https://www.cas.sk/clanok/608292/petr-svenda-z-timu-ktory-upozornil-na-chybu-v-elektronickych-obcianskych-preukazoch-desive-zistenie/

Petr Švenda z tímu, ktorý upozornil na chybu v elektronických občianskych preukazoch: Desivé zistenie!

17

zdieľaní

Zdieľaj Diskusia / **2**

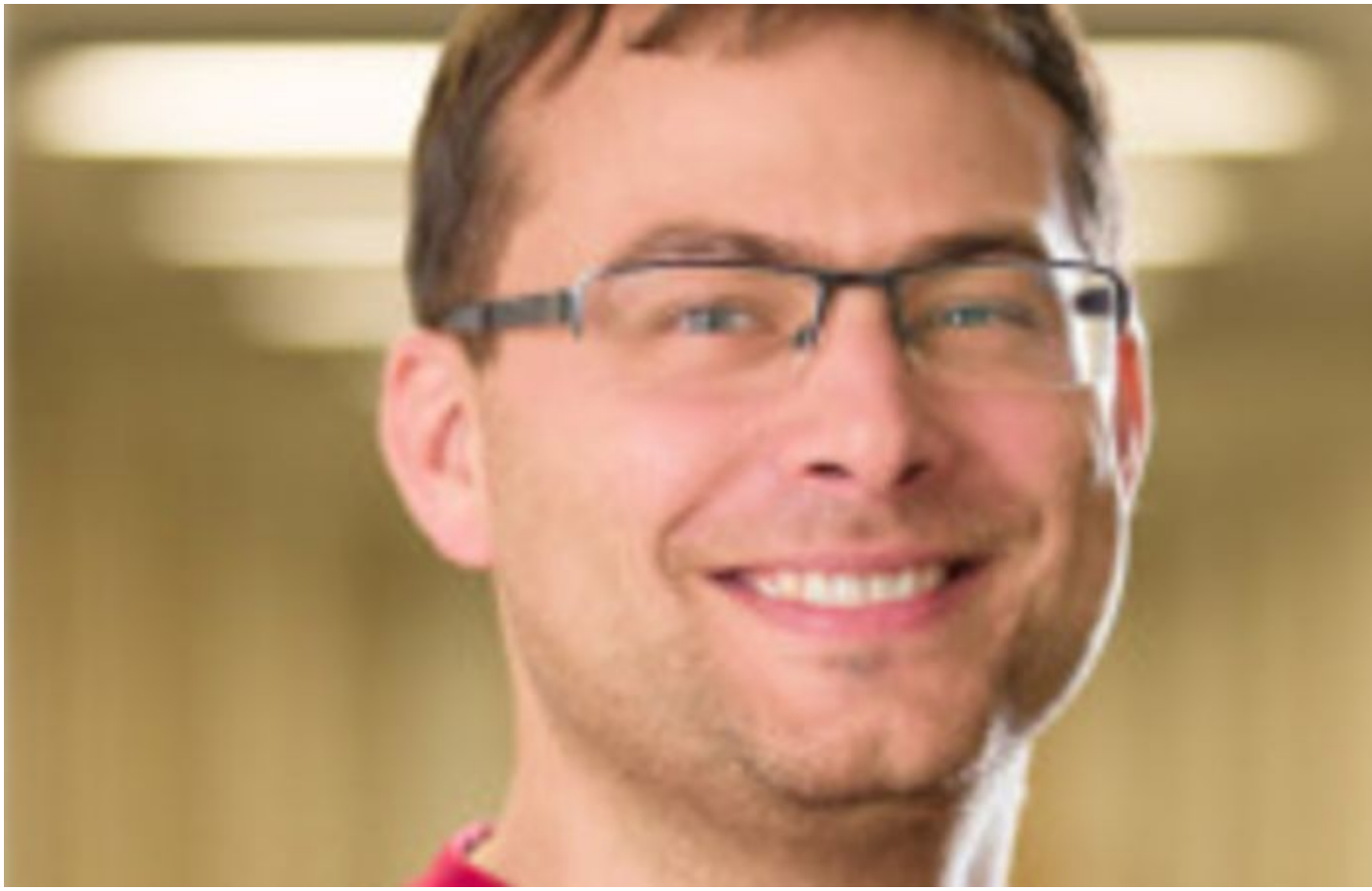
prihlásiť/registrovať

18.10.2017, 14:00

17zdieľaníZdieľaj na Facebooku Zdieľaj

Diskusia / **2**

Máte tip? Dajte nám vedieťMáte tip?



