VALÓDI, VAGY CSAK ANNAK VÉLT BIZTONSÁG A BÖNGÉSZÉSBEN: SSL TANÚSÍTVÁNYOK

REAL OR SUPPOSED SECURITY IN BROWSING: SSL CERTFICATES

KESZTHELYI ANDRÁS egyetemi docens
Óbudai Egyetem Keleti Károly Gazdasági Kar

ABSTRACT

At the beginning, when the would-be internet was started, security was not a point: nobody could even imagine that the day would come when everybody would get access to The Internet, even with bad intents. The points of security came into the foreground later with the rightful need for security in everyday digital life. One, if not the most frequent, realization of security is the (supposedly) secure browsing, the https. In this case not only the data traffic is encrypted between the user's browser and the remote server, but the authenticity of the remote server (netbank, Facebook, Gmail, etc.) is also proven via SSL/TLS certificates. Investigating the publicly known security incidents related to these certificates and the certificate handling mechanism of the web browsers we will find different threats and risks, some of them may be serious. There are a lot of possibilities to manipulate the SSL/ TLS certificates to make it possible to redirect and/or know and/or alter the data traffic of browsers. Most of these possibilities for manipulating can be disclosed by applying relatively simple rules that can significantly strengthen security.

1. Bevezetés – A cikk célja és felépítése

Vázlatos történeti áttekintést követően röviden összefoglalom a nyilvános kulcsú titkosítást, illetve ennek egy megvalósítását, az SSL/TLS tanúsítványok működési alapjait. A működési elv ismeretében számításba vehetők a lehetséges támadási pontok és módok. Az elmúlt évek tanúsítványokkal kapcsolatos, ismertté vált biztonsági eseményei adják a gyakorlati hátteret: megfelelően csoportosítva megfeleltethetők az elméleti alapokon feltárt veszélyes pontoknak, s így bizonyítják, hogy az elméletileg lehetséges sérülékenységek a gyakorlatban ténylegesen kihasználhatók.

Ezen támadási pontok, illetve módszerek egy része a felhasználók szemszögéből nézve független, külső jelenség, előfordulásuk esetleges. A böngészők tanúsítványtára, illetve tanúsítványkezelése azonban a felhasználók hatáskörébe tartozik, ami – tekintettel az emberi tényező általános jelentőségére a biztonság területén – kiemelt fontosságú területté teszi. Ennek a részterületnek a vizsgálata alapján

végül javaslatot teszek ezen problémakör hatékony kezelésére mind vállalati, mind egyéni környezetben.

A javasolt megoldás nemcsak a kockázatot csökkenti hatékonyan, de egyben arra is példa, amikor az emberi tényező okozta kockázatot részben technikai, részben pedig szabályozási síkon kezeljük. A javasolt megoldás ezt kockázatot képes hatékonyan csökkenteni.

2. Történeti kitekintés

Közel fél évszázada, az akkor még csak leendő internet tervezésének kezdetén a biztonság nem volt szempont. 1969 végén, amikor az első hálózat ténylegesen elindult négy (!) számítógéppel, föl sem merült, hogy egy napon bárki hozzáférhet majd a hálózathoz. A felhasználók ekkoriban – értelemszerűen – komoly tudósok és igazi programozók voltak, és – még – nem létezett sem a netbűnöző, sem az „egységsugarú" felhasználó. Ezért az összes hagyományos kommunikációs hálózati protokoll nyílt szöveg alapú: a teljes adattartalom, beleértve a bejelentkezéshez használatos felhasználói neveket és jelszavakat is, nyílt szövegként halad át a hálózaton, tartalmához bárki hozzáférhet különösebb nehézség nélkül, mi több: akár meg is változtathatja feltűnés nélkül.

A helyzet az 1990-es évekre megváltozott. A személyi számítógép és a hálózathoz való csatlakozás általánossá vált, sőt egyre inkább része lett a mindennapi életnek. 1990-ben kezdődött a web projekt a CERN-ben Tim Berners-Lee vezetésével, 1992-ben elkészült az első böngésző, az üzleti világ és a „közösségi" média is megtalálja az új lehetőséget az elkövetkező néhány évben: eBay (1995), Google search engine (1998), PayPal (2002), Facebook (2004), Youtube (2005), etc.

