ไมโครชิพ เปิดตัวไมโครคอนโทรลเลอร์และเฟิร์มแวร์ใหม่ ช่วยป้องกันมัลแวร์ประเภท Rootkit และ Bootkit ในระบบปฏิบัติการที่บูตระบบจากหน่วยความจำแฟลชแบบ External SPI

– ไมโครคอนโทรลเลอร์แบบเข้ารหัสและเฟิร์มแวร์แบบกำหนดเองรุ่นใหม่ ตลอดจนบริการด้านการผลิตจากไมโครชิพ ได้รับการออกแบบมาเพื่อช่วยให้ระบบต่าง ๆ สามารถตรวจจับและหยุดยั้งมัลแวร์ก่อนที่ระบบปฏิบัติการจะเริ่มทำงาน

ด้วยการเติบโตอย่างรวดเร็วของ 5G ไม่ว่าจะป็นโครงสร้างพื้นฐานเซลลูลาร์ใหม่ เครือข่ายและดาต้าเซ็นเตอร์ที่รองรับการประมวลผลคลาวด์ที่กำลังขยายตัว เหล่านักพัฒนาจึงต่างมองหาวิธีการใหม่ ๆ เพื่อให้มั่นใจได้ว่าระบบปฏิบัติการยังคงความปลอดภัยสูงสุดในทุกสถานการณ์ บริษัท ไมโครชิพ เทคโนโลยี จำกัด (Nasdaq: MCHP) ตระหนักถึงความต้องการดังกล่าว และได้เปิดตัวไมโครคอนโทรลเลอร์รุ่นใหม่ CEC1712 MCU ที่รองรับการเข้ารหัส (cryptography-enabled) พร้อมด้วยเฟิร์มแวร์ Soteria-G2 แบบกำหนดเอง (custom firmware) ซึ่งได้รับการออกแบบมาเพื่อหยุดยั้งมัลแวร์อันตราย อาทิ rootkit และ bootkit สำหรับระบบปฏิบัติการต่าง ๆ ที่บูตระบบจากหน่วยความจำแฟลช external Serial Peripheral Interface (SPI) flash memory

เฟิร์มแวร์ Soteria-G2 ที่เขียนไว้ในไมโครคอนโทรลเลอร์ CEC1712 Arm(R) Cortex(R)-M4-based แบบ full-

featured จะทำหน้าที่เป็น secure boot ที่มีความปลอดภัยในระดับฮาร์ดแวร์ (hardware root of trust) โดยทำงานในโหมด pre-boot สำหรับระบบปฏิบัติการที่บูตระบบจาก external SPI flash memory นอกจากนี้ CEC1712 ยังป้องกัน key revocation และ code rollback ในระหว่างปฏิบัติการ ทำให้สามารถอัปเดตความปลอดภัยระดับฟิลด์ (in-field) ได้ CEC1712 ปฏิบัติตามแนวทาง NIST 800-193 โดยสามารถป้องกันและตรวจจับมัลแวร์ รวมทั้งกู้ระบบจากการการเรียกใช้หน่วยความจำผิดพลาด (corruption) เพื่อความยืดหยุ่นของเฟิร์มแวร์ ทั้งนี้ ระบบ secure boot ที่มีความปลอดภัยระดับฮาร์ดแวร์นับว่ามีความสำคัญอย่างยิ่งในการป้องกันระบบจากภัยคุกคาม ก่อนที่ภัยคุกคามเหล่านั้นจะโหลดตัวเองเข้าสู่ระบบได้ และจะอนุญาตให้บูตระบบได้ก็ต่อเมื่อใช้ซอฟต์แวร์ที่ได้รับการยอมรับจากผู้ผลิตเท่านั้น

เฟิร์มแวร์ Soteria-G2 ได้รับการออกแบบมาเพื่อใช้ร่วมกับโมโครคอนโทรลเลอร์ CEC1712 เพื่อช่วยให้นักออกแบบสามารถเร่งการใช้งาน secure boot โดยช่วยลดความยุ่งยากในการพัฒนารหัสและลดความเสี่ยง Soteria-G2 ใช้ CEC1712 เป็น secure bootloader ที่แก้ไขหรือเปลี่ยนแปลงไม่ได้ ซึ่งติดตั้งมาใน Read-Only Memory (ROM) เพื่อความปลอดภัยในระดับระบบ (system root of trust)

