Bezpečná komunikace v praxi – první krůčky

Kamil Malinka, ÚVT MU

V minulém čísle Zpravodaje ÚVT byl zveřejněn článek [1], který se zabýval problematikou bezpečnosti elektronických dat a elektronické komunikace. Vyvolal poměrně velkou čtenářskou odezvu. Řada lidí se cítila článkem oslovena; netušila ale, jak zásady bezpečné komunikace uvést do praxe na svém vlastním osobním počítači. Tento článek má za úkol poskytnout jakýsi jednoduchý návod pro první praktické seznámení s bezpečnostní technologií v oblasti e-mailové komunikace. Je zaměřen na uživatele operačního systému MS Windows používající – na MU hojně rozšířené – poštovní klienty ThunderBird resp. Mozilla.

Enigmail

Enigmail je open-source rozšíření (plugin) e-mailového klienta ThunderBird resp Mozilla, který umožňuje uživateli přístup k ověřování a šifrování zpráv prostřednictvím volně dostupného softwaru GnuPG (multiplatformní implementace standardu OpenPGP – viz RFC2440, nahrazujícího komerční šifrovací software PGP). Tento plugin umožňuje kompletní správu OpenPGP klíčů, šifrování/podepisování zpráv při odesílání a dešifrování/ověřování zpráv při jejich přijímání.

Pro využívání Enigmailu je třeba nejprve nainstalovat GnuPG, a dále přímo v aplikaci ThunderBird přidat samotné rozšíření. Českou lokalizaci a všechny potřebné instalační balíčky lze získat například na serveru `http://enigmail.spi.cz`. Po instalaci doplňku a následném restartu poštovního klienta se v nástrojové liště objeví nová záložka – OpenPGP. Pomocí ní lze provádět veškeré požadované funkce, především:

a) podepisovat své e-maily elektronickým podpisem; ten umožňuje příjemci ověření autentičnosti (autorství e-mailu nelze zpochybnit) a ověření integrity (e-mail nebyl cestou od odesílatele k adresátovi změněn);
b) šifrovat obsah e-mailu (utajení obsahu zprávy pro kohokoliv kromě adresáta);
c) ověřovat autentičnost/integritu přijatých e-mailů opatřených elektronickým podpisem;
d) dešifrovat obsah přijatých zašifrovaných e-mailů;
e) kompletní správu OpenPGP klíčů (jak vlastních privátních klíčů tak i cizích veřejných klíčů).

Elektronický podpis a šifrování zpráv – stručné opáčko

Zopakujme stručně jak funguje elektronický podpis u e-mailových zpráv:

- u odesílatele se pomocí hashovací funkce vypočítá z textu zprávy kontrolní součet;
- tento kontrolní součet je zašifrován privátním klíčem odesílatele a odeslán e-mailem jako podpis;
- příjemce rozšifruje podpis veřejným klíčem odesílatele (ověření autentičnosti), a získá tím kontrolní součet obdržené zprávy;
- příjemce vypočítá vlastní kontrolní součet přijaté zprávy a oba kontrolní součty porovná (ověření integrity).

Postup při výměně šifrovaných zpráv je následující:

- odesílatel zašifruje data veřejným klíčem příjemce a odešle je na adresu příjemce;
- příjemce vezme svůj privátní klíč a zprávu rozšifruje.

A jak to celé funguje v praxi

První věc, kterou je po instalaci Enigmail třeba udělat, je vygenerovat svou dvojici klíčů. Jedním z dvojice je klíč *veřejný*, o jehož distribuci budeme dále hovořit. Tento klíč má každý k dispozici, aby vám mohl zasílat zašifrované zprávy. Zašifrované zprávy může dešifrovat pouze držitel odpovídajícího *soukromého* klíče (tato druhá část vašeho klíče by zcela jistě neměla být k dispozici ostatním a je nezbytné ji mít bezpečně uloženu). Ovšem tyto vlastnosti již byly diskutovány v minulém čísle, takže se jimi nebudeme dále zabývat.

