Software Park Thailand
</Code Camp>

Outline

- การดำเนินการหน่วยประมวลผล
- ระบบเครือข่ายคอมพิวเตอร์
- ความรู้พื้นฐานในการสร้างโปรแกรมคอมพิวเตอร์
- การออกแบบ การดำเนินการ และการใช้งานของอินเตอร์เน็ต
- พื้นฐานของโซเชียลมีเดีย
- แนวคิดความปลอดภัยขั้นพื้นฐาน และการเข้ารหัส (Password Hashing)

Software Park Thailand
</Code Camp>

Objective : แนวคิดความปลอดภัยขั้นพื้นฐาน และการเข้ารหัส

- การเข้ารหัสข้อมูลเบื้องต้น
- การเข้ารหัสข้อมูลที่ไม่มีการเคลื่อนไหว
- การเข้ารหัสทั้งดิสก์
- การเข้ารหัสข้อมูล ระหว่างการส่งผ่าน
- การเข้ารหัสในชั้นการขนส่ง
- การเข้ารหัสจากต้นทาง ถึงปลายทาง

รหัสผ่าน มีไว้ทำไม

- เรามีวิธีการตรวจสอบที่ปลอดภัยยิ่งขึ้น ...
- ใช้ crypto!
- keys คีย์การเข้ารหัสลับยากที่จะจำ :-) ⇒ เก็บไว้!

ประโยชน์ของรหัสผ่าน

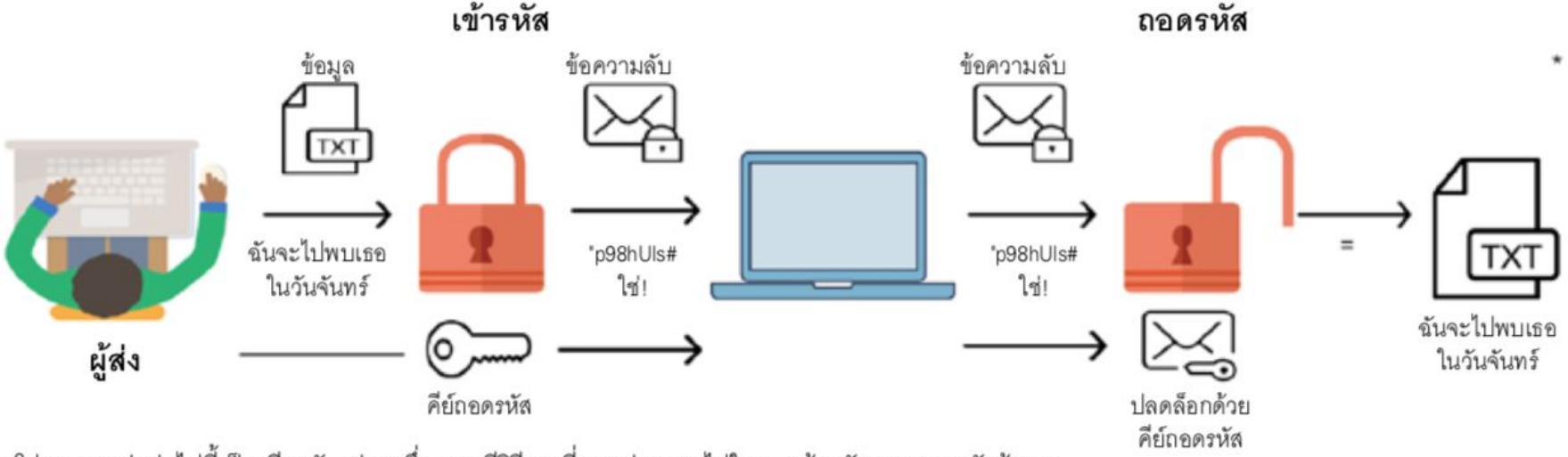
- มีวิธีป้องกันการเข้าถึงคีย์ที่จัดเก็บโดยไม่ได้รับอนุญาต
- ใช้งานง่าย และปลอดภัย!
- authentication การรับรองความถูกต้องด้วยรหัสผ่าน cheap!
  (เหตุผลหลักสำหรับระบบที่ไม่ปลอดภัยตั้งแต่ปี 2479)