“รูทคิตเป็นมัลแวร์ที่มาในรูปของการแอบแฝงตัวโดยเฉพาะ โดยจะโหลดตัวเองขึ้นมาก่อนที่ระบบปฏิบัติการจะเริ่มทำงาน อีกทั้งสามารถซ่อนตัวจากซอฟต์แวร์ anti-malware ทั่วไป จนขึ้นชื่อว่าตรวจจับยาก” เอียน แฮร์ริส รองประธานกลุ่มผลิตภัณฑ์ประมวลผลของไมโครชิพ กล่าว “วิธีหนึ่งที่จะช่วยปกป้องระบบจากรูทคิตก็คือ secure boot ซึ่ง CEC1712 ที่มาพร้อมเฟิร์มแวร์ Soteria-G2 ได้รับการออกแบบมาเพื่อป้องกันมัลแวร์เหล่านี้ ก่อนที่พวกมันจะโหลดตัวเองเข้าสู่ระบบ”

CEC1712 เป็น secure bootloader ที่ทำหน้าที่โหลด ถอดรหัส และรับรองเฟิร์มแวร์เพื่อให้รันบน CEC1712 จาก external SPI flash โดยรหัส CEC1712 ที่ได้รับการตรวจสอบแล้ว จะรับรองเฟิร์มแวร์ที่ถูกเก็บอยู่ใน SPI flash เป็นหน่วยประมวลผลแอปพลิเคชัน (application processor) ตัวแรก โดยหน่วยประมวลผลแอปพลิเคชันสูงสุดสองตัวได้รับการสนับสนุนโดยส่วนประกอบแฟลชสองตัวที่สนับสนุนซึ่งกันและกัน นอกจากนี้ ยังมีบริการผลิต (Pre-provisioning) ตามข้อมูลเฉพาะของลูกค้า เป็นออปชันเสริมจากไมโครชิพ หรือ Arrow Electronics อีกด้วย ทั้งนี้ Pre-provisioning เป็นโซลูชันการผลิตที่ปลอดภัย เพื่อช่วยป้องกันการผลิตมากเกินความต้องการ รวมทั้งป้องกันการปลอมแปลง นอกจากจะประหยัดเวลาในการพัฒนาได้หลายเดือนแล้ว บริการนี้ยังลดขั้นตอนยุ่งยากด้านโลจิสติกส์ ทำให้ลูกค้าดูแลและจัดการอุปกรณ์ได้ง่ายโดยไม่ต้องมีต้นทุนการผลิตหรือค่าโสหุ้ยที่โดยปกติต้องจ่ายให้กับผู้ให้บริการภายนอกหรือหน่วยงานรับรองอิสระ

“การรักษาความปลอดภัยสำหรับผลิตภัณฑ์เรือธงของไมโครชิพถือเป็นองค์ประกอบสำคัญในการให้บริการของเรา ซึ่งเฟิร์มแวร์ Soteria-G2 และไมโครคอนโทรลเลอร์ CEC1712 มีเป้าหมายเพื่อปกป้องระบบ” ไอเดน มิตเชล รองประธานฝ่าย IoT ของ Arrow Electronics กล่าว “ลูกค้าจะมีความต้องการผลิตภัณฑ์และบริการดังกล่าวเพิ่มมาก

ขึ้น ในขณะที่เราเข้าสู่ยุค 5G และรุกเดินหน้าสู่การใช้โซลูชันเชื่อมต่อและเครื่องจักรอัตโนมัติกันมากขึ้น”

นอกจากป้องกันมัลแวร์อันตรายระหว่างการ pre-boot ในระบบปฏิบัติการ 5G และดาต้าเซ็นเตอร์แล้ว การรวมตัวกันของ CEC1712 และ Soteria-G2 ยังช่วยเพิ่มความปลอดภัยให้กับระบบปฏิบัติการของยานยนต์ขับขี่อัตโนมัติ (connected autonomous vehicle), ระบบช่วยเหลือผู้ขับขี่ขั้นสูง (automotive Advanced Driver Assisted Systems (ADAS)) และระบบอื่น ๆ ที่บูตระบบจาก external SPI flash

