Útok na privátní podpisové klíče PGP

# KDYŽ “BURIAN KRYPTOVAL”... (ANEB CO V TECHNICKÉ ZPRÁVĚ NEBYLO)

---

**Nedávný útok na program PGP a formát OpenPGP vzbudil zasloužený rozruch mezi odborníky, ale bohužel se mu dostalo – většinou přičiněním nesprávné interpretace objevu v denním tisku – také falešné a zavádějící publicity mezi laiky. Technickým detailům věnujeme odborně zaměřený článek v rubrice Praxe, zde bychom se rádi vyjádřili k onomu druhému aspektu; činíme tak záměrně, abychom oddělili věci technické od těch, řekněme, “politických”.**

Předem poznamenejme, že tento článek se pouze snaží nesprávné informace, které pronikly na veřejnost, uvést na pravou míru a není míněn jako odvetná reakce na některé kritické názory. Veškeré komentáře, které budeme uvádět dále, budou pouze glosovat vzniklou situaci z pohledu kryptologie jako takové, nikoliv z našich osobních hledisek. V tom se možná budeme od některých “zasvěcených” kritiků lišit.

Ačkoliv jsme se maximálně snažili předpokládat a “ukočírovat” reakce, které vyvolá oznámení zmíněného útoku, musíme přiznat, že jsme zdaleka neodhadli a neuhlídali vše, co se kolem této kauzy nakonec semlelo. Na druhou stranu je ale dobře, že se tak stalo, neboť se nám dostalo té cti blíže poznat myšlení běžných uživatelů i některých takzvaných odborníků. O některé zajímavé postřehy bychom se zde s vámi rádi podělili.

## Kryptologie jako věda a praxe

Možná se někdo zeptá, proč jsme vlastně na prezentaci běžného útoku svolávali hned tiskovku – vždyť na kryptologických konferencích bývají k vidění mnohem vědečtější objevy a novináři se k nim přitom nezvou. Ano, to je pravda. Upřímně řečeno, vůbec si nemyslíme, že objevený útok je z profesního hlediska nějakým vrcholem kryptologických dovedností. Spíše naopak – řekli bychom, že pokud si někdo chce zaslouženě říkat kryptolog, měl by odhalenou slabinu okamžitě vidět. Důvod, proč jsme souhlasili s pořádáním tiskové konference, je totiž někde jinde.

Tady však musíme malinko odbočit. Náš postoj, který bychom zde rádi vysvětlili, jsme se snažili dát najevo už názvem tohoto článku. Klasikovo jméno jsme si s dovolením vypůjčili proto, abychom ilustrovali naše pocity plynoucí ze stále se zvětšující diskrepance mezi tím, co se ví v kryptologii jakožto ve vědě, a tím, co se potom ocitne v praxi. Výsledkem je ostatně i onen příšerný výraz “kryptování”, ze kterého nám naskakuje husí kůže. Už sám o sobě je ztělesněním uspěchaného, rádoby dynamického a s prominutím poněkud přiblblého amerického stylu “radostného” převádění vědy do praxe. Kdopak by se zdržoval s nějakým ověřováním a dlouhými úvahami! Rychle s tím ven, ať si to nějaký hlupák koupí. Pravda, někde takový styl myšlení nevadí, a dokonce přináší výsledky – v kryptologii však bývá většinou osudný.

Budiž, to je přístup komerční praxe. Zarážející ovšem je, že téměř stejně zacházejí s kryptografií i mnozí freewaroví guruové čili skupiny lidí, jimž by výše nastíněné bakelitové myšlení mělo být na hony vzdálené. A přesto i oni si sice dokáží neuvěřitelně dlouho hrát například s laděním čehosi v linuxovém jádru (mimochodem jistě zajímavá a povznášející činnost – to myslíme vážně), ale jakmile dojde na kryptografii, je to “zakryptované” během pár minut. A jaképak s tím štrachy, vždyť ty matematické “bedny” přece to “krypto” navrhly dobře, my to jenom používáme... Stejně jako předchozí přístup i tento většinou neomylně vede ke vzniku napadnutelného systému.

