Capabilities Statement

InfoBeyond Technology LLC
info@infobeyondtech.com
502.371.0909
www.infobeyondtech.com

NAICS: 541411. 541715
DUNS: 877380530
CAGE: 5CYU1

Our expert team is dedicated to developing state-of-the-art solutions to improve military vehicle security, diagnosis, resilience, and maintenance . We specialize in delivering groundbreaking IT and cybersecurity technologies using Blockchain, Risk Management Frameworks, Networking, and AI/Machine Learning to enhance DoD vehicle operations against cyber security. We wield our passion for innovation to provide key enhancements to businesses and organizations around the globe.

CORE COMPETENCIES

Our vision is to actively conduct novel research and develop innovative solutions that improve user experience and security. We are experts in creating cutting-edge applications using the following technologies:

We offer blockchain solution for enhancing OpenFMB-based power grid network and data security, remote system diagnosis operational security, and vehicle intra CAN-Bus communication security to provide data integrity, immutability, confidentiality, and traceability.

Blockchain

We offer software tools to empower you to systematically compose and verify access control policies to ensure they are free of vulnerabilities and flaws before deployment into your organization's enforcement system (PDP, PEP, etc.).

Cybersecurity

We implement tools to help organization to craft Security Controls for an IT system to meet operations as well as the constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations, following FISMA metrics, SP 800-53 controls, FedRAMP standard, and/or NIST CSF baselines.

Compliance

PAST PERFORMANCE

- Auditable Smart Grid Blockchain for Data Integrity and Immutability
- Authentication, Cross-domain Security, Multilevel security, and Network Risk Analysis
- Risk Management Frameworks that simplify NIST SP 800-53, FISMA, CSF, CSA Enterprise compliance
- Access Control Policy Tool, XACML, Policy Editing
- Moving target defense, Distributed data storage, Fragment-based data storage against ransomware
- Image recovery, reconstruction, target identification, tracking, and prediction
- Tactical data analytics, graph representative learning, graph embedding, abnormal event detection.

FEATURED CLIENTS

HCA Healthcare
SAMSUNG
Honeywell
Hamilton Associates
Hewlett Packard Enterprise
Manchester-Boston Regional Airport
MITRE
EMC²
Fermilab
SUN PHARMA
SAIC
Tech Mahindra
IT Services and Telecom Solutions

Are you interesting in transitioning our solution to your system? Contact Sarah Spires: Sarah@InfoBeyondtech.com

InfoBeyond Technology LLC
info@infobeyondtech.com
503.371.0909
www.infobeyondtech.com

NAICS: 541411. 541715
DUNS: 877380530
CAGE: 5CYU1

VehChain: Blockchain Cryptography decentralized Distributed CAN Data Security for Intra-Vehicle Control Systems

The Problem: The U.S. Army GVSC and DoD ground systems continue utilizing Controller Area Network (CAN Bus) communication standards for embedded systems in the Army's manned, unmanned, electric, and autonomous vehicles (EVs, UGVs, UAVs). Due to inherited natures of CAN protocol limitations, these vehicles are vulnerable for cybersecurity attacks while they are connected to external networks. The existing CAN Bus enhanced security solutions require the hardware add-on, CAN Bus protocol modifications, or a centralized security control, which not only cause high cost but also result in backward-incompatibility and a single point of failure (See Army SBIR A20B-T020).

VehChain Solution: As a Blockchain reminiscent solution, VehChain implements reliable CAN Bus message encryption, verification, and error recovery for intra-vehicle communications to provide a means for CAN Bus security. To reduce communication overhead and latency, VehChain is designed based on the nature of CAN Bus, i.e., messages are broadcasted, nodes have no identifiers, and the frame identifier determines the specified node. Distributed message validation at each node secures the CAN bus through MAC, encryption, and key generation reminiscent of Blockchain technology. Each cryptographic key is tied to the CAN frame's identifier, hash (plain-text payload), and hash (previous key). To provide resiliency from corrupting message, a reboot-based recovery approach utilizes CAN's built-in error handling mechanism. Hence, it mitigates the effect of attack propagation bus for ensuring the operational safety, security, and continuity.

Features:

⇒ Distributed and decentralized message confidentiality and validation for intra-vehicle communication networks. Avoid single point of failure.
⇒ Easily integration into the CAN Bus through the firmware revisions.
⇒ No additional CAN hardware or data frame alteration is needed. Compatible with legacy vehicle systems (CAN & MilCAN).
⇒ Proactive threat resilience in CAN Bus through self-reboot recovery mechanism.
⇒ Lessen the communication overhead and delay.

Applicability:

⇒ Army Ground Vehicle System Center—GSVC.
⇒ Army Combat Capabilities Development Command (CCDC)
⇒ U.S. Army Engineering and Support Center (USACE).
⇒ Mission Enabler Technologies Demonstrator (MET-D) Vehicles
⇒ Robotic Combat Vehicles (RCV), Manned Lead Vehicles, Unmanned Vehicles, Unmanned Aerial Vehicle, Unmanned Ground Vehicles, Air force & Navy and other DoD vehicles.
⇒ Commercial Vehicles and systems using CAN.

We are seeking for technical transition. No cost for trial and installation in first year of field-deployment. Contact us (Sarah Spires: Sarah@InfoBeyondtech.com) for demonstration and any questions.