CONFIGURABLE SECURITY EMAIL PROXY

Stanislav Židek
Bachelor Degree Programme (1), FIT BUT
E-mail: xzidek05@stud.fit.vutbr.cz

Supervised by: Daniel Cvrček
E-mail: cvrcek@fit.vutbr.cz

ABSTRACT

This paper deals with design and implementation of multiuser configurable system capable of securing communication via electronic mail. Emphasis is put especially on ability to define very complex security policies and on remote configuration.

1 ÚVOD

Současné systémy pro zabezpečení obsahu emailových zpráv (jmenujme například OpenPGP) se soustřeďují na fungování pouze v rámci jednotlivých počítačů koncových uživatelů, kteří se v podstatě o zabezpečení musí z velké části starat sami. To může být naprosto nevyhovující kupříkladu pro větší organizace, jež mají zájem na zabezpečení komunikace všech svých zaměstnanců.

Cílem mé bakalařské práce bylo vytvořit základ víceuživatelského sytému pro zabezpečení komunikace elektronickou poštou s možností vzdálené konfigurace. Jednou z nejdůležitějších funkcí je možnost centrální definice bezpečnostních politik pro neomezený počet uživatelů, což lze využít například ve velké firmě, kde s minimálním aktivním zapojením většiny zaměstnanců kompletně obstaráme zabezpečení komunikace s okolím. Centrální definice je vhodná zejména z toho důvodu, že odstíní uživatele od věcí, kterým nemusí rozumět, a systém tak ochrání od chyb z toho vyplývajících. To přináší obrovskou výhodu v přenesení téměř veškeré zodpovědnosti z laiků (uživatelů) na odborníky (administrátory).

Aplikace je tedy schopna vnutit určitou bezpečnostní politiku pro daný cíl emailové komunikace a tím eliminovat potenciální (záměrné i neúmyslné) chyby uživatelů při zabezpečování emailových zpráv, které se mohou vyskytnout při použití jiných způsobů zabezpečení.

2 POPIS SYSTÉMU

2.1 ZPŮSOB FUNGOVÁNÍ

Systém funguje jako proxy server umístěný v lokální síti, o které se předpokládá, že je komunikace uvnitř ní bezpečná. Typická komunikace probíhá přibližně takto:

1. Klient se připojí k proxy, jež mu simuluje příslušný server (SMTP, POP3 . . .)

2. Klient požádá o odeslání, respektive přijetí zprávy.

3. Proxy se připojí ke skutečnému serveru a danou zprávu převezme od klienta, respektive stáhne ze serveru.

4. Proxy zprávu zašifruje a podepíše, respektive rozšifruje a ověří podpis.

5. Takto upravenou zprávu proxy předá serveru, respektive klientovi.

Jak je patrné, jediný nutný zásah na počítačích klientů je změna nastavení poštovních serverů v emailovém klientovi. Místo adres skutečně používaných serverů je nutné uvést adresu, na níž běží proxy server.

2.2 KONFIGURACE

Popis fungování v minulé části je samozřejmě velmi zjednodušený. Pokud má proxy odeslat převzatou zprávu, je nutné mít informace o tom, zda a případně jak ji zpracovat (jestli ji má zašifrovat, podepsat, případně obojí). Dále potřebuje informaci o adrese skutečného serveru, k němuž se klient (nebýt proxy) připojoval.
Všechny potřebné informace jsou uloženy v souboru s nastavením. Jde o XML dokument, jenž je uložen na počítači, kde běží proxy. Musíme si v tuto chvíli uvědomit, že pokud nám jde o zabezpečení komunikace většího množství uživatelů, nevyhneme se určité složitosti konfiguračního souboru. Na druhou stranu pak administrátor dostává do rukou poměrně mocný nástroj, který mu umožňuje vytvářet velmi komplexní zabezpečovací pravidla.
Konfigurační soubor je rozčleněn na tyto čtyři části:

