

การปกป้องข้อมูลด้วยการกระจายกุญแจเข้ารหัสเชิงควอนตัม: บอกลาการโจมตีทางไซเบอร์ได้เลยใช่ไหม

สรุป:

การสื่อสารผ่านระบบเครือข่ายที่ได้รับการเข้ารหัสด้วยวิทยาการเข้ารหัสรุ่นใหม่จะไม่สามารถถูกเจาะได้รองรับต่อการเปลี่ยนแปลงในอนาคต และจะช่วยให้การเข้าไปช่วยเหลือและบรรเทาปัญหาทำได้อย่างรวดเร็ว



วิกฤตโรคระบาดกำลังทำให้แรนซัมแวร์ในลักษณะ Double-threat, การโจรกรรมข้อมูล และการโจมตีด้วยเทคนิค Supply-chain attack ที่ซับซ้อนเพิ่มสูงขึ้น โขดยั้งดีที่อาชญากรทางไซเบอร์ถูกขัดขวางไว้ด้วย การเข้ารหัสในระดับองค์กร ซึ่งไม่อาจถูกเจาะเข้าไปได้โดยง่าย

อย่างไรก็ตาม ด้วยการมาถึงของการประมวลผลควอนตัม แม้แต่การปกป้องข้อมูลด้วยวิธีนี้ก็ตกอยู่ในอันตราย เมื่อขุมพลังในการประมวลผลอันทรงพลังอยู่ใกล้แค่เอื้อม อาชญากรทางไซเบอร์จะสามารถหาทางเจาะผ่านอัลกอริทึมการเข้ารหัสได้

งานวิจัยที่เป็นความร่วมมือระหว่างมหาวิทยาลัยในประเทศอินเดียและประเทศไทยได้แสดงให้เห็นแล้วถึง การประยุกต์ใช้คอมพิวเตอร์ควอนตัมในวิทยาการเข้ารหัส และอาชญากรทางไซเบอร์ก็กำลังจับตามองการพัฒนาดังกล่าวอย่างใกล้ชิด

นี่คือเหตุผลที่รายการระดับงานวิจัยด้านความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับควอนตัมของโตชิบาเพื่อให้ ทำหันต่อผู้ไม่ประสงค์ดีเหล่านี้ เมื่อปลายเดือนสิงหาคมที่ผ่านมา ทางบริษัทได้ประกาศความร่วมมือกับ SpeQtral บริษัทด้านเทคโนโลยีควอนตัมที่ตั้งอยู่ที่ประเทศสิงคโปร์ เพื่อเสนอโซลูชันด้านการสื่อสารที่ปลอดภัยในเชิงควอนตัมที่ได้รับการสนับสนุนจากเทคโนโลยีการกระจายกุญแจเข้ารหัสเชิงควอนตัม (QKD) ของโตชิบา

การกระจายกุญแจเข้ารหัสเชิงควอนตัมคืออะไร

การกระจายกุญแจเข้ารหัสเชิงควอนตัม (QKD)

ใช้ในการกระจายรหัสลับดิจิทัลที่สำคัญเพื่อปกป้องข้อมูลที่มีความละเอียดอ่อนสูงที่จำเป็นอย่างยิ่งต่ออุตสาหกรรมหลายภาคส่วน

ข้อมูลที่ปลอดภัยจะเข้าถึงได้เฉพาะเมื่อรหัสดิจิทัลที่ถูกต้องอยู่ในมือของผู้รับแล้วเท่านั้น

แต่ปัญหาคือรหัสดิจิทัลอาจถูกขโมยหรือถูกใช้ในทางที่ผิดได้

แฮ็กเกอร์ทางไซเบอร์สามารถปลดล็อกข้อมูลที่ขโมยมาได้โดยใช้รหัสที่มีความปลอดภัยบกพร่องได้

ส่วนสำคัญของการรักษาความปลอดภัยด้วย QKD ขึ้นอยู่กับการเข้ารหัสแต่ละบิตผ่านโฟตอน (อนุภาคของแสง) แต่ละตัวที่ถูกส่งออกมา ตัวอย่างเช่น ผ่านเส้นใยแก้วนำแสงทั่วไป เนื่องจากความพยายามในการอ่านโฟตอนจะเปลี่ยนการเข้ารหัสที่ทำไว้ จึงทำให้การรักษาความลับของรหัสแต่ละตัวสามารถได้รับการทดสอบและยืนยันได้ นอกจากนี้ QKD

ยังคงมีความปลอดภัยแม้จะมีความก้าวหน้าทางด้านคณิตศาสตร์และการประมวลผลในอนาคต

รวมถึงพลังในการประมวลผลข้อมูลของคอมพิวเตอร์ควอนตัมอีกด้วย

ซึ่งไม่เหมือนกับโซลูชันด้านความปลอดภัยอื่นที่มีอยู่ในปัจจุบัน

ด้วยเทคโนโลยี QKD ข้อมูลที่เข้ารหัสไม่เพียงแต่จะปลอดภัยจากการปลดล็อก แต่ความพยายามใดๆ ในการแฮ็กรหัสดิจิทัลยังถูกตรวจจับได้ตั้งแต่นั้นๆ จึงมั่นใจได้ว่าข้อมูลและข้อความต่างๆ จะเข้าถึงได้โดยผู้รับที่ตั้งใจไว้เท่านั้น

