Securing the connected car

Name Marcus Nissemark

Abstract text Recent years we have seen things that many in the automotive industry hoped would never come. We have witnessed multiple demonstrations by white hat hackers that showed remote attacks on fielded vehicles that put not only our personal information, but also our safety at risk. As an industry, we can no longer bury our heads in the sand when it comes to cybersecurity. It is time to act with a holistic approach to security for the connected car. In this talk, we will take a look at common pitfalls that lead to vulnerabilities as well as an architecture and techniques for building secure and reliable software for the connected car.
• Examine common security challenges encountered when designing automotive- grade software
• Review a software architecture and development techniques for building provably secure software levering software-based separation as a foundational component of the system • Consider aspects beyond the software architecture, including management of the development processes, secure boot, software updates, and key management that are crucial to the overall security of the system