SECURE PROXY SERVER CONNECTED TO PGP

Roman MICHEL, Master Degree Programme (4)
Dept. of Information Systems, FIT, BUT
E-mail: xmiche01@stud.fit.vutbr.cz

Supervised by: Ing. Daniel Cvrček

ABSTRACT

Most of our today's communication is based on sending e-mails. This service was based on sending a plain text, which can be easily catched by attackers. One of the best possibilities is to encrypt or sign confidential messages by various methods. Pretty good privacy (PGP) became accredited as one of the standard e-mail encryption methods. To offer you a complete e-mail security solution, I decided to make Linux proxy server using GnuPG.

1 ÚVOD

Elektronická pošta (e-mail) se řadí k nejpoužívanějším Internetovým a nejpopulárnějším komunikačním službám vůbec. Protože v poslední době stále roste hodnota informací, je nutno řešit problematiku jejich ochrany – šifrování, ověřování autentičnosti, resp. integrity posílaného textu a odesílatele.

Tyto možnosti poskytuje uznávaný způsob asymetrické kryptografie známý jako PGP (Pretty Good Privacy) [3]. Vytvořením poštovního proxy serveru, který bude využívat některý z programů typu PGP lze zajistit vysokou úroveň bezpečnosti a vynutit si dodržování bezpečnostní politiky bez zatěžování koncových uživatelů.

2 ELEKTRONICKÁ POŠTA

E-mail je založen, stejně jako klasická pošta, na přijímání a posílání textových zpráv, případně různých příloh. K odesílání pošty se používá protokol SMTP [1], k přijímání POP3 [2]. Každá zpráva se skládá z:

- adresy odesílatele a příjemce (resp. příjemců)
- nepovinného předmětu zprávy
- samotného textu zprávy
- případných přiložených souborů
- dalších informací – např. času odeslání, prioritě

Formát zpráv je přesně definován standardem [4]. Všechna data jsou posílána jako čistý text. Není složité je odposlechnout, případně odchytit a pozměněné poslat adresátovi. Protokoly samotné šifrování nepodporují. Řešením může být šifrování zpráv

specializovanými programy, v klientských poštovních programech, nebo na úrovni proxy serveru. Poslední případ je ideálním řešením, protože nezatěžuje koncové uživatele jako v 1. případě a na rozdíl od 2. případu je možno definovat jednotnou bezpečnostní politiku.

3 BEZPEČNÁ KOMUNIKACE

Šifrování a bezpečnost dat lze zajistit různými způsoby. Základní dělení je podle počtu klíčů symetrické nebo asymetrické. Rozhodující je v každém případě délka klíče a použitý šifrovací algoritmus. Při zachycení posílané zprávy „třetí stranou“ musí být výpočetně náročné opětovné sestavení původních dat.

3.1 SYMETRICKÉ A ASYMETRICKÉ ŠIFROVÁNÍ

Při symetrickém šifrování se používá stejný klíč jak pro šifrování, tak pro dešifrování. Jeho bezpečná výměna mezi uživateli je plně v jejich režii.

Nesymetrické šifrování naopak zavádí tzv. klíčenku – každý uživatel disponuje svým soukromým klíčem a veřejnými klíči ostatních uživatelů. Zprávy lze poté:

- šifrovat veřejným klíčem adresáta; původní zprávu získá jen adresát použitím svého soukromého klíče
- digitálně podepisovat vlastním soukromým klíčem; tzv. hashovací funkcí [5] se vytvoří otisk zprávy, který podepíšeme – při jakékoliv změně ve zprávě nesouhlasí hodnota podpisu a příjemce má možnost si ověřit, zde zpráva přišla nezměněna od jistého uživatele, který její odeslání zároveň díky použití svého soukromého klíče nemůže popřít

K bezpečné výměně veřejných klíčů je možno využít certifikaci [6]. Certifikát je datová struktura, která se skládá z veřejného klíče a identity jeho vlastníka. To vše může být navíc podepsáno důvěryhodnou třetí stranou – tzv.certifikační autoritou. Pokud získáme certifikát, víme díky identitě komu klíč patří a po ověření podpisu certifikační autority se můžeme ujistit, že nebylo nic pozměněno.