เครื่องมือสนับสนุนการพัฒนา

แพ็กเกจ CEC1712 และ Soteria-G2นำเสนอทางเลือกที่หลากหลายสำหรับการสนับสนุนซอฟต์แวร์และฮาร์ดแวร์ โดยการสนับสนุนซอฟต์แวร์ประกอบด้วยคอมไพเลอร์ MPLAB(R) X IDE, MPLAB Xpress และ MPLAB XC32 compilersของไมโครชิพ ขณะที่การสนับสนุนฮาร์ดแวร์จะถูกรวมอยู่ในโปรแกรมเมอร์และดีบั๊กเกอร์รุ่นต่าง ๆ เช่น MPLAB ICD 4 และPICkit(TM) 4 programmer/debugger

ราคาและการวางจำหน่าย

สามารถสั่งผลิต CEC1712H-S2-I/SX ในปริมาณขั้นต่ำ 10,000 ชิ้น ที่ราคาเริ่มต้น 4.02 ดอลลาร์ (รวมเฟิร์มแวร์ Soteria-G2) สำหรับข้อมูลเพิ่มเติม กรุณาติดต่อพนักงานขายหรือตัวแทนจำหน่ายทั่วโลกที่ได้รับแต่งตั้งจากไมโครชิพ หรือเยี่ยมชมเว็บไซต์ของไมโครชิพ สำหรับผู้ที่สนใจสอบถามราคาจัดซื้อ กรุณาติดต่อ Arrow Electronics ที่อีเมล secure.provisioning@arrow.com และสามารถสั่งซื้อผลิตภัณฑ์ซิลิกอนที่ระบุในข่าวประชาสัมพันธ์ฉบับนี้ได้ที่พอร์ทัลจำหน่ายสินค้าของไมโครชิพ

แหล่งข้อมูลและภาพ

ดูรูปภาพความละเอียดสูงได้ที่ Flickr หรือติดต่อกองบรรณาธิการ (สามารถนำไปเผยแพร่ได้ตามสะดวก):

ภาพการใช้งาน: www.flickr.com/photos/microchiptechnology/49548114798/in/dateposted/เกี่ยวกับไมโครชิพ เทคโนโลยี

บริษัท ไมโครชิพ เทคโนโลยี จำกัด เป็นผู้นำด้านการจัดหาเซมิคอนดักเตอร์สำหรับโซลูชั่นควบคุมแบบฝังที่เป็นอัจฉริยะ เชื่อมต่อ และปลอดภัย เครื่องมือพัฒนาที่ใช้งานง่าย ตลอดจนกลุ่มผลิตภัณฑ์ที่ครอบคลุม ช่วยให้ลูกค้าสามารถสร้างสรรค์งานออกแบบได้อย่างเหมาะสม ซึ่งช่วยลดความเสี่ยง ลดต้นทุนโดยรวมของทั้งระบบ และยังช่วยลดระยะเวลาในการนำผลิตภัณฑ์ออกสู่ตลาด โซลูชั่นของบริษัทให้บริการลูกค้ามากกว่า 120,000 รายในตลาดอุตสาหกรรม ยานยนต์ ผู้บริโภค อวกาศและการป้องกันประเทศ การสื่อสารและการประมวลผล สำนักงานใหญ่ของไมโครชิพตั้งอยู่ที่เมืองแชนด์เลอร์ รัฐแอริโซนา บริษัทนำเสนอการสนับสนุนด้านเทคนิคที่เป็นเลิศ พร้อมกับการขนส่งและคุณภาพที่เชื่อถือได้ สำหรับข้อมูลเพิ่มเติม สามารถเยี่ยมชมเว็บไซต์ของไมโครชิพที่

www.microchip.com

รูปภาพ: https://photos.prnasia.com/prnh/20200310/2731304-1

คำบรรยายภาพ: CEC1712 ไมโครคอนโทรลเลอร์ใหม่จากไมโครชิพ