Accidents Will Happen

David Alan Grier, George Washington University

As we have done with so many technical systems, we tend to think about functionality first and consider security problems only as an afterthought.

The conversation had the rhythm of a poker game. Each participant offered a selected bit of information, hoping to get a larger share in return. We were sitting in slightly dilapidated restaurant on the edge of downtown, swapping lies about the recent Consumer Electronics Show (CES) while Frank Sinatra crooned in the background. “You may ignore my hopeful heart, and chances are not the one to make you fall,” sang Ol’ Blue Eyes, “but accidents will happen after all.”

We were trying to determine what would become the next big thing—the technology that would bring fortune to the entrepreneurial class of 2015. Three of our group had attended the CES while the rest of us followed it on social media. All of us identified a single product category: automotive systems. “The car is no longer a transportation system,” claimed one of us, “but a moving computing platform.” I wanted to make the point that automobiles have been a mobile computing platform for more than 30 years, but it wasn’t the right audience. We were largely a group of entrepreneurs, a community in which a good story about money will always trump the truths of technology.

Our conversation quickly moved to recent reports that the world’s largest search engine firm would have more success with a self-driving car than they had with Google Glass.

The automotive product that attracted the most attention wasn’t the autonomous car, but an interface that connects a car’s information system to a smartphone. This interface not only provides more information about a vehicle than could be found on the dashboard, but also allows parents to monitor their child’s driving from a distance. The interface would transmit the car’s location, its speed, and even the number of occupants who had fastened their seat belts to the watchful parent’s smartphone.

Because this device makes driving much more public, it raises the questions of hacking and privacy. “What will happen when someone learns how to attack the data systems of a car?” someone asked tentatively. “What might a hacker be able to do?” The speaker may have been hoping someone would say, “Attacks are highly unlikely because automobile electronics have been so well designed.”

The real answer, of course, is far more disturbing. We’ve been protected from major attacks on automobiles not because of carefully designed security systems but because no one views vehicles as a tempting cybertarget. In fall 2014, the National Highway Transportation Safety Administration released a report that identified potential security threats to the modern automobile. It isn’t as thorough as we might like, but it’s worrisome nonetheless. With only a modest amount of skill, a hacker could disconnect the brakes, disable the security system, honk the horn, inflate the airbags, or race the engine. Any one of these could be very bad for a driver. The report concludes that it “is recognized that increasing interconnectedness with internal and external networks and growing system complexity could introduce new security vulnerabilities.”

The simplest entry point for a vehicular cyberattack is the onboard diagnostic port (OBD), which is located underneath the steering column on most cars and light trucks. This port has been required on all cars in the US since 1996. The standards for the OBD are well published, and the protocols for automotive electronic control units are easy to find.

As we have done with so many technical systems, we tend to think about functionality first and consider security problems only as an afterthought. We are protected by global ignorance until some event makes us realize that we’ve been vulnerable for years. We enjoy the benefits of a global flow of information but live in a world where people will corrupt that flow to thwart our actions and achieve selfish goals. “Before you know it, I’m sure I’ll know,” Sinatra sang that night, “accidents will happen after all.”

DAVID ALAN GRIER is a professor of international science and technology policy at George Washington University. Contact him at grier@gwu.edu.