

Zabezpečenie elektronickej pošty

Medzi základné bezpečnostné riziká elektronickej pošty patria:

- zachytenie správy
- zablokovanie správy
- odchytenie a znovuposlanie správy
- modifikácia obsahu správy
- modifikácia pôvodu správy
- sfalšovanie obsahu alebo pôvodu správy treťou stranou
- sfalšovanie obsahu alebo pôvodu správy príjemcom
- zablokovanie prenosu

Zabezpečenie dôvernosti správy a ochrana proti falšovaniu obsahu sú zvyčajne riešené pomocou šifrovania. Šifrovanie tiež môže pomôcť pri ochrane proti znovuposlaniu správy (replay útok), musel by však byť použitý protokol, v ktorom je každá správa niečím výnimočná a teda unikátna.

Požiadavky na bezpečnosť

- dôvernosť správy - správa nie je prečítaná cestou k prijímateľovi
- integrita správy - prijímateľ vidí to, čo odosielateľ odoslal
- autenticita odosielateľa - prijímateľ si môže byť istý odosielateľom
- nepopierateľnosť - odosielateľ nemôže poprieť že odoslal správu

Nie všetky z týchto bodov sú nutné pre každú správu, pri ideálnej bezpečnej elektronickej pošte by sa však tieto body mali dať voliť selektívne.

Návrhy

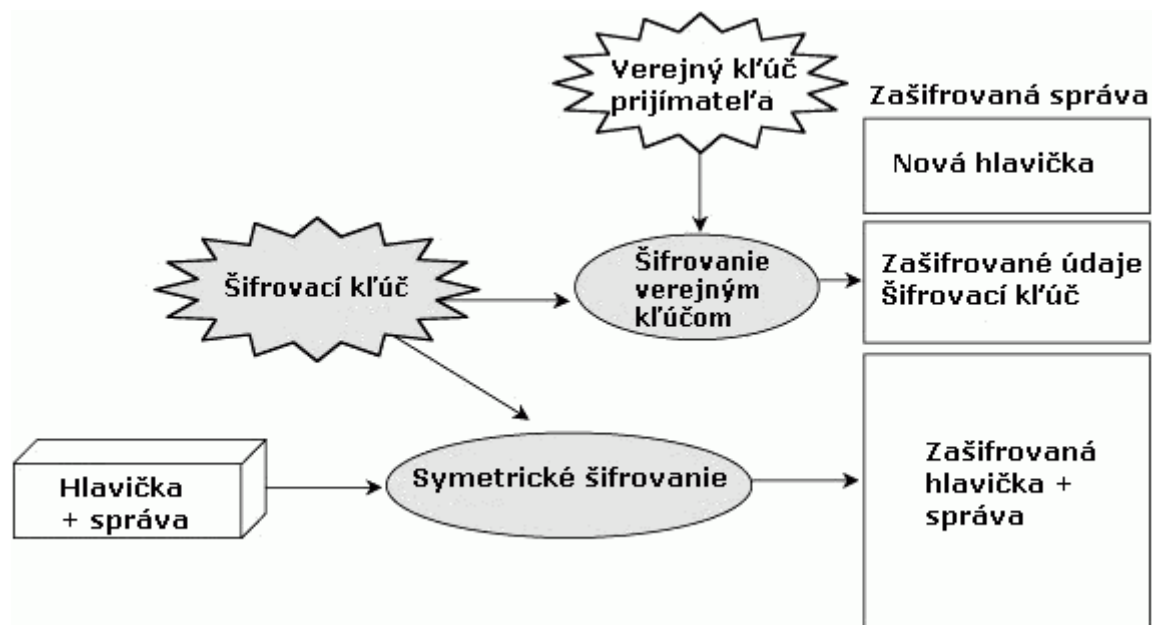
Štandard šifrovanej elektronickej pošty bol vyvinutý spoločnosťou Internet Society, dokumentovaný je v RFC 1421-1424.

Jedným z cieľov pri návrhu bolo umožniť prenos zabezpečenej správy cez bežné systémy elektronickej pošty. Celé zabezpečenie sa teda týka tela správy.

