HCC Embedded Stand at Embedded World: Hall 4-104

HCC Embedded Releases IPSec/IKEv2 Protocol Suite to Boost Network Security

HCC's robust, verifiable network stacks make embedded IoT devices less vulnerable to attacks

Embedded World, Nürnberg, Germany – 22 February 2016 – HCC Embedded, experts in securing embedded data, has added an IPSec/IKEv2 module to its growing range of embedded networking and security software. HCC's verifiable network stacks now have a full set of security protocols and can handle all popular forms of secure network traffic. IPSec/IKEv2 works seamlessly with HCC's IPv4/v6 stacks to create robust host-to-host, host-to-gateway, and gateway-to-gateway security.

IPSec provides a secure virtual channel for embedded data applications used in cars, point-of-sale terminals, medical devices, industrial equipment, and other devices requiring machine-to-machine (M2M) communications. It ensures integrity, confidentiality, and authentication between two devices in a network, providing strong defense against threats such as "man in the middle" attacks and packet sniffers.

While not all embedded software for transmitting or storing embedded data is developed using recognized quality standards, HCC's networking and security software is based on quality that can be verified. Using a formal development process, HCC delivers its IPSec/IKE module with a static analysis report based on full MISRA compliance to help developers ensure that their data is less susceptible to security risks.

HCC's IPSec module with IKEv2 support provides all database management functionality required to administer the storage of authentication certificates and encryption keys and works seamlessly with HCC's Embedded Encryption Module (EEM) to provide a complete security solution. Part of HCC's MISRA-compliant TCP/IP stack, IPSec/IKEv2 conforms to HCC's Advanced Embedded Framework, meaning that it can be dropped into any RTOS, processor, or compiler environment without the need for integration.

Dave Hughes, CEO of HCC Embedded, said, "HCC has built its reputation on protecting the integrity of embedded data, and IPSec/IKEv2 is another high-quality addition to an extensive range of networking options for our customers. Our focus on verifying software quality gives developers a level of security not previously available."

Visit http://www.hcc-embedded.com/embedded-systems-software-products/tcp-stack-networking for more information.

About HCC Embedded

HCC Embedded's software solutions ensure that any data stored or communicated by an embedded IoT application is secure, safe, and reliable. With 15+ years' deep understanding of flash, HCC secures data for customers in IoT, medical, transport, industrial, and aerospace markets. All software is developed using formal software processes, system-level knowledge, and recognized quality practices to ensure robustness and verifiable quality. HCC's product portfolio includes communications products (USB, TCP/IPv4, IPv6, TLS/SSL, IPSec/IKE stacks) and storage products (file systems, media drivers, flash translation layers (FTL), smart-meter software, bootloaders), as well as encryption technology. Because all software is portable, target-independent, and can be dropped onto any RTOS, MCU, or tool-chain, any embedded system can be upgraded to be safer, more reliable, and more secure.
www.hcc-embedded.com

Media Contact:
Angie Hatfield for HCC Embedded
Hughes Communications, Inc.
angie@hughescom.net
425-941-2895

HCC Embedded Contacts:

HCC Embedded USA
1999 S. Bascom Av. Suite 700
Campbell, California 95008
+1- 831-205-9136

George Brooks
info@hcc-embedded.com

HCC Embedded EU
22 Stafford Street
Edinburgh EH3 7NS, UK
+44-7918-787-571

David Brook
www.hcc-embedded.com

WEB: http://www.hcc-embedded.com/
Facebook: http://www.facebook.com/HCCEmbedded

Twitter: http://twitter.com/HCCEmbedded
LinkedIn: http://www.linkedin.com/company/hccembedded