https://www.root.cz/clanky/tretina-kryptografickych-cipu-generuje-slabe-rsa-klice-prolomeni-je-snadne/

Třetina kryptografických čipů generuje slabé RSA klíče, prolomení je snadné

Petr Krčmář 18. 10. 2017

TPM čipy společnosti Infineon vyrobené v posledních pěti letech obsahují vážnou bezpečnostní chybu, která vede ke slabým RSA klíčům. Tyto čipy jsou součástí notebooků, routerů, ale i šifrovacích tokenů.

Facebook Twitter

32 názorů

Bezpečnostní čipy používané nejen v počítačích obsahují chybu, která způsobuje generování slabých RSA klíčů. To může ohrozit uložená hesla, šifrované disky nebo třeba šifrovanou síťovou komunikaci. Za objevem problému stojí vědci z brněnské Masarykovy univerzity, britské společnosti Enigma Bridge a italské Foscari University of Venice.

<img src="https://go.eu.bbelements.com/please/showit/22843/2/1/4/?typkodu=img&keywords=" style="border-width:0" alt="">

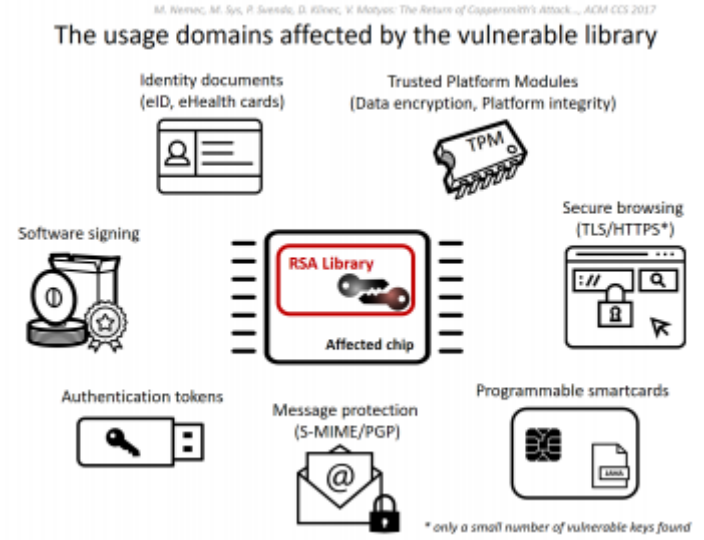
<img src="https://go.eu.bbelements.com/please/showit/22843/2/1/12/?typkodu=img&keywords=" style="border-width:0" alt="">

Problém dostal název ROCA (Return of Coppersmith's Attack) a má označení CVE-2017–15361. Týká se softwarové knihovny, která je součástí smartkaret, tokenů a dalších čipů

vyráběných společností **Infineon Technologies**. Odhaduje se, že problémem trpí přibližně **třetina** podobných řešení dostupných na trhu.

Privátní klíč za pár hodin

Chyba dovoluje provést praktický faktorizační útok, během kterého útočník z veřejného klíče vypočítá ten privátní. To je možné za předpokladu, že uživatel používá klíče o délce 1024 či 2048 bitů generované některým z čipů Infineon vyrobených v roce 2012 a později. Takové klíče nejsou vygenerovány dostatečně náhodně, což výrazně zjednodušuje jejich prolomení.



Dopady chyby ROCA

Útočníkovi přitom stačí pouze znalost veřejného klíče, nemusí mít vůbec fyzický přístup k zařízení. Nejedná se přitom o výrobní vadu, která by například postihovala jen část generátorů náhodných čísel. Chyba je implementačního rázu a týká se úplně všech RSA klíčů generovaných čipy společnosti Infineon.

Na faktorizaci privátního klíče pak nejsou potřeba žádné ohromné výkony, podle odhadů vědců bude útočník potřebovat následující výkon (použit je procesor Intel E5–2650 v3@3GHz Q2/2014) počítaný v procesorových jádrech:

- 512 bit RSA – 2 CPU hodiny
- 1024 bit RSA – 97 CPU hodin
- 2048 bit RSA – 140,8 CPU let

Útok je tedy prakticky proveditelný velmi snadno, pokud jsou použity klíče o délce 512, 1024 či 2048 bitů. U delších klíčů dramaticky roste doba potřebná k prolomení, ale vědci upozorňují na to, že se pravděpodobně ještě podaří útok zefektivnit, čímž by doba mohla klesnout do přijatelných hodnot.

Také prý nemusí vždy nutně platit, že delší klíč automaticky znamená delší dobu prolomení. Některé délky jsou podle vědců lépe faktorizovatelné než jiné. Odhaduje se, že klíč o délce 2048 bitů je na výpočetním cloudu Amazonu možné prolomit přibližně za 40 000 dolarů, s polovičním klíčem si poradíte už za 76 dolarů.

Dopady jsou rozsáhlé

Čipy značky Infineon jsou velmi rozšířené napříč různými zařízeními jako jsou čipové karty, šifrovací tokeny, routery, IoT zařízení nebo třeba firemní PC. Problém tak mají velké značky jako například Acer, ASUS, Fujitsu, HP, Lenovo, LG, Samsung a Toshiba. Klíče generované na všech jejich zařízeních s využitím čipů jsou velmi slabé.

Problém se ale týká například také známých tokenů YubiKey, naštěstí jen při generování klíčů pro OpenPGP – funkce FIDO U2F, OTP a OATH fungují správně. Postiženy také nejsou všechny tokeny, starší verze jsou v pořádku.

Google také varoval, že problém má i velká řada Chromebooků, uživatelé musí aktualizovat, poté zařízení smazat (powerwash) a poté zaškrtnout „Update firmware for added security“. Tím dojde k vymazání čipu a je potřeba celé úložiště Chromebooku přešifrovat.

Konkrétní dopady jsou pak závislé na délce klíče a konkrétním nasazení. Vědci tvrdí, že analyzovali velké množství veřejně dostupných klíčů z různých oblastí jako jsou podepsané dokumenty, autentizační tokeny, podpisy softwarových balíčků či klíče používané v HTTPS (TLS) nebo PGP. Podařilo se jim takto odhalit 760 000 slabých RSA klíčů, pravděpodobně jich ale bude několikanásobně více.

Specifická struktura použitých prvočísel umožňuje velmi snadné odhalení slabých klíčů i v poměrně velké sbírce. To na jedné straně usnadňuje uživatelům odhalení slabého místa, zároveň to ale napomáhá útočníkům, kteří mohou snadno vytipovat případnou oběť.

Vědci nabídli sadu nástrojů k odhalení slabých klíčů. K dispozici je offline tester, stejně jako online testovací nástroj. Stačí jim předložit **veřejný** klíč a nástroje poznají, zda je vygenerován na slabém zařízení. Je to jediný spolehlivý způsob, jak ověřit, že ve svém počítači (například) máte slabý TPM čip. Nástroje jsou prý velmi přesné a netrpí falešnými hlášeními, vědci proto doporučují otestovat také již používané klíče.

Tento klíč je v pořádku

Pokud na svém zařízení objevíte problém, měli byste vyhledat, zda váš výrobce nenabízí softwarovou záplatu, případně nahradit zařízení jiným. Řešením je také použít ke generování nových klíčů softwarovou metodu (OpenSSL) a poté bezpečně vygenerovaný klíč do tokenu nahrát.