

ปัจจุบันการสื่อสารข้อมูลบนเครือข่ายอินเทอร์เน็ตเป็นสิ่งจำเป็นทั้งภายนอกและภายในของทุกองค์กร ทั้งนี้การสื่อสารภายในมักจะมีข้อมูลสำคัญที่ต้องการปกปิดเป็นความลับ ผู้ส่งและผู้รับจำเป็นต้องระมัดระวังเป็นอย่างมาก รวมถึงการขยายช่องทางการซื้อขายสินค้าและชำระเงินออนไลน์ ซึ่งผู้บริโภคต้องการข้อมูลสำคัญในการทำ



นวัตกรรม

ระบบความปลอดภัยธุรกรรมโลกไซเบอร์

ธุรกรรมทางการเงินบนเครือข่ายอินเทอร์เน็ต ทำให้กลุ่มมิจฉาชีพสามารถใช้ช่องดังกล่าวในการโจรกรรมข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับต่างๆเพื่อนำไปแอบอ้างในการทำธุรกรรมทางการเงิน

ดังนั้น ผศ.ดร.ศรวรัตน์ ชิวปรีชา อาจารย์ประจำภาควิชาวิศวกรรมโทรคมนาคม จากคณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง (สจล.) จึงพัฒนาอุปกรณ์การเข้ารหัสลับที่ปลอดภัยสูงขึ้น ในลักษณะของการเข้ารหัส - ถอดรหัสลับแบบเคออสติก (Chaotic encryption - decryption) เพื่อรองรับความปลอดภัย

จากการโจรกรรมข้อมูลและการทำธุรกรรมบนเครือข่ายอินเทอร์เน็ตต่างๆ ต่อเรื่องนี้ ผศ.ดร.ศรวรัตน์ ชิวปรีชา ในฐานะเจ้าของนวัตกรรมรักษาความปลอดภัยของข้อมูล กล่าวว่าการเข้ารหัส - ถอดรหัสลับ เป็นอีกหนึ่งเทคโนโลยีที่ใช้ในการป้องกันข้อมูลอย่างแพร่หลาย ซึ่งเทคโนโลยีนี้มีหลากหลายรูปแบบ ทางทีมวิจัย

จึงได้พัฒนารูปแบบของกรเข้ารหัสลับข้อมูลให้มีความปลอดภัยสูงขึ้น โดยประยุกต์ใช้ทฤษฎีเคออส (Chaos) ที่มีจุดเด่นคือ เป็นระบบที่ไวต่อการเปลี่ยนแปลงของค่าเงื่อนไขเบื้องต้น ทำให้สามารถทำนายค่าระบบเคออสติกได้ในระยะยาว ซึ่งการเข้ารหัสลับทั่วไปเมื่อป้อนข้อมูลเข้าเหมือนเดิมซ้ำๆ ข้อมูลที่ผ่านการเข้ารหัสลับจะไม่มีการเปลี่ยนแปลง ทำให้เกิดความสับสนระหว่างข้อมูลเข้ากับข้อมูลออกได้ แต่สำหรับการเข้ารหัสลับแบบเคออสติก สัญญาณที่ผ่านการเข้ารหัสลับมีลักษณะคล้ายสัญญาณรบกวน และไม่สามารถถูกความสับสนใดๆกับสัญญาณข้อมูลเข้า แม้แต่ในกรณีที่มีการป้อนข้อมูลซ้ำเหมือนเดิมซ้ำๆ ดังนั้นการเข้ารหัส - ถอดรหัสลับแบบเคออสติกจึงมีประสิทธิภาพ



ภาพสูงในการนำมาประยุกต์ใช้ในด้านการรักษาความปลอดภัยของข้อมูล ทั้งนี้ทีมงานวิจัยได้พัฒนาอุปกรณ์ต้นแบบในการรักษาความปลอดภัยบนเครือข่าย โดยสร้างระบบการเข้ารหัส - ถอดรหัสลับแบบเคออสติกบนอุปกรณ์ Raspberry Pi ที่ใช้เป็นตัวกลางสำหรับรักษาความปลอดภัยของข้อมูลกับการสื่อสารข้อมูลระหว่างคอมพิวเตอร์ในเครือข่ายที่ใช้รูปแบบการสื่อสารเช่นเดียวกับเครือข่ายอินเทอร์เน็ต คือ โปรโตคอล TCP/IP โดยผู้ส่งสารที่ส่งข้อมูล ต้นฉบับ (Plain Text) ออก

