บทที่ 3
การลักลอบใช้สัญญาณโทรศัพท์เคลื่อนที่

การลักลอบใช้สัญญาณโทรศัพท์เคลื่อนที่เกิดจากการพัฒนาทางเทคโนโลยีที่มีการดัดแปลงนำเทคโนโลยีมาปรับใช้เพื่อการลักลอบใช้สัญญาณโทรศัพท์เคลื่อนที่ซึ่งซับซ้อนกว่าการพ่วงสายโทรศัพท์ธรรมดาที่ไม่มีข้อยุ่งยากในการจัดทำ และแนวคิดในการลักลอบใช้สัญญาณโทรศัพท์เคลื่อนที่ได้พัฒนามาจากการพ่วงสายโทรศัพท์ธรรมดา

การลักลอบใช้สัญญาณโทรศัพท์เคลื่อนที่หรือโทรศัพท์มือถือเป็นการแย่งสิทธิ์การใช้จากเจ้าของ แม้การแย่งสิทธิ์นี้ไม่เป็นเหตุให้เจ้าของสูญเสียสิทธิ์ในการใช้โทรศัพท์เคลื่อนที่โดยตรงก็ตาม แต่ผู้ลักลอบใช้โทรศัพท์เคลื่อนที่ก็มีเจตนาทุจริตในการแย่งสิทธิ์ดังกล่าวและเป็นเหตุให้เจ้าของโทรศัพท์เคลื่อนที่ที่แท้จริงต้องรับภาระในค่าบริการเพิ่มมากขึ้น กรณีดังกล่าวควรถือเป็นการกระทำโดยทุจริต

3.1 วิธีการทางเทคนิคในการลักลอบใช้สัญญาณโทรศัพท์เคลื่อนที่

วิธีการทุจริตโทรศัพท์เคลื่อนที่พบมากที่สุดได้แก่ การปรับแต่งสัญญาณโทรศัพท์ว่าการลักลอบปรับแต่งหรือทำซ้ำคลื่นสัญญาณโทรศัพท์เคลื่อนที่ (Cloning the cell phone) ภาษาไทยเรียกว่า"จูน") ซึ่งกรรมวิธีทุจริตเริ่มจากการที่โทรศัพท์มือถือของบุคคลสุจริตทั่วไปเปิดเครื่องไว้ไม่ว่าจะมีการใช้เครื่องโทรศัพท์นั้นหรือไม่ก็ตาม เครื่องโทรศัพท์จะส่งสัญญาณอิเล็คโทรนิค(electronic signal) ออกมาตลอดเวลา ผู้กระทำทุจริตใช้เครื่องตรวจจับสัญญาณ (Scanner) เพื่อทำการอ่านและเก็บคลื่นสัญญาณอิเล็คโทรนิคที่โทรศัพท์เคลื่อนที่ของบุคคลสุจริตส่งออกมา จากนั้นก็นำข้อมูลเกี่ยวกับหมายเลขโทรศัพท์เคลื่อนที่(Cellular phone number) หมายเลขประจำตัวอิเล็คโทรนิค(Electronic serial number) ไปบรรจุเข้าไปในเครื่องโทรศัพท์มือถือที่เตรียมไว้แล้ว เป็นการปรับแต่งคลื่นสัญญาณโทรศัพท์เคลื่อนที่หรือที่คนไทย

เรียกว่า "จูนโทรศัพท์มือถือ" เมื่อนำโทรศัพท์ที่ปรับแต่งคลื่นสัญญาณโทรศัพท์ไปใช้รายการจะถูกบันทึกการใช้และส่งไปเรียกเก็บเงินจากเจ้าของที่แท้จริง [9]

การทุจริตเกี่ยวกับโทรศัพท์มือถือ (Cellular telephone)และโทรศัพท์เคลื่อนที่ส่วนตัว (PCS) แบ่งออกตามลักษณะเทคโนโลยีเป็น 2 ประเภท คือ

1 การทุจริตใช้เทคนิคขั้นต่ำ (low-tech fraud) เช่น การทุจริตโดยใช้เอกสารหลักฐานเท็จ (subscription fraud) ในการสมัครขอใช้บริการเป็นประเภทที่กระทำความผิดได้ง่ายที่สุดและพบเห็นมากที่สุด จากการสำรวจของบริษัทที่ปรึกษาคาดว่าการทุจริตโทรคมนาคมโดยใช้หลักฐานเอกสารเท็จนั้นคิดเป็นร้อยละ 80 ของการทุจริตโทรศัพท์เคลื่อนที่ส่วนตัว (PCS)[10] โดยที่บุคคลธรรมดามักแจ้งเท็จในเรื่องเครดิตตนเอง เช่น ชื่อ-สกุล หมายเลขประกันสังคม การแจ้งเครดิตและอัตราเงินเดือนอันเป็นเท็จ วิธีการทุจริตแบบนี้ผู้ทุจริตสามารถใช้บริการได้โดยไม่ต้องเสียค่าบริการเลย บริษัทผู้ให้บริการทำการระงับบริการแต่ก็ไม่เคยตามเรียกเก็บหนี้หรือค่าเสียหายได้ แม้ว่าจะถูกบริษัททำการระงับบริการโทรศัพท์ บุคคลที่ทุจริตก็ยังสามารถใช้โทรศัพท์โดยทุจริตได้นอกเขตพื้นที่บริการของบริษัทผู้ให้บริการ (home carrier service area) ด้วยเหตุที่มีระยะหน่วงเวลา (time delay) สำหรับการส่งคลื่นสัญญาณโทรศัพท์แบบตระเวน (roaming service) กับการตรวจสอบการใช้โทรศัพท์ไปยังสถานีหลักของบริษัทผู้ให้บริการ จึงเป็นการทุจริตรูปแบบหนึ่งซึ่งถึงอย่างไรบริษัทที่เป็นเจ้าของเครือข่ายยังคงต้องรับผิดชอบสำหรับการทุจริตโทรศัพท์ประเภทที่ใช้สัญญาณตระเวนนอกพื้นที่หลักของบริษัทผู้ให้บริการ

