A software-based anti-spoofing defense system for the CAN bus; Cyder Security (Ramot)

code: 7-2016-1011

Avishai Wool, T.A.U Tel Aviv University, Engineering, Engineering - General Department

If an attacker compromises one of the car's electronic control units (ECUs), and from there tries to attack another, more critical, ECU, the designed system blocks this lateral movement. Hence, this defense system can be added as a software-only patch to any standard ECU. The system was implemented and tested for its "behavior" in detailed experiments. With 'CAN' controllers that are able to transmit fast enough it was successful in disabling the attacking ECU in 100% of experiments. For slower controllers, if the combination of benign CAN traffic, this system's defense, and a helper ECU's traffic, produces a well-timed pulse of high-enough bus load, the system is able to block the cyber-attack.

Modern cars have multiple dedicated computers under the hood called “electronic control units” (ECUs). These ECUs control all aspects of the car's operation: from the engine, breaking and steering controls to the car's entertainment systems. The ECUs are connected to each other in a network that typically uses the CAN bus protocol. CAN bus is a simple serial protocol, with absolutely no security components: it was designed under the assumption that all ECUs are legitimate, trustworthy, and operating according to their specifications. However, over the last few years researchers have shown that many ECUs are vulnerable to attack. Since CAN bus in itself is so naive, any attack on one ECU can immediately allow lateral movement, to attack other, more critical, ECUs; the subverted ECU can trivially spoof (masquerade as) any other ECU and cause significant damage. Replacing CAN bus with a more robust technology is probably a good idea. However, due to the huge investment made by manufacturers, and the decades it takes until old cars are scrapped, it is an important goal to improve the security stance of cars within the limitations of CAN bus. Thus, finding methods to block the lateral movement, from the originally compromised ECU to others is of utmost importance.

Simple Integration: Car-Cyber solution as a software only patch, to any standard ECU

Some existing proposals to defend the CAN bus require a specific topology (so a “firewall” can be placed in the path of the CAN traffic. This is a major change to the car’s network which can be expensive and does not protect ECUs that are “on the same side” of the firewall, from each other. Unlike previous firewall-based solutions or cryptography-based solutions, the attack messages are identified and destroyed by the legitimate message ID's owner. This method doesn't merely drop messages that are non-conforming with policy: the defense system typically disconnects the compromised ECU from the bus.

Other proposals rely on cryptography with a central management system combined with the ability to destroy unwanted packets. However, the cryptography requires complex key management, and the ability to destroy messages requires violating the CAN protocol rules, which implies using a custom CAN controller (hardware).

unlike previous solutions, that require a modified controller (since they violate the CAN bus protocol), this novel approach is able to shut down the attacker while obeying the protocol rules.

This solution can work with any network topology, does not rely on any cryptography, and works entirely within the rules of the CAN protocol, so it can be deployed as a software-only update: making it a low-cost method that can be deployed relatively quickly.

Key Advantages

• Software only
o Fast Deployment
o Reduced Cost & Complexity
□ No requirement for special hardware
□ No modification to current hardware
□ No change in Network topology
□ CAN bus type intolerant
□ Improved efficiency

Patent Status

US provisional filed

Related Publications

1) R. Kurachi, Y. Matsubara, H. Takada, N. Adachi, Y. Miyashita and S. Horihata, "CaCAN-centralized authentication system in CAN (controller area network)," ESCAR, 2014 .
2) R. Kurachi, H. Takada, T. Mizutani, H. Ueda, and S. Horihata, "SecGW secure gateway for in-vehicle networks", ESCAR, 2016.
3) T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, and K. Oishi, ”A method of preventing unauthorized data transmission in controller area network", IEEE Vehicular Technology Conference, 2012
4) Y. Ujiie, T. Kishikawa, T. Haga, H. Matsushima, T. Wakabayashi, M. Tanabe, Y” A method for disabling malicious CAN messages by using a centralized monitoring and interceptor ECU, ESCAR, 2015.

Contact for more information:
Ofer Shneyour ✉, VP Business Development, ICT, +972.3.640.6496

Ramot at Tel Aviv University Ltd. P.O. Box 39296, Tel Aviv 61392 ISRAEL
Phone: +972-3-6406608
Fax: +972-3-6406675