nokia 6681 ไปยังเครื่องเป้าหมายอื่น ๆ โดยการทดสอบพบว่าโทรศัพท์เป้าหมายรุ่นต่าง ๆ สามารถถูกโจมตีได้ในลักษณะที่แตกต่างกันดังนี้

- Nokia 6300 และ Nokia 5300 สามารถถูกเชื่อมต่อและถูกโจมตีได้หลายรูปแบบ ได้แก่ การอ่านข้อมูลของเครื่อง การเปลี่ยนแปลงแก้ไขข้อมูลส่วนตัวในเครื่อง การเปิดดูข้อมูลการใช้โทรศัพท์เช่น รายการโทรเข้า-ออกหรือสายที่ไม่ได้รับ การสั่งปิดเครื่อง และการบล็อกเครื่องไม่ให้ใช้งานได้ แต่อย่างไรก็ตามไม่สามารถใช้เครื่องเป้าหมายเพื่อโทรออกและอ่านข้อความได้
- Nokia 6120, 7610, N72 และ N73 สามารถถูกเชื่อมต่อ ดูข้อมูลของเครื่อง และสั่งปิดเครื่องได้
- Sony Ericson w550i และ Sony Ericson k750 สามารถถูกโจมตีได้หลายรูปแบบ แต่ส่วนที่สำคัญคือ ผู้บุกรุกสามารถสั่งให้เครื่องเป้าหมายโทรออกได้
- Sumsung E690 สามารถถูกเชื่อมต่อ ดูข้อมูลของเครื่อง ดูรายการโทรเข้า-ออกหรือสายที่ไม่ได้รับ และสั่งปิดเครื่องได้
- Sumsung D900 ไม่สามารถถูกโจมตีใด ๆ ได้เลย เนื่องจากผู้บุกรุกไม่สามารถเชื่อมต่อได้ เพราะโทรศัพท์รุ่นนี้ไม่รองรับการใช้งานโปรแกรมจาวา

จากผลการทดลองของการโจมตีแบบ BlueSnarfing แสดงให้เห็นว่า ยี่ห้อและรุ่นของโทรศัพท์เป็นปัจจัยสำคัญที่ทำให้ตระหนักได้ว่า โทรศัพท์ที่ใช้อยู่ทั่วไปมีความปลอดภัยต่อการถูกโจมตีได้มากน้อยเพียงใด และจากจุดอ่อนของการเชื่อมต่อที่มีการเก็บคีย์ที่ใช้ในการเชื่อมต่อไว้ในเครื่อง เพื่อใช้ในการเชื่อมต่อครั้งต่อไปไม่ต้องมีการสร้างคีย์ใหม่นั้น ทำให้ผู้บุกรุกสามารถเชื่อมต่อโทรศัพท์เป้าหมายได้ทันที และสามารถขโมยความลับหรือเปลี่ยนแปลงข้อมูลเครื่องเป้าหมายได้

จุดอ่อนที่พบอีกประการหนึ่งคือ การตั้งค่าคีย์ในการเชื่อมต่อ สามารถตั้งค่าที่เป็นตัวเลขเดิม ๆ ได้ เช่นตัวเลขที่นิยมใช้คือ 1234 ในการเชื่อมต่อครั้งต่อไปกับอุปกรณ์ตัวใหม่ก็ยังสามารถใช้คีย์ 1234 ได้อีก ซึ่งผู้ศึกษาเห็นว่ามันง่ายแก่การคาดเดา ผู้บุกรุกส่วนใหญ่สามารถค้นหาตัวเลขเหล่านี้เพื่อเชื่อมต่อเครื่องเป้าหมายได้อย่างแน่นอน ซึ่งเป็นอันตรายต่อเครื่องเป้าหมายอย่างยิ่ง

