Kolm paranoilist õppetundi: nad saavad su paroolid kätte ka arvutisse häkkimata

11 aastat tagasi - 15.01.2015 Autor: AM

Sa oled oma arvuti viirusetõrjet täis toppinud, paroole ei hoia mitte kuskil üleskirjutatuna, vaid need on viimseni pähe tuubitud ning kogu andmeside netiga saab tugevalt krüpteeritud. Kuid nad saavad su salasõna ikka kätte. Ja veel niimoodi, et sellest ei jää mingit jälge.

Siin on kolm võimalust. Õnneks pole ükski neist väga lihtne, aga tehnika ja oskuste arenedes muutub see kõik aina kergemaks.

Foto: (CC) Ivan David Gomez Arce / Flickr

1. Arvuti lekitab kõike otse eetrisse, tuleb ainult osata kuulata

Kineskoopide ajastul muutus kõik lihtsaks juba 90ndate lõpul - teleka kineskoop kiirgas võimsalt pildi-infot kümnete meetrite kaugusele, nii et spetsiaalsete aparaatidega sai taastada kuvaripildi ehk selle, mis arvutiekraanidel näha oli. Sealt muidugi paroole veel alati kätte ei saanud, aga leidis muud huvitavat. Nö vahejaama sai peita kasvõi õhupüssi kuuli sisse, mis tulistati pealtkuulatava akna raami külge. Sealt edastati ekraanipilt juba "mustade klaasidega mikrobussi"

tänaval.

Vahepeal on aeg edasi arenenud ja kuvarid enam nii palju ei kiirga, kuid õhukesed vähevarjestatud sülearvutid saadavad endiselt eetrisse igasuguseid signaale, millest annab välja rehitseda näiteks ka klahvivajutusi.

Atlantas asuv Georgia Tehnoloogiainstituut uuris, mida siis arvutid kiirgavad ja kas neis signaalides võiks ola ka midagi kasulikku pealtkuulajale.

Suurimad kiirgusallikad on kondensaatorid, protsessorid, aga ka muud elektroonilised komponendid, sealhulgas ka klaviatuuriga seotud komponendid. Uuringu üks läibiviiatest Alenka Zajic siiski rahustab meid natuke, väites, et neid "õigeid" signaale on väga raske eetri kaudu kätte saada ja selekteerida.

Siiski õnnestus neil lõpuks saada arvutist kätte klaviatuuril sisestatud paroolid, kirjutab Discovery, kasutades pealtkuulamiseks lühilaineraadiot ja ümberehitatud mobiiltelefoni. Need seadmed pidid olema kuulatavast arvutist mõne meetri kaugusel. Näiteks kohvikus laua all.

Veelgi peenem töö on tundlike mikrofonidega üles võtta helid, mida tekitavad arvutis asuvad kondensaatorid. Ka see on võimalik, kuid veelgi keerulisem.

Lahendusena nähakse instituudis tarkvaralisasid, mis spetsiaalselt segavad signaali ja tekitavad eetris tarbetut müra, mille seest kindlaid mustreid oleks raskem leida. Varjestamine pole paraku lahendus, kuna arvutid ja mobiilseadmed on muutunud nii õhukeseks, et iga lisagramm ja lisamillimeeter on kaalul.

2. Juhtmevaba klaviatuur saadab klahvivajutused mitte ainult sinu arvutisse

Jätkame paranoiaõppetunniga nr 2, kus räägime arvutiturvalisuse uurija ja asjatundja Samy Kamkari loodud lihtsast USB-laadijast, mis pole tegelikult päris see, millena paistab.

Samy ehitas Arduinol põhineva lihtsa *keylogger*i ehk klahvivajutuste salvestaja, mis ei ärata mingit tähelepanu - näeb välja nagu üks tavaline mobiili USB-laadija. Tegelikult aga kuulab eetrit ja salvestab sealt juhtmevaba klaviatuuri klahvivajutused.

Jällegi ei pea arvutisse sisse häkkima, jällegi ei jää nuhkimisest mitte mingisugust jälge.

KeySweeper pole niisama lapse mänguasi. See sisaldab veebipõhist liidest online´is klahvivajutuste jälgimiseks, võib "omanikule" saata SMS-se mingite märksõnade ilmnemisel ja registreerib veebiaadresse, kasutajanimesid ja paroole eraldi muude klahvivajutuste vahelt. Juhul, kui keegi seina "unustatud" mobiililaadija seinast eemaldab, töötab see klahvivajutuste registraator mõne aja veel edasi, sest sisse on peidetud ka väike aku. Samy Kamkar sai selle vidina valmis jõulude ajal, kui oli rohkem aega.

