ไมโครชิพ เปิดตัวโซลูชั่น Pre-provisioned ครั้งแรกของวงการ รองรับการใช้งานทุกขนาด ช่วยให้การรักษาความปลอดภัย IoT บนฮาร์ดแวร์เป็นเรื่องง่าย

– Trust Platform ของไมโครชิพ ช่วยให้การจัดเก็บข้อมูลสำคัญบนฮาร์ดแวร์มีความปลอดภัย สำหรับการใช้งานในปริมาณต่ำ ปานกลาง และปริมาณมาก พร้อมเปิดให้สั่งซื้อแล้ววันนี้ในจำนวนขั้นต่ำเพียง 10 ยูนิต

อุปกรณ์เชื่อมต่อในปัจจุบันมีจำนวนและประเภทเพิ่มมากขึ้นอย่างรวดเร็ว ทำให้เกิดการแบ่งส่วนตลาดและเกิดช่องโหว่ด้านความมั่นคงปลอดภัยในอินเทอร์เน็ตออฟธิงส์ (IoT) ซึ่งนับเป็นความท้าทายที่สำคัญสำหรับบรรดานักพัฒนา ความมั่นคงปลอดภัยของฮาร์ดแวร์ถือเป็นวิธีเดียวที่จะช่วยปกป้องกุญแจสำคัญจากการโจมตีทางกายภาพ (physical attack) และการสกัดจากระยะไกล (remote extraction) แต่การกำหนดค่าและจัดสรรพื้นที่จัดเก็บสำหรับอุปกรณ์แต่ละชิ้นต้องอาศัยความเชี่ยวชาญด้านความมั่นคงปลอดภัยอย่างครอบคลุม เช่นเดียวกับเวลาและต้นทุนในการพัฒนาก็เป็นสิ่งจำเป็น และเนื่องจากบริษัทต่าง ๆ ผลิตอุปกรณ์เชื่อมต่อตั้งแต่หลักร้อยถึงหลักล้านต่อปีจากทุกที่ทั่วโลก ความสามารถในการขยายสถาปัตยกรรมจึงอาจกลายเป็นอุปสรรคใหญ่ที่ขัดขวางการดำเนินการ ขณะที่ผู้ผลิตโดยทั่วไปทำได้เพียงสนับสนุนการกำหนดค่าและการแบ่งพื้นที่เพื่อรองรับคำสั่งซื้อปริมาณมากเท่านั้น ส่งผลให้บริษัทขนาดเล็กถึงกลางไม่มีทางเลือกมากนัก ดังนั้น เพื่อตอบสนองความต้องการดังกล่าวในตลาดใหญ่ บริษัท ไมโครชิพ เทคโนโลยี จำกัด (Nasdaq: MCHP) จึงขอแนะนำโซลูชั่นแบบ Pre-provisioned ตัวแรกของวงการที่ช่วยให้จัดเก็บข้อมูลสำคัญได้อย่างปลอดภัยสำหรับการใช้งานอุปกรณ์ในปริมาณต่ำ กลาง และสูงโดยใช้ชิป

secure element รุ่น ATECC608A ทั้งนี้ Trust Platform สำหรับตระกูล CryptoAuthentication(TM) ของไมโครชิพ ทำให้บริษัททุกขนาดสามารถดำเนินการพิสูจน์ตัวตนอุปกรณ์ได้อย่างปลอดภัยและง่ายดาย

