Adv Automob Eng 2018, Volume 7
DOI: 10.4172/2167-7670-C1-012

Seizing the wheel: Hacking the connected car

Ken Munro
Pen Test Partners, UK

The connected car is highly vulnerable and the attack vectors we have previously seen that required local access are now being replaced by more sophisticated methods. Virtual carjacking, steal-to-order, malware and ransomware and even crypto-mining are all now plausible placing the public at risk. Specialist automotive ethical hackers, experienced in attacking manufacturer's cars at their behest, will perform live demonstrations of how these vehicles can be compromised. This practical presentation will cover the techniques that thieves and malicious attackers use to override systems and how security mechanisms can be reverse engineered and exploited to unlock or deactivate safety features. We will explore the following: how telematic control units (TCUs) can be compromised remotely, allowing the attacker to attempt access from a distance, and how this could pave the way for fleet wide attacks? how current safeguards, such as OTA updates, are inadequate and can themselves be exploited and used to compromise a vehicle in the form or rogue firmware updates? and how even the most advanced manufacturers who are supposedly leading the field in autonomous tech are still susceptible to attack by sharing our latest ground-breaking research into the security of the Tesla vehicle platform?

sarah@newshoundcomms.co.uk