ฟอร์ติเน็ตสาธิตการป้องกันภัยคุกคามคอนเนคเต็ดคาร์ ในงาน CES ลาสเวกัส

ในงาน CES 2018 ที่จัดขึ้นที่เมืองลาส เวกัส รัฐเนวาด้า ประเทศสหรัฐอเมริกาเมื่อเดือนมกราคมที่ผ่านมานี้ ฟอร์ติเน็ต (Fortinet® NASDAQ: FTNT) ได้จับมือกับเรอเนซัส อิเล็กทรอนิกส์ (Renesas Electronics) สาธิตโซลูชั่นด้านความปลอดภัยไซเบอร์อันทันสมัยปกป้องการทำงานที่เชื่อมโยงภายในรถยนต์อัจฉริยะ ซึ่งรวมถึงระบบเพาเวอร์เทรน (Power Train) เทเลเมติคส์ (Telemetics) และอินโฟร์เทนเม้นต์ (Infotainment)

ไมเคิล ซี ผู้ก่อตั้ง ประธานและหัวหน้าเจ้าหน้าที่ฝ่ายเทคโนโลยีของฟอร์ติเน็ตกล่าวว่า “คอนเนคเต็ดคาร์ (Connected Car) หรือยานพาหนะอัจฉริยะเป็นนวัตกรรมทางเทคโนโลยีที่สำคัญ มีระบบการทำงานที่เชื่อมต่อกันแบบอัตโนมัติขั้นสูงบนเครือข่ายและอุปกรณ์ที่หลากหลาย รวมถึงการทำแผนที่แบบ 3D การประมวลผลด้วยเซนเซอร์ อุปกรณ์สมาร์ทดีไวซ์แบบบูรณาการนานาประเภท ใช้บริการต่างๆ บนคลาวด์ ใช้เครือข่ายทั้งแบบ LAN และ CAN (Car’s controller area network) และการขับขี่ได้เองแบบอิสระ จึงทำให้ความเสี่ยงด้านภัยไซเบอร์เป็นเรื่องใหญ่ และนอกจากนี้ ด้วยอุปกรณ์ไอโอทีที่เชื่อมต่อกับเครือข่ายของรถยนต์เพื่อเข้าถึงคอนเท้นท์และแอปพลิเคชันในรถยนต์ จึงยิ่งทำให้โอกาสในการถูกโจมตีมีขนาดใหญ่ขึ้น นอกจากนี้ ผู้ผลิตเองได้เริ่มพัฒนายานยนต์ที่ต้องการระบบความปลอดภัยแบบอัตโนมัติ ทำงานด้วยระบบข้อมูลอัจฉริยะด้านภัยคุกคามแบบเรียลไทม์ ในการปกป้องสถาปัตยกรรมของรถคอนเนคเต็ดคาร์ที่ซับซ้อนนี้ ฟอร์ติเน็ตจึงได้เข้ามามีบทบาท และขยายความเป็นผู้นำระดับโลกจากตลาดความปลอดภัยของระบบเครือข่ายขององค์กรไปยังอุตสาหกรรมยานยนต์”