1. nastavení pro jednotlivé uživatele

2. nastavení pro jednotlivé domény

3. celkové nastavení systému

4. veřejné klíče subjektů, které leží mimo síť dané proxy

Zabezpečovací politika má dvě části, uživatelskou a doménovou. Díky tomu je možné například nadefinovat, aby všechna komunikace mezi dvěma doménami probíhala zabezpečeně a není tak nutné specifikovat všechny kombinace odesilatelů a příjemců. Pokud by však byla definována jak politika pro domény, tak pro konkrétní uživatele, projeví se tyto nastavení v obou částech zabezpečovací politiky.
Ani v rámci jedné části není zjišťování politiky triviální. Celkové, administrátorské nastavení systému (část číslo 3) má přednost před vlastním nastavením konkrétního uživatele či domény (část 1 nebo 2). I v této úrovni zanoření je potřeba zohlednit priority jednotlivých nastavení, protože si uživatel může například vytvořit skupinu kontaktů se stejnou politikou a toto nastavení pak „přebít“ jiným jen pro jeden kontakt z této skupiny.

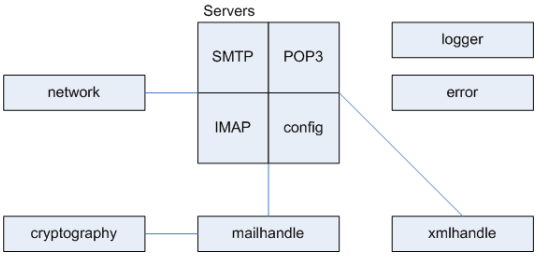
2.3 VZDÁLENÁ KONFIGURACE

Konfigurace na dálku probíhá kvůli dostupnosti elektronickou poštou přes vyhrazenou emailovou schránku, kterou si proxy v pravidelných intervalech testuje na přítomnost konfiguračních emailů (ve formátu XML).

Implementace je pak poměrně jednoduchá. Je možné provádět tři příkazy (vytvoř, smaž, změň), jež jsou zároveň i jménem kořenového uzlu konfiguračního emailu. Mají jeden (při vytváření a rušení) nebo dva (při změně – obsahuje aktuální a požadovanou verzi) poduzly se stejnou strukturou jako příslušná část konfiguračního souboru. Potom stačí jednoduše pomocí knihovních funkcí modifikovat strom XML v paměti a uložit jej do konfiguračního souboru.

2.4 STRUKTURA

Jádro systému tvoří jednotlivé proxy servery – SMTP, POP3, IMAP a konfigurační server. Starají se o obsluhu připojených klientů, kterým předstírají funkčnost skutečných serverů. Tyto servery využívají služeb ostatních částí, mezi něž patří například síťový modul (funkce pro zjednodušení práce se sítí), kryptografický modul (funkce pro šifrování/dešifrování a podepisování/ověření) a modul pro práci s XML konfiguračním souborem (zjišťování potřebných nastavení a zabezpečovacích politik).



Obrázek 1: Schéma systému

3 ZÁVĚR

Popsané řešení bylo úspěšně naimplementováno a omezené míře byla otestována jeho funkčnost; v budoucnu by však bylo vhodné otestovat systém při praktickém nasazení v prostředí s větším počtem uživatelů.
Povedlo se vytvořit základ systému vhodného k centrálnímu zabezpečení emailové komunikace větší skupiny uživatelů. Rád bych zmínil především velmi komplexní systém výběru zabezpečovací politiky – ten probíhá ve několika krocích s různou úrovní důležitosti. Rovněž stojí za zmínku poměrně elegantní implementace vzdálené konfigurace – v detailech jistě ještě projde změnami, ale její filosofie se už pravděpodobně měnit nebude.
Celkově vytvořená proxy představuje velmi komplexní systém. V současné době probíha portace systému na vestavěné zařízení, což by mohlo zvýšit použitelnost díky lepší možnosti zabezpečení přístupu k systému a uspoření nákladů na počítač, na kterém proxy běží.

PODĚKOVÁNÍ

Rád bych poděkoval svému vedoucímu, Danielu Cvrčkovi, za mnoho užitečných rad a podporu při implementaci tohoto projektu.