<img src="https://t3.aimg.sk/magaziny/JHUpXG1mTMjum0334R9nBQ~Ako-sa-d-elektronick-podpis-ukradn-a-ko-ko-to-stoj-pe-az-Nov-mu-asu-prezradil-len-t-mu-Petr-venda.jpg?t=LzI5eDI5NDoxMTIxeDkwOC84MDB4NDUwL3NtYXJ0&h=A2ue9QG-NCCuzIfK_RxCXg&e=2145916800&v=3"> 1

Ako sa dá elektronický podpis ukradnúť a koľko to stojí peňazí, Novému Času prezradil člen tímu Petr Švenda.

Zdroj: apš

Všetko sa začalo pred vyše dvoma rokmi, keď sa tím troch slovenských a dvoch českých expertov z Masarykovej univerzity v Brne rozhodol preveriť bezpečnosť čipov od firmy Infineon.

Pri skúmaní však zistili, že elektronický podpis niektorých čipových občianskych preukazov, vrátane tých zo Slovenska sa dá ľahko zneužiť. Ako sa dá elektronický podpis ukradnúť a koľko to stojí peňazí, Novému Času prezradil člen tímu Petr Švenda z Katedry počítačových systémov a komunikácií na Masarykovej univerzite v Brne.

<img src="https://t2.aimg.sk/magaziny/kw-lvRNuTb_z7UY5gun-ZQ.640~Na-chybu-v-bezpe-nosti-slovensk-ch-ipov-ch-ob-ianskych-preukazov-upozornil-t-m-expertov-z-Masarykovej-univerzity-v-Brne.jpg?t=LzB4Mzg6NjQweDM5Ny8yNjB4MTc0L3RvcC9zbWFydA%3D%3D&h=GuqWQIpBzVGaAsAVq9bIyg&e=2145916800&v=3">

Slovenskom otriasa obrovský škandál s elektronickými občianskymi preukazmi: Identitu vám ukradnú za dva týždne!

Čo sa vám podarilo zistiť?

Zistili sme, že čipy od jedného výrobcu generujú kľúče so štruktúrou, ktorá sa dá útočníkom ľahko zneužiť. Takéto čipy sú aj v slovenských občianskych preukazoch. Zariadenie totiž vždy vygeneruje dve polovice kľúčov - jedna je určená na verejné overenie elektronického podpisu a druhá musí byť uchovaná v tajnosti. Je to totiž tá časť kľúča, ktorou človek podpisuje dokument. My sme ukázali, že prostredníctvom tej verejnej časti sa dá dopočítať aj tá súkromná - chránená časť.

Dá sa tak ukradnúť niekoho elektronický podpis? Ako to funguje?

Útočník sa musí dostať k verejnému kľúču čipu. Najjednoduchším spôsobom je, ak človek použil slovenský občiansky preukaz s čipom na podpis nejakého dokumentu. Tam sa totiž verejný kľúč klasicky prikladá, aby sa dalo overiť, že podpis je skutočne váš. Na dopočítanie tajného kľúča občianskeho potom páchateľ potrebuje tak 17-tisíc eur. Ak sa však digitálny podpis dá využiť na prevod nehnuteľnosti, tak sa to útočníkovi oplatí. Tiež platí, že tieto útoky sa stávajú stále rýchlejšie a lacnejšie.

Ide len o občianske preukazy?

Netýka sa to len občianskych preukazov, problém je v čipoch, ktoré tento výrobca vyrába, a tie sa využívajú aj pri vstupoch do systémov či v osobných počítačoch. Týkalo sa to aj iných štátov, ako je Estónsko a iné. Napríklad pasy by mali byť v poriadku, pretože tam sa používajú iné algoritmy, ale vždy je to nutné overiť. Závisí to od toho, pre aký algoritmus sa štát rozhodol.

Koho ste na chybu upozornili?

Chybu sme objavili koncom januára a ihneď sme upozornili priamo výrobcu, ten zase upovedomil aj slovenskú stranu. Informácia sa zverejňovala na úrovni štátov v rámci Európy. Keď výrobca chybu preveril, zachoval sa seriózne. Ihneď sa snažili zamedziť ďalším chybám a riešili, ako notifikovať už stálych zákazníkov.

Ako možno zabrániť zneužitiu rizikových čipov?

Jedna možnosť je stiahnuť všetky čipy a vymeniť ich za nové, to je ale komplikované. Čipy sú extrémne drahé a je nutné, aby si ľudia prišli vymeniť občianske preukazy osobne. Existujú však aj iné alternatívy, ktoré závisia od toho, ako vyzerá program na čipovej karte. Myslím, že napríklad v Estónsku si vybrali prechod na iný algoritmus, aby nemuseli vymieňať všetky preukazy.

Môžu si Slováci bezpečnosť svojich zariadení nejako overiť?

Uvoľnili sme nástroj, ktorý umožňuje detekciu zraniteľných kľúčov. Slováci si môžu na stránke www.keychest.net/roca otestovať, či sú ich kľúče v ohrození.