Global, Innovative, Computer Technology Protection Services

PRODUCT QUICK GUIDE: HIPPOGRIFF LLC AUTOMOTIVE CAN BUS FIREWALL SYSTEM (PATENT PENDING - FILING # 62/375,448)

As solution engineers Hippogriff technologists have created products and approaches that are practical, reliable, and intuitive; with ease of use and implementation. Automated and Brute Force cyber attacks are not limited to traditional notions of IT infrastructure; automotive transportation mechanisms are at risk of exploitation too.

The Hippogriff automotive Controller Area Network (CAN) bus firewall system is an electronic chip which functions as a gatekeeper at the most crucial aspect in vehicle security; the entry points for multimedia, navigation, telecomm, keyless entry, or anything network enabled. Components of a vehicle are manufactured by multiple vendors; therefore the difficulty in securing multiple systems which have been centralized is apparent. The weakest link is generally the entry-point of an attack surface.

The Hippogriff automotive CAN bus firewall system is a product which denies unknown/unauthorized signal credentials between vulnerable systems and Mission Critical Systems (MCS's). This is a middle-tier device -- bridging input/output processes and services for embedded and external devices -- which functions in a transparent manner by avoiding the common pitfall of affecting vehicle performance or system integration.

The Hippogriff automotive CAN bus firewall system filters CAN bus commands at the bottleneck of the vehicles communication network, which makes it possible to protect vulnerable systems from complex MCS's and unknown Common Vulnerability and Exposures (CVE's).

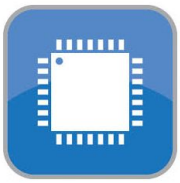
The Hippogriff automotive CAN bus firewall system is a more cost-effective solution for manufacturers and aftermarket suppliers. This concept offers faster adoption while providing due-diligence security.

"Consumer vehicles may not be the primary target for these directed attacks, however. Commercial businesses and gov't agencies could find themselves on the receiving end of targeted attacks that take out an entire fleet of vehicles." | *"They (Terrorists) want to drive trucks into civilians,* ***and it's not too much to think they can hack a car*** *and do the same thing."* – John Carlin, U.S. Dept. of Justice, CarAndDriver.com

Vulnerable Communication Links

Including but not limited to any device capable of receiving wireless or physical data transfer such as:

802.11 WiFi, Bluetooth, GPS, Universal Serial Bus, Cellular Service, Radio AM/FM/XM, Infrared Camera Input, Internet of Things (IoT) Capable Products, Navigation System, In-Vehicle Infotainment (IVI), USB Input



Vehicle Whitelist Rules

Whitelist overrides all Blacklist rules allowing for authorized use of:

Steering Wheel Volume Controls, Dashboard Mounted External Devices, Head Lights, Climate Controls, Motorized Seat Adjustment, Rear-Facing Backup Camera, Dash Video Display, Windshield Head-Up Display, or any vehicle feature needed by user.

CAN bus Attached Device Systems

Critical vehicle systems integrated to the CAN bus include but are not limited to:

Power Management, Transmission, Fuel Management, Emergency Systems, Traction Control, Body Control Module, Brakes, Air Bag, Safety Restraint, Cruise Control, Fuel Management, Lock System

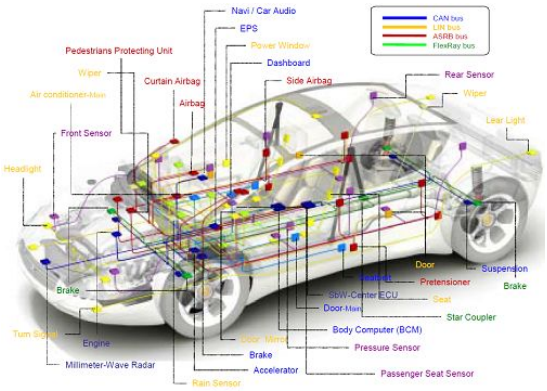
Vehicle Blacklist Rules

Default firewall set to deny ALL. Vulnerable communication links for IVI, Bluetooth, Navigation System, Undercarriage Sensors, and other third-party connections or non-critical sub-systems do not need access to MCS's such as:

Engine Cooling, Ignition System, Battery, Windshield Wipers

Application Overview:

The Hippogriff automotive CAN bus firewall system is integrated by placing a small Field Programmable Gate Array (FPGA) chip in-between the transmit/receive wiring of two CAN bus enabled devices. The chip functions as an inline component, only allowing the correct commands to be re-transmitted throughout the automobile's network, these chips can be re-programmed to function differently without being replaced. This is a highly adaptive approach allowing for the device to remain isolated from compromised systems ensuring integrity. By applying this methodology, multiple vehicle classes qualify for a modular safeguard against current and future malicious CVE's exploits of automotive electrical/computing systems.



The Hippogriff automotive CAN bus firewall system is a reliable and agile shield against inevitable system(s) violation attempts. Instead of a much more time consuming and expensive task to buttress poor software engineering via panicked after-the-fact code review, Hippogriff's proprietary solution eliminates the most modern system ineptitude altogether.

Trend Direction:

A plateau has been reached in the voluntary development and implementation of proactive measures by manufacturers - to protect consumers from the dangers of constantly evolving technology exposure. Government regulators and corporate legal teams are under increased scrutiny from judicial, legislative, and social bodies to mandate up-to-date precautions are taken by business professionals in every sector; cutting-edge capabilities must be acquired and deployed to stave off consequences that effect public safety and national security. Factors to consider:

- Rental vehicles are exposing more drivers and occupants to identity theft. Residual external personal device data -- remaining on a rented automobile's systems after termination of transportation -- grants automotive thieves an additional profit through extraction and sale of this information.
- Security researchers are consistently demonstrating the ability to remotely hijack a contemporary vehicle and literally take control of steering, breaking, navigation, and other systems due to non-existence embedded digital protections. Public awareness and alarm of vehicle design shortcomings is impacting consumer confidence.
- Malicious software infection of future autonomous road vehicles is guaranteed to affect not only superficial process behaviors, but also MCS's - endangering pedestrians, stationary infrastructure, and other road travelers.
- Location tracking of vehicles for communication or diagnostic purposes are being utilized by nefarious parties - allowing for criminal acts to be carried out against private citizens, enterprise or government assets.

U.S. Toll Free Phone: 1-866.273.2436, E-mail: inquiry@hippogriff.tech, Web: http://www.Hippogriff.TECH