2. การทุจริตใช้เทคนิคขั้นสูง (high tech fraud) การทุจริตประเภทนี้อาศัยเครื่องมือที่ใช้เทคนิคขั้นสูง(hi-tech fraud)ในการกระทำทุจริตนับตั้งแต่เริ่มจนจบ คือการปรับคลื่นสัญญาณโทรศัพท์เคลื่อนที่ (Cloning cell phone fraud) (คนไทยเรียกติดปากว่าเป็น

---

[9] พีรพันธ์ เปรมภูติ, " มาตรการทางกฎหมายในการปราบปรามการลักลอบปรับสัญญาณโทรศัพท์เคลื่อนที่" , หน้า 8-36.

[10] O'Bren, John T., Telecommunications Fraud Opportunities for Techno-Criminals , p 21.

การ"จูน" ซึ่งตรงกับภาษาอังกฤษคือ"Tune" แปลว่า การปรับคลื่นเสียงดนตรีให้ตรงกันหรือปรับความถี่คลื่นสัญญาณวิทยุ โทรทัศน์ ให้ตรงกับความถี่ที่ต้องการรับ[11]) วิธีการทุจริตโดยการลักลอบปรับคลื่นสัญญาณโทรศัพท์เคลื่อนที่ (Cell Phone Cloning) ทำได้โดยแบ่งเป็นขั้นตอนดังต่อไปนี้

1) ข้อมูลบัญชีผู้ใช้โทรศัพท์เคลื่อนที่(Acquire legitimate account information)

การที่บุคคลทุจริตทำการหาข้อมูลเกี่ยวกับบัญชีผู้ใช้โทรศัพท์ไม่ว่าจะทำการลักขโมยข้อมูลเหล่านั้น หรือใช้วิธีดักจับคลื่นสัญญาณโทรศัพท์จากตัวเครื่องโทรศัพท์ทั้งระบบโทรศัพท์มือถือ(Cellular) โทรศัพท์เคลื่อนที่ส่วนตัว (PCS) ที่เปิดเครื่องไว้ แม้ว่าจะไม่ได้ใช้พูดเพื่อรับหรือส่งสัญญาณก็ตาม

2) การป้อนข้อมูลลงในเครื่องโทรศัพท์เคลื่อนที่ (Programming a cellular or PCS telephone)

เมื่อคนร้ายได้บรรดาข้อมูลทั้งหมดของหมายเลขบัญชีผู้ใช้โทรศัพท์แล้วจากนั้นคนร้ายก็จะนำเอาข้อมูลทั้งหมดป้อนบรรจุลงไปในเครื่องโทรศัพท์มือถือ (Cellular) หรือโทรศัพท์เคลื่อนที่ส่วนตัว(PCS) ก็ทำให้ได้เครื่องรับส่งโทรศัพท์มือถือหรือโทรศัพท์เคลื่อนที่ส่วนตัวที่ถูกปรับคลื่นสัญญาณ (จูน) ให้มีคลื่นความถี่ที่ถูกต้องตรงกับคลื่นสัญญาณของเจ้าของที่แท้จริง (legitimate phone)

การลักลอบใช้สัญญาณโทรศัพท์เคลื่อนที่โดยวิธีปรับจูนมีการกระทำต่อโทรศัพท์เคลื่อนที่ 2 ระบบด้วยกันคือ

1. โทรศัพท์เคลื่อนที่ระบบ 800 เป็นระบบที่ลักลอบใช้สัญญาณได้ง่ายมากกว่าระบบอื่น ๆ เพราะกลุ่มผู้กระทำความผิดได้หาซื้อเครื่องลักลอบใช้สัญญาณหรือเครื่องปรับจูนซึ่งผลิตในต่างประเทศได้ไม่ยาก แหล่งผลิตเครื่องมือดังกล่าวส่วนมากอยู่ในประเทศ

---

[11] AP Cowie, "Oxford Advanced Learner's Dictionary of Current English ", Oxford University, 4th Edition , 1989, p.1376.

