AUBURN UNIVERSITY

1856 2006

Wireless Engineering Research and Education Center

Securing Connected Vehicles

Dr. Tao Zhang

Chief Scientist, Cisco Systems, San Jose, CA

Abstract

A growing range of vehicle security vulnerabilities have been revealed recently. Researchers and hackers were able to modify the software on electronic control units (ECUs). They have placed unauthorized devices and software on vehicles to control a wide range of vehicle functions. More worrisome are attacks over wireless communications. The wireless signals from vehicle Key fobs have been hijacked to open vehicle doors and start vehicle engines even when the key fobs are far away from the car. Security keys used to protect messages from key fobs have been broken. Wireless tire pressure monitoring systems have been hacked to set bogus time pressure status. Malware can propagate onto vehicle electronic systems through multiple venues. The most damaging security vulnerabilities, however, are only emerging as vehicles begin to connect to the external world such as with the Internet, other vehicles, wireless networks at vehicle dealers, and roadside Intelligent Transportation System (ITS) networks.

Solutions to vehicle security challenges must address many unique challenges that have not been well addressed in other types of networks. For example, many devices on vehicles have significantly limited abilities due to cost constraints. Security operations should be highly automated and should not require driver intervention. Vehicle security threat detections must be performed with extremely low error rates to reduce the probabilities of wrongfully blaming innocent vehicles and drivers. Any security capability placed onboard vehicles must be kept up-to-date over a vehicle's long lifecycle without causing inconvenience to the vehicle owner or consuming excessive wireless bandwidth. A solution must be highly scalable to support, for each automaker, millions of new vehicles each year, tens of millions of vehicles in operation, tens to over a hundred devices on each vehicle, and many more spare parts. This list goes on.

This talk will highlight these security challenges and discuss selected solutions.

Bio

Dr. Tao Zhang is the Chief Scientist for Cisco Connected cars at Cisco Systems. He is a Fellow of the IEEE. For over 25 years, he has been directing research and product development in mobile and vehicular networks. He has co-authored two books "Vehicle Safety Communications: Protocols, Security, and Privacy" and "IP-Based Next Generation Wireless Networks" published in 2012 and 2004 respectively by John Wiley & Sons. He holds 33 US patents covering areas such as security, mobility management, information dissemination, and energy-conversing protocols for wireless, mobile ad-hoc, sensor, and vehicular networks. Dr. Zhang was a founding member of the Board of Directors of the Connected Vehicle Trade Association (CVTA) in the US. He is the Chair of the IEEE Communications Society Technical Committee on Vehicular Networks and Telematics Applications. He has been serving on editorial boards or as a guest editor for a number of leading technical journals. He has been serving on the industry advisory boards for several research organizations and has been an adjunct professor at multiple universities.

MONDAY, NOVEMBER 11, 2013, 4:00 P.M.

235 BROUN HALL

http://www.eng.auburn.edu/~pagrawal/seminar/2013/index.html