• โดยฟอร์ติเน็ตได้สาธิตให้เห็นว่าระบบปฏิบัติการ FortiOS ของฟอร์ติเน็ตที่พัฒนาขึ้นมาเพื่อการทำงานด้านความปลอดภัยโดยเฉพาะ จะสามารถทำงานร่วมกับระบบ R-Car H3 System-on-chip ของเรอเนซัส ซึ่งช่วยป้องกันเครือข่ายของรถยนต์ บริการและแอปพลิเคชั่นที่ทำงานบนคลาวด์ได้
• ทั้งสององค์กรได้ร่วมกันจำลองภัยไซเบอร์ขึ้นมาคุกคามคอนเนคเต็ดคาร์รถยนต์ต้นแบบ อันได้แก่ ภัยคุกคามประเภทไอพีเอส (Intrusion Prevention System: IPS) และภัยประเภทดีดอส (Distributed Denial of Service: DDOS) ที่สามารถทำให้บริการหยุดชะงักลงได้ เพื่อแสดงให้เห็นถึงศักยภาพของระบบความปลอดภัยแบบอัตโนมัติที่สามารถป้องกันไม่ให้การทำงานของรถยนต์ถูกครอบงำโดยภัยที่คุกคามเข้ามา
• ในงาน CES 2018 นั้น ฟอร์ติเน็ตและเรอเนซัส ได้สาธิตให้เห็นการใช้เทคโนโลยีซีเคียวริตี้แฟบริคกับชิป R-Car H3 SoC ในการป้องกันการทำงานเพาเวอร์เทรน และการสื่อสารในรถ ซึ่งรวมถึงเครือข่ายแอลทีอี ระบบการสื่อสารระหว่างยนต์กับยานยนต์ ระบบแอคเซสพ้อยท์ไร้สาย ระบบควบคุมเครื่องยนต์ และอื่นๆ อีกมาก

รายงาน ON World Connected Car Markets Report (April 2017) คาดว่าจะมีรถคอนเนคเต็ดคาร์จำนวน 300 ล้านคันภายในปีคศ. 2025 ซึ่งเพิ่มจากจำนวน 37 ล้านคันในปีคศ. 2016 และอุตสาหกรรมอุปกรณ์รถที่เชื่อมต่อกันนี้ และบริการที่เกี่ยวข้องทั้งหลายจะมีรายได้ต่อปีมากกว่า 250,000 ล้านเหรียญสหรัฐอเมริกา ซึ่งปัจจัยสำคัญที่ผลักดันให้ความต้องการต่อรถคอนเนคเต็ดคาร์ทั่วโลกเพิ่มมากขึ้น เกิดจากความต้องการคุณสมบัติในการขับขี่ได้ด้วยตนเอง การใช้ข้อมูลในการตัดสินใจขับเคลื่อน และการเชื่อมต่อภายในรถ เช่น การใช้งานสมาร์ทโฟน การเปิดเพลงแบบออน์ดีมานด์ การเชื่อมต่ออินเทอร์เน็ตและความบันเทิงภายในยานพาหนะ

รถคอนเนคเต็ดคาร์ทำงานได้โดยมีการเชื่อมต่ออินเทอร์เน็ตและเครือข่ายแลน (LAN) ช่วยให้ผู้ขับขี่สามารถแชร์การเชื่อมต่ออินเทอร์เน็ตกับอุปกรณ์อื่นๆ ทั้งภายในและภายนอกรถ เช่น เซิร์ฟเวอร์กลางเพื่อประมวลผลต่างๆ ทั้งนี้ เพื่อให้การป้องกันไซเบอร์ที่เหมาะสมและสร้างความเชื่อมั่นผู้บริโภคผู้ผลิตรถยนต์ ผู้ผลิตคอนเนคเต็ดคาร์จึงจำเป็นต้องออกแบบและใช้เทคโนโลยีที่เน้นความปลอดภัยมาเป็นอันดับแรก นอกจากนี้ เนื่องจากระบบรักษาความปลอดภัยต้องทำงานครอบคลุมทั่วทั้งเครือข่าย อุปกรณ์ และมาตรฐานการสื่อสารทั้งหมด จึงทำให้ต้องเป็นระบบที่ให้ศักยภาพในการมองเห็นภายในการเชื่อมโยง การทำงานร่วมกันระหว่างระบบและอุปกรณ์ ให้การควบคุมนอกเหนือจากยานพาหนะที่ขับขี่นั้น ไปยังระบบนิเวศด้านการขนส่งในขนาดที่ใหญ่ขึ้น ซึ่งรวมถึงระบบควบคุมการจราจรและถนน