3.2 PGP

PGP je program zajišťující navenek asymetrickou kryptografii. Ve skutečnosti se k šifrování zprávy používá symetrická šifra, protože je několikanásobně rychlejší než asymetrická. Ta se použije pouze k zakódování klíče symetrické šifry.

V současné době je program PGP zdarma pro nekomerční využití. Ze skupiny podobných programů je jedním z nejznámějších GnuPG [7], který je zcela zdarma a navíc jsou k dispozici i zdrojové kódy. Proto jsem se rozhodl použít raději tuto variantu.

4 PRINCIP PROXY SERVERU

Proxy server obecně slouží jako brána mezi vnitřní sítí a Internetem. Je to brána na aplikační úrovni vyřizující požadavky. Klientská aplikace zašle požadavek proxy serveru, ten jej vyšle do Internetu a odpověď předá zpět aplikaci.

V našem případě funguje jako SMTP i POP3 server. Odchozí zprávy jsou podepisovány nebo šifrovány. U příchozích je možné ověřit podpis, příp. zprávu dešifrovat a až poté předat adresátovi (resp. klientské aplikaci). Ideální je, pokud běží přímo na lokální pracovní stanici,

nebo tvoří bránu mezi intranetem a Internetem. První případ je ideální pro osobní použití, druhý pro firmu, kde se vyžaduje dodržování jednotné bezpečnostní politiky. V jiném případě (umístění na Internetu nebo mimo důvěryhodnou zónu) nemá jeho použití význam.

5 BEZPEČNOSTNÍ POLITIKA

Bezpečnostní politika je souhrn pravidel, které je potřeba dodržovat k udržení vlastní informační bezpečnosti. Výhodou proxy serveru je možnost definovat jednotné pravidla pro všechny. Podle odesílatele, domény adresáta, případně dalších atributů může server rozhodnout, jak bude s konkrétním e-mailem naloženo. Jestli bude beze změny odeslán, nebo je potřeba jej podepsat, či zašifrovat. Příchozí e-maily může dešifrovat, resp. ověřit podpis a poslat zprávu adresátovi do intranetu, nebo jej informovat o příchodu zprávy s neplatným podpisem.

6 ZÁVĚR

Cílem práce je vytvoření jednoduchého proxy serveru zajišťujícího bezpečnou komunikaci pomocí předem známých a ověřených technologií. Díky nezávislosti na poštovních klientech a vlastní autonomii může být jeho existence koncovým uživatelům skryta – to umožní vytvoření a dodržnování jednotné bezpečnostní politiky.

Další rozvoj by mohl směřovat k vytvoření uživatelsky přívětivého konfiguračního rozhraní, případně vyčlenění části programu do konfiguračních souborů. Například vytvořit soubor obsahující všechny výzvy a hlášení programu pro zjednodušení tvorby jazykových mutací, nebo vyčlenění příkazů pro GnuPG. Jejich záměnou za jiné příkazy se stejnou funkcí by bylo jednoduché přecházet na jiné verze GnuPG, případně na jiné programy z rodiny PGP, kde jsou příkazy podobné, ne však stejné.

Server by dále šel rozšiřit o další doplňující funkce – filtrování spamu, „inteligentní“ chování při práci s pravidly a vlastní upravování si bezpečnostní politiky…

LITERATURA

[1] Postel, J.: Simple mail transfer protocol, RFC-821, University of Southern California, 1982

[2] Myers, J., Rose, M.: Post office protocol – Version 3, RFC-1939, 1996

[3] www.pgp.cz, www.pgp.net

[4] Crocker, D.: Standard for the format of ARPA-Internet text messages, STS11, RFC-822, Department of electrical engineering, University of Delaware, 1982

[5] Rivest, R.: The MD5 message-digest algorithm, RFC-1321, MIT laboratory for computer science, 1992

[6] Gerck, E.: Overview of certification systems: X.509, CA, PGP and SKIP, 1998

[7] www.gnupg.org