Keysweeper töötab Microsofti juhtmevabade klaviatuuridega ja veel hiljuti oli kõik pealtkuulatav ka täiesti uue, poest ostetud klaviatuuriga. Seade kasutab ära võimalust, mis ei nõua MAC-aadressi teadmist, et krüptitud liiklust lahti dešifreerida.

Autor on lahke ja jagab lähtekoodi ka Githubis.

Vaata videot:

3. termokaamera on muutunud käepäraseks ja paljastab paroolid

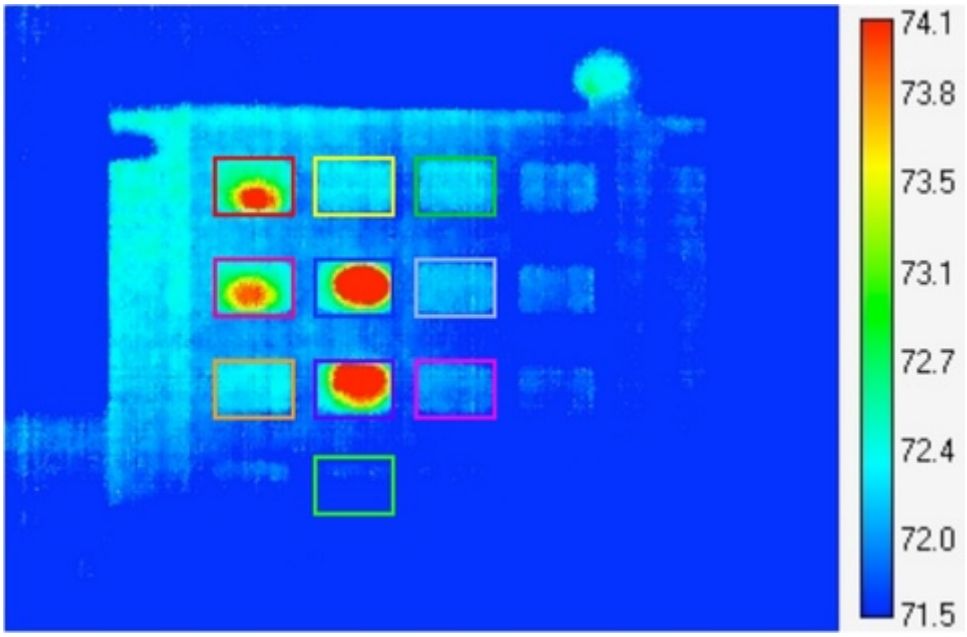
Kui veel mõni aasta tagasi räägiti võimalusest õues pangaautomaadi klaviatuurilt termokaameraga lugeda, mis järjekorras soe inimsõrm milliseid klahve vajutas, siis oli see pigem ülikalli tehnikaga varustatud kurjamite unelmate teoreetiline võimalus.

Termokaamerad odavnevad, nüüd on need saadaval lausa mobiililisanditena ja Hans Lõugas Eesti Päevalehest tegigi järgi kodumaise testi, kas selle lihtsa mobiililisandiga õnnestub klaviatuurilt sisestatud tähemärke ära arvata.

Üle 300 euro maksev Flir One, mis teeb telefonist soojuskaamera, siiski selles testis PIN-koodi ära arvata ei suutnud. Soojusjälg oli klahvidel liiga pisike.

Seega on ikka endiselt vaja väga tundlikke, võimsaid ja kalleid suuri termokaameraid, mis sellist pahategu lubaksid teha.

Üks uuring nende võimaluste kohta on avaldatud siin: PDF. Sealt selgub, et ka klahvide äraarvamise puhul neljakohalises koodis tuleb ikkagi proovida keskmiselt 24 korda, enne kui õige paroolini jõuda. Kolme vale PIN-iga aga tavaliselt parool lukustub. Kui klahve vajutatakse suurema vahega, siis muidugi saab veel hinnata soojusjälje tugevust ja sellest järeldada klahvide vajutamise järjekorda, aga ka siis on võimalus, et näiteks paroolis on mitu sama numbrit, aga mis järjekorras, seda jällegi ei tea. Seega kerge ei saa äraaarvamine olema.



Pilt on pärit viimasena lingitud uurimistööst - pangaautomaadi klahvide pilt termokaameraga.

- Uudised

- Turvalisus