จากทางฝั่งผู้ส่งข้อมูลไปบนเครือข่าย ข้อมูลจะผ่านการเข้ารหัสลับแบบเคออสติกก่อนด้วยต้นแบบของอุปกรณ์ที่ได้พัฒนาขึ้น และเมื่อข้อมูลส่งไปถึงฝั่งผู้รับข้อมูลก็จะถูกทำการถอดรหัสลับเพื่อให้ได้ข้อมูลต้นฉบับกลับคืนมาด้วยอุปกรณ์ที่ได้พัฒนาขึ้นเช่นกัน โดยดูอุปกรณ์ที่ใช้ในกระบวนการเข้ารหัส - ถอดรหัสลับทั้งฝั่งของผู้ส่งและผู้รับจะคือเครื่องรับ-ส่งข้อมูลแบบไร้สาย (Wi-Fi) เครื่องรับ-ส่งข้อมูลแบบมีสาย (Ethernet) และคอมพิวเตอร์เครื่องอื่นที่ทำการดึงข้อมูลบนเครือข่าย ข้อมูลที่ดึงกลับคืนนี้จะเป็นข้อมูลลับ (Cipher Text) ที่ผ่านการเข้ารหัสลับแบบเคออสติก

"อุปกรณ์ต้นแบบชิ้นนี้สามารถนำไปพัฒนาต่อยอดและประยุกต์ใช้งานในองค์กรหรือหน่วยงานที่ต้องการความปลอดภัยในการสื่อสารข้อมูลสำคัญ และเพื่อให้เป็นความลับเฉพาะในองค์กรเดียวกันเท่านั้น รวมทั้งในขณะนั้นทางทีมวิจัยมีความตั้งใจและกำลังพัฒนาระบบต้นแบบการเข้ารหัสลับแบบเคออสติกให้เป็นแอปพลิเคชันที่สามารถใช้งานได้บนสมาร์ตโฟน และแท็บเล็ตสำหรับการรับ - ส่งข้อความสั้น (SMS) ซึ่งจะช่วยป้องกันการโจรกรรมข้อมูลลับและข้อมูลสำคัญในการทำธุรกรรมทางการเงินต่างๆ ได้ รวมถึงการพัฒนาแอปพลิเคชันสำหรับการปกป้องข้อมูลการสนทนาทางเสียงบนระบบโทรศัพท์ทั้งในรูปแบบสมาร์ตโฟนและโทรศัพท์พื้นฐานอีกด้วย"

อย่างไรก็ตามปัญหาหนึ่งของคนในสังคมให้ความสำคัญเป็นอย่างมากคือความปลอดภัยของข้อมูลสำคัญต่างๆ จากภัยคุกคามบนอินเทอร์เน็ตในขณะรับ - ส่งข้อมูลสำคัญ รวมถึงทำธุรกรรมทางการเงินผ่านเครือข่ายอินเทอร์เน็ต อาทิ หมายเลขบัตรประจำตัวประชาชน หมายเลขบัญชีธนาคาร หมายเลขบัตรเครดิต เป็นต้น หากนำนวัตกรรมระบบรักษาความปลอดภัยของข้อมูลไปใช้จริงในระบบต่างๆ บนเครือข่ายอินเทอร์เน็ต จะทำให้ผู้บริโภคมีความมั่นใจในการใช้บริการและการทำธุรกรรมบนเครือข่ายอื่นๆ เพิ่มมากขึ้น ขณะที่การประมวลผลด้านความปลอดภัยจะมีประสิทธิภาพที่ดีขึ้นเช่นกัน



• ผศ.ดร.ศรวรัตน์ ชิวปรีชา