Röpke egy évtized alatt az internet játékszerből komoly és általános kommunikációs csatornává alakult át, s a digitálisan tárolt adatoknak nemcsak a mennyisége, de a tőlük való függésünk mértéke mindmáig napról napra növekszik.

A biztonság iránti jogos igény utólag próbálja meg a biztonság szempontját érvényesíteni. Ennek egyik – talán a leggyakrabban alkalmazott – megvalósítása a biztonságos (vagy annak hitt) böngészés, a https, amit az SSL/TLS tanúsítványok alkalmazása teszi lehetővé. Ekkor a felhasználó böngészője és a távoli kiszolgáló gép (Gmail, Facebook, netbank, Neptun, ETR stb.) közötti adatforgalom titkosított, sőt, mi több, a kiszolgáló hitelessége is garantált.

Ennek matematikai alapját az 1977-ben publikált RSA-algoritmus jelenti, ami máig de facto szabványa a nyilvános kulcsú titkosításnak. Ennek első implementációja a máig közismert PGP (Pretty Good Privacy, Phil Zimmermann, 1991.). Az évtized közepére a legszükségesebb eszközök készen állnak: az ssh (secure shell – biztonságos távoli bejelentkezés) 1995-ben, az SSL (secure socket layer – biztonságos szoftvercsatorna réteg[7]) 1996-ban már csatasorban állt. Ez utóbbit

7 A socket kifejezésnek általánosan elfogadott és széles körben használatos magyar megfelelője eddig még nem honosodott meg.

később átnevezték: TLS (transport layer security – biztonságos szállítási réteg), illetve sokszor SSL/TLS lett belőle.

Mivel a legtöbb és legtipikusabb tevékenységek, amelyek alapvetően igénylik a biztonságot, a weben történnek, böngészővel, szükségessé vált a böngészés biztonságának kényelmesen és lehetőleg önműködően használható megvalósítása. Ezt teszi lehetővé a tanúsítványok használata.

Megvizsgálva azonban az ezen tanúsítványokkal kapcsolatos, a közelmúltban nyilvánosságra került biztonsági eseményeket és a böngészők tanúsítványkezelését, meglepő módon akár súlyossá is válható problémákat, veszélyforrásokat találunk. Számos lehetőség van ugyanis az SSL tanúsítványokkal kapcsolatos különféle manipulációkra, amelyek lehetővé tehetik a böngésző adatforgalmának rossz szándékú, illetéktelen eltérítését, megismerését, akár megváltoztatását. Ezen manipulációs lehetőségeket azonban aránylag egyszerű szabályok betartásával jórészt kizárhatjuk, jelentősen lecsökkentve a böngészőnk adatforgalmának biztonságára leselkedő veszélyeket.

A probléma jelentőségét hangsúlyozza, hogy korunkat nyugodtan nevezhetjük a netháborúk (Cserháti, 2011), a netbűnözés (LB, 2015), vagy akár a korlátlan lehallgatás korának (MTI, 2015), csak egy-egy jellemző példát említve.

Bencsáth Boldizsár, a Műegytemen működő CrySyS Lab munkatársa arról beszél egy interjúban (Ruzsbaczky, 2014), hogy a számítógépes bűnözés mára nagyobb üzletté vált, mint a drog, sőt a Kaspersky Lab szerint megjelent a számítógépes hálózati bűnözéshez szükséges eszközök mint szolgáltatás biztosítása a feketepiacon. (Kaspersky, 2014)

Ebben a helyzetben kiemelkedően fontos, hogy a megbízhatatlan hálózaton keresztül megbízható kommunikációt lehessen megvalósítani, s ennek tétje napról-napra nagyobb. Mivel ezen a területen a messze leggyakoribb eszköz a biztonságos böngészést elvileg lehetővé tevő HTTPS (HTTP Secure), ami az SSL/TLS tanúsítványok megfelelő használatán alapul, érdemes ezt a területet közelebbről is szemügyre venni.

3. Technikai alapok – A nyilvános kulcsú titkosítás

Az SSL/TLS tanúsítványok a nyilvános kulcsú titkosításon alapulnak. Ennek talán legnagyobb előnye az, hogy nincs szükség biztonságos csatornára a kulcsok előzetes cseréje során. Ennek egy lehetséges matematikai alapját Ron Rivest, Adi Shamir és Len Adleman fejlesztették ki a hetvenes években (Rivest, 1983), amit nevük kezdőbetűi alapján máig RSA-eljárásnak nevezünk.