การเข้ารหัสข้อมูล คืออะไร

การเข้ารหัสข้อมูล คือ วิธีการเปลี่ยนแปลงหรือปกปิดข้อความโดย การใช้ขั้นตอนต่างๆที่มีการตั้งโปรแกรมคอมพิวเตอร์ [ซอฟต์แวร์ การเข้ารหัส] เพื่อว่าหากข้อมูลตกอยู่ใน ‘มือของคนที่ไม่ใช่ผู้รับที่ต้องการ’ บุคคลที่เห็น หรืออ่านข้อความนั้น จะไม่สามารถเข้าใจข้อความดังกล่าวได้ ยกตัวอย่างเช่น มี การเปลี่ยนข้อความอย่าง เช่น “ฉันจะไปพบเธอในวันจันทร์” เป็นข้อความที่เข้ารหัส อย่างเช่น “p98hUls#yeb!”

การถอดรหัสข้อมูล

ข้อความที่อ่านไม่เข้าใจหรือข้อความลับนี้จะถูกส่งให้ผู้รับผ่าน ทางอินเทอร์เน็ต ผู้รับข้อความต้องมี ‘คีย์ถอดรหัส’ ที่ผู้ส่งได้มอบให้ผู้รับไว้โดยที่ผู้อื่นไม่ทราบ เพื่อใช้ปลดล็อก หรือกู้ข้อความเดิมกลับมา กระบวนการดังกล่าว เรียกว่า การถอดรหัสข้อมูล หากไม่มีคีย์ดังกล่าว จะไม่สามารถอ่านข้อความได้ หรือไม่สามารถดูรูปภาพได้



* โปรดทราบว่าต่อไปนี้เป็นเพียงตัวอย่างหนึ่ง และมีวิธีการที่แตกต่างออกไปในการเข้ารหัสและถอดรหัสข้อมูล

การเข้ารหัสข้อมูลที่ไม่มีการเคลื่อนไหว คืออะไร

ข้อมูล “ที่ไม่มีการเคลื่อนไหว” คือ ข้อมูลที่จัดเก็บไว้ที่ใดที่หนึ่ง ไม่ว่าจะเป็นอุปกรณ์มือถือ แล็ปท็อป เซิร์ฟเวอร์ หรือฮาร์ดไดรฟ์ภายนอก เป็นต้น เมื่อไม่มีการเคลื่อนไหว ข้อมูลจะไม่เคลื่อนย้ายจากที่หนึ่งไปยังอีกที่หนึ่ง

การเข้ารหัสทั้งดิสก์ คืออะไร

ตัวอย่างของรูปแบบการเข้ารหัสที่ปกป้องข้อมูลที่ไม่มีการเคลื่อนไหวคือ **“ การเข้ารหัสทั้งดิสก์ (full-disk encryption) ”** (บางครั้งเรียกว่า “การเข้ารหัสอุปกรณ์”) การเปิดใช้ การเข้ารหัสทั้งดิสก์ จะเข้ารหัสข้อมูลทั้งหมดที่เก็บไว้ในอุปกรณ์ และปกป้องข้อมูลโดยใช้กลุ่มคำรหัสผ่าน หรือการตรวจสอบยืนยันวิธีอื่น คุณสมบัตินี้ในอุปกรณ์มือถือ หรือแล็ปท็อปจะดูเหมือนหน้าจอล็อก โดยทั่วไปของอุปกรณ์ ซึ่งต้องมีการป้อนรหัสผ่าน กลุ่มคำรหัสผ่าน หรือสแกนลายนิ้วมือ อย่างไรก็ตามการล็อกอุปกรณ์ (เช่น การต้องป้อนรหัสผ่านเพื่อ “ปลดล็อก” อุปกรณ์ของคุณ) ไม่ได้หมายความว่ามีการเปิดใช้งานการเข้ารหัสทั้งดิสก์

การเข้ารหัสทั้งดิสก์

สมาร์ทโฟนและแล็ปท็อปที่แต่ละอุปกรณ์มีหน้าจอ “ล็อก” ที่ปกป้องด้วยรหัสผ่าน

การเข้ารหัสทั้งดิสก์ (ต่อ)