สหรัฐอเมริกา เยอรมันและไต้หวัน ซึ่งสามารถหาซื้อได้ในประเทศไทย [12] ส่วนมากแหล่งจำหน่ายจะเป็นร้านที่ขายอุปกรณ์ที่เกี่ยวกับการสื่อสาร ราคาซื้อขายกันปัจจุบันตกอยู่ในราว 60,000 บาทในระยะก่อนนั้นราคาจะสูงกว่านี้ คือประมาณ 100,000 บาท อุปกรณ์ดังกล่าวประกอบด้วย

(1) เครื่องตรวจจับสัญญาณ (Scanner) ปกติช่างเรียกว่าเครื่องมืออิเล็คโทรนิคที่ประกอบขึ้นเพื่อทำหน้าที่ดูดคลื่นหรือดักคลื่นสัญญาณโทรศัพท์เคลื่อนที่ต่าง ๆ ที่อยู่ในอาณาบริเวณรัศมี 100-200 เมตร เมื่อดูดคลื่นสัญญาณแล้วก็จะแปลงสัญญาณเป็นรหัส เมื่อทราบรหัสแล้วก็จะทราบว่าโทรศัพท์ที่ถูกดูดคลื่นหรือดักคลื่นมีรหัสข้อมูลหมายเลขอะไร เมื่อทราบแล้วก็จะเอาข้อมูลของรหัสไปแปลงใส่โทรศัพท์เคลื่อนที่อีกเครื่องหนึ่ง

(2) เครื่องป้อนสัญญาณหรือเครื่องแปลงสัญญาณ (Adapter Communication Channel) เป็นเครื่องมืออิเล็คโทรนิคที่แปลงรหัสข้อมูลจากตัวดูดสัญญาณหรือตัวดักสัญญาณแล้วนำเอาข้อมูลจาก ตัวดูดสัญญาณหรือตัวดักสัญญาณไปใส่กับเครื่องโทรศัพท์อีกเครื่องหนึ่งที่ต้องการปรับจูน

(3) เครื่องรับสัญญาณ (Receiver) เป็นวงจรอิเลคทรอนิกส์ที่ถูกออกแบบให้รับสัญญาณที่ถูกส่งออกมาทางช่องสื่อสาร และทำการแปลงสัญญาณให้กลับไปในรูปแบบที่ผู้รับปลายทางสามารถเข้าใจได้ เช่น ตัวรับสัญญาณจากดาวเทียม หรือโทรศัพท์เคลื่อนที่

2. โทรศัพท์เคลื่อนที่ระบบ 900 การลักลอบปรับจูนโทรศัพท์เคลื่อนที่ระบบนี้มีความสลับซับซ้อนมากกว่าโทรศัพท์เคลื่อนที่ระบบ 800 หรืออาจกล่าวอีกนัยหนึ่งก็คือระบบนี้สามารถปรับจูนได้ยากกว่าระบบ 800 แต่ก็ปรากฏว่ามีการแอบลักลอบปรับจูนหรือลักลอบใช้สัญญาณโทรศัพท์เคลื่อนที่ระบบ 900 ด้วย เนื่องจากพนักงานผู้เกี่ยวข้องกับการเก็บรหัสข้อมูลของบริษัทที่รับสัมปทาน ได้ลักลอบนำเอาข้อมูลของโทรศัพท์เคลื่อนที่ระบบ 900 ทุกเครื่องที่ประชาชนซื้อหรือเช่าสัญญาณไป นำมาขายให้กับกลุ่มผู้กระทำความผิดซึ่งเป็นชาว

---

[12] กองกำกับการสืบสวนตำรวจนครบาลใต้, รายงานจากบันทึกการจับกุมนายสมยศ ไกรวุฒิวงศ์ เมื่อวันที่ 16 ตุลาคม 2539.

ต่างประเทศ ได้แก่ จีน ไต้หวันและบางประเทศของยุโรป [13] จากนั้นกลุ่มผู้กระทำความผิดที่รับซื้อมาก็จะนำเอารหัสข้อมูลไปใส่ในแผ่นดิสก์ที่ใช้กับเครื่องคอมพิวเตอร์ แล้วนำไปก๊อปปี้ขายให้กับกลุ่มพ่อค้าที่รับปรับจูนตามร้ายขายเครื่องอุปกรณ์สื่อสารทั่วไป ส่วนมากจะเป็นตามห้างสรรพสินค้าต่าง ๆ เมื่อผู้ใดต้องการจะปรับจูนโทรศัพท์เคลื่อนที่ระบบ 900 กลุ่มพ่อค้าก็จะนำเอาข้อมูลในแผ่นดิสก์โดยผ่านตัวแปลงสัญญาณปรับจูนเข้ากับโทรศัพท์เคลื่อนที่ที่ต้องการปรับจูน รหัสข้อมูลดังกล่าวถูกนำมาขายครั้งแรก 600,000 บาท แล้วนำเอาข้อมูลในแผ่นดิสก์มาก๊อปปี้แล้วขายให้กับกลุ่มพ่อค้าแผ่นละประมาณ 60,000 บาท