Snad už teď začíná být jasnější, proč jsme to celé neodbyli tiše v koutku některé z konferencí. Vůbec jsme se nechtěli “zviditelňovat” jako nějací lamači kryptoschémat, ale poukázat na evidentní diskrepanci mezi teorií a praxí, jejíž vinou vzniká řada systémů, o nichž se lidé domnívají, bůhvíjak nejsou bezpečné, a ony přitom v sobě obsahují školácké chyby!

Považme jen, že program, kterého se to zejména týká, má veřejně dostupné zdrojové kódy a používá ho asi 10 milionů lidí. Ale kryptologové se jím (ani formátem OpenPGP) zřejmě nezabývali – vždyť ty tři "hrubky", které jsme viděli my, by museli objevit taky. Jenomže: proč by se něčím takovým vůbec zabývali? Takových formátů a programů je... V kryptologii jsou zajímavější věci (třeba faktorizovat velká čísla), než se hrabat ve zdrojácích nějakého programu, do nichž se "dostat" je ostatně záležitostí programátora, a ne kryptologa. V tom je ta příčina ovšem také.

Měli bychom teď asi zdůraznit, že nijak neodsuzujeme formát OpenPGP a aplikace z něho vycházející. Naopak jsme jim vděčni za to, že nám poskytly krásný celosvětově platný příklad, na kterém lze jednoduše ukázat, kam až může vést ono "kryptování". Věříme nicméně, že jak OpenPGP, tak i příslušné aplikace se z této drobné epizodky rychle vzpamatují a situaci využijí k získání předstihu před konkurenty, kteří (bohužel) stále ještě "kryptují"...

Kromě formátu OpenPGP bychom měli vlastně také poděkovat našemu mateřskému jazyku za to, že v něm ono hrůzostrašné slovo "kryptování" vůbec může vzniknout. Vlastně ani nevíme proč, ale praktické zkušenosti ukazují, že jakmile toto slovo někdo hojně a s oblibou používá (a není zrovna obchodník – těm se asi musí leccos prominout), je možné s jistotou říci, kolik uhodilo. Že nemá význam se s takovým odborníkem pouštět do "žádných větších akcí", je pak předem jasné. (Na náš pomyslný Olymp se zatím dostal odborník, který už také dokázal prohlásit, že je to "zaenkryptované".)

## Reakce doma a v zahraničí

Mohli bychom opět parafrázovat slova jiného klasika a říci, že "názory na útok se různily jak v tisku, tak i v tlači". Zahraniční ohlasy se přitom zdají o poznání kladnější a věcnější nežli ty domácí. Pozitivní reakce ponecháme stranou – ostatně člověk by se měl učit hlavně z **kritických připomínek**. Budeme se proto věnovat výhradně jim a ukážeme, co nám na těchto ohlasech připadalo zajímavé.

Souhrnně lze říci, že zahraničním ohlasům vadilo asi nejvíce to, že celý útok stavěl do špatného světla jejich "miláčka" PGP, ochraňujícího je už deset let před strýčkem Samem – místo toho, aby to pěkně natřel té "potvoře" Microsoftu. Bohužel, stalo se, co se stalo, a ukázalo se, že i v tak obletovaném systému, jako je PGP, resp. formát OpenPGP, mohou být poměrně velké "mušky". Musíme říci, že nás ani příliš nepřekvapila reakce NAI, která dokázala téměř nemožné – kromě jedné světlé výjimky se na stránkách nejrůznějších periodik k celé kauze pravidelně vyjadřovali jen lidé z vedení NAI nebo sám Philip Zimmermann.