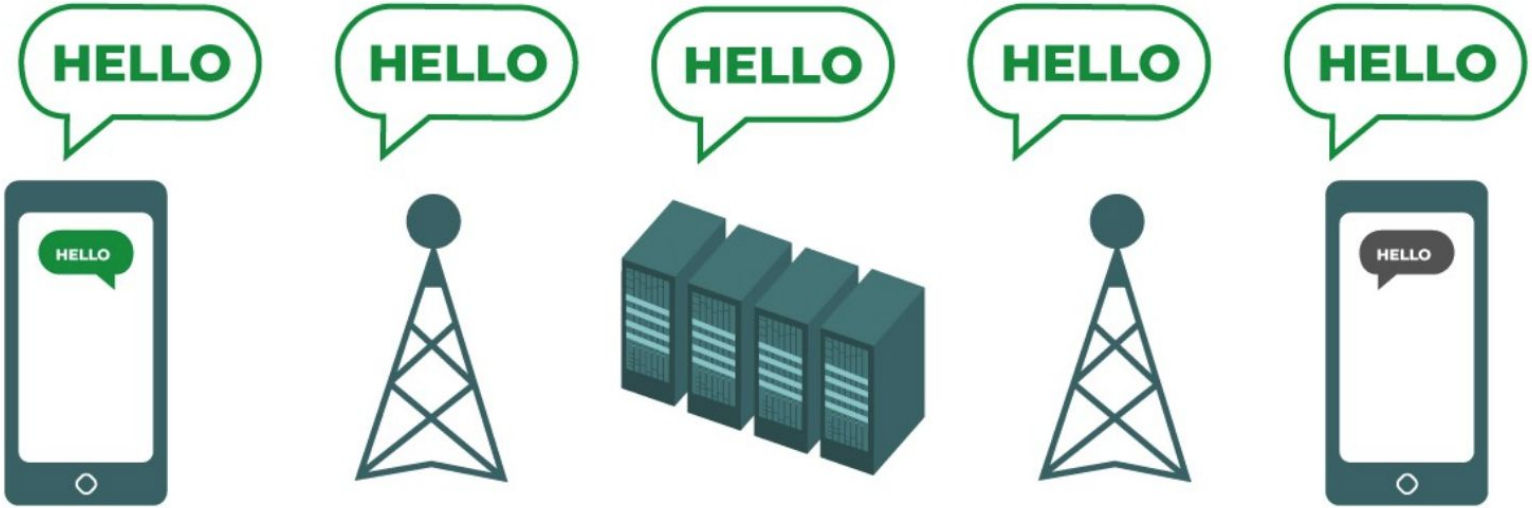
ตรวจให้แน่ใจว่าระบบปฏิบัติการของอุปกรณ์ที่คุณใช้งานใช้วิธีใดในการเปิดใช้งานและจัดการการเข้า รหัสทั้งดิสก์ ระบบปฏิบัติการบางระบบมีการเปิดใช้งานการเข้ารหัสทั้งดิสก์ตามค่าเริ่มต้น ขณะที่บางระบบไม่ได้มีการเปิดใช้ นั่นหมายความว่า ใครก็ตามสามารถเข้าถึงข้อมูลในอุปกรณ์มือถือของคุณได้เพียงแค่ปลดล็อกอุปกรณ์เท่านั้น โดยไม่ต้องปลดล็อกคีย์การเข้ารหัส เนื่องจากอุปกรณ์ ไม่ได้มีการเข้ารหัสไว้ บางระบบยังจัดเก็บ ข้อมูลในรูปแบบเพลนเท็กซ์ไว้ใน RAM ถึงแม้จะมีการใช้การเข้ารหัสทั้งดิสก์ก็ตาม RAM คือพื้นที่จัดเก็บข้อมูลชั่วคราว ซึ่งหมายความว่าหลังจากมีการปิดอุปกรณ์ ไม่นาน โดยทั่วไปจะไม่สามารถอ่านข้อมูลในหน่วยความจำได้ แต่ผู้ไม่ประสงค์ดีที่มีความเชี่ยวชาญ สามารถใช้ การโจมตีแบบโคลด์บูต (cold boot attack) และนำเนื้อหา ที่สามารถอ่านได้ใน RAM ไป

การป้องกันตัวจากการสอดแนม

ใน “**การป้องกันตัวจากการสอดแนม (Surveillance Self-Defense)**” เราได้จัดทำคู่มือสำหรับการเปิดใช้งานการเข้ารหัสในอุปกรณ์ ถึงแม้จะมีคำ อธิบายแบบละเอียดเกี่ยวกับตัวเลือกการเข้ารหัสข้อมูลที่ไม่เคลื่อนไหวที่สามารถค้นหาได้ ทางออนไลน์ (และมีอยู่ในข้อมูลของ Surveillance Self-Defense หรือ SSD ด้วย!) แต่ขอให้ระวังว่าตัวเลือกเหล่านี้มีการเปลี่ยนแปลงอยู่บ่อยครั้งและคำแนะนำที่มีอาจล้าสมัยได้อย่างรวดเร็ว

