Slováci objavili kritický svetový bezpečnostný problém, milióny RSA kľúčov sa dajú prelomiť

Značky: bezpečnosťSlovenskokryptografiakauza zraniteľných eID

http://www.dsl.sk/article.php?article=20329&title=

DSL.sk, 16.10.2017

Pondelok 16. októbra bude navždy zapísaný v
histórii počítačovej bezpečnosti ako čierny deň. Po zverejnení informácií o vážnom bezpečnostnom probléme vo WiFi protokole boli dnes zverejnené informácie o ďalšom mimoriadne vážnom bezpečnostnom probléme.

Na problém upozornili DSL.sk priamo samotní autori, ktorí problém objavili.

Na objavení tohto problému sa totiž podieľali slovenskí bezpečnostní experti z Masarykovej univerzity v Brne, Matúš Nemec, Marek Sýs a Dušan Klinec. Ďalšími členmi tímu sú Petr Švenda a Vašek Matyáš.

Slabé RSA kľúče

Problém je pomerne jednoduchý, populárne hardvérové kryptografické čipy od popredného výrobcu Infineon generujú slabé kľúče pre asymetrický šifrovací algoritmus RSA.

Môže za to knižnica použitá na týchto čipoch. Generované RSA kľúče majú špecifickú štruktúru, ktorá umožňuje pomerne ľahko zistiť z verejnej zložky RSA kľúča jeho privátnu zložku pomocou transformovanej Coppershmithovej faktorizácie.

Verejná časť RSA kľúča je z podstaty tohto algorimu často bežne skutočne sprístupnená verejnosti a problém tak umožňuje útočníkom získať privátne kľúče, ktoré umožňujú napríklad falšovať elektronické podpisy, prihlasovať sa, atď.

Technické detaily akú štruktúru majú kľúče zverejnia autori o dva týždne na konferencii ACM CCS.

Ktoré sú prakticky prelomené?

Na prelomenie takýchto kľúčov je potrebný pri faktorizácii ešte vysoký výpočtový výkon a miera praktického prelomenia závisí na dĺžke kľúča a cene za realizáciu potrebných výpočtov.

Bohužial sú reálne ale prelomiteľné aj 2048-bitové kľúče, ktoré sa dnes ešte bežne používajú. Na prelomenie takéhoto kľúča treba 140.8 rokov výpočtov na jednom jadre 3 GHz Intel Xeonu. Výpočty je možné úplne lineárne paralelizovať, teda tisíc jadrami je možné rýchlosti zvýšiť tisícnásobne.

Cena za prelomenie 2048-bitového RSA kľúča vygenerovaného zraniteľnými Infineon

čipmi pri prenajatí serverov Amazonu je v najhoršom 40 tisíc dolárov, v priemernom prípade iba 20 tisíc dolárov.

Podľa infomácií Klinca pre DSL.sk autori pracujú navyše na zlepšenom útoku, ktorý by mohol náklady ešte redukovať.

U 1024-bitových kľúčov je potrebných 97 dní výpočtov a cena je od 40 do 80 dolárov, cena za prelomenie 512-bitových kľúčov je 6 amerických centov.

Prelomenie 4096-bitových kľúčov na druhej strane nie je praktické.

Prelomiteľnosť nie je len o dĺžke kľúča, efektívne sa dajú prelomiť kľúče len niektorých dĺžok, medzi nimi teda ale všetky najbežnejšie vrátane 2048 a 1024. Konkrétne sa problém prejavuje pri 512 až 704 bitoch, 992 až 1216 a 1984 až 2144 bitoch.

Experti prelomenie s reálnym kľúčom pre potrebný výpočtový výkon a náklady testovali len na kratších kľúčoch, v dĺžke kľúča ale principiálny rozdiel nie je, spravili syntetický test s veľkosťou 2048 bitov s vygenerovaným kľúčom, u ktorého hľadanie trvalo kratšie, a samozrejme okrem iného ich zistenia sú považované za správne aj samotným Infineonom a práca bola prijatá na prestížnu konferenciu ACM CCS 2017.

Čo má problém

Čipy Infineonu s týmto problémov sa vyrábajú od roku 2012 a sú použité v mnohých produktoch, napríklad v TPM moduloch na doskách notebookov a počítačov ale tiež v špecifických autentifikačných riešeniach ako niektoré verzie yubikey.

Autori už identifikovali 760 tisíc konkrétnych prelomiteľných kľúčov, ktoré sú prístupné ľahko verejne. Celkovo ale očakávajú minimálne podľa oznámenia stovky miliónov zraniteľných kľúčov.

Špeciálne vážnou oblasťou je použitie týchto čipov v rozličných smart kartách a identifikačných dokladoch. Problematický čip je napríklad použitý v nových elektronických občianskych eID v Estónsku vydaných od októbra 2014, ktorých je 750 tisíc.

Estónci majú na eID kľúče pre autentifikáciu aj podpis, oba sú 2048-bitové RSA a sú zraniteľné. V Estónsku majú dokonca verejný register verejných kľúčov, ktokoľvek s dostatočnými prostriedkami si tak môže vypočítať privátny kľúč pre osoby, na ktoré sa zameria.

Riešenie

Čo sa týka existujúcich kľúčov, ktoré boli alebo mohli byť generované zraniteľnými čipmi, v prvom rade je potrebné overiť či sú naozaj zraniteľné. Autori zverejnili nástroje, ktoré umožňujú overiť zraniteľnosť verejného RSA kľúča.

K dispozícii sú ako webové služby tak stiahnuteľný softvér, odkaz na ne je možné nájsť v oznámení.

Zraniteľný kľúč je samozrejme potrebné prestať používať.

Čo sa týka zariadení s týmto čipom, univerzálne riešenie nie je k dispozícii. Pre niektoré typy zariadení môžu byť k dispozícii aktualizácie, môže sa do nich importovať inde generovaný kľúč alebo sa môže začať používať iný typ kľúča podporovaného kartou,

napríklad ECC.

Napríklad Estónsko podľa Klinca podľa posledných informácií prejde na ECC bez výmeny kariet, keď sa zneplatnia doterajšie certifikáty. Malo by sa to zrealizovať na diaľku.