Kuidas häkkida eemalt valguse ja heliga

16. märts 2017 - 22:31 Autor: AM

Arvutitesse häkitakse sisse tavaliselt üle võrgu. Mõnikord ka lisaseadmetest - näiteks klahvivajutuste simulaatoriga USB-pulgalt. Kuidas häkkida aga siis, kui arvutile lähedale ei pääse? Siis tuleb appi võtta valgus ja heli. Mitte arvutitesse, vaid ka muudesse nutiseadmetesse häkkimiseks.

Valgus reedab masina sisu

Kui pahavara on mingil moel saadud arvutisse, mida ei hoita avalikus netis, kuid mis sisaldab salajast infot, siis sinna see jääbki - pole erilist lootust andmeid kätte saada. Või siiski... igasugustest tulemüüridest, eraldatud võrkudest ja kaitsetest saab mööda lihtsa arvuti LED-tulukese abil. Tavaliselt on see kõige ihaldatum info just neis võrgust eraldatud arvutites.

Jättes seekord kõrvale teema, kuidas sellisesse arvutisse pahavara sisse saadi, räägime sellest, kuidas häkkida infot sealt välja, kui "oma mees" ehk trooja hobune juba sisse toimetatud on. "Trooja hobuseks" võib olla mõnele töötajale sokutatud nakatunud USB pulk või muu andmekandja, mis arvutisse vajaliku programmijupi toimetab.

Arvutil on tavaliselt küljes mitmesuguseid LED-tulesid - kõvakettatuli, sisse-välja lülitamise tuli, võrguühenduse indikaator, isegi klaviatuuri *Caps Lock* ja *Numpad´i* tuled. Kõiki neid annab programmeerida, kui arvutis on olemas vastav sinna sokutatud tarkvara. LED tuluke võib vilkuda kuni 6000 korda sekundis, see teeb kõva 6 kilobitti sekundis - vähe, aga olulise dokumendi teksti edastamiseks üsna piisav. Kui keskmine masinakirjalehekülg on 3000 tähemärki ehk 3 kilobaiti ehk 24 kilobitti, siis võiks infot salajasest arvutist välja lekkida kiirusega üle kümne lehekülje minutis.

Iisraelis Ben-Gurion Ülikooli küberturvalisuse osakonnas just sellist häkkimistehnikat katsetati. Vaja on otsenähtavust ja kui tegemist on mitmekordse kontorihoonega, siis peab akna taha lendama - näiteks drooniga.

Nii see käibki:

Remove video

Kuidas häkkida heliga?

Jah, põhimõtteliselt saab ka helipiiksudega edastada samamoodi infot, nagu vanasti tegid modemid telefoniliinidel. 64 kbit/s oli keskmine modemikiirus, eks tegelikult hea kuuldavuse korral saaks kätte ka suuremaid kiirusi, kuid selline häkkimine ärataks kindlasti tähelepanu, kui mõni arvuti hakkaks järsku nagu eelmise sajandi modem hirmsasti häälitsema vana modemi moodi.

Heliga häkkimine puudutab aga rohkem hoopis selliseid nutiseadmeid, millel on sees kiirendusandur. Sellisteks seadmeteks võivad olla puuteekraaniga sülerid, tahvlid, nutitelefonid, nutikellad ja isegi auto pardakompuutrid.

Michigani Ülikoolis USA-s prooviti mõjutada MEMS kiirendusandureid, mida kasutavad paljud eelpoolnimetatud seadmed. Tavaliselt arvutid ja nutiseadmed usaldavad oma sisemisi andureid ja puudub igasugune turvakontroll, kas nende kaudu ehk midagi võidaks paha teha. Isegi lennukid ja meditsiiniseadmed usaldavad tingimusteta kiirendusandureid ja ei kontrolli neid.

Michiganis leiti, et teatud sagedusega helilainetega mõjutades võib seadme panna arvama, et kiirendusanduri näidu järgi toimub mingi liikumine. Aga mis siis? Liikumine ei tähenda ju veel midagi. Kuid Michigan Engineeringu insenerid arvavad, et sellest on juba mõnel juhul küllalt. Vähemalt hirmutada juba saab, kui mitte enamat. Näiteks pandi katse käigus helilainetega mõjutades mobiiltelefon robotit juhtima, mida muidu juhtis kasutaja telefoni kallutades ja liigutades. Samuti sai kiirendusanduri näitudega mängides kirjutada mobiiliekraanile teateid või teha aktiivsusmonitoriga tuhandeid petusamme, mida kasutaja ise ei teinud. Kui midagi juhitakse seadmega, mis juhtimisliigutuste registreerimiseks kasutab kiirendusandurit, siis ongi võimalik juba helilainega millegi (drooni, mänguauto, päris-auto, lennuki) juhtimine üle võtta.

Katse edukus sõltub kiirendusandurite resonants-sagedustest. Testis leiti paarikümne erineva tootja kiirendusandurite resonants-sagedused ja neid õigesti ette mängides annabki see andur seadmele tegelikust liikumisest erineva, manipuleeritud tulemuse.

Uudised
Andmeside
Droonid
Komponendid
Mobiiltelefonid
Nutikellad
Turvalisus