Software Park Thailand
</Code Camp>

การเข้ารหัสข้อมูล ระหว่างการส่งผ่าน



Software Park Thailand
</Code Camp>

ข้อมูลระหว่างการส่งผ่าน (ต่อ)

การตรวจสอบว่าบทสนทนาระหว่างคุณและผู้รับข้อความมีการเข้ารหัสถือเป็นสิ่งสำคัญ รวมทั้งการรับทราบว่าบทสนทนาถูกเข้ารหัสผ่าน **การเข้ารหัสในชั้นการขนส่ง (transport-layer encryption)** หรือ **การเข้ารหัสจากต้นทางถึงปลายทาง (end-to-end encryption)**.

มีสองวิธีในการเข้ารหัสข้อมูลระหว่างการส่งผ่าน ได้แก่ **การเข้ารหัสในชั้นการขนส่ง (transport-layer encryption)** และ **การเข้ารหัสจากต้นทางถึงปลายทาง (end-to-end encryption)** ประเภทการเข้ารหัส ที่ผู้ให้บริการรองรับถือเป็นปัจจัยสำคัญในการตัดสินว่า การบริการใดเหมาะสำหรับการใช้งานของคุณ ตัวอย่างด้านล่างแสดงให้เห็นความแตกต่างระหว่าง “การเข้ารหัสในชั้นการขนส่ง” และ “การเข้ารหัสจากต้นทางถึงปลายทาง”

Software Park Thailand
</Code Camp>

การเข้ารหัสในชั้นการขนส่ง (ต่อ)

นอกจากนี้ การเข้ารหัสในชั้นการขนส่งยังเรียกว่า การรักษาความปลอดภัยในชั้นการขนส่ง (transport layer security) (หรือ TLS) ซึ่งจะปกป้องข้อความขณะส่งผ่าน จากอุปกรณ์ของคุณไปยังเซิร์ฟเวอร์ของแอป และจากเซิร์ฟเวอร์ของแอปไปยังอุปกรณ์ของผู้รับ ระหว่างการส่งผ่าน ผู้ให้บริการส่งข้อความ — หรือเว็บไซต์ที่คุณเข้าดูข้อมูล หรือแอปที่คุณใช้งาน — สามารถเห็นสำเนาของข้อความที่ไม่ได้มีการเข้ารหัสได้ เนื่องจากเซิร์ฟเวอร์ของ บริษัทสามารถ เห็นข้อความของคุณได้ (และมักมีการจัดเก็บข้อความไว้ในเซิร์ฟเวอร์) ทำให้ข้อความดังกล่าวเสี่ยงต่อ การร้องขอของหน่วยงานบังคับใช้กฎหมายหรือการรั่วไหลในกรณีที่เซิร์ฟเวอร์ของบริษัทตกอยู่ในอันตราย

การเข้ารหัสในชั้นการขนส่ง (ต่อ)

ตัวอย่างการเข้ารหัสในชั้นการขนส่ง : HTTPS

การเข้ารหัสในชั้นการขนส่ง (ต่อ)