อัตราการลักลอบปรับจูนโทรศัพท์เคลื่อนที่ทั้ง 2 ระบบคือระบบ 800 ทั้งสองแบนด์และระบบ 900 ระยะเริ่มแรกที่มีการปรับจูนโทรศัพท์เคลื่อนที่ใหม่ ๆ จะคิดเครื่องละ 3,000 ถึง 5,000 บาท ต่อมาเมื่อมีการปรับจูนมากขึ้นและร้านที่ปรับจูนก็แพร่หลายมากขึ้นราคาปรับจูนจึงตกเหลือเครื่องละ 500 ถึง 1,000 บาท แต่ในปัจจุบันได้มีกลุ่มผู้กระทำความผิดพัฒนาการลักลอบปรับจูนโทรศัพท์เคลื่อนที่ด้วยวิธีการใหม่คือโดยการขายโทรศัพท์เคลื่อนที่พร้อมด้วยหมายเลขที่ปรับจูนแล้วแก่ประชาชนผู้บริโภคในราคาเครื่องละประมาณ 15,000 ถึง 20,000 บาท ผู้ที่รับซื้อไปก็ไม่ต้องเสียค่าใช้บริการโทรศัพท์รายเดือนแต่อย่างไร และไม่มีสัญญาผูกพันกับบริษัทที่เกี่ยวข้องอย่างไรและผู้ที่ปรับจูนนอกจากขายเครื่องพร้อมหมายเลขโทรศัพท์เคลื่อนที่ที่ปรับจูนแล้ว ยังมีบริการในรูปแบบใหม่โดยการให้เช่าเครื่องโทรศัพท์เคลื่อนที่พร้อมกับหมายเลขที่ปรับจูนไว้เรียบร้อยแล้ว ให้กับผู้มาใช้บริการโดยทั่วไปโดยคิดค่าเช่าเดือนละ 2,000 บาท ถึง 3,000 บาท แต่ถ้าขณะนำไปใช้เครื่องสัญญาณถูกหน่วยงานที่เกี่ยวข้องหรือบริษัทที่รับสัมปทานตรวจสอบแล้วรับได้จึงตัดสัญญาณ กลุ่มพ่อค้าก็จะนำเอาเครื่องโทรศัพท์เคลื่อนที่ที่ลูกค้าเช่าไปนำกลับมาปรับจูนหมายเลขโทรศัพท์เครื่องใหม่ให้กับผู้เช่าคนใหม่ต่อไปอีก [14]

3) การนำโทรศัพท์มือถือออกขาย ใช้หรือให้เช่า (Sell/Use for free/rent out)

---

[13] กองกำกับการสืบสวนตำรวจนครบาลใต้, รายงานจากบันทึกการจับกุม นายรณภพ ธนบวรมงคล เมื่อวันที่ 16 ตุลาคม 2539.

[14] กองกำกับการสืบสวนตำรวจนครบาลใต้, รายงานจากบันทึกการจับกุมนายยาชีพ อาลี เมื่อวันที่ 9 ตุลาคม 2539.

ตระเวนใช้โดยไม่ต้องเสียเงินค่าใช้บริการ หากทางบริษัทผู้ให้บริการทำการระงับบริการผู้ที่ใช้โทรศัพท์ที่จูนคลื่นสัญญาณโทรศัพท์ข้างต้นก็ยังคงสามารถนำไปใช้ได้ในเขตพื้นที่ที่มีสัญญาณตระเวน(roaming service) ซึ่งก็เป็นการกระทำความผิดฐานฉ้อโกงอีกฐานหนึ่งนั่นเอง

ดังนั้นไม่ว่าจะเป็นโทรศัพท์มือถือ (Cellular) หรือโทรศัพท์เคลื่อนที่ส่วนตัว (PCS) ต่างก็เสี่ยงต่อการที่จะถูกกระทำทุจริตจากประเภทเทคนิคขั้นต่ำ ส่วนความเสี่ยงในการถูกกระทำทุจริตประเภทเทคนิคขั้นสูงยังคงขึ้นอยู่กับเทคโนโลยีที่บริษัทผู้ให้บริการนำมาใช้ในระบบเครือข่าย

บริษัทผู้ให้บริการโทรศัพท์มือถือส่วนใหญ่นิยมใช้เทคโนโลยีโทรศัพท์เคลื่อนที่สมัยใหม่(Advanced Mobile Phone Service - AMPS) ซึ่งจะเป็นการส่งคลื่นสัญญาณอนาล็อกระบบเอฟเอ็มที่ยังไม่เข้ารหัส (unencrypted analog frequency modulated (FM) signal)อันเป็นคลื่นสัญญาณความถี่ที่เครื่องรับวิทยุระบบเอฟ.เอ็ม.ทั่วไปก็สามารถรับฟังได้ เช่น เครื่องตรวจจับสัญญาณ (scanner) ซึ่งมีทั้งผลิตและวางจำหน่ายในสหรัฐอเมริกา โดยจะถูกปลดคลื่นความถี่ก่อนออกจำหน่ายในตลาด แต่คนร้ายมักนำไปปรับแต่งโดยเพียงแต่ตัดสายเชื่อม 2-3 แห่งก็ใช้เป็นเครื่องตรวจจับคลื่นสัญญาณโทรศัพท์มือถือได้แล้ว เครื่องรับโทรทัศน์ที่เป็นระบบคลื่นความถี่สูง (Ultra high frequency) ก็สามารถทำการปรับแต่งให้สามารถตรวจดักจับคลื่นความถี่ข้างต้นได้ แต่ถึงอย่างไรก็ตามโทรศัพท์มือถือเทคโนโลยีสมัยใหม่(AMPS) ก็ยังเสี่ยงถูกกระทำทุจริต