Poněkud více nás překvapila reakce domácích médií. Zcela uznáváme, že prvotní humbuk vyvolaný článkem v Lidových novinách byl velmi nešťastný a rozjel spoustu věcí špatným směrem. Lze pochopit, že někteří lidé měli pocit podlého útoku na svou vlastní práci, a tak se bránili. Bránili se ovšem leckdy takovým způsobem, že přestávalo být zřejmé, co je větší hloupost. K tomu odkudsi přispěchalo několik "povolaných" vykladačů celé kauzy, kteří také nechodili pro nesmysly zrovna daleko. Výsledkem byla docela slušná šlehačková bitva, kterou by asi nejlépe charakterizoval další klasik svým: "Vinnej, nevinnej, berte to po řadě!"

Zkrátka celý útok nakonec ve svém sekundárním efektu rozkryl mnohem více všeobecné neznalosti a tápání, než bychom v úvodu předpokládali. Nechceme zde samozřejmě nikoho z ničeho obviňovat, takže v dalších komentářích ponecháme autory "nejlepších seků" v anonymitě. Navíc smícháme tuzemské i zahraniční reakce – jde nám skutečně jen o jediné: "narovnat" některá tvrzení z odborného hlediska (jejich původce nechť případně narovnává někdo jiný...).

**Slyšeli jste to také?**

Publikování útoku způsobilo více odborných "faux pas", než bychom předpokládali, a velmi to připomínalo pořad "Nikdo není dokonalý". Řada výroků totiž předváděla učebnicové příklady elementárních neznalostí. Tak například u diskusí kolem souvislostí se zákonem o elektronickém podpisu (ZoEP) se vyskytl krásný argument, který tvrdil, že zpráva **zašifrovaná** v prostředí PGP není elektronický podpis. To je sice možné uznat, protože je to tautologie (tedy za všech okolností platný výrok), leč dává to asi tolik informace jako sdělení, že párek není banán.

K obecným prohřeškům "vykladačů" patřilo také snad až příliš familiární zacházení s logikou. Při pročítání některých reakcí člověk jako by opět slyšel otřepaný vtip, který se občas používá jako motivace ke studiu základního kurzu matematické logiky. V něm otec říká svému potomkovi, že pokud nesní celou večeři, nebude se smět dívat na večerníček. Řada autorů nejrůznějších výroků byla věrnou podobou synka, který vše poctivě zhltal, a pak se divil, že večerníček stejně nebyl. Vidíte, a tak ošklivá může být logika.

**Souvislost se ZoEP**

Asi nejvíce omílaným tématem byla souvislost celé kauzy se zákonem o elektronickém

podpisu. Chápeme, že nastalý humbuk politikům poněkud pobouřil voličskou obec, takže rychle přispěchali a své ovečky chlácholili nejrůznějšími argumenty. Abychom předešli možnému druhému kolu rozruchu, hned v úvodu této diskuse (také logicky špatně) předesíláme, že námi prezentovaný útok opravdu nijak “bezprostředně” **neohrožuje systémy stavěné dle ZoEP** a už vůbec nezpochybňuje princip elektronického podpisu jako takový (i to se dalo vyčíst z některých novinových titulků). Původně jsme se domnívali, že lidé pohybující se kolem tohoto zákona a jeho vyhlášek by si mohli přece jen útok prostudovat, aby alespoň věděli, čemu se mají vyhnout. Dnes se však zdá, že dotyční by si měli spíš znovu prostudovat zmíněný zákon a poslední návrh vyhlášek. Pak by se v jejich reakcích nemuselo tak vehementně zdůrazňovat, že PGP nemá zakotvení v ZoEP, když **žádný** konkrétní produkt nemá zakotvení v ZoEP.

Zákon jako takový o žádných konkrétních produktech nehovoří. Jeho vyhlášky snad budou konkrétnější, avšak jsou zatím pouze ve stadiu návrhu. Ačkoliv je tedy možné, že PGP by ve smyslu budoucích vyhlášek nebyl uznán jako bezpečný prostředek, nelze takovou věc říkat napřed a jako tvrzení přímo plynoucí ze ZoEP.

