**C2A Security and NXP provide a combined solution to protect connected and automated vehicles**

*Joint solution addresses demand for iron-clad perimeter cybersecurity protection for vehicle OEMs.*

**Frankfurt, Germany – September 12, 2019, 7am UTC (IAA 2019, Hall # 5 Booth #30B)** – [C2A Security](http://c2a-sec.com), a global leader in automotive cybersecurity, has today announced a collaboration agreement with NXP to develop a comprehensive automotive security solution.

Delivering complete protection and guaranteeing that automotive OEMs have the upper hand against even the most sophisticated cyberattacks, the move marks the launch of the industry's first comprehensive software-hardware cybersecurity solution.

Working together, a task force from C2A and NXP has identified all CAN bus-related attack vectors for perimeter devices. Their joint solution allows OEMs to leverage both software and hardware security capabilities and covers all attack vectors. In doing so, the joint task force provides complete CAN bus protection where it is needed most, a first of its kind. The unique synergetic solution allows OEMs to gain the most comprehensive CAN bus security solution available in the market and improve their security posture.

This synergetic solution consists of:

* NXP's Secure CAN Transceiver for a vehicle's controller area network (CAN) bus, which detects and prevents malicious activity at the CAN bus level;
* C2A’s Stamper, a decentralized firewall for the controller area network (CAN) bus, which adds a patented security layer for CAN bus communication;
* C2A’s SecMon Intrusion Detection and Prevention Software (IDPS), which detects potentially malicious activity by combining deterministic and machine learning capabilities, and then uses state-of-the-art in-vehicle SOC to enable an appropriate response.

With vehicle safety the highest priority, it is critical that OEMs have the ability to provide passengers with an optimal defense against cyber threats. The synergetic C2A/NXP solution enables automotive manufacturers to finally own hermetic protection from CAN bus cyberattacks, especially on the perimeter where the attack surface is the largest.

"C2A is looking to provide the automotive industry with comprehensive security solutions, covering all relevant attack vectors," said Nathaniel Meron, chief product and marketing officer at C2A Security. "Our solution approach to security with NXP is vital for manufacturers to ensure their passengers’ safety," added Meron.

Commenting, Timo Roermund, head of automotive security at NXP, said: "NXP's secure CAN Transceiver is a perfect hardware complement to C2A software solutions, one that aims to deliver a complete security solution for increasingly connected cars". Roermund added: "We are looking forward to deepening cooperation between the two companies to further explore unique synergetic security solutions.

Visit C2A Security at IAA 2019, New mobility world Hall 5 Booth 30B to discover more about this industry-first comprehensive security solution.

**ABOUT C2A SECURITY**

C2A Security was founded in 2016 by Michael Dick, who previously co-founded NDS. C2A is dedicated to providing the automotive industry with end-to-end in-vehicle cyber security protection. Combining multi-disciplinary world-renowned leaders from the automotive, embedded security and academic domains, C2A has created an innovative solution for in-vehicle cyber security, providing car manufacturers with comprehensive, yet practical, vehicle security solutions.

ABOUT NXP

NXP Semiconductors N.V. enables secure connections and infrastructure for a smarter world, advancing solutions that make lives easier, better, and safer. As the world leader in secure connectivity solutions for embedded applications, NXP is driving innovation in the secure connected vehicle, end-to-end security, and privacy and smart connected solutions markets. Built on more than 60 years’ of combined experience and expertise, the company has approximately 30,000 employees in more than 30 countries.