U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND – GROUND VEHICLE SYSTEMS CENTER

Ground Systems Cyber Engineering (GSCE) – May 2020

Jeffrey Jaczkowski
Associate Director

DISTRIBUTION A. Approved for public release; distribution unlimited. OPSEC# 4115
Mission
To identify cyber vulnerabilities and adaptively secure joint service ground vehicles, watercraft and support systems by engineering resilient cyber solutions.

Priorities
#1 Ensure cyber resiliency for new ground vehicle systems
#2 Mitigate “Critical” vulnerabilities in fielded systems

Baking security into the vehicle architecture will significantly reduce the cyber attack surface.
Baking security into the vehicle architecture will significantly reduce the cyber attack surface.
• Technical Challenge 1: Ability to send and receive encrypted messages across the vehicle databus to update the electronic control units (ECUs) (e.g. powertrain components and engine control module) firmware securely.

• Gap: Lack the ability to provide confidentiality and integrity to the electronic control units (ECUs) through utilization of firmware signing and message encryption

• Barrier: Each OEM uses their own priority software to update firmware via hardware connection.

• Resolution Timing: 2–4 years
TECHNICAL FOCUS AREA: SUPPLY CHAIN RISK

• Technical Challenge 2: Device Security/ Supply Chain Provenance
• Gap: Lack the ability to harden against reverse engineering, tampering or unauthorized updates to hardware and software; Lack the ability to mitigate malicious supply chain risk and latent vulnerabilities in microelectronics and embedded software
• Barrier: Vehicle system, subsystem and component level supply chain is global and diverse
• Technical Challenge 3: Virtualization of hardware and software ground vehicle components.
• Gap: lack the ability to virtualize ground vehicle cyber-affected components. The Hypervisor will be able to spin-up near instant replacements for compromised or failed components. Additionally, the hypervisor will provide complete segmentation between operational and safety-critical vehicle bus messages.
• Barrier: There are very limited vehicle components today that are designed to be virtualized.
• Resolution Timing: 2–3 years
• Technical Challenge 4: Securing Connected and Autonomous Systems
• Gap: When cyber vulnerabilities in a current military vehicle’s firmware are found, the vehicle firmware must be updated by manually plugging in a diagnostic and maintenance device in order to service and update firmware located on several devices located within the vehicle.
• Barrier(s): The development of a secure centralized onboard vehicle controller utilizing robust and secure protocols to arbitrate the on-vehicle unpacking, verification and secure distribution of received firmware updates. This is already a significant problem with manned vehicles, in the future this problem will be compounded with autonomous vehicles due to the lack of manned personnel on the platform to perform this function directly, especially if continuous and uninterrupted remote operation of the platform is required.
• Resolution Timing: 3–5 years
INVESTMENT STRATEGY

Existing Contracts FY19-20
• Vehicular Intrusion Defense- three performers: DG Technologies, Percpecta Labs, South West Research Institute (~$450K each for base effort) Development and demonstration (vehicle/SIL environment) of cyber intrusion detection/defense (via DATC/Detroit Arsenal Automotive (DA2) OTA)

• Opportunities for Partnership FY20-21
  DATC/Detroit Arsenal Automotive (DA2) OTA RFPP (Closed 1 May 2020)
  Assurance and Verification of Vehicular Microelectronic Systems (AV2MS) up to 2 awards ~ ($500K-$1M)

• NAMC/Ground Vehicle Systems (GVS) Other Transaction Agreement (OTA) FY21 AP RPP 20-01 W15QKN-17-9-1025- RPP-20-01 (closed 17 April 2020)
• ASM-21-01: Cyber-resiliency Technologies for Military Ground Vehicles Fiscal Year 2021 (FY21) Annual Plan (AP) Request for Prototype Proposals (RPP)
Opportunities for Partnership FY21-22
• Request for Information (RFI) for the procurement of a Hypervisor. The objective of the RFI is to better understand the availability and capabilities of products and the potential of the manufacturers.
https://beta.sam.gov/opp/2f1f5c6a21e04d42ad871607cc22e886/view
Closes 1600 hrs 5 June 2020

Opportunities for Partnership FY22-25
• Future RFP(s) for Advanced Vehicular Cyber Resiliency capabilities Base with options - under Ground Vehicle Systems OTA or Detroit Arsenal Automotive OTA
• Funding estimated ~$1.0M-$3M/year
ONE-ON-ONES

Sign-up for one-on-one meetings with *Ground Systems Cyber Engineering* by filling out the request form on the main page and submitting.