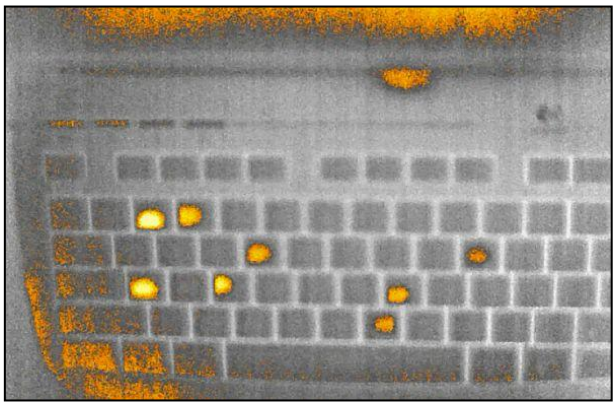
Hőkamerával és mikrofonnal visszafejthetők a jelszavak

Biztonsági kutatók ötvözték egy hőkamera képét a billentyűleütések hangjával azért, hogy így rekonstruálják a jelszavakat.

A *Gene Tsudik*, a Kaliforniai Egyetem (Irvine) professzora által vezetett csoport a Black Hat Asia nevű biztonsági konferencián bemutatott módszert Thermanatornak nevezte el. A csapat tagja volt még *Ercan Ozturk* és *Tyler Kaczmarek*, szintén a Kaliforniai Egyetem (Irvine) PhD-hallgatói, valamint *Pier Paolo Tricomi*, a Padovai Egyetem mester hallgatója.



A szakemberek egy kereskedelmi forgalomban kapható hőkamerával (FLIR SC620) fotóztak le egy átlagos billentyűzetet, amellyel valaki korábban megadta a jelszavát. 30 másodperccel a billentyűk lenyomása után még mindig felismerhetők voltak a hőképek. Mindez a műanyagok hővezető képességével van összefüggésben. Az ujjbegyek által átvitt hő a lenyomott gombokat legfeljebb 60 másodpercig teszi láthatóvá. A játékosok által használt fémbillentyűzetek esetében ugyanakkor ez a módszer nem volt alkalmazható.

Tsudik hangsúlyozta, hogy az az idő, amíg a hőkép látható, függ az ujj méretétől és a környezet hőmérsékletétől is. Az átlagos idő 30 másodperc, a részleges minták azonban még 60 másodperc után is láthatók. Tízujjas gépelés esetén rosszabb eredmények születtek, mert a tenyér által leadott hő eltorzítja a mintafelvételt.

A szakértők tanulmányozták a mikrofon segítségével rögzített billentyűhangokat is. Jól kivehető volt, hogy valaki milyen sorrendben nyomta le a gombokat és hogy melyiket nyomta le esetleg több alkalommal is, vagy egymás után. Különböző módszerek, így a gépi tanulás és a beszédfelismeréshez alkalmazott Mel-frekvenciás kepsztrális komponens (Mel Frequency Cepstral Coefficients) segítségével a kutatók ötvözték a hőkamerák képeit és a billentyűhangokat. A munka egy része *Daniele Lain* korábbi Black Hat konferenciás előadásán alapult. A kutató szintén a hangok alapján rekonstruálta a beírt szövegeket.

A mostani kísérleteknél az eredmények a következőképpen alakultak: ha a szakértők 1-5 alkalommal próbálkoztak, akkor az összes eset 20 százalékában koronázta siker az erőfeszítéseiket, míg, ha 45-ször, akkor gyakorlatilag teljes sikert könyvelhettek el. Az utóbbihoz ugyanakkor akár több napon át meg kellett figyelniük a célszemélyt. Arra viszont nem sikerült magyarázatot találni, hogy a jó jelszóváltozat megadásának esélye miért nőtt 87 százalékra akkor, ha az áldozat a Logitech egyik klaviatúráját használta. Az Azio és a Dell billentyűzetei esetében ugyanis az arány sokkal kisebb volt.

A kísérletek során ugyanakkor kizárták a véletlenszerűen generált, bonyolult jelszavakat. Tsudik ezt azzal indokolta, hogy azokat a résztvevők nem tudták megjegyezni, ez pedig késleltetett belépéshez és megbízhatatlan akusztikai elemzésekhez vezetett.

Forrás: https://sg.hu/cikkek/it-tech/135841/hokameraval-es-mikrofonnal-visszafejthetok-a-jelszavak

Válogatta: Berke Barnabásné