3.2 แนวทางในทางเทคนิคเพื่อป้องกันการทุจริตโทรศัพท์เคลื่อนที่

สำหรับการป้องกันการทุจริตโทรศัพท์เคลื่อนที่(Fraud Prevention) นั้นบริษัทผู้ให้บริการโทรศัพท์เคลื่อนที่นำมาตรการต่างๆเพื่อป้องกันการทุจริตลักลอบจูนโทรศัพท์ โดยมิให้คนร้ายใช้โทรศัพท์ได้ โดยติดตั้งส่วนที่เป็นฮาร์ดแวร์ (hardware-based) เพื่อเป็นกลไกการตรวจสอบและป้องกันการใช้โทรศัพท์เคลื่อนที่โดยมิชอบด้วยกฎหมาย บริษัทผู้ให้บริการโทรศัพท์เคลื่อนที่จะมอบหมายเลขรหัสส่วนตัว 4 หลัก (Personal Identification Number - PIN) ทุกครั้งผู้ใช้โทรศัพท์ต้องป้องรหัสส่วนตัวก่อนใช้เสมอ บริษัทผู้ให้บริการระบบ AMPS บางแห่งกำหนดการส่งหมายเลขรหัสส่วนตัว(PIN) พร้อมทั้งข้อมูลบัญชีไปตามความถี่คลื่นต่าง ๆ กัน เพื่อป้องกันคนร้ายไม่ให้สามารถทำการตรวจจับคลื่นสัญญาณโทรศัพท์หรือเอารหัสส่วนตัวไปใช้ มาตรการการตรวจสอบความถูกต้อง (Authentication) ก็เป็นอีกมาตรการที่ใช้

ได้ผลในการป้องกันการทุจริตโทรศัพท์เคลื่อนที่ แต่เสียดายที่มาตรการตรวจสอบความถูกต้องไม่มีใช้ในระบบโทรศัพท์เคลื่อนที่ AMPS

ในประเทศไทยบริษัทผู้ให้บริการโทรศัพท์ในประเทศไทยใช้มาตรการ 2 ประการเพื่อป้องกันปัญหาในการลักลอบใช้สัญญาณโทรศัพท์เคลื่อนที่ กล่าวคือ

(1) การกำหนดหมายเลขประจำตัวเจ้าของ (Subscriber Identity Security)

(2) การควบคุมการใช้ทุจริต (Fraud Management) เป็นการตรวจสอบการใช้งานโทรศัพท์เคลื่อนที่ถึงสถานที่ จำนวนครั้งและระยะเวลาที่โทรออกมาประมวลผลว่าผิดปกติจากการใช้ธรรมดา โดยขณะที่ใช้ความถี่คลื่นวิทยุ (Radio Frequency (RF))เป็นกลไกในการตรวจจับความเคลื่อนไหวเส้นทางเดินของการใช้โทรศัพท์(fingerprinting)ของคลื่นสัญญาณวิทยุที่ใช้ในการรับส่งสัญญาณโทรศัพท์มือถือ เพราะเหตุที่เครื่องนี้สามารถตรวจสอบสัญญาณที่ส่งออกมาจากเครื่องว่าเครื่องใดเป็นเครื่องโทรศัพท์มือถือจริงเครื่องใดเป็นโทรศัพท์เคลื่อนที่ที่ลักลอบจูน เทคโนโลยีสมัยใหม่ถูกนำมาใช้ในระบบเครือข่ายและสามารถป้องกันมิให้เครื่องโทรศัพท์ที่ได้มาจากการปรับจูนคลื่นสัญญาณสามารถทำการติดต่อโทรศัพท์ บริษัทผู้ให้บริการบางรายใช้เทคโนโลยีที่ระบบสามารถตรวจสอบลายพิมพ์นิ้วมืออีเลคโทรนิคสำหรับการโทรศัพท์ติดต่อที่มาจากนอกเครือข่ายบริการเข้ามาในพื้นที่บริการ เมื่อระบบตรวจสอบถูกต้องก็จะเชื่อมเครือข่ายให้ใช้บริการได้

บริษัทผู้ให้บริการโทรศัพท์เคลื่อนที่ในเมืองใหญ่มักเสนอเทคโนโลยีการให้บริการที่เรียกว่าระบบการแบ่งย่อยห้วงเวลา(Time Division Multiple Access-TDMA) ซึ่งการทำงานของระบบเครื่องโทรศัพท์มือถือนี้จะใช้เทคโนโลยี TDMA แปลงคลื่นสัญญาณเกี่ยวกับข้อมูลบัญชีผู้เช่าโทรศัพท์และเสียงพูดให้เป็นตัวเลขฐานสอง (binary) ซึ่งประกอบด้วยตัวเลข 0 กับ 1 จากนั้นคลื่นสัญญาณจะถูกส่งออกไปในรูปข้อมูลตัวเลข(digitized information) ที่เป็นเลขฐานสอง (binary) ในช่วงระยะเวลาที่กำหนดที่สั้นมากซึ่งคิดแล้วประมาณไม่กี่เศษส่วนพันของวินาที (several thousandths of a second long) บรรดาตัวเลขฐานสองเหล่านี้จะถูกแยกส่งไปเป็นกลุ่มซึ่งยังไม่เป็นข้อมูลที่สมบูรณ์(incomplete information)จึงทำให้เทคโนโลยีระบบ TDMA ยากแก่การถูกตรวจจับคลื่นสัญญาณเพื่อนำไปจูนสัญญาณ บริษัทผู้ให้บริการบางรายยังทำการเข้ารหัส (Encrypted) หรือเพิ่มมาตรการป้องกันเพิ่มเข้าไปอีก

