Mobile app security issues in the automotive sector- and possible improvements

Presentation Abstract

In the main part of the presentation, we will demonstrate how compromising a mobile device with malware, leads to lost credentials and eventually hijacking and ħtealing¨of a car. The described attack methods, will not only be put in context of other flar attacks¨but also be used to illustrate the general problem of how lack of adequate protection, constitutes a great risk to appħ which are dealing with sensitive information, as for example mobile banking, mobile payment or mobile authentication. In the presentation, a wide range of attack vectors will be described. The fundamental attack scenario will show how widely available attack tools and methods, can be used, even on non-rooted mobile devices (Android) to steal essential information as the user is interacting with a Tesla mobile app. The stolen information is then mis-used in a second step to show how an attacker may hijack or even steal the Tesla car of the user. The attack methods used will range from relatively simple keylogging attacks, to state-of-the-art malware methods as currently seen in banking malware for mobile. ¨Along with the presentation of various attack techniques, we will elaborate on how various security fiest practices' and other counter measures, could have greatly reduced the risk of such an attack. In the presentation a mix of demonstration methods will be used, including:

o A video showing how the hijacked Tesla can be remote controlled, and even stolen.

o A screen video (and screenshots) of the mobile phone of the user and attacker, to illustrate how the attacker may spy on the owner, following the cars exact location, or how app-hijacking leads to the owner being un-able to detect that the car is stolen and something is wrong.

The Tesla-hack illustrates the fact that security in the automotive space, is not only about the security of the car itself, but even more importantly the security of the app used to access and control the car. An essential part of the security paradigm for the automotive industry is to protect the appħ which are used to access, monitor and control the car. Attacking the car by attacking the application controlling it, typically requires a low level of expertise, and very little resources. Hence, the first line of defence for the automotive industry, an essential first step, should be in protecting the mobile app. In addition to following basic best practices for the security of the car (and communication to and from).