2020 IEEE Conference on Communications and Network Security (CNS)

Off is Not Off: On the Security of Parked Vehicles

Kyong-Tak Cho
University of Michigan, Ann Arbor
ktcho@umich.edu

Kang Shin
University of Michigan, Ann Arbor
kgshin@umich.edu

Yu Seung Kim
Ford Motor Company
ykim41@ford.com

Byung-Ho Cha
Ford Motor Company
bcha@ford.com

***Abstract*—While various ways of attacking and thus controlling the vehicle have been demonstrated, all these attacks were shown to be feasible and effective only while the vehicle is running, i.e., ignition is on. In this paper, we invalidate the conventional belief that remote vehicle attacks are feasible and hence their defenses are required only when the vehicle's ignition is on. We first analyze how operation (e.g., normal, sleep, listen) modes of electronic control units (ECUs) are defined in various in-vehicle network standards and how they are implemented in real vehicles. From this analysis, we discover that an adversary can exploit the wake-up function of in-vehicle networks—which was originally designed for enhanced user experience/convenience (e.g., remote diagnosis, remote temperature control)—as an *attack vector*. Ironically, the battery-saving feature in in-vehicle networks makes it easier for an attacker to wake up ECUs and, therefore, mount *Battery-Drain* (BD) or *Denial-of-Body-control* (DoB), and *Unattended Control* (UC). In particular, we** can disable, abuse, and/or access parked vehicles with the ignition off. Ironically, the main reason for this feasibility is the "wake-up functions" — which are intended to enhance the driver's convenience — let the adversary wake up ECUs (of a parked vehicle) and then control them. That is, the wake-up functions that were originally designed for a good cause become an *attack vector*. Wake-up functions are standardized, implemented, and provided in various in-vehicle networks so that manufacturers can provide remote standby functions, such as remote diagnostics, door control, and anti-theft. Although only a few ECUs of a parked vehicle can be awakened by the wake-up function and then controlled, these attacks are still feasible mainly because they are achieved by controlling ECUs that are asleep, but not completely turned off. The rationale