บริษัทผู้ให้บริการที่ใช้เทคโนโลยีระบบ TDMA บางรายยังไม่ได้ใช้เทคโนโลยีที่กล่าวข้างต้นทั่วพื้นที่บริการ จึงทำให้ผู้ใช้โทรศัพท์มือถือในเขตพื้นที่ดังกล่าวสามารถใช้เทคโนโลยีโทรศัพท์ระบบคู่ คือจะเข้าสู่แบบ AMPS ถ้าหากขณะที่ใช้นั้นไม่มีเทคโนโลยีแบบTDMA เมื่อมีการใช้เทคโนโลยีแบบ AMPS จะทำให้โทรศัพท์มือถือนี้ง่ายต่อการตกเป็นเป้าของการตรวจจับคลื่นสัญญาณโทรศัพท์ของพวกแก๊งค์จูนโทรศัพท์มือถือ

บริษัทผู้ให้บริการโทรศัพท์เคลื่อนที่ส่วนตัว(Personal communication service) มักเลือกใช้ระบบเทคโนโลยีต่าง ๆ บนเครือข่ายของตน แต่ระบบที่นิยมมากในโลกปัจจุบันมี 2 ระบบด้วยกัน คือ

1) ระบบโทรศัพท์เคลื่อนที่สากล (Global System for Mobile Communication-GSM) เป็นการใช้เทคโนโลยีเข้ามาทำการแปลงข้อมูลเกี่ยวกับบัญชีของผู้ใช้โทรศัพท์ซึ่งถูกบรรจุไว้ในบัตรเก็บข้อมูลแสดงตนของผู้ใช้โทรศัพท์ (Subscriber's Identity Module - SIM) และแปลงคลื่นเสียงให้เป็นตัวเลขแล้วส่งออกไปในห้วงเวลาที่กำหนด ซึ่งปกติแล้วบัตรต้นแบบข้อมูล SIM มักมีขนาดเท่ากับดวงแสตมป์หรือขนาดไม่เกินบัตรเครดิต ซึ่งผู้ใช้โทรศัพท์ต้องบรรจุเข้าไปในเครื่องโทรศัพท์มือถือเมื่อต้องการเปิดใช้เครื่องโทรศัพท์ กล่าวคือเมื่อผู้ใช้โทรศัพท์เปิดเครื่องโทรศัพท์มือถือ ระบบเครือข่ายของ GSM จะดำเนินการติดต่อและโต้ตอบการตรวจสอบจากบัตรต้นแบบข้อมูล(SIM) ว่าเป็นข้อมูลถูกต้องหรือไม่ หากบัตรต้นแบบข้อมูล (SIM) ตอบด้วยข้อมูลที่ถูกต้องระบบเครือข่าย GSM ก็จะเชื่อมสายโทรศัพท์ในการติดต่อให้โดยจะเข้ารหัสด้วยการใช้ข้อมูลที่บรรจุอยู่ในบัตรต้นแบบข้อมูล (SIM) ผู้เชี่ยวชาญทางเทคโนโลยียังยืนยันว่าขณะนี้ระบบ GSM ยังปลอดภัยจากการทุจริตโทรศัพท์ถูกจูน เพราะถึงแม้ว่าคนร้ายจะได้ข้อมูลบัญชีที่ถูกต้องของเจ้าของบัญชีโทรศัพท์ไปไว้ในครอบครองโดยการลักขโมยไป ก็ไม่คุ้มกับการลงทุนค่าใช้จ่ายหรือเสียเวลาที่จะทำการปลอมบัตรต้นแบบข้อมูล(SIM) สำหรับคนร้าย แต่เมื่อไม่นานมานี้ปรากฏรายงานว่ามีบริษัททางการค้าแห่งหนึ่งได้ทำการพัฒนาโปรแกรมคอมพิวเตอร์ขึ้นมา สามารถทำปลอมบัตรต้นแบบข้อมูล(SIM) โดยโปรแกรมที่กล่าวต้องนำไปเชื่อมใช้กับเครื่องมืออุปกรณ์คอมพิวเตอร์ (peripheral equipment) ที่ต่อเข้ากับเครื่องคอมพิวเตอร์แบบกระเป๋าหิ้ว (Laptop computer) [15]

---

[15] The Yankee Consulting Group, "The Weakest Links" , Wireless World (January 1997) , p.40.