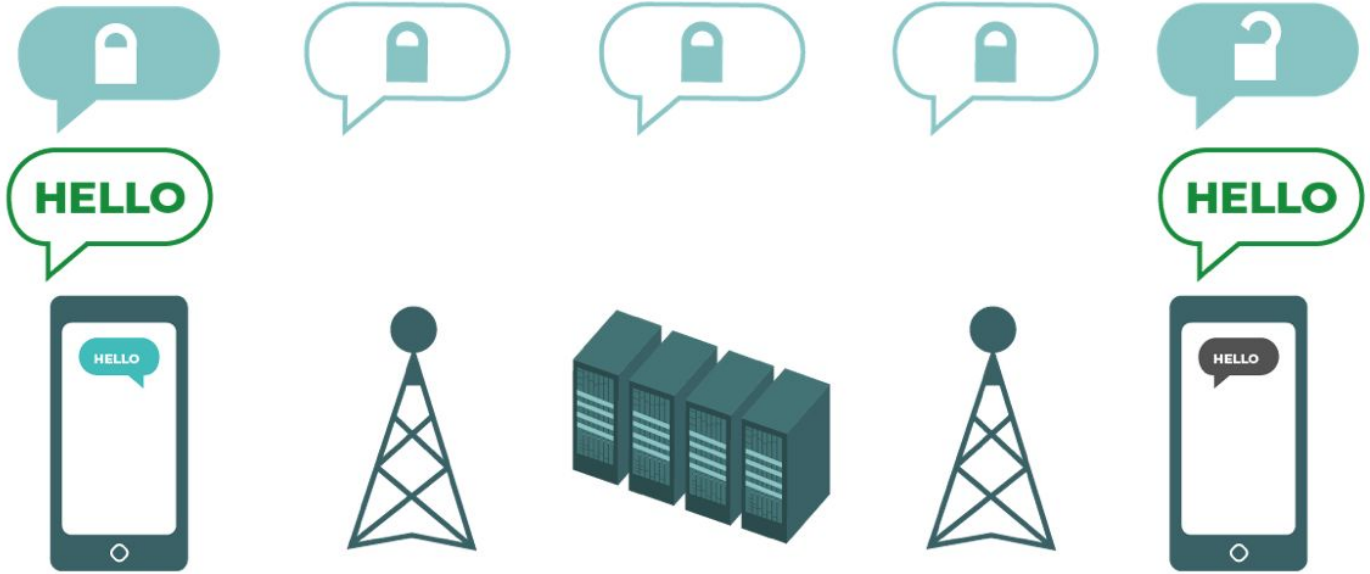
คุณสังเกตเห็นตัวล็อกสีเขียว “https://” ข้างที่อยู่เว็บ ssd.eff.org ในส่วนที่อยู่เว็บของหน้าต่างเบราว์เซอร์หรือไม่ HTTPS คือ ตัวอย่างของการเข้ารหัส ในชั้นการขนส่ง ที่เราพบเห็นอยู่บ่อยครั้งบนเว็บ รูปแบบดังกล่าวมีการรักษาความปลอดภัยมากกว่า HTTP ที่ไม่มีการเข้ารหัส เหตุผลคือ เซิร์ฟเวอร์ของเว็บไซต์ HTTPS ที่คุณเรียกดู ข้อมูลสามารถเห็นข้อมูลที่คุณป้อนในเว็บไซต์ของตน (เช่น ข้อความ, การค้นหา, หมายเลขบัตรเครดิต และข้อมูลล็อกอิน) แต่ผู้ที่เข้ามาสอดแนมจะไม่สามารถอ่านข้อมูล นี้ได้บนเครือข่าย

การเชื่อมต่อแบบ HTTP

การเชื่อมต่อแบบ HTTP ไม่มีคุณสมบัติการปกป้องหากมีใครแอบเข้ามา สอดแนมเครือข่าย และพยายามดูว่าเว็บไซต์ใดที่ผู้ใช้เข้าดูข้อมูล ในทางตรงข้าม การเชื่อมต่อด้วย HTTPS จะซ่อนเพจบางเพจในเว็บไซต์ที่คุณเข้าดูข้อมูล — ซึ่งคือทุกข้อมูล “หลังจากเครื่องหมายสแลช” ตัวอย่างเช่น หากคุณใช้ HTTPS เพื่อเชื่อมต่อกับเว็บไซต์ “https://ssd.eff.org/en/module/what-encryption” ผู้ที่เข้ามาสอดแนมจะเห็นเพียง “https://ssd.eff.org” เท่านั้น

Software Park Thailand
</Code Camp>

การเข้ารหัสจากต้นทาง ถึงปลายทาง



การเข้ารหัสจากต้นทาง ถึงปลายทาง (ต่อ)