Ennek lényege felhasználói szempontból, hogy minden résztvevő saját magának generál egy kulcspárt. A kulcspár egyik tagját nevezzük nyilvános kulcsnak, és a lehető legszélesebb körben lehet (célszerű) terjeszteni. A másik fele a privát, vagy titkos kulcs, amit a gazdája a lehető legbiztosabb módon titokban tart. A működés lényege: amit az egyik kulccsal titkosítottak, azt a párjával lehet dekódolni.

Így tehát, ha Aladár titkos üzenetet akar küldeni Bélának, akkor Béla nyilvános kulcsát fogja használni a titkosításhoz, mert azt csak Béla titkos kulcsával lehet dekódolni, az pedig csak Béla birtokában lehet. Ha pedig azt szeretné bizonyítani, hogy az üzenet valóban tőle származik, akkor saját titkos kulcsával fog kódolni (digitális aláírás).

A rendszernek van egy hátránya: a kulcsok nélkül is fejthető elméletileg, és ehhez semmi másra nincs szükség, mint egy szám prímtényezőinek meghatározására. Ha ez a szám elég nagy, prímfelbontását megcsinálni emberi léptékű időben reménytelen vállalkozás. Napjainkban úgy tűnik, hogy a négy kilobites kulcsméret megnyugtató mértékű biztonságot jelent.

A biztonsági szabályok roppant egyszerűek. A felhasználó titkos kulcsának feltétlenül titokban (saját kizárólagos használatában) kell maradnia, hiszen annak birtokában a neki címzett titkos küldemények fejthetők, s ami a nagyobb baj, a nevében digitális aláírást lehet csinálni. A másik szabály: mások begyűjtött nyilvános kulcsait használat előtt ellenőrizni kell, hogy valóban ahhoz a személyhez (szervezethez) tartozik-e, akiének véljük. Ha ezt a lépést kihagyjuk, nem tudjuk kizárni a közbeékelődéses támadás (MITM) lehetőségét.

Ha Aladár egy olyan dokumentumot ír alá digitálisan, amelyik tartalmazza Béla nyilvános kulcsát és Béla személyi adatait, akkor bárki, aki birtokolja Aladár nyilvános kulcsának egy hiteles példányát – például úgy, hogy Aladártól magától kapta azt –, ellenőrizheti Aladár digitális aláírását. Ha rendben találja, elfogadhatja Béla nyilvános kulcsát is hitelesnek – feltéve, hogy megbízik Aladárban, hogy alaposan és gondosan ellenőrizte Béla személyazonosságát, mielőtt aláírta volna a szóban forgó dokumentumot. Így kezd kiépülni a bizalmi lánc, hiszen nyilvánvalóan a sor folytatható. Vegyük észre, hogy a folyamatban sehol nincs központi szerepű elem.

Ha ez a dokumentum, ami tartalmazza a nyilvános kulcs gazdájának leírását és magát a nyilvános kulcsot, szabványos szerkezetű, akkor alkalmassá válik önműködő gépi feldolgozásra. Így jutunk el a tanúsítvány (CERT – certificate) fogalmához.

Ha egy vállalat anyagi ellenszolgáltatás fejében végez ilyen aláíró tevékenységet (a kulcs gazdája személyazonosságának üzletszabályzatban rögzített módon való gondos ellenőrzését követően), a tanúsítványkiadó (CA – certificate authority) fogalmához jutunk el. Logikus, hogy a tanúsítványkiadó létének alapját az jelenti, hogy az ő hiteles nyilvános kulcsát a világon bárhol és bárki birtokol(hat) ja, tehát az ő aláírását bárki, bárhol és bármikor könnyedén ellenőrizheti.

