BALOUGH LAW OFFICES, LLC

Cyberattacks on Cars Coming in 2016 and Beyond

Cyberattacks on automobiles will increase in 2016 and beyond, "likely resulting in lost lives" according to McAfee Labs' 2016 Threats Prediction.

The problem is acute because there has been a rapid deployment of hardware in cars connected to the internet and much of the hardware is "built without foundational security principles," leaving the systems vulnerable to cyberattack. By 2017, driverless cars and smart highways will further expose drivers and passengers to threats.

In order to protect cars and drivers, the interconnected systems should include features such as "secure boot, trusted execution environments, tamper protection, isolation of safety-critical systems, message authentication, network encryption, data privacy, behavioral monitoring, anomaly detection, and shared threat intelligence." Unfortunately, McAfee says, "many connected cars lack some or most of these security features."

In the past several years, researchers have reported the ability to hack into cars and take control of them. The legal implications of these vulnerabilities have been explored by Balough Law Offices in several presentations and publications. McAfee predicted that in 2016 more automotive system vulnerabilities will be found and it is possible that some of the vulnerabilities "will be found and exploited in the wild by cybercriminals who may threaten people's lives, impact road safety, and create transportation deadlocks."

Other non-safety related cyberattacks to cars include monitoring a vehicle's location, listening to conversations using the car's microphone, or even recording video using the car's cameras. "We predict that 2016 will be the beginning of attack campaigns that may be discovered only months after the original infections," the report said.

Balough Law Offices, LLC, is a Chicago-based law firm which focuses on cyberspace, internet, and business law. Our homepage is balough.com.