ในภูมิภาคเอเชียตะวันออกเฉียงใต้ มหาวิทยาลัยแห่งชาติสิงคโปร์ (National University of Singapore) กำลังดำเนินการเพื่อให้เทคโนโลยี QKD ใช้งานได้อย่างแพร่หลายมากขึ้นในอุตสาหกรรมเพื่อปกป้อง "ตัวเข้ารหัสที่ทนต่อควอนตัม" ประเภทใหม่ลงในบริการด้านการเงิน ภาครัฐ และธุรกิจด้านการดูแลสุขภาพ ที่ทำงานร่วมกับข้อมูลที่มีความละเอียดอ่อนสูง

นอกจากนี้ ประเทศไทยก็มีการค้นคว้าวิจัยด้านวิทยาการเข้ารหัสที่เข้มข้น

มหาวิทยาลัยเชียงใหม่ได้ร่วมมือกับศูนย์ความเป็นเลิศด้านฟิสิกส์ในการศึกษาระบบการดักจับอะตอมเดี่ยว

นอกจากนี้ยังมีมหาวิทยาลัยอื่นที่กำลังศึกษาเทคโนโลยีควอนตัม เช่น มหาวิทยาลัยเทคโนโลยีสุรนารี

สถาบันมาตรวิทยาแห่งชาติ รวมถึงกิจการเพื่อสังคมอย่าง บริษัท ควอนตัมเทคโนโลยีฟาวเดชั่น

(ประเทศไทย) จำกัดอีกด้วย ประเทศไทยยังทำงานร่วมกับห้องปฏิบัติการวิจัยระดับโลกในอเมริกา จีน ญี่ปุ่น และรัสเซียเพื่อแลกเปลี่ยนความคิดเห็นในการวิจัยด้วย

ตัวอย่างการใช้งาน QKD ในการรักษาความปลอดภัยทางไซเบอร์ในปัจจุบันมีนับไม่ถ้วน ตั้งแต่

การถ่ายโอนข้อมูลด้านจีโนมที่ละเอียดอ่อนไปจนถึงการถ่ายโอนข้อมูลระหว่างโครงสร้างพื้นฐานที่มีความสำคัญทางอุตสาหกรรม



นายฮิโรชิ ฟูกุจิ ผู้แทนองค์กรประจำภูมิภาคเอเชีย แปซิฟิก บริษัท โตชิบา คอร์ปอเรชั่น และกรรมการผู้จัดการ บริษัท โตชิบา เอเชีย แปซิฟิค พีทีอี แอลทีดี กล่าวว่า “ภูมิภาคเอเชียตะวันออกเฉียงใต้เป็นฐานด้านการพัฒนาและการตลาดที่มีศักยภาพอย่างมากสำหรับ QKD โตชิบาได้สร้างพาร์ตเนอร์ทางอุตสาหกรรมไว้ในช่วงแรกที่เราปรับใช้เทคโนโลยีควอนตัมในประเทศญี่ปุ่น สหรัฐอเมริกา และสหราชอาณาจักร เราตื่นเต้นที่ได้เป็นส่วนหนึ่งที่ทำให้อุตสาหกรรม QKD ของโลกขยายตัวและออกสู่ตลาดในประเทศสิงคโปร์และภูมิภาคเอเชียตะวันออกเฉียงใต้”

การร่วมมือกับอาชญากรรมทางไซเบอร์ด้วย QKD

ย้อนกลับไปในปี 2003 โตชิบาได้เป็นผู้บุกเบิกในการค้นคว้าวิจัยวิทยาการเข้ารหัสเชิงควอนตัมที่ Cambridge Research Laboratory ของ Toshiba Research Europe Limited ในปี 2004 กลุ่มบริษัทได้กลายเป็นรายแรกที่ประกาศว่าสามารถกระจายกุญแจเข้ารหัสเชิงควอนตัมผ่านสายสัญญาณที่มีความยาวมากกว่า 100 กิโลเมตรได้สำเร็จ และเป็นรายแรกที่มีอัตราการเข้ารหัสต่อเนื่องเกิน 1Mbps ในปี 2010 และเกิน 10Mbps ในปี 2017

ปัจจุบัน ด้วยกระแสการเร่งให้เกิดการเปลี่ยนแปลงให้เป็นดิจิทัลทั่วโลก ปริมาณของข้อมูลดิจิทัลที่ถูกใช้และถูกเก็บไว้จะเพิ่มสูงขึ้นมากด้วยอัตราที่เป็นทวีคูณ จากแนวโน้มนี้ เราได้เห็นการร้องเรียนจำนวนมากเกี่ยวกับภัยด้านอาชญากรรมทางไซเบอร์ที่เข้ามาขโมยและสร้างรายได้จากข้อมูลที่มีค่า