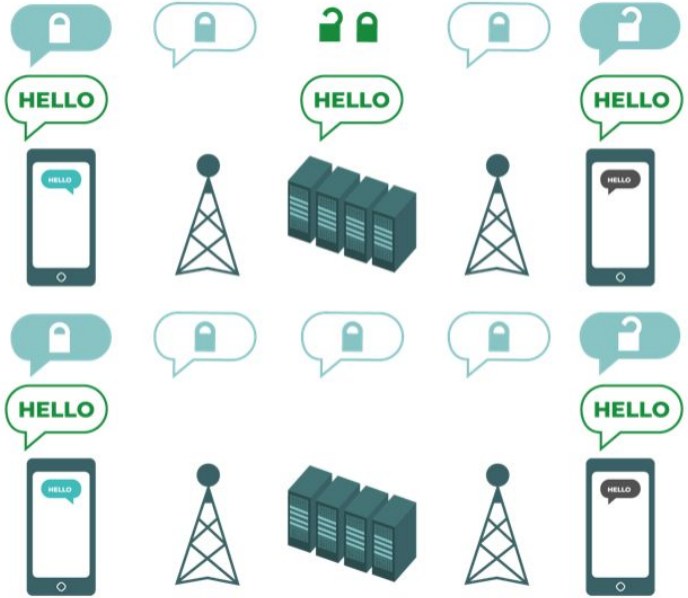
การเข้ารหัสจากต้นทางถึงปลายทางจะปกป้องข้อความในระหว่างการส่งผ่านจากผู้ส่งไปจนถึงผู้รับ วิธีการดังกล่าวจะทำให้ผู้ส่งต้นทางเปลี่ยนข้อมูลเป็นข้อความลับ (“จุดการสื่อสาร” ต้นทาง) และเฉพาะผู้รับปลายทาง (“จุดการสื่อสาร” ปลายทาง) เท่านั้นที่จะสามารถปลดล็อกข้อความดังกล่าวได้ ไม่มีใคร หรือแม้แต่แอป ที่คุณใช้งานที่จะสามารถ “แอบฟัง” และสอดแนมกิจกรรมของคุณได้

การเข้ารหัสจากต้นทาง ถึงปลายทาง (ต่อ)

การใช้งานข้อความที่มีการเข้ารหัสจากต้นทางถึงปลายทางในแอปที่ติดตั้งในอุปกรณ์ที่คุณใช้งานจะทำให้บริษัทที่สร้างแอปไม่สามารถอ่านข้อความดังกล่าวได้ ซึ่งถือเป็นคุณลักษณะสำคัญของการเข้ารหัสที่ดี : ซึ่งแม้แต่ผู้ที่ออกแบบ และเปิดใช้การเข้ารหัสยังไม่สามารถทำลายการป้องกันดังกล่าวได้

Software Park Thailand
</Code Camp>

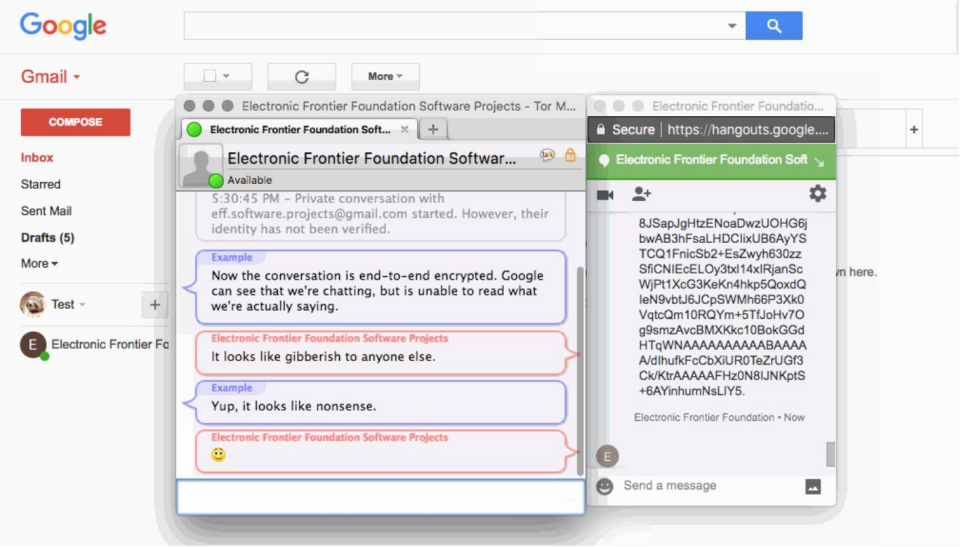
จะใช้การเข้ารหัสในชั้นการขนส่ง หรือการเข้ารหัสจากต้นทางถึงปลายทางดี