สรุปแล้วเมื่อกล่าวทางทฤษฎีแล้วระบบเทคโนโลยีที่ใช้กับโทรศัพท์ระบบ GSM ยังคงได้รับการประกันว่ามีความปลอดภัยจากการที่จะถูกจูนอันเนื่องมาจากการตระเวนไปตามที่ต่าง ๆ นอกจากนั้นโทรศัพท์ระบบ GSM ยังสามารถกำหนดให้ระบบเครือข่ายสถานีต้นทาง (home carrier) ให้ทำการตรวจสอบข้อมูลทุกครั้งกับผู้ใช้โทรศัพท์ที่ใช้บริการตระเวน (roaming service) ซึ่งวิธีการนี้ช่วยเสริมความปลอดภัยให้กับระบบเครือข่ายป้องกันการถูกลักลอบจูนโทรศัพท์ใช้แบบไม่เสียเงินจากคนร้าย

2) ระบบเข้าด้วยการแบ่งย่อยรหัส (Code Division Multiple Access-CDMA)เป็นระบบเทคโนโลยีของโทรศัพท์เคลื่อนที่ส่วนตัว (Personal Communication Services - PCS)ป้องกันการรับสัญญาณที่ไม่มีอำนาจ ระบบ CDMA จะทำการแปลงสัญญาณให้เป็นเลขฐานสองแล้วบวกด้วยรหัสของผู้ใช้โทรศัพท์เข้าไป เฉพาะเครื่องรับโทรศัพท์มือถือที่มีรหัสของผู้ใช้โทรศัพท์บรรจุอยู่เท่านั้นจึงสามารถทำการรับส่งติดต่อกันได้ ระบบ CDMA จะทำการส่งข้อมูลของเจ้าของโทรศัพท์มือถือไปตามช่วงความถี่เดียวกันพร้อมกัน แต่ใช้รหัสที่ต่างกันออกไปกับเจ้าของโทรศัพท์มือถือรายอื่นคือ ไม่มีซ้ำกันแม้ว่าโทรศัพท์ระบบนี้ยากต่อการถูกดักฟังโทรศัพท์ที่ใช้เทคโนโลยีระบบ CDMA ก็ยังไม่มีความปลอดภัยเท่าที่ควร เว้นแต่มีการเข้ารหัสคลื่นสัญญาณด้วย บริษัทผู้ให้บริการโทรศัพท์มือถือหลายแห่งกำลังวางแผนเพื่อการป้องกันการถูกจูนหรือดักฟังด้วยการใช้เทคนิคการเข้ารหัส(encrypted) แต่เป็นที่น่าเสียหายเพราะในระยะเวลาเพียงไม่กี่สัปดาห์คณะผู้วิจัยจากบริษัทที่ปรึกษาแห่งหนึ่งที่มีความเชี่ยวชาญทางด้านการเข้ารหัสสามารถเข้าไปในระบบรหัสที่ใช้ในเครือข่ายทั้งระบบ CDMA และ TDMA [16] แม้ว่ามีการรับรองว่า CDMA เป็นระบบเครือข่ายที่ป้องกันการถูกดักฟังการสนทนาและป้องกันการถูกดักจับสัญญาณก็ตาม

3.3 การตรวจจับการทุจริตโทรศัพท์เคลื่อนที่ (Fraud Detection)

บรรดาบริษัทที่เป็นผู้ให้บริการโทรศัพท์เคลื่อนที่ (Mobile Telephone Services Provider) ในประเทศสหรัฐอเมริกาต่างก็ให้ความสำคัญต่อปัญหาการทุจริตฉ้อโกงโทรศัพท์เคลื่อนที่ จึงนำเอาเทคโนโลยีสมัยใหม่มาใช้ในการป้องกันการกระทำความผิด

---

[16] Paul Rubin, , "Sure It's Secure - But is It Really Safe ?", Counterpane Systems, Tele.com, May 1997.

ดังกล่าวซึ่งปกติก็เป็นการเขียนโปรแกรมคอมพิวเตอร์ขึ้นมาเพื่อเชื่อมใช้กับระบบเครือข่ายบริการโทรศัพท์เคลื่อนที่ซึ่งใช้เทคโนโลยีสมัยใหม่ควบคุมระบบทำงานอยู่แล้ว สำหรับโปรแกรมคอมพิวเตอร์ที่เขียนขึ้นมา เน้นรูปแบบของการตรวจจับการลักลอบใช้โทรศัพท์เคลื่อนที่ของคนร้ายที่ลักลอบจูนโดยใช้หมายเลขประจำตัวผู้ใช้โทรศัพท์เคลื่อนที่ (Subscriber's Identification Systems) รหัสผ่าน (Code) มาใช้โดยที่เจ้าของที่แท้จริงไม่ทราบและเป็นการตรวจจับการใช้โทรศัพท์มือถือเครื่องที่ลักลอบจูนคลื่นสัญญาณความถี่ในโปรแกรมคอมพิวเตอร์บางรุ่น เน้นการตรวจสอบความเคลื่อนไหวของการใช้โทรศัพท์ของตัวเจ้าของผู้ใช้โทรศัพท์เคลื่อนที่แล้วทำการตรวจเปรียบเทียบกับรายการใช้ที่บันทึกเก็บไว้ หากระบบตรวจพบว่ามีความผิดเกิดขึ้นจากที่บันทึกไว้ในฐานข้อมูลหลัก ระบบก็จะส่งสัญญาณเตือนและแจ้งให้เจ้าหน้าที่ฝ่ายสืบสวนป้องกันการทุจริตโทรศัพท์เคลื่อนที่ บางโปรแกรมคอมพิวเตอร์ก็ทำการตรวจติดตามความเคลื่อนไหวในรายการการใช้โทรศัพท์มือถือและการใช้ที่ยาวนานกว่าปกติ เช่น มีการใช้โทรศัพท์เคลื่อนที่บ่อยมากแบบติดต่อกัน เช่น รายการที่ผู้ใช้โทรศัพท์เคลื่อนที่คนเดียวกัน การใช้โทรศัพท์ทางไกลที่มีราคาค่าบริการสูง การโทรศัพท์ออกจากหรือเข้าไปติดต่อกับโทรศัพท์สาธารณะ (pay telephones) การใช้โทรศัพท์เคลื่อนที่จากสถานที่ต้องสงสัยหรือเวลาที่ต้องสงสัย เมื่อเกินมาตรฐานที่กำหนดไว้แล้วระบบก็จะส่งสัญญาณเตือนหรือแจ้งให้ฝ่ายสืบสวนป้องกันปราบปรามของบริษัทผู้ให้บริการโทรศัพท์ทราบ