และนี่คือจุดที่เทคโนโลยี QKD ของโตชิบาจะเข้ามามีความสำคัญมากกว่าที่เคย ความร่วมมือกับ SpeQtral จะทำให้ผู้ที่อาจกลายเป็นผู้ใช้ในภูมิภาคเอเชียตะวันออกเฉียงใต้มีความเข้าใจถึงความจำเป็นและพิจารณาใช้โซลูชัน QKD เพื่อรักษาความปลอดภัยแก่การสื่อสารของตน โดยเราเริ่มจากการจัดสัมมนาบนเว็บและเวิร์กช็อปเพื่อแบ่งปันความรู้โดยไม่มีค่าใช้จ่าย



ในฐานะที่เป็นศูนย์กลางระดับโลกในแอปพลิเคชันด้านการเงิน ประเทศสิงคโปร์จึงเป็นจุดสำคัญสำหรับการโทรคมนาคม ศูนย์ข้อมูล และโครงสร้างพื้นฐานด้านการเชื่อมต่อกับระบบคลาวด์ อุตสาหกรรมเหล่านี้ประมวลผลข้อมูลที่มีความสำคัญและมีมูลค่าสูงอย่างยิ่ง จึงจำเป็นที่จะต้องมีการทบทวนความปลอดภัยอย่างต่อเนื่องเกี่ยวกับการสื่อสารเหล่านี้ รวมถึงการพัฒนาระบบปัจจุบันให้รับมือต่อภัยในอนาคตได้

นอกจากนี้ เนื่องจากแต่ละองค์กรมีการกำหนดการเชื่อมต่อข้อมูลและความต้องการด้านการรักษาความปลอดภัยที่ต่างกัน ความร่วมมือระหว่าง SpeQtral และโตชิบาจะช่วยมอบโซลูชัน QKD เพื่อตอบสนองต่อความต้องการที่ต่างกัน

เป็นผู้นำโลกในการพัฒนา QKD

การค้นคว้าวิจัยด้านควอนตัมมาหลายทศวรรษของโตชิบาได้นำไปสู่การพัฒนาอุปกรณ์ QKD สองอย่างที่ใช้งานได้จริงเพื่อการติดตั้งในการใช้งานแบบมัลติเพล็กซ์ (สูงสุด 70 กม.) และการใช้งานในระยะไกล (สูงสุด 120 กม.)

ผลิตภัณฑ์ทั้งสองที่พร้อมจำหน่ายสู่ตลาดได้รับการออกแบบมาให้ปรับใช้งานได้อย่างยืดหยุ่นและคุ้มค่า จึงทำให้นักวิจัยด้านควอนตัมในภูมิภาคเอเชียตะวันออกเฉียงใต้และในโลกทำการค้นคว้าได้มากขึ้นด้วยต้นทุนที่คุ้มค่าและเชื่อถือได้

ในขณะเดียวกัน

การกระจายกฎแฉเข้ารหัสเชิงควอนตัมเป็นขั้นส่วนสำคัญเพื่อรักษาการสื่อสารข้อมูลให้ปลอดภัยจากเศรษฐกิจดิจิทัลที่เกิดขึ้นจากการเร่งปรับใช้เทคโนโลยี

การผสมรวมโครงสร้างพื้นฐานด้านโทรคมนาคมที่เกิดขึ้นใหม่ และการใช้งานเครือข่าย 5G

นั่นเป็นเหตุผลที่โตชิบายังคงลงทุนในการศึกษาวิจัยเชิงลึกเกี่ยวกับ QKD และสาขาที่เกี่ยวข้องในวิทยาศาสตร์ควอนตัมอย่างต่อเนื่องเพื่อให้เป็นประโยชน์ในการป้องกันภัยทางไซเบอร์ล่วงหน้าให้แก่หน่วยงานรัฐ สถานศึกษา และอุตสาหกรรม

ในแง่บวก

ควอนตัมอินเทอร์เน็ตแห่งอนาคตจะนำพาประโยชน์จากความก้าวหน้าทางเทคโนโลยีในยุคใหม่มาให้แก่โลกใบนี้ นี่คือนวัตกรรมที่โตชิบา คอร์ปอเรชั่น ซึ่งมีพันธกิจที่จะเร่งสร้างนวัตกรรมและความเชื่อมั่นเพื่อช่วยเหลือโลกใบนี้ในทุกระดับ มุ่งมั่นอย่างเต็มที่

หากต้องการข้อมูลเพิ่มเติม โปรดไปที่ [โตชิบา เอเชีย แปซิฟิค](#)

หากต้องการดูเรื่องราวเพิ่มเติม โปรดไปที่ [Toshiba Clip](#)