Dôvernosť

Zabezpečenie dôvernosti je zaistené nasledovne:

Odosielateľ si zvolí (náhodný) symetrický šifrovací kľúč a zašifruje ním celú správu vrátane hlavičky FROM, TO, SUBJECT a DATE. Následne pripojí nešifrované hlavičky. Na riadenie výmeny kľúčov zašifruje odosielateľ symetrický šifrovací kľúč verejným kľúčom prijímateľa a pripojí výsledok k správe.



Výsledkom šifrovania je náhodný reťazec. Veľa systémov elektronickej pošty však očakáva, že sa v správe budú nachádzať len tlačiteľné znaky, netlačiteľné znaky sa používajú v kontrolných signáloch. Na vyriešenie tohto problému sa zašifrovaná správa prekóduje na tlačiteľné znaky.

V systéme zabezpečenia sa teda používa symetrické aj asymetrické šifrovanie. Je však možné použiť čisto symetrické šifrovanie, predpokladom však je, že sa prijímateľ aj odosielateľ predtým dohodli na kľúči pomocou iných kanálov (telefón, fax atp.).

Štandard podporuje viacero šifrovacích algoritmov, napr. DES, 3DES a AES na zabezpečenie dôvernosti a RSA a Diffie-Hellman na výmenu kľúčov.

Ďalšie bezpečnostné vlastnosti

Zašifrované správy elektronickej pošty vždy nesú aj digitálny podpis, čím je zabezpečená pravosť a nepopierateľnosť odosielateľa. Tiež je tým zabezpečená integrita, keďže podpis obsahuje aj výstup hashovacej funkcie.

Hlavička v zašifrovanej správe sa môže odlišovať od novej hlavičky, ktorá je pridaná k zašifrovanej správe, čím sa dá zabezpečiť utajenie napr. predmetu správy.

Hlavným problémom šifrovanej elektronickej pošty je správa kľúčov. Certifikácia je výborný spôsob na priradzovanie identít k verejným šifrovacím kľúčom, problémom je však budovanie hierarchie, keď certifikáty musia byť uznané certifikačnou autoritou. Riešením tohto problému je systém PGP, ktorý bol vyvinutý ako jednoduchšia forma šifrovanej elektronickej pošty.

PGP

Skratka znamená Pretty Good Privacy, systém vynašiel Phil Zimmerman v roku 1991, v roku 1996 ho prevzala spoločnosť Network Associates. Existuje komerčná aj voľne šíriteľná verzia.

PGP adresuje problém distribúcie kľúčov zavedením takzvanej "kľúčenky". Používatelia systému si do nej podľa vlastnej vôle pridávajú verejné kľúče ostatných ľudí získané buď priamo zo zašifrovaných správ elektronickej pošty alebo zo serverov. PGP neustanovuje politiku na budovanie dôvery. Každý používateľ sa môže slobodne rozhodnúť komu dôveruje.

PGP vykonáva niektoré alebo všetky z nasledujúcich činností, v závislosti od toho, či je zvolená dôvernosť, integrita, pravosť, alebo nejaká ich kombinácia:

- vytvorenie náhodného relačného kľúča pre symetrický algoritmus
- zašifrovanie správy pomocou relačného kľúča (dôvernosť)
- zašifrovanie relačného kľúča verejným kľúčom prijímateľa
- vytvorenie hash správy, podpis hash správy zašifrovaním odosielateľovým privátnym kľúčom (integrita, pravosť)
- pripojenie zašifrovaného relačného kľúča k zašifrovanej správe a zašifrovanému hash-u
- prenos správy k prijímateľovi

S/MIME

Všeobecná špecifikácia MIME definuje formát a zaobchádzanie s prílohami elektronickej pošty. S/MIME je štandard na zabezpečenie týchto príloh.

Rozdiel medzi S/MIME a PGP je v metóde výmeny kľúčov. S/MIME používa hierarchicky uznané certifikáty, väčšinou vyjadrené vo formáte X.509. Tým pádom pri S/MIME odosielateľ ani prijímateľ nepotrebujú poznať svoje verejné kľúče pokiaľ obaja používajú rovnakú certifikačnú autoritu ktorej dôverujú.

Na rozdiel od PGP dokáže S/MIME pracovať s rôznymi údajovými formátmi, ako sú obrázky, videá, zvuky a podobne.