



## Hogyan hamisítsunk SSL tanúsítványt?

### Avagy sok-sok matematika és 200 PS3 csodákra képes.

Kicsit újságírók kezdés, de a szaksajtó tele van az utóbbi napokban Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik és Benne de Wege publikációjával (<http://www.win.tue.nl/hashclash/rogue-ca/>), akik egy érdekes kísérlet során a gyakorlatban is hasznosították Xiaoyun Wang és Hongbo Yu 2004-ben felfedezett MD5 ütközési elméletét, valamint ennek Marc Stevens általi 2007-es továbbfejlesztését. A cél az volt, hogy készítsenek egy olyan köztes CA tanúsítványt, amivel tetszőleges SSL tanúsítványt lehet kibocsátani, a root CA tanúsítványa pedig egy böngészők által ismert elem legyen. Amennyiben a fenti folyamat sikerrel zárul lehetővé válik hamis tanúsítványok kiállítása bármelyik szervezet nevében. (Például elkészíthető és saját célokra felhasználhatóvá válik az [www.amazon.com](http://www.amazon.com) SSL tanúsítványa.)

A támadás első lépéseként információt kellett szerezniük arról, hogy mely hitelesítés-szolgáltatók (HSZ) állítanak még ki MD5 lenyomattal tanúsítványt. Ezt ugye már nem illik megtenni, Magyarországon például a Nemzeti Hírközlési Hatóság már csak az SHA-1 és a RIPEMD algoritmusok használatát engedi a HSZ-eknek. A vizsgált 30.000 tanúsítványos mintában a RapidSSL szolgáltató tanúsítványai tűntek a legtámadhatóbbnak, így náluk indult a kísérlet. A cél az volt, hogy egy olyan aláírói tanúsítványt szerezzenek, melynek lenyomata megegyezik a kutatók által előállított köztes CA tanúsítványának lenyomatával. Ehhez először meg kellett jósolni az érvényességi időt és a sorozatszámot, mert ezeket a támadó nem tudja kontrollálni. Miután elköltöttek 700 dollárt tanúsítványra, sikerült egy olyan elemet előállítani, ami megfelelt a követelményeknek.

Ezután már „csak” meg kellett találni azt a tanúsítványtartalmat, ami megfelel a hivatalos lenyomathoz. Méghozzá úgy, hogy a keresgélest 204 byte-nyi szabad hely felhasználásával kell megtenni. Itt került a képbe a 200 PS3 játékgép, ami architektúrája szerint a legalkalmasabb kriptográfiai műveletek elvégzésére. Ezzel a gépparkkal 64 óra alatt sikerült megtalálni azt a bitsorozatot, amivel az aláírói tanúsítványból létre lehetett hozni a köztes CA tanúsítványt, ami így már tanúsítvány kibocsátásra is alkalmassá vált. A módszer segítségével sikeresen létrehozhatunk egy olyan SSL tanúsítványt, aminek a köztes CA-ja a hamisított tanúsítványú, a root CA pedig egy hiteles, böngésző által elfogadott tanúsítványú.

Természetesen nincs ok pánikra, ez a támadás a már kiállított tanúsítványokat nem befolyásolja, Magyarországon pedig már nem adnak ki MD5 lenyomattal tanúsítványt. Legalábbis a bejegyzett hitelesítés-szolgáltatók nem. A többiekre viszont nagyon figyeljünk oda! A lenyomat típusa ellenőrizhető a tanúsítvány részletes adatai között magyarul „ujjlenyomat-algoritmus” angolul „certificate signature algorithm” ami jó esetben SHA-1 lesz.

Szerző: Krasznay Csaba  
Információ biztonsági tanácsadó

Ellenőrizte: Bártfai Attila  
Üzletfejlesztési igazgató

#### Felelősség kizárás:

Felhívjuk tisztelt ügyfeleink figyelmét, hogy a sorozatban megjelenő publikációk a Kancellár.hu véleménynyilvánításának minősülnek, az azokban megjelent tartalmak további felhasználásából eredő bárminemű következményért, kárért, hátrányért a Kancellár.hu felelősséget nem vállal. A Kancellár.hu nem vállal felelősséget a publikációkban található információk értelmezéséért, sem azokért a cselekvésekért, amelyeket a publikációban található információk alapján hajtanak végre a felhasználók.

