Infineon เปิดตัวชุดซอฟต์แวร์โอเพ่นซอร์สสำหรับ TPM 2.0 เพิ่มความปลอดภัยการใช้งานในภาคอุตสาหกรรมและยานยนต์

ปัจจุบันภาคอุตสาหกรรมมีความสนใจอย่างมากที่จะยกระดับความปลอดภัยของการใช้ IoT, IIoT, Industry 4.0 และแอปพลิเคชันในด้านยานยนต์ ด้วยเหตุนี้ จึงนำมาสู่การเปิดตัวชุดระบบซอฟต์แวร์แบบโอเพ่นซอร์ส (open source software stack) สำหรับ Trusted Platform Module (TPM) 2.0 ซึ่งเป็นโซลูชั่นความปลอดภัยโดยใช้ฮาร์ดแวร์ที่ได้มาตรฐาน เพื่อรักษาความปลอดภัยการใช้งานในภาคอุตสาหกรรม ยานยนต์ และการใช้งานอื่นๆ อาทิ อุปกรณ์เครือข่าย และยังถือเป็นมิดเดิลแวร์ TPM แบบโอเพ่นซอร์สตัวแรกที่มีคุณสมบัติสอดคล้องกับ Software Stack (TSS) Enhanced System API (ESAPI) ขององค์กร Trusted Computing Group (TCG)

การเปิดตัวชุดซอฟต์แวร์ TPM 2.0 ESAPI นี้จะผลักดันให้มีการนำ TPM 2.0 ไปใช้ในระบบฝังตัว (embedded systems) ได้เร็วขึ้น และทำให้การติดตั้ง TPM 2.0 ในการใช้งานทุกประเภทเป็นเรื่องง่าย ซึ่งความสะดวกสบายในการติดตั้งลงบนระบบปฏิบัติการ Linux และแพลตฟอร์มแบบฝังตัวอื่นๆ นับเป็นการสร้างคุณค่าที่สำคัญให้กับชุมชนโอเพ่นซอร์ส

นอกจากทำให้ TSS ESAPI layer สามารถเข้าถึงได้สำหรับทุกคนแล้ว Infineon Security Partner Network (ISPN) ยังนำเสนอคลังซอฟต์แวร์ที่มีความหลากหลายอย่างมาก ตอบโจทย์ความต้องการการใช้งานที่แตกต่างกัน และกำหนดเป้าหมายแพลตฟอร์มที่ได้รับการสนับสนุนจากกลุ่มผู้เชี่ยวชาญด้านความปลอดภัยของ ISPN

เนื่องด้วยทำงานบน ESAPI layer ชุดซอฟต์แวร์นี้จึงรองรับ OpenSSL และสามารถใช้ Infineon OPTIGA(TM) TPM เพื่อปกป้องการสื่อสารในอุปกรณ์ที่ได้รับการป้องกันความปลอดภัยด้วย SSL/TLS ผ่านอินเทอร์เฟซที่ได้มาตรฐาน โดยใช้ TPM 2.0 เป็นคีย์สโตร์ (key store) ที่ปลอดภัยสำหรับ OpenSSL จึงช่วยป้องกันกุญแจที่สำคัญจากช่องโหว่ต่างๆ อาทิ Heartbleed

ชุดซอฟต์แวร์ TSS stack และ ESAPI layer ได้รับการเผยแพร่ภายใต้ใบอนุญาต BSD แบบ permissive 2-clause ซึ่งมีความยืดหยุ่นสูง และทำให้เกิดการใช้งานมากขึ้น โดย ESAPI ได้รับการออกแบบและผ่านการตรวจสอบจากชุมชนนักพัฒนาเพื่อมอบคุณภาพและเสถียรภาพในระดับสูงตามที่กำหนดไว้ในระบบฝังตัว และระบบ IoT ที่ทันสมัย ขณะเดียวกัน เพื่อลูกค้าในกลุ่มอุตสาหกรรมและกลุ่มยานยนต์ จึงมีการพัฒนารหัสโดยใช้มาตรฐานอุตสาหกรรม

การติดตั้งระบบและการทดสอบอย่างต่อเนื่อง ขั้นตอนการตรวจทานแบบสอง ฝ่าย และระบบตรวจวิเคราะห์โค้ดโปรแกรม อาทิ clang และ Coverity(TM) นอกจากนี้ ชุดซอฟต์แวร์นี้ยังผ่านการทดสอบและประเมินบน Infineon OPTIGA(TM) TPM SLB 9670 ที่รวมข้อกำหนดล่าสุดของ TPM ขณะที่การพัฒนาระบบในอนาคตจะรวมถึงการรองรับการเข้ารหัสดิสก์ Cryptsetup/LUKS และเวอร์ชั่นที่มีระบบรองรับ ESAPI สำหรับอุปกรณ์ของ TPM ด้วย

การเปิดให้ใช้งาน

นักพัฒนาแอปพลิเคชันสามารถใช้ OPTIGA(TM) TPM SLB 9670 Iridium boards ของ Infineon และดาวน์โหลดรหัส TSS ผ่านทาง Github เพื่อเริ่มใช้งาน

ดูข้อมูลเพิ่มเติมเกี่ยวกับ OPTIGA(TM) TPM ของ Infineon ได้ที่ www.infineon.com/TPM

ดูข้อมูลเพิ่มเติมเกี่ยวกับ Github Project (ซึ่งมีรหัสที่สามารถดาวน์โหลดได้) ได้ที่ https://github.com/tpm2-software/tpm2-tss-engine/blob/master/README.md

รูปภาพ – https://photos.prnasia.com/prnh/20181112/2296721-1