เราได้สร้างภาพเคลื่อนไหวด้านล่างเพื่อสาธิตให้เห็นวิธีการทำงานของการเข้ารหัสจากต้นทางถึงปลายทางและการเข้ารหัสในชั้นการขนส่งสำหรับข้อมูลที่อยู่ระหว่างการส่งผ่านทางด้านซ้าย คือ เครื่องมือ แชทสำหรับการเข้ารหัสจากต้นทางถึงปลายทาง (หน้าต่างแชทที่ใช้ Off-the-Record (ไม่มีการบันทึกข้อมูล) (หรือ “OTR”)

โปรโตคอลการส่งข้อความแบบทันทีที่มีการเข้ารหัส

โปรโตคอลการส่งข้อความแบบทันทีที่มีการเข้ารหัส) ทางด้านขวา คือ หน้าต่างแชท สำหรับการเข้ารหัส ในชั้นการขนส่ง (เข้ารหัสผ่านการใช้ HTTPS ในเว็บไซต์ของ Google Hangout)

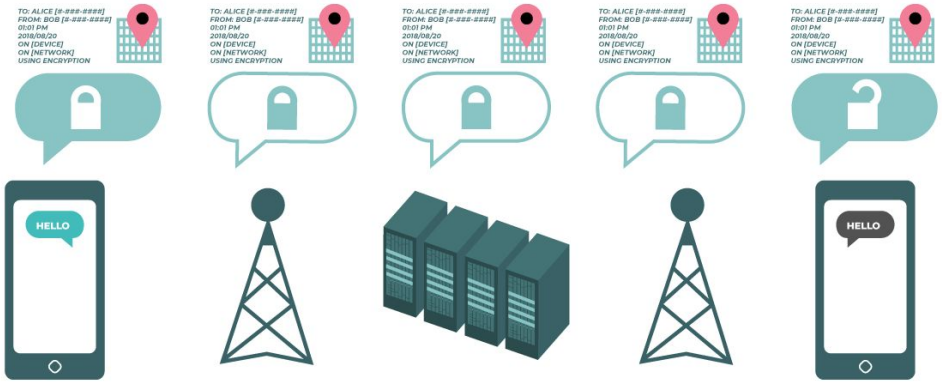


สิ่งที่ไม่ได้เกิดขึ้นในการเข้ารหัสระหว่างการส่งผ่านข้อมูล

การเข้ารหัสไม่ใช่วิธีการแก้ปัญหาแบบครอบคลุมครบวงจร ถึงแม้คุณจะส่งข้อความที่ผ่านการเข้ารหัส ข้อความดังกล่าวจะถูกปลดล็อกโดยบุคคลที่คุณสื่อสารด้วย หากจุดรับการสื่อสาร (อุปกรณ์ที่คุณใช้ในการสื่อสาร) ตกอยู่ในความเสี่ยง การสื่อสารที่ผ่านการเข้ารหัสก็อาจตกอยู่ในความเสี่ยงด้วย นอกจากนี้ บุคคลที่คุณสื่อสารด้วยสามารถถ่ายภาพหน้าจอหรือเก็บบันทึก (การบันทึกข้อมูล) ข้อมูลการสื่อสารของคุณได้

สิ่งที่ไม่ได้เกิดขึ้นในการเข้ารหัสระหว่างการส่งผ่านข้อมูล (ต่อ)

หากคุณจัดเก็บการสำรองข้อมูลของการสนทนาที่ผ่านการเข้ารหัสไว้ใน “คลาวด์” (คอมพิวเตอร์เครื่องอื่น) อย่าลืมตรวจสอบว่ามีการเข้ารหัสข้อมูลที่สำรองด้วย เช่นกัน เพื่อให้แน่ใจได้ว่ามีการเข้ารหัสการสนทนา ของคุณทั้งในระหว่างการส่งผ่านและในช่วงเวลาอื่น ๆ ทั้งหมดด้วย



การใช้งานร่วมกัน

เมื่อใช้ร่วมกัน การเข้ารหัสทั้งข้อมูลระหว่างการส่งผ่าน และข้อมูลที่ไม่มีการเคลื่อนไหว จะทำให้การรักษาความปลอดภัย มีความครอบคลุม มากกว่าการใช้การเข้ารหัสเพียงรูปแบบเดียว นี่คือวิธีการ ที่ผู้เชี่ยวชาญในการรักษาความปลอดภัย ของข้อมูลเรียกว่า “การป้องกันแบบครอบคลุม” การใช้วิธีการต่าง ๆ ที่หลากหลายเพื่อปกป้องข้อมูลจะทำให้คุณได้รับการปกป้อง ในระดับที่ครอบคลุมกว่า