Trust Platform ของไมโครชิพ ประกอบด้วยชิป secure element แบบ 3 ชั้น พร้อมใช้งานได้ทันที ซึ่งได้แก่ pre-provisioned, pre-configured หรือ fully customizable ที่สามารถปรับแต่งได้อย่างเต็มที่ จึงทำให้นักพัฒนาสามารถเลือกแพลตฟอร์มที่เหมาะกับการออกแบบของตนเองมากที่สุด โดย Trust&GO เป็นโซลูชั่นตัวแรกที่มอบการพิสูจน์ตัวตนอย่างปลอดภัยแบบสำเร็จรูปเพื่อรองรับตลาดใหญ่ เป็นชิป secure element แบบ pre-provisioned ที่ติดตั้งได้ง่าย (zero touch) และสามารถสั่งซื้อในปริมาณขั้นต่ำ (MOQ) เพียง 10 ยูนิต ขณะที่ข้อมูลรับรองอุปกรณ์ (credentials) ถูกตั้งโปรแกรมมาแล้ว อีกทั้งถูกติดตั้งไว้ภายใน ATECC608A เพื่อการขึ้นระบบคลาวด์โดยอัตโนมัติ หรือการพิสูจน์ตัวตน LoRaWAN(TM) พร้อมกันนี้ ใบรับรองที่เกี่ยวข้อง และกุญแจสาธารณะ (public keys) จะถูกส่งมอบในรูปแบบไฟล์ “manifest” ซึ่งสามารถดาวน์โหลดได้ผ่านทางร้านอีคอมเมิร์ซ และพันธมิตรตัวแทนจำหน่ายชั้นนำของไมโครชิป นอกจากจะช่วยประหยัดเวลาพัฒนาได้หลายเดือนแล้ว โซลูชั่นนี้ยังลดความยุ่งยากด้านโลจิสติกส์ลงได้เป็นอย่างมาก ทำให้เป็นเรื่องง่ายสำหรับลูกค้าในตลาดใหญ่ที่จะสร้างความปลอดภัยและบริหารจัดการอุปกรณ์ในระบบ edge ได้โดยไม่ต้องมีค่าใช้จ่ายในการดำเนินธุรกิจจากการให้บริการแบบบุคคลที่ 3 หรือผู้ให้บริการออกใบรับรอง

ด้วยความสามารถในการพิสูจน์ตัวตนกับโครงสร้างพื้นฐานคลาวด์ทั้งแบบสาธารณะหรือแบบส่วนตัว Trust Platform ของไมโครชิพจึงมีความยืดหยุ่น และสามารถปรับแต่งได้ โดยสำหรับลูกค้าที่ต้องการการปรับแต่งมากขึ้น โปรแกรมนี้มีแพลตฟอร์ม TrustFLEX และ TrustCUSTOM รวมอยู่ด้วย โดย TrustFLEX ซึ่งเป็นชั้นที่สองในโปรแกรมนี้ มอบความยืดหยุ่นในการใช้ทางเลือกในการหาผู้ให้บริการออกใบรับรองของลูกค้า ขณะเดียวกันก็ยังได้รับประโยชน์จากกรณีการใช้งานแบบกำหนดค่าไว้ก่อนด้วย กรณีการใช้งานเหล่านี้ ได้แก่ มาตรการด้านความมั่นคงปลอดภัยพื้นฐาน อาทิ การพิสูจน์ตัวตนที่เข้มข้นขึ้น Transport Layer Security (TLS) เพื่อเชื่อมโยงกับเครือข่ายบน IP ตัวใดก็ได้โดยใช้สายการออกใบรับรอง (certificate chain) สายใดก็ได้, การพิสูจน์ตัวตน LoRaWAN, ระบบบูตแบบ secure boot, การอัพเดทแบบ Over-the-air (OTA), การป้องกัน IP, การปกป้องข้อมูลผู้ใช้ และ key rotation วิธีนี้ช่วยลดเวลาและความซับซ้อนในการปรับแต่งอุปกรณ์โดยที่ไม่ต้องใช้หมายเลขชิ้นส่วนที่ปรับแต่งแล้วสำหรับลูกค้าที่ต้องการปรับแต่งดีไซน์ทั้งหมด TrustCUSTOM ซึ่งเป็นชิปชั้นที่ 3 ในโปรแกรมนี้ จะช่วยให้ลูกค้าสามารถกำหนดค่าแบบเฉพาะเจาะจงได้ อีกทั้งให้ใบรับรองแบบกำหนดค่าได้ด้วยเช่นกัน