ตารางที่ 2 ผลการทดสอบการโจมตีแบบ BlueJacking และ BlueSnarfing

ยี่ห้อรุ่นโทรศัพท์	BlueJacking			BlueSnarfing					
	ส่งข้อความ	อ่านข้อมูลของเครื่องโทรศัพท์	เปิด อ่าน ข้อความ	เปลี่ยนแปลงข้อมูลส่วนตัว	เปิดดูข้อมูลการใช้โทรศัพท์	ลบปิดเครื่อง	บล็อกการใช้เครื่อง	ส่งให้ใครออก	ไม่สามารถเชื่อมต่อได้
Nokia 6300	✓	✓		✓	✓	✓	✓		
Nokia 5300	✓	✓		✓	✓	✓	✓		
Nokia 6120	✓	✓				✓			
Nokia 7610	✓	✓				✓			
Nokia N72, N73	✓	✓				✓			
Sony Ericson w550i	✓	✓		✓	✓	✓	✓	✓	
Sony Ericson k750	✓	✓		✓	✓	✓	✓	✓	
Sumsung E690	✓	✓			✓	✓			
Sumsung D900	✓	✓							✓

บทสรุป

บทความนี้ศึกษาหลักการทำงาน ระบบรักษาความปลอดภัยในการยืนยันตัวตนและการเข้ารหัส ความเสี่ยงต่อการถูกโจมตี เครื่องมือที่ใช้ในการโจมตี รูปแบบการโจมตี และทดลองโจมตีโทรศัพท์เคลื่อนที่ที่ติดตั้งอุปกรณ์บลูทูธ ซึ่งเป็นอุปกรณ์ที่นิยมใช้กันอย่างแพร่หลายในปัจจุบัน เพื่อศึกษากระบวนการทำงานและตระหนักถึงภัยคุกคามใกล้ตัว เพื่อให้รู้เท่าทันและสามารถป้องกันตนจากภัยเหล่านั้นได้

ระบบรักษาความปลอดภัยในการเชื่อมต่ออุปกรณ์ของบลูทูธมีระบบป้องกัน คือ การร้องขอการเชื่อมต่อไปยังเครื่องเป้าหมายทุกครั้ง จะต้องใส่รหัสและยืนยันตัวตนที่ตรงกันก่อน จึงจะเชื่อมต่อได้สำเร็จ แต่อย่างไรก็ตาม เมื่อเชื่อมต่อครั้งแรกสำเร็จแล้ว การเชื่อมต่อครั้งต่อไปสามารถใช้คีย์เดิมที่เก็บอยู่ในเครื่อง เชื่อมต่อแบบอัตโนมัติได้ทันที โดยไม่ต้องสร้างคีย์ใหม่ นอกจากนี้ยังมีการแชร์คีย์อยู่บนเครือข่ายอีกด้วย ทำให้ระบบรักษาความปลอดภัยยังไม่มากเพียงพอ หากจะนำบลูทูธไปใช้ในงานที่ต้องการความปลอดภัยสูง

สิ่งที่ควรทำในอนาคต

ในการรักษาความปลอดภัยของระบบบลูทูธ อาจทำได้โดยกระบวนการเข้ารหัสรูปแบบอื่น ๆ ที่มีความปลอดภัยสูงและง่ายต่อการใช้งานกว่ากระบวนการในปัจจุบัน เพื่อให้บลูทูธสามารถนำไปใช้ในงานที่ต้องการความปลอดภัยสูงได้ นอกจากนี้ในการทดลองยังมีข้อจำกัดในด้านอุปกรณ์ที่ไม่สามารถครอบคลุมกลุ่มตัวอย่างได้ทั้งหมด เนื่องจากการทดลองเป็นเพียงการโจมตีโดยใช้ซอฟต์แวร์สำเร็จรูป และต้องได้รับการยอมรับจากเครื่องเป้าหมายก่อนทำการเชื่อมต่อ ไม่ใช่การบุกรุกที่สมบูรณ์ หากมีการทดลองวิธีการที่สามารถเชื่อมต่อโดยเครื่องเป้าหมายไม่ทราบ จะทำให้ทราบช่องโหว่ของบลูทูธอย่างแท้จริงมากกว่า และครอบคลุมกลุ่มโทรศัพท์เคลื่อนที่ที่เป็นที่นิยมจะทำให้ได้รับข้อมูลที่ครอบคลุมขึ้น ดังนั้นคณะผู้วิจัยจึงเห็นว่าสิ่งเหล่านี้เป็นแนวทางที่น่าสนใจมาก และสามารถนำไปทำวิจัยต่อไปในอนาคตได้

