ความปลอดภัยของการสื่อสารข้อมูลผ่านไฟเบอร์ออพติก

น.ต.ผศ.ดนัย ปฏิยุทธ
ผู้ช่วยศาสตราจารย์ ฝ่ายศึกษา โรงเรียนนายเรือ

---

๑. บทนำ

การรักษาความปลอดภัยของการสื่อสารข้อมูลนั้นคล้าย ๆ กับเกมแมวจับหนู กล่าวคือ ตลอดเวลาตั้งแต่อดีตจนถึงปัจจุบันไม่ว่าเราจะสร้างกำแพงกั้นโจรสูงเท่าใดก็ตาม เหล่ามิจฉาชีพก็สามารถแอบเข้าบ้านได้เสมอ การรักษาความปลอดภัยของการสื่อสารข้อมูลเริ่มล้าสมัย โดยระบบรักษาความปลอดภัยใด ๆ จะแข็งแรงเท่ากับจุดอ่อนของมัน จุดอ่อนหนึ่งของระบบรักษาความปลอดภัยในปัจจุบันคือการแจกจ่ายกุญแจเข้ารหัส (Key Distribution) การวิจัยในหัวข้อใหม่เรื่อง Quantum Cryptography จึงเกิดขึ้น

โดย Quantum Cryptography เริ่มใช้งานครั้งแรกเมื่อปี ค.ศ.๑๙๙๖ โดยทำงานผ่านเส้นใยแก้วนำแสงที่ความยาวคลื่น ๑.๓ ถึง ๑.๕๕ ไมครอน (ซึ่งเป็นความยาวคลื่นที่นิยมใช้มากที่สุดในโครงข่ายไฟเบอร์ออพติกและการสื่อสารโดยไฟเบอร์ออพติก) สาเหตุที่ใช้ Quantum Cryptography เพราะจุดอ่อนของการปกป้องความปลอดภัยแบบอื่นที่ไม่สามารถส่ง Secret key ไปตามสายสื่อสารได้แต่ Quantum Cryptography สามารถกระทำได้นั่นเอง อีกทั้ง Quantum Cryptography ยังไม่ต้องการตัวกลางในการลงทะเบียนอีกด้วย

๒. คุณลักษณะทั่วไป

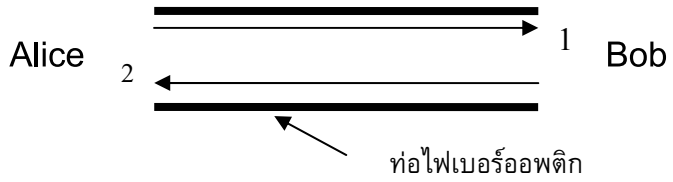
เส้นใยแก้วนำแสงหรือไฟเบอร์ออพติกเป็นตัวกลางที่นำสัญญาณแสงจากจุดหนึ่งไปยังอีกจุดหนึ่ง โดยแสงในเส้นใยแก้วนำแสงจะถูกสะท้อนกลับไปกลับมาระหว่างรอยต่อของแกนกลาง (Core) และฉนวนที่หุ้ม (Cladding) จากปลายข้างหนึ่งไปยังอีกปลายข้างหนึ่งของเส้นใยแก้วนำแสง โครงสร้างของเส้นใยแก้วนำแสงไม่มีส่วนประกอบของตัวนำไฟฟ้าจึงทำให้ไม่มีคุณสมบัติทางไฟฟ้า (การนำไฟฟ้าหรือการเหนี่ยวนำไฟฟ้า) ซึ่งทำให้ข้อมูลข่าวสารที่ส่งไปยังปลายทางไม่ถูกรบกวนทางไฟฟ้าจากภายนอกไม่ว่าจากสัญญาณไฟฟ้าแรงสูงหรือคลื่นแม่เหล็กไฟฟ้า

๓. ความปลอดภัย

จากการศึกษาในเรื่อง Quantum ทำให้เกิดแขนงสาขาความรู้ที่สามารถนำไปปฏิบัติได้จริงที่เรียกว่า “Quantum Cryptography” (บางครั้งเรียกว่า Quantum Key Distribution) ซึ่งเป็นวิธีที่ทำให้การส่งข้อมูลผ่านไฟเบอร์ออพติกอย่างปลอดภัย โดยมีหลักการทำงานคือการใช้ Quantum Mechanic เพื่อผลิต

Key ที่ใช้ในการเข้ารหัส (Encrypt) ข่าวสาร (Message) โดย Quantum Cryptography นั้นสามารถส่งข้อความที่ถูก Coded ได้ระยะไกล ๒๐ กิโลเมตร โดย Quantum Cryptography จะตรวจสอบถึงความเป็นไปได้ที่เกิดขึ้นที่ชิ้นส่วนเล็ก ๆ ที่เหมือนกันภายใน (Intertwined) แต่อยู่แยกจากกัน โดยอะตอมและโมเลกุลนั้นมีความสามารถคือการส่งข้อมูลที่ไม่สามารถทำให้ขาดตอนได้ (Unbreakable) และความสามารถในการคำนวณและการค้นหาข้อมูลที่รวดเร็วและมีกำลังแบบ Exponential ที่เรียกว่า “Quantum Computing”