“การโจมตีโซลูชั่นความปลอดภัยบนซอฟต์แวร์ที่ประสบความสำเร็จเพิ่มขึ้น ตอกย้ำให้เห็นถึงความจำเป็นที่บริษัทต่าง ๆ ต้องนำแนวปฏิบัติที่ดีของอุตสาหกรรมไปใช้ ซึ่งรวมถึงการแยกกุญแจส่วนตัว (private key) ในชิป secure element” Nuri Dagdeviren รองประธานธุรกิจผลิตภัณฑ์ความปลอดภัยของไมโครชิพ กล่าว “Trust Platform ของไมโครชิพทำให้การรักษาความมั่นคงปลอดภัยบนฮาร์ดแวร์เป็นเรื่องง่ายและคุ้มค่าเพื่อให้บริษัททุกขนาดนำไปใช้ได้ จึงช่วยขจัดอุปกรรคที่มักพบเจอในการกำหนดค่าและการปรับแต่งอุปกรณ์”

ไมโครชิพทำงานร่วมกับ Amazon Web Services (AWS) เพื่อช่วยให้ผลิตภัณฑ์ที่ออกแบบโดย Microchip Trust Platform รูปแบบต่างๆ สามารถเข้าสู่บริการ AWS IoT ได้อย่างง่ายดาย ไม่ยุ่งยากซับซ้อน

ATECC608A ทำให้การจัดเก็บกุญแจมีความปลอดภัยในระดับ “สูง” ตามมาตรฐาน Common Criteria Joint Interpretation Library (JIL) ทำให้ลูกค้ามั่นใจได้ว่า อุปกรณ์ใช้แนวปฏิบัติด้านความมั่นคงปลอดภัยที่ได้รับการยอมรับจากอุตสาหกรรมมาแล้ว และทำให้การจัดเก็บกุญแจมีความปลอดภัยในระดับสูงสุด และด้วยการจัดเก็บ Root-of-Trust ในระดับฮาร์ดแวร์ และมาตรการตอบโต้การเข้ารหัส อุปกรณ์ตัวนี้จึงป้องกันการโจมตีทางกายภาพได้อย่างครอบคลุมที่สุด โดยโรงงานผลิตที่ปลอดภัยของไมโครชิพจะสำรองกุญแจไว้อย่างปลอดภัย จึงรับประกันว่ากุญแจจะไม่ถูกนำไปเปิดเผยให้แก่ผู้ใดในระหว่างการสำรองหรือตลอดช่วงอายุของอุปกรณ์ตัวนี้

เครื่องมือสนับสนุนการพัฒนา

ATECC608A ใช้งานได้กับทุกระบบ และสามารถจับคู่กับไมโครคอนโทรลเลอร์และไมโครโปรเซสเซอร์แบบใดก็ได้ และเพื่อการผลิตต้นฉบับโซลูชั่นความปลอดภัยได้อย่างรวดเร็ว (rapid prototyping) นักออกแบบจะสามารถใช้ชุดเครื่องมือออกแบบ Trust Platform Design Tool Suite ซึ่งประกอบไปด้วย:

– “เครื่องมือใช้งาน” พร้อมคำแนะนำ
– วิธีใช้งานด้วยภาษาโปรแกรม Python ที่สามารถใช้งานได้บนโน้ตบุ๊ก Jupyter
– ตัวอย่างรหัสภาษา C สำหรับการใช้งานแต่ละรูปแบบ
– โปรแกรม “secret exchange”
– ชุดพัฒนาฮาร์ดแวร์ Trust Platform

ราคาและการวางจำหน่าย

อุปกรณ์ใน Trust Platform ของไมโครชิพ เปิดให้สั่งซื้อปริมาณมากแล้ววันนี้ เมื่อสั่งซื้อขั้นต่ำ (MOQ) ดังนี้:

– Trust&GO for TLS (ATECC608A-TNGTLSx-B): ราคา 1.20 ดอลลาร์ เมื่อสั่งซื้อขั้นต่ำ 10 ยูนิต*
– Trust&GO for TLS (ATECC608A-TNGTLSx-G): ราคา 0.77 ดอลลาร์ เมื่อสั่งซื้อขั้นต่ำ 2000 ยูนิต*
– Trust&GO for LoRaWAN (The Things Industries ATECC608A-TNGLORAx-B and Actility ATECC608A-TNGACTU-B): ราคา 1.40 ดอลลาร์ เมื่อสั่งซื้อขั้นต่ำ 10 ยูนิต*
– TrustFLEX for LoRaWAN สำหรับเซิร์ฟเวอร์ที่เข้าร่วม (ATECC608A-TFLXLORAx): ราคา 0.938 ดอลลาร์ เมื่อสั่งซื้อขั้นต่ำ 2000 ยูนิต*TrustFLEX (ATECC608A-TFLXTLSx): ราคา 0.845 ดอลลาร์ เมื่อสั่งซื้อขั้นต่ำ 2,000 ยูนิต*
– TrustCUSTOM (ATECC608A-TCSTMTLSx): ราคา 0.883 ดอลลาร์ เมื่อสั่งซื้อขั้นต่ำ 4,000 ยูนิต*
*uDFN (x = U) หรือ SO8 (x = S)

เครื่องมือสนับสนุนการพัฒนาใน Trust Platform ของไมโครชิพ มีจำหน่ายดังนี้:

– ชุดเครื่องมือ CryptoAuth Trust Platform Kit ราคา 13 ดอลลาร์
– ชุดเครื่องมือ ATECC608a Trust Platform Kit ราคา 14 ดอลลาร์

สามารถดูข้อมูลเพิ่มเติมและซื้อผลิตภัณฑ์ที่ระบุถึงในข่าวได้ที่ พอร์ทัลจำหน่ายผลิตภัณฑ์ ของไมโครชิพ หรือติดต่อตัวแทนจำหน่ายที่ได้รับอนุญาตจากไมโครชิพ

แหล่งข้อมูลและภาพ

ดูรูปภาพความละเอียดสูงได้ที่ Flickr หรือติดต่อกองบรรณาธิการ (สามารถนำไปเผยแพร่ได้ตามสะดวก):

ภาพการใช้งาน: https://www.flickr.com/photos/microchiptechnology/48650099116
ภาพเครื่องมือ: https://www.flickr.com/photos/microchiptechnology/48631110133

เกี่ยวกับไมโครชิพ เทคโนโลยี

บริษัท ไมโครชิพ เทคโนโลยี จำกัด เป็นผู้นำด้านการจัดหาเซมิคอนดักเตอร์สำหรับโซลูชั่นควบคุมแบบฝังที่เป็นอัจฉริยะ เชื่อมต่อ และปลอดภัย เครื่องมือพัฒนาที่ใช้งานง่าย ตลอดจนกลุ่มผลิตภัณฑ์ที่ครอบคลุม ช่วยให้ลูกค้าสามารถสร้างสรรค์งานออกแบบได้อย่างเหมาะสม ซึ่งช่วยลดความเสี่ยง ลดต้นทุนโดยรวมของทั้งระบบ และยังช่วยลดระยะเวลาในการนำผลิตภัณฑ์ออกสู่ตลาด โซลูชั่นของบริษัทให้บริการลูกค้ามากกว่า 125,000 รายในตลาดอุตสาหกรรม ยานยนต์ ผู้บริโภค อวกาศและการป้องกันประเทศ การสื่อสารและการประมวลผล สำนักงานใหญ่ของไมโครชิพตั้งอยู่ที่เมืองแชนด์เลอร์ รัฐแอริโซนา บริษัทนำเสนอการสนับสนุนด้านเทคนิคที่เป็นเลิศ พร้อมกับการขนส่งและคุณภาพที่เชื่อถือได้ สำหรับข้อมูลเพิ่มเติม สามารถเยี่ยมชมเว็บไซต์ของไมโครชิพที่ www.microchip.com