V nabídce ThunderBirdu zvolte možnost Správa OpenPGP klíčů. Zde můžete využít služeb průvodce, který vás provede celou procedurou. Zvolíte identity, které mohou využívat vygenerované

klíče, dále přístupové heslo a několik dalších vlastností. Průvodce je do detailu popisuje a jsou poměrně intuitivní, takže není třeba se jim hlouběji věnovat. Defaultní nastavení by mělo být dostatečné pro počáteční používání, přesto doporučujeme zvážit modifikaci následujících možností:

- *Doba platnosti klíče* – jak již název napovídá, určuje dobu platnosti. Technologie elektronického podpisu je založena na výpočetní složitosti. S technickým vývojem se zrychlují výpočetní možnosti strojů, a je tedy nutno brát tento fakt v potaz. Nedoporučuji tedy volit nějaké přehnaně velké hodnoty.
- *Velikost klíče* – určuje i odolnost klíče vůči útokům, kde čím delší klíč tím bezpečnější. Platí zde totéž co pro čas. Jen nutno brát v potaz vývoj a v současnosti se již nedoporučuje používání klíčů menších než 2048 bitů. Na druhou stranu, čím delší klíč, tím delší dobu trvá šifrování a ostatní funkce.

Po vygenerování soukromého a veřejného klíče budete vyzváni k vytvoření *revokačního certifikátu*. Tento certifikát může být použit pro zneplatnění klíče, např. při ztrátě soukromého klíče.

Vytvořený klíč je uložen ve správci pluginu Enigmail a pomocí něj provádíte příslušné operace. Jak již bylo zmíněno výše, váš veřejný klíč by měl být k dispozici ostatním uživatelům, aby si byli schopni ověřit vaši identitu. Jedním z možných způsobů je využití tzv. *keyserveru*. Uložením vašeho veřejného klíče na některém keyserveru umožníte ostatním využívat ho pro komunikaci s vámi. Pro ukládání veřejného klíče lze doporučit například server `pgp.mit.edu` nebo `pks.gpg.cz`. Další možností je zveřejnění klíče na vašich osobních webových stránkách. Zde ovšem člověk, který s vám chce komunikovat, nemá žádnou jistotu o pravosti tohoto klíče. Je několik možností, jak si ji ověřit. Jednou z možností je vytvoření tzv. *sítě důvěry* (web of trust). Váš veřejný klíč může být podepsán třetí osobu, např. kolegou z práce, a tím získává na jisté důvěryhodnosti; vytváří se tak jakási síť klíčů, které si navzájem věří. Jinou možností je vytvoření otisku vašeho klíče, tzv. *fingerprint*, a předání tohoto otisku bezpečnou cestou osobě, která s vámi chce komunikovat. Pomocí tohoto otisku lze ověřit pravost veřejného klíče. Zde už se ovšem dostáváme k otázkám distribuce veřejných klíčů, které jsou mimo rámec našeho článku.

Vraťme se tedy zpět k použití vygenerovaných klíčů. Při instalaci pluginu je nastaveno, že veškeré odchozí e-maily budou podepisovány vaším soukromým klíčem. Při tvorbě e-mailu si dále můžete přes nastavení OpenPGP nastavit i šifrování zprávy.

Výhodou rozšíření Enigmail je uživatelská transparentnost. Pokud vám dojde podepsaný resp. zašifrovaný e-mail a vy máte veřejný klíč odpovídající odesílateli, dojde k automatickému ověření resp. dešifrování zprávy, a vám se v aplikaci zobrazí již přímo text e-mailu. Tato možnost se dá volitelně vypnout – pak si můžete vychutnat pohled na zašifrovaný tvar zprávy.

Pomocí správy klíčů samozřejmě můžete vytvářet další klíče, pro odlišné scénáře použití. Například soukromý a pracovní, nebo můžete importovat již vytvořené veřejné klíče jiných účastníků komunikace; ale to je již běžná praxe.

Závěr

Práce s rozšířením Enigmail poštovního klienta ThunderBird/Mozilla je velmi intuitivní a po počátečních nastaveních nevyžaduje téměř žádnou režii. Co dodat závěrem? Pokroky v této oblasti jdou mílovými kroky vpřed a bezpečnostní technologie se začínají dostávat k masám. Pokud jste s nimi neměli dosud žádné zkušenosti, měl by vám tento článek pomoci při prvních krůčcích směrem k vyšší bezpečnosti vaší elektronické komunikace.

Literatura

[1] A. Kropáčová. *Bezpečnost elektronických dat a elektronické komunikace*. Zpravodaj ÚVT MU. ISSN 1212-0901, 2006, roč. 16, č. 4, s. 15–20. □