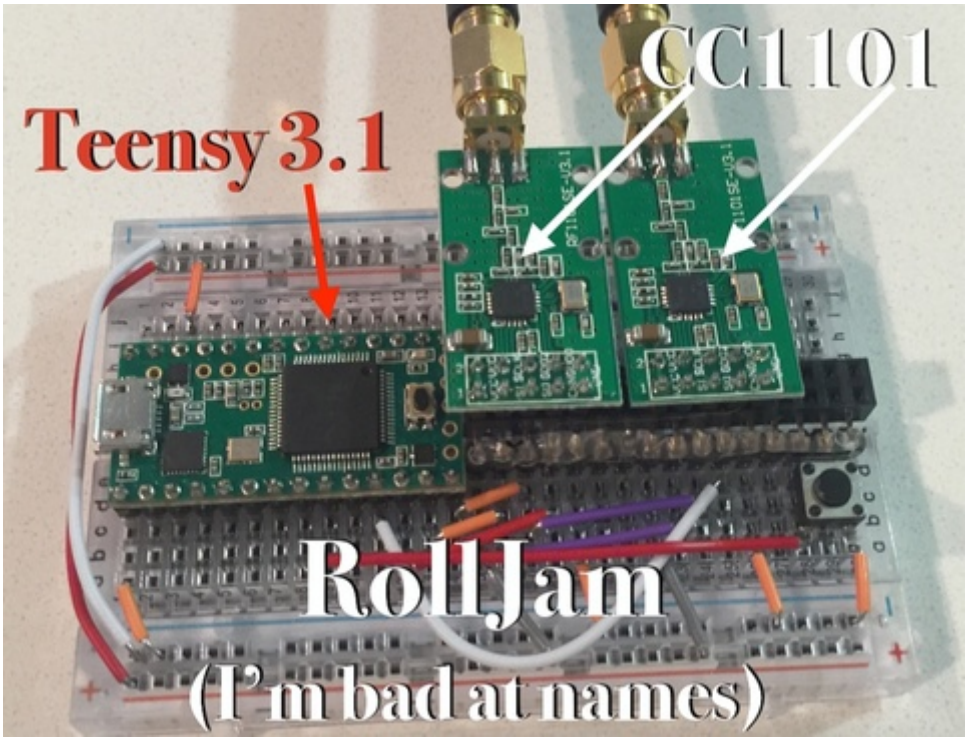
Kas tõesti võimalik? 32-dollarine raadioseade avab pea iga auto või garaažiukse

11 aastat tagasi - 11.08.2015 Autor: Kaido Einama



Hiljuti lõppenud DEF CONi konverentsilt tuleb huvitavaid teateid erinevatest häkkimistest ja turvaaukudest. Alles see oli, kui muugiti Tesla Model S-i. Raadiohäkker Samy Kamkar, kes on varemgi suletud uksi lahti teinud, pani kokku lihtsa raadioseadme, mille komponendid maksavad kokku vaid 32 dollarit ja häkkeri väitel suudab see lahti teha raadio teel puldist avatava garaažiukse või autoukse, mis kasutab levinud National Semiconductori “High Security Rolling Code” kiipi.

Turvakiip hoolitseb selle eest, et igal avamisel saadetakse puldist seadmele alati uus turvakood, et seda ei saaks pealt kuulates uuesti kasutada.

Kuid just siia ongi koer maetud.

Puldid saadavad avatavale autole või uksele iga kord uue koodi. Vahepealne seade aga, mis peab asuma häkitava ukse lähedal, napsab selle koodi ära, segades auto raadiovastuvõtjat ning jätab ukse avamata. Nüüd proovib kasutaja loomulikult uuesti - saadetakse järgmine võti, mis hoitakse vahepeale paigutatud seadmes alles. Raadioeetri segamine auto jaoks lõpetatakse ja edastatakse

esimene kinninabitud kood, millega loomulikult uksed avanevad. Kuid järgmine, teisena salvestatud kehtiv kood jääb häkkimis-seadmesse tallele ja sobival hetkel tuleb häkker, kasutab seda salvestatud koodi ja saabki niimoodi ka hiljem ukse lahti. Kasutaja ei märka midagi - avastab ainult, et üks kord pulti vajutades see ei töötanud ja auto ei avanud uksi. Kuid juba teise vajutusega oli kõik korras.

Kamkar tegi selle häkkimisseadme tõestamaks tootjatele, et nende süsteemis on turvaauk. Autode muukimise seadmeid ta müüma ei kavatse hakata, vaid loodab, et see turvaauk kiiresti kõrvaldatakse - krüpteerides võtmeid, kasutades uusi algoritme, ajalukke jne. Loodame meiegi. Praegu on Kamkar testinud oma seadet Nissani, Cadillaci, Fordi, Toyota, Lotuse, Volkswageni ja Chrysleri autode ukseavajate peal, samuti töötab häkk Cobra ja Viperi alarmseadmete ning Genie ja Liftmasteri garaažiavajatega.

Vaata Kamkari slaide DEF CONi ettekandest.

PILT DEF CON-I SLAIDILT