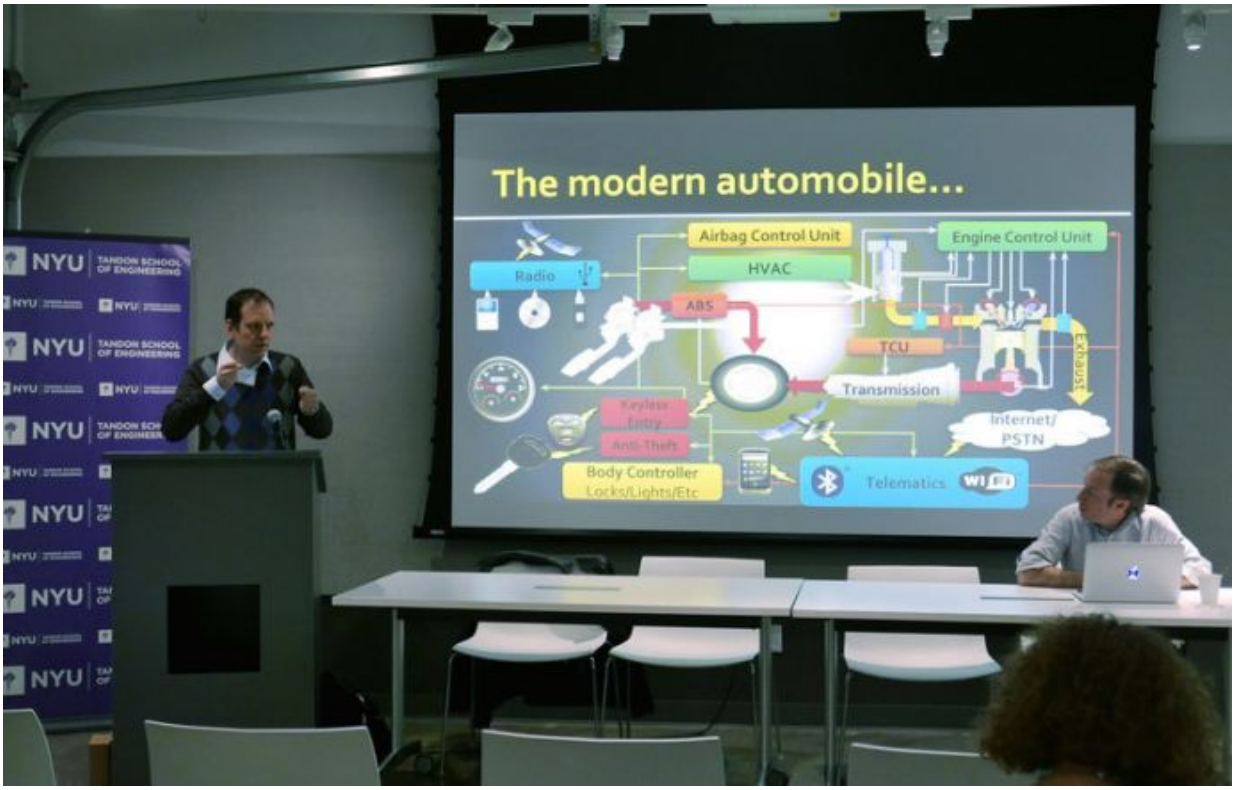
Call issued to white hat hackers—find the flaws in new automotive software updater

January 19 2017



NYU Tandon Professor Justin Cappos (L) gives a brief background on security in cars. Co-panelist Sam Lauzon (R) is an automotive cybersecurity developer in University of Michigan's Transportation Research Institute's Engineering Systems Group.

A consortium of researchers today announced the development of a

universal, free, and open-source framework to protect wireless software updates in vehicles. The team issued a challenge to security experts everywhere to try to find vulnerabilities before it is adopted by the automotive industry.

The new solution, called Uptane, evolves the widely used TUF (The Update Framework), developed by NYU Tandon School of Engineering Assistant Professor of Computer Science and Engineering Justin Cappos to secure software updates. Uptane is a collaboration of NYU Tandon, the University of Michigan Transport Research Institute (UMTRI), and the Southwest Research Institute (SwRI), and is supported by contracts from the U.S. Department of Homeland Security, Science and Technology Directorate.

Modern cars contain dozens of computers—called ECUs (Electronic Control Units)—that control everything from safety equipment (airbags, brakes, engine, and transmission, and more) to entertainment systems. The increasing complexity of modern cars accompanies an increasing likelihood of flaws in the software. To combat this, vehicle makers are equipping ECUs with a secure Software Over-The-Air (SOTA) update capability, allowing the software to be changed without visiting a service depot, resulting in fewer recalls and greater customer satisfaction. However, hackers can target these software update mechanisms to install malicious software, viruses, or even ransomware, the results of which could be catastrophic.

In 2013, a single attack, spread by software updates and configuration management systems in South Korea, cost banks and media companies an estimated three-quarters of a billion dollars. The notorious Target attack spread the same way. Experts agree: Cars and trucks are similarly vulnerable.

"Although widespread attacks are still difficult and expensive, they lie

within the capabilities of nation-state cyber warriors, and it is time to begin securing the infrastructure, particularly as automotive electronics increase," Cappos said.

Uptane goes beyond TUF in order to address the unique problems posed by automotive software. For example, it allows automakers to completely control critical software but to share control when appropriate—for example, when law enforcement needs to tune a vehicle for off-road conditions. It also helps automakers to quickly deploy secure fixes for a vulnerability exploited in an attack or to remotely (and inexpensively) update a car's electronics.

In a meeting at UMTRI's Ann Arbor, Michigan, headquarters yesterday with automakers representing more than three-quarters of the vehicles on U.S. roads, plus automotive suppliers and government agencies, the Uptane working group publicly released the Uptane design. The group has been holding regular design workgroups to develop a universal framework that could enhance the security mechanisms, protecting cars as soon as next year.

As is standard practice in open-source projects, the team called upon security experts everywhere to help them find flaws in the proposed framework so that a secure final version can be adopted.

More information: The Uptane design and software is available at uptane.github.io

Provided by New York University

hackersfind-flaws.html