๓.๑ วิธีการเข้ารหัสและการตรวจสอบของ IBM’s Almaden Research Center



วิธีปฏิบัติคือ

๑. Alice ผลิต Proton (ชิ้นส่วนที่ทำให้เกิดแสง) อย่างสุ่มและส่งไปให้ Bob (และรู้ว่า Proton ที่ผลิตนั้นมีค่าเป็น ๑ หรือ ๐)

๒. Bob คำนวณว่า 1’s มีจำนวนเป็นคู่ (Even) หรือคี่ (Odd) จาก 16 bits แรกและส่งกลับไป Check กับ Alice (ซึ่งจะคำนวณในขณะเดียวกันและใช้ Subset ของ Proton ที่เหมือนกันกับของที่ Bob ใช้)

๓. โดยการเปรียบเทียบ Parities ความผิดพลาดที่เกิดขึ้นในการสื่อสารก็สามารถถูกหาได้ว่าเกิดขึ้นที่ใดและสามารถถูกทำการแก้ไขได้

๔. เมื่อทำการแก้ไขเรียบร้อยทั้ง Alice และ Bob ก็จะมี Bits ที่เหมือนกันและใช้เป็น Secret Key นั่นเอง

๓.๑.๑ จุดอ่อน

จุดอ่อนของการเข้ารหัสในการสื่อสารและวิธีแก้ไขผ่านสื่อแบบไฟเบอร์ออพติกแบบนี้มีดังตารางข้างล่าง

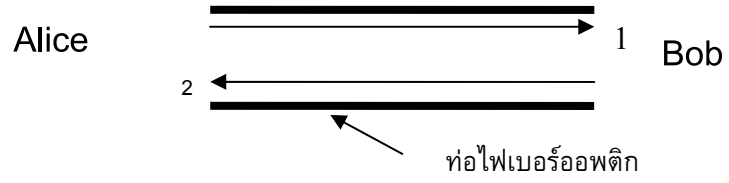
จุดอ่อน	วิธีแก้ไข
๑. Spy แอบดูและขโมยข้อมูล	๑. ใช้วิธี “Privacy Amplification” กล่าวคือการยอมสูญเสียบาง Bits ไปและสร้าง Bits ใหม่ขึ้นมาแทนที่ (Spy จะขโมย Bits ได้น้อยลงเพราะเราทิ้ง บาง Bits ที่ได้ถูกขโมยไปนั่นเอง)

จุดอ่อน	วิธีแก้ไข
๒. ผู้ประสงค์ร้ายสามารถ Eavesdrop โดยการใช้อุปกรณ์แยกลำแสง (Beam-spitting Device) เช่น ครึ่งหนึ่งของกระจกเงิน (Half-silvered Mirror) เพื่อดึง Protons ออกมา เพื่อนำมาถอดและได้ข่าวสารที่ต้องการ	๒. ส่ง Proton ในการติดต่อสื่อสารครั้งละ ๑ Proton เท่านั้น (เพราะ Proton ๑ ตัวไม่สามารถแยกออกได้อีก)
๓. ผู้ประสงค์ร้ายสามารถ Intercept การ Request จาก Alice และเก็บ Protons เพื่อนำมาวิเคราะห์และ Retransmit มันไปยัง Bob	๓. เปลี่ยนวิธีที่ ๑ และ ๐ ใช้แทนค่า นั่นคือการ Encode Polarization State ของ Proton (ใช้ Vertical Vibration แทน ๑ และ Horizontal Vibration แทน ๐ หรือ Clockwise Rotation แทน ๐ และ Anticlockwise แทน ๑)
๔. ไฟเบอร์ออพติกมีจุดด้อยตรงที่ไม่สามารถรักษา Proton Polarization State ได้	๔. ส่ง Light Pulse ไปตามท่อไฟเบอร์ออพติกเพื่อปรับสิ่งที่อาจเปลี่ยนแปลง หรือใช้ Passive Technique เพื่อให้ตอบสนองต่อการเปลี่ยนแปลง
๕. ยากในการตรวจพบ Proton ตัวเดียว	๕. ประยุกต์ใช้ Detector เพื่อให้สามารถทำงานได้ดีขึ้น

๓.๒ วิธีการเข้ารหัสและการตรวจสอบของ Northern University

วิธี High-speed Quantum Cryptography นี้สามารถเข้ารหัสข้อมูลและส่งไปตามเส้นไฟเบอร์ออพติกด้วยความเร็ว ๒๕๐ mbps โดยการใช้ Detector แบบธรรมดาในการตรวจหา Proton