References

Bluetooth SIG. (2001). **Specification of the Bluetooth System.** [Online]. Available: http://www.bluetooth.com

Haataja, K. M.J. (2006). **Security in Bluetooth, WLAN and IrDA: a comparison.** [Online]. Available: http://www.cs.uku.fi/research/publications/reports/A-2006-1.pdf.

Persso, J., and Smeets, B. (2000). Bluetooth Security an Overview. Information Security **Technical Report.** 5(3): 32-43.

Potter, B. (2003). Bluetooth Security Optional. **Network Security.** 2003(5): 4-5.

Marek, B. (2006). **Bluetooth Security Review,** Part 1. [Online]. Available: http://www.securityfocus.com/print/infocus/1830.

Marek, B. (2006). **Bluetooth Security Review, Part 2.** [Online]. Available: http://www.securityfocus.com/print/infocus/1836.

Solon, A.J., Callaghan, M.J., Harkin, J., and McGinnity, T.M. (2006). Case Study on the Bluetooth Vulnerabilities in Mobile Devices. **International Journal of Computer Science and Network Security.** 6(4): 125-126.

Vainio, J.T. (2000). **Bluetooth Security.** [Online]. Available: http://www.niksula.hut.fi/~jiitv/bluesec.html.

Kitsos, P., Sklavos, N., Papadomanolakis, K., and Koufopavlou, O. (2003). Hardware Implementation of Bluetooth Security. **IEEE Pervasive Computing.** 2(1): 21-29.

Suranaree J. Soc. Sci. Vol. 3 No. 1; June 2009 (113-130)

Three Fundamental Concepts for Genre Transfer Studies: A Case of Postgraduate Dissertation to Research Article

Issra Pramoolsook*

School of English, Institute of Social Technology, Suranaree University of Technology

Abstract

Studies on genre transfer are relatively unexplored when compared with other aspects of genre studies. To gain a good understanding about and for such studies, at least three fundamental concepts should be thoroughly explained and taken into consideration. This analytical review article aims to provide basic understandings about the three concepts, namely; genre, genre studies and genre categorization. In the first part, the notion of genre is explained through a variety of definitions proposed by genre researchers. Secondly, studies on genre and its implications are the topic of the discussion. The three distinct but interrelated traditions or approaches of genre studies are reviewed with a comparison and contrast among the three. The way each of the three approaches is informative for a genre transfer investigation is also provided as an example. Lastly, the concept of genre categorization involving different ways of classifying genres is examined. A special emphasis is placed on categorizing the dissertations and research articles which are two crucial genres for graduate students around the globe these days. This article concludes with an example of how the three fundamental concepts can be employed to establish the dissertations and research articles as two separate genres, so that their distinctions can serve as a foundation for a study of genre transfer between the two. The review of the three concepts is expected to shed more light on the genre transfer studies especially from the dissertation to research article with the hope that more of such investigations will emerge for the benefit of graduate students and dissemination of their research.

Keywords: genre (ประเภทการสื่อสาร); genre studies (การศึกษาประเภทการสื่อสาร); genre categorization (การจัดหมวดหมู่ประเภทการสื่อสาร); dissertation (วิทยานิพนธ์); research article (บทความวิชาการ)

* *Corresponding author. Tel.: +66 4422 4335; Fax: +66 4422 4205*
E-mail address: issra@sut.ac.th