A biztonságos böngészéshez (https) úgy jutunk el, hogy a nagy nemzetközi és nemzeti tanúsítványkiadó cégek saját tanúsítványait a böngészők fejlesztői beépítik a böngészőkbe. Így ezek – a böngésző szemszögéből nézve – teljesen hitelesek. Ha ezután a felhasználó a böngésző címsorába beír egy „https://" kezdetű címet, a böngésző bekéri a cím tanúsítványát, s ha annak aláírását végesen kevés lépésben vissza tudja vezetni a saját tanúsítványtárában lévő, teljesen hiteles, ún. legfölső

szintű tanúsítványok valamelyikére, akkor indulhat a biztonságos böngészés, ami három fontos dolgot jelent:

bizalmasságot, azaz az adatforgalom a kapcsolat egésze alatt titkosított,

adatépséget, azaz az adatcsomagokat digitális aláírás védi az illetéktelen módosítástól,

hitelességet, azaz a böngésző felhasználó biztos lehet abban, hogy valóban a címben szereplő számítógéppel forgalmaz, s nem valami kalózoldallal.

Ha nem, akkor hibaüzenetet jelenít meg („Ez a kapcsolat nem megbízható..."), és a felhasználóra van rábízva, hogy mit is tesz: milyen gondosan ellenőrzi a meglátogatni kívánt oldal tanúsítványát, mielőtt azt a böngésző számára megbízhatónak minősíti. Pont ez a lépés rejti a kockázatot: az átlagos felhasználó általában nincs tisztában maradéktalanul a részletekkel.

4. Közbeékelődéses támadás

A fent vázolt rendszer úgyszólván tökéletes. A kép – mondhatni – túl szép ahhoz, hogy igaz lehessen. Pedig igaz, feltéve, hogy a fentebb ismertetett két biztonsági szabály maradéktalanul érvényesül. Sikeres támadáshoz pont az szükséges, hogy ezen szabályokat a támadó valahogy meg tudja kerülni, ami a felhasználók, illetve az üzemeltetők valamilyen mértékű gondatlanságát (esetleg csak balszerencséjét) tételezi föl.

A lehetséges támadási pontok elvileg a következők:

- kriptográfiai törés, ha a támadónak elegendően nagy számítási teljesítmény áll a rendelkezésére,
- a támadónak sikerül ellopnia a kiszolgáló gép titkos kulcsát,
- a tanúsítványkiadó sikeres megtévesztése következtében illetéktelenül jut hozzá a támadó valaki más tanúsítványához,
- felhasználói oldalon: a böngésző tanúsítványtárának a támadó általi sikeres manipulálása,
- egyéb lehetőségek, amelyek azonban az előzőek valamelyikére vezetődnek vissza.

Az általános körülmények között megvalósítandó kriptográfiai töréshez elképzelhetetlenül nagy számítási teljesítményre lenne szükség. Öt évvel ezelőtt, 2010 elején a 768 bites kulcs törése belátható erőforrás-felhasználással sikeres volt. (Seltzer, 2010) A siker azonban nem volt könnyű. Kleinjung és kollégái fél évig dolgoztak 80 processzorral a polinomiális kiválasztáson, ami a teljes munka nagyjából 3%-át tette ki. A fő feladatot, magát a szitálást sok száz gép végezte, és majdnem két évig tartott. Egy egymagos, 2,2 GHz órajelű AMD Opteron processzorú gépen, 2 GB memóriával ez mintegy másfél ezer évig tartott volna. (Kleinjung, 2010)

2013-ban, két évvel ezelőtt a Google bejelentette, hogy megduplázza az általa használt kulcsok méretét, azaz 2048 bitesre növeli azt 2013 végétől. (McHenry, 2013)

Általános esetben tehát a prímfelbontáson alapuló törés reménytelennek tűnik. Van lehetőség azonban a hatékonyság javítására, amennyiben a támadó tudhatja, hogy a kulcsgenerálásnál használt véletlenszámok nem teljesen véletlenszerűek.

A The Guardian (Greenwald, 2013) szerint az NSA évente mintegy 250 millió dollárt költ arra, hogy közvetve úgy befolyásolja a titkosítási szabványokat, hogy a rendelkezésére álló számítási teljesítménnyel esélye legyen törni a biztonságosnak hitt titkosításokat is.

A Snowden által kiszivárogtatott dokumentumokból kiderül, hogy az RSA vállalat egy tízmillió dolláros üzlet fejében egy problémás véletlenszámgenerátort épített be a termékeibe. (Gálffy, 2013.)

