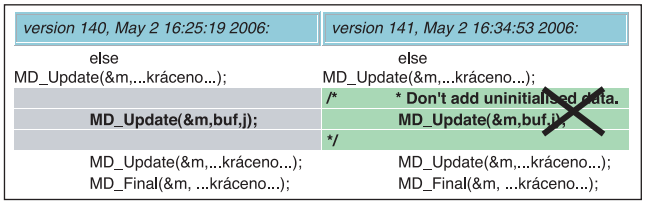
Jak pašák opravil sušák

Nedávno si jeden z autorů zakoupil elektrický sušák ručníků do koupelny: Stačilo vyvrtat do zdi díry na hmoždinky, přišroubovat, zapnout do zásuvky a sušit. Díry do zdi vycházely přesně ve výšce zásuvek, to se mi moc líbilo, protože sušák vytvářel s nimi jednu linii. S estetickým elánem jsem elektrickou vrtačkou vyvrtal první díru nedaleko zásuvky, ale zhaslo světlo. „Vrtačka asi narazila na kámen, a to zřejmě vyhodilo pojistky," zabrblal jsem, nahodil pojistky a vyvrtal druhou díru. Sušák od té doby bezproblémově funguje. „Jsem pašák," řekl jsem si.



version 140, May 2 16:25:19 2006:	version 141, May 2 16:34:53 2006:
else MD_Update(&m,...kráceno...);	else MD_Update(&m,...kráceno...);
	/* * Don't add uninitialised data.
MD_Update(&m,buf,j);	MD_Update(&m,buf,j);
	*/
MD_Update(&m,...kráceno...); MD_Final(&m, ...kráceno...);	MD_Update(&m,...kráceno...); MD_Final(&m, ...kráceno...);

Obr. 1 Osudné zakomentování „problematického" kódu

Pašáci Debianu

Uvedený příběh ukazuje, jak pašáci (tedy ti, co „všechno ví, a hned jdou na věc") umí vyřešit skutečné problémy, na něž ve své praxi narazí. Podívejme se na další takový příběh. Ve ST 5/08 jsme psali o tom, že v praktických kryptografických aplikacích mívá poslední slovo její Popelka, a to generátor náhodných čísel. To jsme netušili, jak velký poprask Popelka způsobí v Linuxovém světě (viz http://www.debian.org/security/2008/dsa-1571). Tentokrát byli pašáky přímo tvůrci operačního systému Debian, kteří přidáním pouhých čtyř znaků (konkrétně /**/) do kvalitní kryptografické knihovny OpenSSL z ní udělali bezzubý nástroj a začlenili ho do Debianu. Takto „vylepšená" knihovna se promítala do dalších systémů a dva roky se místo kvalitních 2048bitových klíčů (RSA, DSA) vydávaly klíče 15bitové!

Co bylo znehodnoceno

Aplikace a protokoly, jež používaly tyto slabé klíče, jsou: knihovna OpenSSL 0.9.8c-1 až do verze před 0.9.8g-9 na operačních systémech založených na Debianu, OpenSSH (jak serverové, tak uživatelské klíče), OpenVPN, Openswan, StrongSWAN, DNSSEC, klíče pro X.509, encfs, Tor, postfix, exim4, sendmail, cyrus imapd, courier imap/pop3, uw-imapd, dovecot s imaps/pops, apache2 (SSL certifikáty), dropbear, cfengine, puppet, xrdp, tinc, gitosis, vsftpd SSL certifikáty pro FTPS, proftpd SSL/TLS certifikáty pro FTPS, ftpd-ssl SSL certifikáty pro FTPS, telnetd-ssl SSL certifikáty pro SSL-Telnet, DomainKeys (DK), DKIM,… Těžko spočitatelná řada uživatelů těchto protokolů a aplikací v květnu po odhalení chyby a vydání záplaty zjistila, že se někam nemůže přihlásit, že něco nefunguje jako dřív apod. Příčinou bylo, že záplaty použily tzv. blacklisty a vyloučily z dalšího používání všechny možné klíče, které se těmito systémy generovaly (jsou jich pouhé desetitisíce). Všechny podpisové klíče DSA a všechny RSA klíče musely být považovány za zkompromitované. To mj. znamená, že ten, kdo zaznamenával komunikaci dotčených uživatelů, si ji může v klidu nyní dešifrovat. Dále všechny podpisové klíče generované těmito systémy musí být zneplatněny a odvolány. Aplikace, které používaly silné klíče, jsou bohužel částečně dotčeny také, neboť komunikovaly se slabými stranami, tudíž jeden směr jejich komunikace je také dešifrovatelný (například pokud používal slabý klíč server internetového obchodu, všechna data uživatelů, kteří tam nakupovali, byla a jsou nyní dešifrovatelná).