Někteří kritici mávali pojmem “zaručeného elektronického podpisu". To, že se ho PGP netýká, bychom si ale podle zákona netroufali říci. V definici tohoto pojmu totiž není uvedena **žádná přímá** spojitost s konkrétním prostředkem. Tu nalézáme až u pojmu “kvalifikovaný elektronický podpis”, který je nově zaveden v současném návrhu vyhlášek. Možná měli na mysli pojem “prostředek pro bezpečné vytváření elektronického podpisu”, ale i tak nemohli o PGP v tomto směru nic tvrdit – vyhlášky ještě nejsou vydány a nelze předjímat rozhodnutí Úřadu pro ochranu osobních údajů (ÚOOÚ), který to bude teprve posuzovat.

Zajímavé bylo také tvrzení, že jiné (lepší) systémy uchovávají privátní klíče ve formátu přesně dle litery ZoEP. To ve světle skutečnosti, že ZoEP právě o žádném **přesném** formátu nehovoří, je jistě jasnozřivý postřeh. Přes ZoEP a jeho navrhované vyhlášky se můžeme dopracovat pouze k velmi obecným vlastnostem, které takový formát musí splňovat. Můžeme proto pouze předpokládat, že určitý druh formátu by dle ZoEP a jeho vyhlášek “prošel”. To by se však autoři OpenPGP před oznámením našeho útoku bývali byli mohli domnívat také.

**Je to praktické?**

Objevily se také názory, že celý útok je velmi málo praktický, neboť většinou si uživatelé své soubory s privátními klíči chrání tak dobře, že útočník nemá šanci se k nim dostat. V takovém případě se přímo nabízí otázka, proč se tedy privátní klíč v takovém souboru šifruje. Vždyť pokud se k němu nelze dostat, pak je šifrování spolu s nutností volby a zapamatování si přístupového hesla jen zbytečným šikanováním uživatelů!

Domníváme se, že autoři OpenPGP, stejně jako autoři jiných rozumných formátů, šifrují privátní klíče prostě proto, že sami příliš nedůvěřují systémovým ochranám a obezřetnosti samotných uživatelů. My jsme jim ale ukázali, že tato ochrana je velmi slabá a *téměř* odpovídá stavu, kdy by privátní klíč šifrován nebyl. Pokud tedy nastane situace, které se autoři OpenPGP obávali, když se rozhodli privátní klíč zašifrovat, potom je popsaný útok velmi nebezpečný. Je to něco podobného jako tvrzení, že vaše auto má airbag, a on tam přitom místo něho je jen pouťový balonek. Vše funguje hladce – až do chvíle první větší havárie. Zkuste to ale říci výrobci a svolat k tomu tiskovku... A to je přesně ten případ s OpenPGP. Airbag, který zde představuje silná šifra chránící privátní klíč, tu sice je, ale nefunguje správně, a kromě toho jsou tu povolené ještě nějaké šroubky...

Nechceme zde vypočítávat všechny situace, kdy popsaný útok je a kdy není možný. Lze připustit, že pokud celý systém pracuje bez jediné chybičky (a to včetně chyb na straně uživatelů), potom se jeho použití není třeba bezprostředně obávat. Jenže je tu ještě další aspekt, a sice **záměrný a připravovaný** útok na celý systém. Jak zaznělo v některých reakcích, pokud někdo mermomocí bude chtít nějaký systém napadnout, cestu si vždy najde. Otázkou ovšem je, jak bude tato cesta snadná. Domníváme se, že námi prezentovaný útok ji činí podstatně schůdnější, neboť útočníkovi postačí modifikovat pouze **datový** soubor se zašifrovaným privátním klíčem. Někomu možná připadá útok modifikací dat stejný jako útok modifikací programů. Když ale dojde na “lámání chleba”, většinou zjistíme, že to totéž rozhodně není. Modifikace dat většinou bývá podstatně jednodušší než modifikace programů. Námi popsaný útok tedy neznamená bezprostřední konec stávajících aplikací na bázi OpenPGP, ale výrazné snížení složitosti jejich napadení.