A titkos kulcsok ellophatók lehetnek adott esetben. Technikailag erre bármilyen módszer alkalmas, amellyel a támadó képes jogosulatlan hozzáférést szerezni („betörés") a távoli kiszolgálóhoz. Ennek hatékonysága megkérdőjelezhető, mivel a sikeres betörés általában nyomokat hagy maga után, így az üzemeltető ezt észleli. Gondatlan vagy véletlen (vagy kevésbé véletlen) programozási hibák is vezethetnek a titkos kulcs jogosulatlan, sőt észrevétlen megszerzéséhez. Ilyen volt például az ún. Heartbleed hiba, ami lehetővé tette a sérülékeny rendszerekből a titkos kulcs nyomok nélküli megszerzését. (CVE 2014) További példák is ismertek.

A tanúsítványkiadó cégek (CA) korrumpálása vagy korrumpálódása is egy lehetőség. Ismertté vált esetek: a holland DigiNotar esete (Kormányzati, 2012). 2013 elején a Google hamis tanúsítványokat fedezett föl, amelyeket a francia DG Trésor bocsátott ki a Google valamely doménnevére. (Ducklin, 2013/A) 2011-ben a Turktrust nevű török tanúsítványkiadó cégnél egy hibás üzleti folyamat eredményeképpen kerültek ki inkorrekt tanúsítványok. (Ducklin, 2013/B) A Stuxnet vírus is hamis tanúsítványokat használt föl arra, hogy saját hiteles eszközvezérlő mivoltát bizonyítsa. (Cserháti, 2011).

5. A probléma – Tanúsítványkezelés a felhasználó jogán

A böngészők a többfelhasználós operációs rendszerek korában felhasználói jogosultságokkal működnek, így a tanúsítványok és a kivételek kezelése is felhasználói jogosultsággal történik. Ha a felhasználónak nincsenek megfelelő szintű ismeretei a tanúsítványok kezelésével kapcsolatosan, a következmények beláthatatlanok lehetnek. Egy alkalmas rosszindulatú program, pl. böngészőbővítmény manipulálhatja a tanúsítványok listáját. Ami még rosszabb: a felhasználókat a támadó ráveheti arra a „nagy süket duma" (social engeineering) eszközével, hogy saját maguk végezzék el a szükséges műveletet, pl. egy hamis legfölső szintű tanúsítvány importálását.

További lehetőségeket rejt magában az a körülmény, hogy az ismertebb böngészőket (a Firefox kivételével) http protokollon lehet letölteni, azaz semmi sem akadályozza meg az esetleges támadót, hogy a letöltést manipulálja, és az eredeti

telepítőkészletet kicserélje olyanra, amelyikben a számára szükséges hamis tanúsítvány már importálva van.

Ha pedig a megfelelő hamis tanúsítvány ott van a felhasználó böngészőjének tanúsítványtárában, akkor a https adatforgalom már kijátszható, a böngésző nem fog hibaüzenetet megjeleníteni, amikor az adatforgalom a kalóz-kiszolgálóra terelődik át.

6. A javasolt megoldás – Tanúsítványkezelés rendszergazdai jogosultsággal

Vállalati környezetben nem tételezhetjük föl, hogy minden dolgozó alapos elméleti és gyakorlati ismeretekkel rendelkezik a területen, továbbá hogy folyamatos éberséggel figyeli az esetleg előforduló rendellenességeket. Épp ezért az a megoldás, hogy a tanúsítványokat tartalmazó fájl a rendszergazda tulajdonába kerül, a felhasználónak nincs rá írási joga. Ha bármilyen tanúsítványokkal kapcsolatos probléma fölmerül, forduljon a rendszergazdához, ő a megfelelő szaktudás és a vállalati szabályzatok ismeretének birtokában el tudja dönteni, hogy az adott helyzetben mi a teendő.

Otthoni, saját használatú gépen ugyancsak megfontolandó, hogy a tanúsítványtárat ne hagyjuk meg a felhasználó tulajdonában. Ugyanez vonatkozik a böngészők bővítményeire is.

A helyzet hasonló ahhoz az alapvető szabályhoz, hogy a munkaállomás Windows operációs rendszereit korlátozott felhasználói fiókkal használjuk.

A javasolt megoldás nemcsak a kockázatot csökkenti hatékonyan, de arra is példa, amikor az emberi tényező okozta kockázatot részben technikai, részben pedig szabályozási síkon kezeljük. A végső és általános megoldás azonban mindenképpen az „emberi tényező" fejlesztése: az oktatás, gyakorlás, továbbképzés – a biztonság kultúrájának a kialakítása, illetve fejlesztése, amint azt részletesen kifejti Lazányi (2015/A,B). A technika és a szabályzatok hatékonyságát jelentősen javíthatja ugyanis, ha a felhasználók tisztában vannak azok hátterével és alapjaival.

FELHASZNÁLT IRODALOM

CVE database (2014). 2014.04.08. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

Cserháti, A. (2011). A Stuxnet vírus és az iráni atomprogram, in: Fizikai Szemle, 2011/5. p/pp. 150-155.

Ducklin, P. (2013/A). Serious Security: Google finds fake but trusted SSL certificates for its domains, made in France, Naked Security - Award-winning computer security, news, opinion, advice and research from SOPHOS, 2013.12.09., https://nakedsecurity.sophos.com/2013/12/09/serious-security-google-finds-fake-but-trusted-ssl-certificates-for-its-domains-made-in-france/

Ducklin, P. (2013/B). The TURKTRUST SSL certificate fiasco - what really happened, and what happens next?, Naked Security - Award-winning computer security, news, opinion, advice and research from SOPHOS, 2013.01.08., https://nakedsecurity.sophos.com/2013/01/08/the-turktrust-ssl-certificate-fiasco-what-happened-and-what-happens-next/

Gálffy, Cs. (2013). Szándékosan gyengíthetett az RSA, hwsw.hu, 2013.12.23. http://www.hwsw.hu/hirek/51525/rsa-nsa-dual-ec-drbg-veletlenszam-generator-biztonsag-snowden.html#kommentek

Greenwald, G. (2013). Revealed: how US and UK spy agencies defeat internet privacy and security, The Guardian, 2013.09.06. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Kaspersky Lab (2014). The hackers' bounty: how much do cybercriminals make from innocent users? [A hekkerek nagylelkűsége: mennyit profitálnak a netbűnözők az ártatlan felhasználókból?] http://www.kaspersky.com/about/news/virus/2014/how-much-do-cybercriminals-make-from-innocent-users, 2014.11.25.

Kleinjung, T. et al. (2010). Factorization of a 768-bit RSA modulus, Cryptology ePrint Archive, Report 2010/006, http://eprint.iacr.org/2010/006.pdf

Kormányzati Eseménykezelő Központ (2012). Újabb hamis digitális aláírást használó káros szoftverre bukkantak, 2012.03.19. http://tech.cert-hungary.hu/tech-blog/120319/ujabb-hamis-digitalis-alairast-hasznalo-karos-szoftverre-bukkantak

Lazányi, K. (2015/A): A biztonsági kultúra, TAYLOR Gazdálodás- és szervezéstudományi folyóirat VIKEK –Taylor Vezetéstudományi Brand, 2015/1-2. szám VII. évfolyam 1-2. szám No 18-19, Szeged 2015

Lazányi K. (2015/B): Mire jó a biztonsági kultúra?, VIKEK –Taylor Vezetéstudományi Brand, közlésre elfogadva.

LB (2015). Feltűnés nélkül loptak 300 millió dollárt, Index, 2015.02.16., http://index.hu/tech/2015/02/16/feltunes_nelkul_loptak_300_millio_dollart/

McHenry, S. (2013). Changes to our SSL Certificates, Google Online Security Blog, 2013.05.13. http://googleonlinesecurity.blogspot.hu/2013/05/changes-to-our-ssl-certificates.html

MTI (2015). Optikai kábelt "csapolhattak" meg a németek, Belgium vizsgálódik, in: HVG, 2015. május 29., http://hvg.hu/vilag/20150529_optikai_kabelt_csapolhattak_meg_a_nemetek

Rivest, R. et al. (1983). Cryptographic communications system and method, US 4405829 A, 20-09-1983. https://www.google.com/patents/US4405829

Ruzsbaczky, Z. (2014). A kiberbűnözés a drognál is nagyobb üzlet, in: Magyar Nemzet, 2014.09.24, p/pp. 6.

Seltzer, L. (2010). 768-bit RSA Keys Factored. 1024-bit Next, 2010.01.08., http://securitywatch.pcmag.com/security-software/284178-768-bit-rsa-keys-factored-1024-bit-next