FOR IMMEDIATE RELEASE

NMFTA Releases Whitepaper on Secure Device Provisioning Best Practices: Heavy Truck Edition

Alexandria, Virginia – November 21, 2019 -- To address a rapidly evolving threat landscape, the National Motor Freight Traffic Association (NMFTA), comprised of motor carriers operating in interstate, intrastate and foreign commerce, today unveiled a new whitepaper on the best practices for provisioning automotive control systems (i.e. ECUs) at scale. The paper was commissioned by NMFTA and written by leading global cyber security services firm, NCC Group. NCC Group has specific expertise in assessing transportation cyber security by not only focusing on understanding their clients’ operational technology, but by also marrying it with their deep knowledge in IT security, hardware and software assessments.

Today’s heavy trucks include complex, segmented networks consisting of numerous Electronic Control Units (ECUs) that control power trains, critical safety systems, sensors, fleet management and telemetry systems, internet-connected infotainment systems, repair and diagnostic equipment and more. Each component provides valuable benefits but simultaneously increases the attack surface and cyber risk to these critical systems. The purpose of this paper is to strengthen the security posture of the heavy vehicle ecosystem by providing best practices for helping secure critical vehicle components and safeguard the supply chain.

“This research and resulting paper demonstrate NMFTA’s continued commitment to increasing the resilience of the transportation sector and to protect it against cyber threats. It adds on to other research and work by NMFTA and its partners to secure heavy vehicle CAN networks, such as the cyber security best practices for extreme fast charging electric vehicle supply equipment (EVSE), development of the Open Telematics API and the cyber security templates for telematics systems procurement,” said NMFTA’s Chief Technology Officer, Urban Jonson.

Secure device provisioning can help ensure the system is, and remains, secure for the defined lifetime. Device provisioning is the process of attaching a certificate to a specific device to identify, validate and authenticate it as the intended and trusted connection point. (In other words, what identify verification is to humans, secure device provisioning is to connected devices.) A secure system retains its integrity. It is able to detect whether the system has been tampered with and that the system is fit for its purpose. ECUs must protect the communication paths between each other by forming trusted relationships even when each is manufactured by a different supplier. As well, interactions with eternal services like diagnostics and repair systems, V2V and V2I systems must be managed securely. CAN bus segmentation is gaining traction, but its effectiveness may be blunted.
by the need for more interconnection of systems and connectivity to the internet that autonomous vehicles (AV), vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications require.

The whitepaper was authored by Rob Wood, Technical Vice President of NCC Group, with input from the NMFTA and other heavy vehicle industry partners. It covers threat modeling, challenges and practical solution requirements. Some of the challenges covered include: manufacturing; distributed ecosystem; right to repair; and common mistakes. Security best practices, such as secure boot, authenticated access, cryptographic concepts, side channel attack resistance and key management are discussed in detail.

Wood continued: “By following the requirements laid out in this paper, the heavy trucking industry can build, integrate or acquire a robust provisioning system ready to support the desired security guarantees of the vehicle system, throughout the lifetime of the vehicle. A provisioning system is by no means sufficient to fully secure ECUs and vehicles, however they provide a strong foundation upon which a secure vehicle system may be built.”


About NMFTA

The National Motor Freight Traffic Association, Inc. (NMFTA) is a nonprofit membership organization headquartered in Alexandria, Virginia. Its membership is comprised of motor carriers operating in interstate, intrastate and foreign commerce. NMFTA publishes the National Motor Freight Classification® (NMFC®) and ClassIT®, the online version of the NMFC. NMFTA also assigns the Standard Carrier Alpha Codes (SCAC®) and the Standard Point Location Codes® (SPLC). For more information on NMFTA, the National Motor Freight Classification, SCAC or SPLC, contact us at 800-539-5720, sales@nmfta.org, or visit www.nmfta.org.

For more information: Please contact Alison Hwang at Alison.Hwang@nmfta.org.

About NCC Group

NCC Group (https://www.nccgroup.trust) is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever-evolving threat landscape. With the company’s knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate & respond to the risks they face. NCC Group is passionate about making the Internet safer and revolutionizing the way in which organizations think about cyber security.

Headquartered in Manchester, UK, NCC Group has over 35 offices across the world, including key North America offices in New York, San Francisco, Boston, Chicago, Seattle,
Atlanta, Austin and Waterloo. It employs more than 1,800 people and is a trusted advisor to 15,000 clients worldwide.

For more information: Please contact Paula Dunne at 408-893-8750 or paula@contosdunne.com.

###

PRESS CONTACT:
CONTOS DUNNE COMMUNICATIONS +1-408-893-8750 (m)
+1-408-776-1400 (o) NCCGroup@cdc.agency (e)