๓.๑.๑ วิธีปฏิบัติ



๑. Alice ส่ง Secret Key ให้ Bob และทั้งคู่ก็ใช้ Key เดียวกัน (ก่อนการสื่อสารใดๆ)

๒. Alice ใช้ Secret Key นั้นในการ Manipulate แสง ทำให้เกิดรูปแบบของการส่งข้อมูลที่ยุ่งยากกว่าการส่งแบบ ๑ หรือ ๐ แบบธรรมดา ๆ (การรวมตัวกันของ ๑ และ ๐ จะใช้แทนข่าวสาร) โดยคุณลักษณะของ Quantum Noise (เกิดจากการ Granularity ของแสง) จะปรากฏตัวออกมาจากรูปลักษณะของ Secret Key เท่านั้น โดยการเปลี่ยน Granularity ของแสงนั้นสามารถกระทำได้โดยการ Polarizing แสงอย่างสุ่ม Eve ที่เป็น Eavesdropper จะไม่สามารถถอดรหัสข้อมูลได้เพราะข่าวสารที่ได้ยินนั้นจะกระจัดกระจาย (Fuzz) แต่ Bob ที่มี Secret Key จะสามารถเข้าใจรูปแบบ (Pattern) และจะได้สัญญาณที่มีการรบกวนที่น้อยกว่า และสามารถถอดรหัสข่าวสารที่ Alice ส่งมาให้ได้

๔. สรุป

ด้วยความชาญฉลาดของนักวิทยาศาสตร์จึงสามารถคิดค้นวิธีในการเข้ารหัสและส่งข้อมูลไปตามเส้นไฟเบอร์ออพติกสาธารณะได้ โดยอาศัยคุณสมบัติการยักย้ายถ่ายเท (Manipulation) ของความลื่น (Slippery) และการหลบเลี่ยง (Elusive) ขององค์ประกอบที่เล็กที่สุดของวัตถุ วิธีนี้จะขึ้นอยู่กับคุณลักษณะที่พิเศษของอะตอม กล่าวคือความพยายามใด ๆ ก็ตามที่จะวิเคราะห์ข้อมูลที่ได้เข้ารหัสแล้ว จะไปเปลี่ยนแปลงคุณลักษณะของอะตอม (หรือของ Proton นั่นเอง) นั่นคือ Encoded State เปลี่ยนไปและทำให้การส่งถ่ายครั้งนั้นไม่เกิดประโยชน์ใดๆ นั่นคือสำคัญที่ Quantum Cryptography ได้รับความนิยมในการเข้ารหัสข้อมูลเพื่อใช้ในเชิงธุรกิจและทางทหารนั้นเพราะการยากต่อการถูกโจมตีนั่นเอง ข้อดีอีกประการหนึ่งของ Quantum Cryptography คือกำลังในการคำนวณที่มีมากนั่นอง

แม้จะมีข้อดีหลายข้อแต่อุปสรรคที่ทำให้ศาสตร์ของ Quantum Cryptography ไม่ก้าวไกลเท่าที่ควรเพราะการส่งข้อมูลที่เข้ารหัสไปตามเส้นใยแก้วนำแสงนั้นได้ผลดีจนถึงระยะ ๒๐ กิโลเมตรเท่านั้น หลังจากระยะนี้แล้ว Error Rate ก็จะเพิ่มมากขึ้นถึงแม้การแก้ปัญหาโดยการใช้ Repeater มาช่วยบรรเทาแล้วก็ตามปัญหาก็ยังคงมีอยู่โดยจะไปรบกวนสถานะของ Quantum ใน Key Data โดยระยะที่ไกลที่สุดนั้นคือระยะ ๙๐ กิโลเมตรเท่านั้นเองและขณะนี้ก็ยังคงกระทำได้เฉพาะสื่อไฟเบอร์ออพติกเท่านั้น ยังไม่สามารถกระทำได้กับ Internet การวิจัยยังลงไปดูถึงความเป็นไปได้ในการส่ง Proton ไปทางอากาศแทนที่จะส่งไปตามเส้นไฟเบอร์ออพติกอย่างเดียว

เมื่อถึงเวลาที่ปัญหาและจุดอ่อนต่าง ๆ ได้ถูกขจัดไปจาก Quantum Cryptography ได้แล้ว สถาบันด้านการเงินหรือหน่วยงานทหารก็จะหันมาใช้บริการการเข้ารหัสแบบนี้แทนการเข้ารหัสแบบปัจจุบันที่ใช้อยู่ (แบบ Mathematical Algorithm) เพราะระบบปัจจุบันนี้เริ่มมีปัญหาเมื่อกำลังในการคำนวณเริ่มเพิ่มมากขึ้นเรื่อย ๆ ตามกาลเวลาที่เปลี่ยนไป

เราก็ได้แต่หวังว่าสักวันหนึ่งเมื่อมันเกิดขึ้นมา ก็จะสามารถป้องกันไม่ให้ขโมยเข้ามาภายในระบบได้

๕. เอกสารอ้างอิง

ดร. รัชภาคย์ จิตต์อารีม “ใยแก้วนำแสง”, เทคโนโลยีสื่อสาร, ปีที่ ๒ ฉบับที่ ๑๓ ปี ๒๕๔๐

http://www.afcea.org/signal/articles/anmviewer.asp?a=๓๐๐&z=๘๖

Hengerer, R. “Quantum Cryptography represents the next line of IT Security”, ๒๐๐๑.