Jak k tomu došlo?

Kryptografickou knihovnu OpenSSL vyvíjí jedna skupina lidí ve světě, aby světové veřejnosti byla k dispozici zdarma kvalitní kryptografie. Velmi záslužná činnost! Knihovnu pak využívají skutečně na celém světě mnohé aplikace, banky, mobilní operátoři i vládní instituce (!), operační systémy aj. Knihovnu OpenSSL použili i vývojáři operačního systému Debian (část světa Linuxu). Protože u operačního systému je velmi důležitá každá maličká chyba nebo nestabilita, existují na zjišťování takových chyb dokonce velmi sofistikované nástroje (zde konkrétně Valgrind a Purify). Vývojáři je použili ke kontrole kódu operačního systému. Stále je otravovalo hlášení, že v knihovně OpenSSL je použita neinicializovaná paměť v části generátoru náhodných čísel. Neinicializovaná proměnná věští normálně téměř jistě vážnou zakuklenou chybu, takže ji tento nástroj dobře zachytil a upozorňoval na ni tak vehementně, že se hláška nedala „utlouci". Vývojář poté zjistil přesně, co tuto hlášku způsobuje, a ověřil to zakomentováním dvou řádků ve zdrojovém kódu knihovny OpenSSL (poté již kontrola proběhla v pořádku) – to jsou ony čtyři znaky /**/. Řádky vyhlížely velmi jednoduše (*obr. 1*), ale přesto raději poslal dotaz do poštovní konference openssl-dev a očekával reakce od vývojářů knihovny OpenSSL. Dostal neslané nemastné odpovědi, což je samostatná kapitola tohoto příběhu, mimo jiné proto, že to nebyla ta správná poštovní konference, mimo jiné proto, že mu nezáporně odpověděl i člen týmu OpenSSL, místo toho, aby mu to přísně zakázal, atd. atd. Na základě toho se náš pašák rozhodl zakomentování ponechat, protože se domníval, že neinicializovaná paměť stejně nemůže nějak zvlášť přispívat k náhodnosti. Proto se tyto zakomentované řádky kódu dostaly dne 17. 9. 2006 do operačního systému Debian a zůstaly tam skoro dva roky, až do 13. května 2008, kdy byla chyba odhalena.

Co se vlastně stalo?

Podstata je velmi jednoduchá. Prostřednictvím té tzv. neinicializované paměti (viz buffer buf na obrázku vlevo tučně) se do generátoru náhodných čísel přidávala entropie. Vyřazení příkazu z kódu způsobilo, že generátor náhodných znaků nedostával žádnou jinou entropii než číslo procesu (PID). Těchto čísel je ale pouze 32767, a tak všech možných klíčů mohlo být generováno také pouze 32767.

Záplaty

Pokud někdo ihned nenainstaloval záplatu, mohl se kdokoliv místo něho přihlásit do příslušného systému. Na internetu se totiž ihned po oznámení chyby objevil nástroj (http://www.deadbeef.de/rsa.2048.tar.bzip2), který vyzkoušel všechny slabé klíče a zkusil se za uživatele přihlásit. V současné době dotčené záplatované systémy kontrolují, zda tyto klíče nejsou používány, a ignorují komunikaci s nimi. Také existují samostatné blacklisty těchto klíčů.

Podobný problém s generováním slabých SSL klíčů (nikoli věcně, ale důsledkem) měly Windows 2000/XP. Na rozdíl od okamžité reakce Debianu, Redmond opravil chybu, objevenou 4. listopadu 2007 (neoprávněným zkoumáním kódu Windows…), až 6. května 2008 v SP3 Windows XP. Pro Windows 2000 oprava pravděpodobně není a problém se zřejmě táhne již od Windows 95.

Závěr

Poučení z tohoto případu je mnoho, ale ještě více otázek kolem bezpečnosti to vyvolává. Abychom tento opravdu varovný případ trochu odlehčili, doporučujeme podívat se na stránku s popisem problému ve francouzštině (http://sid.rstack.org/blog/index.php/275-du-hasard-et-de-ses-consequences) a zvolit její překlad Googlem do češtiny.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

LITERATURA

[1] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz