File 20100517.0740: I put a paper on the wiki for next week: 'Experimental Security Analysis of a Modern Automobile' by Koscher, et al. (Oakland, California: IEEE Symposium on Security and Privacy, 16–19 May 2010). On an internal Lockheed Martin mailing list, I posted a short article called 'Automobiles are Cross Domain Systems' in which I made the case that they are that, and manufacturers do not recognise it yet, but the same techniques that are used to interconnect classified networks are applicable to the LANs running in the chassis of your car. The key point of the research by Koscher, et al. is that the particular car tested was not air-gapped. One component (the telematics ECU) connected to both the low-speed untrusted network and the high-speed safety-critical network and was found not to implement the required authentication as specified in the CANbus standard. So any device on the untrusted network (such as the stereo) could re-flash the telematics ECU, add new code to act as a network bridge, and compromise the trusted network. The researchers gained full control of throttle, brakes, door locks, lights, windscreen washer and wipers, and instrument panel displays.

References