

Wednesday, August 12. 2015

Hacks an Autos sollen zu schwer sein...

Heute las ich einen Artikel, dass Sicherheitsforscher der Meinung sind dass Auto-Hacks schwer zu kopieren sind.

Meine Erfahrungen gehen in die andere Richtung: Alles wird versucht zu vereinheitlichen innerhalb eines Konzerns, um Synergie-Effekte zu haben. Das bedeutet dass dieselben Komponenten (Hard- aber auch Software) Ä¼berall benutzt werden.

Und weil "Security by Obscurity" so gut funktioniert wird erwartet dass "weil ja niemand etwas weiss" alles sicher ist. Selbst wenn "nur" das Auto raustelefonieren darf - was hindert mich daran, von innen eine TCP-Verbindung aufzumachen und stehenzulassen? Okay, ich brauche eventuell physischen Zugriff. Oder ein speziell angepasstes mp3-StÄ¼ck welches ich dem Inhaber des Autos mitgebe. Standard-Libraries (Open Source) haben den Vorteil dass sie fÄ¼r Firmen kostenlos zu benutzen sind und daher auch gerne eingesetzt werden. Wohin das fÄ¼hrt sah man schon bei vielen snmp-Bugs, wo plÄ¼tzlich Hersteller wie Cisco, Juniper, ... alle auffÄ¼llig zeitgleich ihre Systeme patchen mussten.

Also sorry, ich glaube nicht dass es ausreicht sich darauf zurÄ¼ckzuziehen, dass es zu schwer wird oder es sich nicht lohnt.

Posted by rince in CCCS at 10:18