3.4 ความเสียหายจากการทุจริตโทรศัพท์เคลื่อนที่ (The Cost of Fraud)

สมาคมอุตสาหกรรมโทรศัพท์เคลื่อนที่(The Cellular Telecommunications Industry Association - CTIA) มีการประชุมสัมมนาเกี่ยวกับการป้องกันปราบปรามการลักลอบจูนโทรศัพท์เคลื่อนที่ ณ เมือง ออลันโด มลรัฐฟลอริด้า ประมาณว่าความเสียหายสำหรับการกระทำทุจริตในการใช้โทรศัพท์มือถือโดยมิชอบด้วยกฎหมาย จากการสำรวจความเสียหายของการทุจริตในระบบโทรศัพท์เคลื่อนที่ส่วนตัว (PCS) และโทรศัพท์มือถือ (Cellular) ทำให้บริษัทผู้ให้บริการได้รับความเสียหาย ดังนี้

ปี ค.ศ.1994	440,000,000 ดอลลาร์
ปี ค.ศ.1995	650,000,000 ดอลลาร์
ปี ค.ศ.1996	710,000,000 ดอลลาร์

ที่มาของข้อมูล : CTIA Wireless Fraud Conference , Orlando , Florida, September 30-October 2 , 1997.

การกระทำทุจริตโทรศัพท์มือถือหรือโทรศัพท์เคลื่อนที่นับวันยิ่งก่อปัญหาให้กับบรรดาบริษัทผู้ให้บริการโทรศัพท์เคลื่อนที่ (Mobile Telephone Services Provider) ในช่วงระยะ 2-3 ปี ที่ผ่านมา โดยคนร้ายมักใช้เครื่องตรวจจับสัญญาณ (Scanner) ทำการจับคลื่นสัญญาณหมายเลขประจำตัวอิเล็คโทรนิค(Electronic Serial Number)รวมถึงการที่พวกแหกด่าน (Crackers) ลักลอบเจาะเข้าไปในเครือข่ายระบบคอมพิวเตอร์ซึ่งมักมีการใช้โทรศัพท์มือถือหรือโทรศัพท์เคลื่อนที่ บัตรโทรศัพท์และการสั่งซื้อสินค้าทางโทรศัพท์ที่ต้องแจ้งหมายเลขบัตรเครดิต [17]

สหรัฐอเมริกาโดยทางรัฐบาลกลางได้กำหนดให้ผู้บริการโทรศัพท์เคลื่อนที่ (Mobile Telephone Service Provider) ทั้งระบบโทรศัพท์มือถือ (cellular telephone) และโทรศัพท์เคลื่อนที่ส่วนตัว (Personal Communication Services) ดำเนินการติดตั้งเครื่องมือให้บริการสัญญาณตระเวน (roaming service) ให้เสร็จเรียบร้อยภายในปี ค.ศ.1999 ซึ่งยิ่งเป็นปัจจัยเอื้ออำนวยให้เกิดการทุจริตประเภทนี้มากขึ้น

อย่างไรก็ตามประเทศไทยได้มีการบัญญัติกฎหมายที่เกี่ยวข้องไว้โดยเฉพาะเพื่อควบคุมกิจการโทรเลขและโทรศัพท์ วิทยุคมนาคม ซึ่งใช้บังคับมานานไม่ครอบคลุมกิจการโทรศัพท์เคลื่อนที่แต่อย่างใด กฎหมายดังกล่าวจึงไม่อาจนำมาใช้บังคับกับการกระทำในลักษณะที่เป็นการลักลอบใช้สัญญาณโทรศัพท์เคลื่อนที่ได้

---

[17] David Icove , Karl Seger and William VonStorch, Computer Crime - A Crimefighter's Handbook. (California : O'Reilly&Associates, Inc., 1995) , p.33.