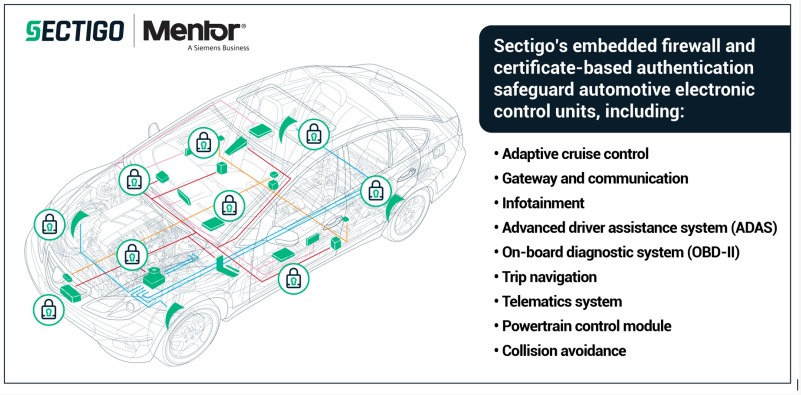
Sectigo and Mentor Present “How to Protect Connected Cars from Emerging Cybersecurity Threats” in 18 February Webinar

Hear design examples of in-production OEM flagship projects using a system-level framework for secure comms by integrating a firewall into existing ECU systems.



Sectigo's Embedded Firewall for Automotive helps protect car network connections from cyberattacks.

ROSELAND, NEW JERSEY, UNITED STATES, February 10, 2020 /EINPresswire.com/ -- To address the growing demand for more cybersecurity in automotive ECUs, Mentor (a Siemens business) has partnered with Sectigo to present a special webinar that will demonstrate the advantages of Mentor’s VSTAR technology with Sectigo’s Embedded Firewall for Automotive. The complementary online event will take place at 9:00 AM EST on Tuesday, Feb. 18.

Modern vehicles are truly ‘software on wheels.’ They are increasingly connected, with growing numbers of entry points and highly sophisticated internal networks controlling critical functions. However, with increased E/E and software complexity comes increased risk of cybersecurity attacks. Several researchers and white hat hackers have demonstrated security gaps that must be addressed before deployment of automotive-grade embedded software. These internet-based threats include packets with malicious connection states, contents or sources, denial of service (DoS) attacks, broadcast storms, and packet flood conditions—threats that call for a multi-layered approach to ensuring vehicle security, safety, and reliability.

> “Modern vehicles are ‘software on wheels.’ They are increasingly connected, with more entry points and sophisticated internal networks controlling critical functions, increasing cybersecurity risks.”
>
> *Alan Grau, VP of IoT/Embedded Solutions, Sectigo*

WHEN:

Tuesday, February 18, 2020 at 9:00 am EST / 15:00 Europe (Berlin)

WHERE:

Register now to reserve your space!
https://www.mentor.com/embedded-software/events/protect-connected-cars-from-emerging-cybersecurity

WHAT:

Experts with Mentor and Sectigo will discuss practical design examples from in-production OEM flagship projects using a system-level framework for secure communications by integrating the firewall into existing ECU systems. The presenters will also discuss the role of authentication and encryption in secure communication, as well as how digital certificates and PKI enable strong identities to support secure communication between vehicles and external systems.

Who should attend:
- Automotive related product management and solution architects
- Automotive product security engineers and managers
- Product security officers, engineering managers, and technology directors

What you will learn:
- Recent security vulnerabilities and threats for connected cars
- Efforts by governments globally to define cybersecurity requirements for connected cars and legislate liabilities
- Role of embedded firewalls, authentication, encryption, & digital certificates in multi-layered vehicle security solutions
- Security architectures for protecting both vehicle network entry points and in-vehicle networks

WHO:

Ahmed Majeed Khan, Senior Engineering Manager, Mentor/Siemens

Dr. Ahmed Majeed Khan is an engineering enthusiast, experienced in working with cross-functional groups to push the envelope of technology implemented in diverse automotive and consumer electronic domains. Having a proficiency to manage on-shore and off-shore development of innovative and disruptive products, he led teams around the globe to produce several high-volume, high-quality system-level solutions. Currently, Dr. Khan is a Senior Engineering Manager at Mentor – A Siemens Business, where he assisted in creation of a market-leading automotive-grade product portfolio. He is also Mentor's liaison to the international automotive software consortium of AUTOSAR. He holds a doctorate in Engineering Management from George Washington University, an MS in Electrical Engineering from Michigan State University, and has a decade of experience working with embedded systems.

Alan Grau, VP of IoT/Embedded Solutions, Sectigo

Alan Grau has 30 years of experience in telecommunications and the embedded software marketplace. Mr. Grau joined Sectigo the world's largest commercial Certificate Authority and provider of purpose-built, automated PKI solutions, in May 2019 as part of the company's acquisition of Icon Labs, a leading provider of security software for IoT and embedded devices, where he was CTO and co-founder, as well as the architect of Icon Labs' award-winning Floodgate Firewall. He is a frequent industry speaker and blogger and holds multiple patents related to telecommunication and security.

Read more about the Mentor and Sectigo partnership.

Please visit the VSTAR website for more details on all of Mentor's VSTAR solutions.

Liza Colburn
Sectigo
+1 781-562-0111
email us here