

Hoe steel ik een auto zonder een schrammetje te maken, een praktische aanval op KeeLoq

KeeLoq is een beveiligingstechnologie die vaak gebruikt wordt in de antidiefstalsystemen van auto's, onder andere voor het ontgrendelen van de portieren en het uitschakelen van het alarm. Recent zijn onderzoekers van de afdeling ESAT-COSIC er samen met collega's uit Israël in geslaagd om KeeLoq te breken.

Tegenwoordig beschikt zowat iedere auto over een afstandsbediening om de deursloten te openen en het diefstalalarm uit te schakelen. Maar hoe werken deze systemen, en nog belangrijker, zijn ze wel veilig?

De oudste dergelijke systemen zijn heel eenvoudig. De afstandsbediening zendt iedere keer een zelfde, vaste geheime code uit. Zodra de auto de correcte code ontvangt, worden de sloten geopend en het alarm uitgeschakeld. Maar natuurlijk kan niet enkel de auto deze code ontvangen. Omdat de code in deze systemen steeds dezelfde is, volstaat het om deze één keer te onderscheppen, en daarna gewoon opnieuw uit te zenden.

KeeLoq, dat stamt uit de jaren '80 maar desondanks nog steeds vaak gebruikt wordt, is een van de systemen van de volgende generatie.

Deze beweren niet vatbaar te zijn voor de problemen waarmee de vorige generatie van systemen kampte, omdat zij steeds een andere geheime code uitzenden. Het onderscheppen van transmissies is dus zinloos.

KeeLoq bevat ook meer geavanceerde functionaliteit, waarbij een tweewegscommunicatie tussen de sleutel en de auto gebruikt wordt.

In de COSIC onderzoeksgroep van de K.U.Leuven hebben we, samen met enkele collega's uit Israël, de veiligheid van het KeeLoq systeem onderzocht. We zijn tot de conclusie gekomen dat KeeLoq absoluut niet zo veilig is als wel beweerd werd. Bij deze demo wordt meer informatie gegeven over hoe dat in zijn werk gaat, en wat de gevolgen hiervan zijn.