รถคอนเนคเต็ดคาร์ต้องการใช้ระบบรักษาความปลอดภัยหลายรูปแบบที่ทำงานเป็นระบบเดียวกัน ดังนั้น จึงจำเป็นต้องทำงานเชื่อมโยงกับฟังก์ชันในระบบที่สำคัญๆ เช่น ระบบส่งกำลัง (Powertrain) ระบบเทเลเมติคส์ (Telematics) ที่ช่วยบันทึกข้อมูลตลอดการขับขี่ เช่น อัตราการเร่ง อัตราความเร็ว การเบรค และแจ้งเตือนในกรณีต่างๆ อาทิ แจ้งเตือนเมื่อมีการขับขี่ออกนอกเส้นทาง การบอกเส้นทาง รวมถึงระบบความบันเทิงภายในยานพาหนะ (Infotainment) ทั้งนี้ เพื่อให้แน่ใจว่าภัยคุกคามจะถูกกักกันและบรรเทาโดยอัตโนมัติ นอกจากนี้ รถคอนเนคเต็ดคาร์ต้องการระบบการอัพเดทภัยคุกคามแบบเรียลไทม์ เช่น ระบบ FortiGuard Labs ของฟอร์ติเน็ตที่จะป้อนข้อมูลด้านความเสี่ยงล่าสุดให้แก่รถยนต์ เพื่อให้มีการป้องกันที่มีประสิทธิภาพสูงสุด เป็นไปอย่างอัตโนมัติตลอดเวลา และสร้างการเชื่อมต่อกลับไปยังเครือข่ายคลาวด์เพื่อแชร์ข้อมูลภัย รับแพทช์ด้านความปลอดภัยและปรับปรุงข้อมูลภัยได้อย่างทันท่วงที

ทั้งนี้ ในปีคศ. 2015 มีการทดสอบแฮกรถ Jeep Cherokee โดยสามารถเข้ามาควบคุมระบบรถที่สำคัญๆ ได้และการทดสอบแฮกล่าสุดของรถ Tesla Model S ที่สามารถเข้ามาควบคุมระบบเบรค การล็อคประตู ควบคุมระบบรายงานคอมพิวเตอร์จากระยะทางไกลถึง 12 ไมล์ได้ แสดงให้เห็นว่า ผู้ผลิตยังต้องการระบบความปลอดภัยและป้องกันการละเมิดข้อมูลในระบบของรถคอนเนคเต็ดคาร์ที่มีประสิทธิภาพสูง

เกี่ยวกับฟอร์ติเน็ต
ฟอร์ติเน็ต (NASDAQ: FTNT) ปกป้องค์กร ผู้ให้บริการ หน่วยงานรัฐบาลที่ใหญ่ที่สุดในโลก ฟอร์ติเน็ตช่วยให้

ลูกค้าสามารถมีข้อมูลเชิงลึกและการป้องกันที่ราบรื่นเพื่อให้พ้นภัยคุกคาม และยังเพิ่มประสิทธิภาพการทำงานที่เยี่ยมยอดให้เครือข่ายที่ไร้พรมแดนในวันนี้และในอนาคต ซีเคียวริตี้แฟบริค ซึ่งเป็นสถาปัตยกรรมใหม่จากฟอร์ติเน็ตเท่านั้นที่จะช่วยสร้างเกราะความปลอดภัยโดยจะไม่ยอมแพ้แก่ภัยที่เข้ามา ไม่ว่าจะอยู่ในเครือข่าย แอปพลิเคชั่น คลาวด์ หรือโมบาย ฟอร์ติเน็ตดำรงตำแหน่งเป็น #1 ในการได้ส่งอุปกรณ์ด้านความปลอดภัยสู่ตลาดโลกมากที่สุด และมีลูกค้ามากกว่า 330,000 รายทั่วโลกที่ให้ความไว้วางใจฟอร์ติเน็ตในการช่วยสร้างเกราะป้องกันองค์กรของตน รู้จักฟอร์ติเน็ตเพิ่มเติมได้ที่ www.fortinet.com และ The Fortinet Blog หรือ FortiGuard Labs