**PGP je zastaralý a slabý?**

Objevilo se také pár názorů, že vše je způsobeno tím, že PGP je zastaralý program, který je určen toliko pro šifrování dat. Letmý pohled na internetové stránky věnované této problematice jasně ukazuje, že autoři těchto výroků asi nevěděli, o čem vlastně mluví. A docela bychom rádi viděli, co by se dělo, kdyby zkusili své tvrzení říci ne do kamery, ale třeba prodejcům tohoto

programu...

Je fakt, že PGP má za sebou desetiletou historii, ale to rozhodně neznamená, že dnes aktuální verze je 10 let stará (navíc poznamenejme, že útok jsme vyzkoušeli na té nejnovější) – stejně jako kdybychom o nějaké luxusní značce aut prohlásili, že to jsou zastaralé plechovky, protože se vyrábějí už několik desetiletí. Vlastně takový Unix by se také měl okamžitě přestat používat – je přece tak nemožně starý!

Také je zajímavé, že by "...PGP nebyl určen k podepisování". To by potom chtělo vysvětlit, proč se autoři tohoto mastodonta (pardon, ale osmimegabajtový zkomprimovaný instalační program...) mořili s tím, aby do něho tuto službu vůbec implementovali. Patrně neobstojí argument, že to bylo proto, že neměli zrovna co jiného na práci.

Kdesi jsme si také povšimli tvrzení, že opravdové systémy prý používají mnohem bezpečnější algoritmy, než je tomu v případě PGP. PGP se naopak právem může chlubit tím, že používá algoritmy AES/DH/DSS, patřící k absolutní špičce. A opět se zde ukazuje, jak malé je všeobecné povědomí o kryptografii. Nezáleží totiž jen na tom, **čím** data chráníme, ale také **jak** to děláme. To, co bylo předvedeno v případě OpenPGP, se bohužel opravdu nedá nazvat jinak než jako zmíněné "kryptování", a to je ten problém.

**Metafory váznou**

Na jednu stranu musíme ocenit snahu mnohých komentátorů přiblížit náročnost útoku běžným občanům. Na druhou stranu musíme ale konstatovat, že použité metafory, ať už se jednalo o klíče v šuplíku, na střeše auta, pod rohožkou či kdovíkde ještě, byly vždy poněkud mimo. Je to pochopitelné, neboť v reálném světě prakticky neznáme pojem "zašifrovaný klíč". Alespoň jsme tedy neslyšeli o tom, že by si děda Lebeda strkal pod práh zašifrovaný dozický klíč od své sekničky.

V tom je právě ten problém. Každý, kdo by si nechával klíčky od svého luxusního auta (privátního podepisovacího klíče) na kapotě, je pochopitelně davem označen za tupce, který si koleduje o průšvih. My jsme pak byli v očích posluchačů už jen ti ošklivý hoši, co klíčky čmajzli. Omyl. V digitálním světě můžete své milované auto zaparkovat před svým domem a zavřít ho ve zlomku vteřiny do nejlepšího digitálního trezoru na světě. Pak stačí naťukat na digitálním zámku jen vám známou kombinaci a můžete klidně odejít. My ošklivý hoši jsme ale zjistili, že výrobce tomuto trezoru pro lepší porozumění mezi lidmi montuje zadní stěnu z překližky. Sám velký tvůrce tohoto díla nám pak zavolal, a když jsme mu situaci vysvětlili, řekl tisku, že to není žádná praktická hrozba, jen zajímavé matematické pozorování...

**Závěr**

V tomto trochu oddychově laděném příspěvku jsme se snažili vysvětlit jednak důvody, které nás vedly k uveřejnění celého útoku, jednak myšlenky, které se nám honily hlavou, když jsme pročítali reakce na naše oznámení. Doufáme, že se nám podařilo vás nejen pobavit, ale hlavně vysvětlit některé zcela (ne)okrajové aspekty celé této kauzy.

*Vlastimil Klíma | v.klima@decros.cz*
*Tomáš Rosa | t.rosa@decros.cz*