VIRUS CHECKING MODULE FOR THUNDERBIRD

Lukáš Ďurfina
Bachelor Degree Programme (3), FIT BUT
E-mail: xdurfi00@stud.fit.vutbr.cz

Supervised by: Petr Peringer
E-mail: peringer@fit.vutbr.cz

ABSTRACT

This paper deals with development of virus checking module for e-mail client Thunderbird. The module checks e-mail content using AVG tools. It is accomplished by scanning attachments in incoming and outgoing e-mails. I implemented module using XUL, XPCOM, JavaScript and DOM. I show the possible reactions to infected message. Finally, the results of module testing are presented.

1 ÚVOD

Problém kontroly elektronickej pošty spočíva v komunikácii s poštovým serverom pomocou šifrovaného protokolu, pretože sa tým stráca možnosť kontroly obsahu pošty pri jej sťahovaní klientom. Cieľom mojej práce je vytvoriť zásuvný modul pre poštový klient Mozilla Thunderbird, ktorý bude na strane klienta kontrolovať prichádzajúcu a odchádzajúcu poštu pomocou systému AVG [3] firmy AVG Technologies, ktorá podporovala jeho vývoj. Tým, že modul je integrovaný priamo v klientskej aplikácií bude možné kontrolovať e-maily, ktorých kontrola by inak bola znemožnená šifrovaným protokolom, a takisto modul umožní užívateľovi lepšiu kontrolu nad vykonávanými akciami s infikovanou poštou.

2 NÁVRH MODULU

Návrh sa skladá z niekoľkých častí. Najprv budú popísané dve najvýraznejšie technológie platformy Mozilla, ktoré zahrňujú tvorbu GUI a aplikačnú logiku. Následne sú rozobraté jednotlivé možnosti reakcie na infikovanú správu, ktoré modul umožňuje.

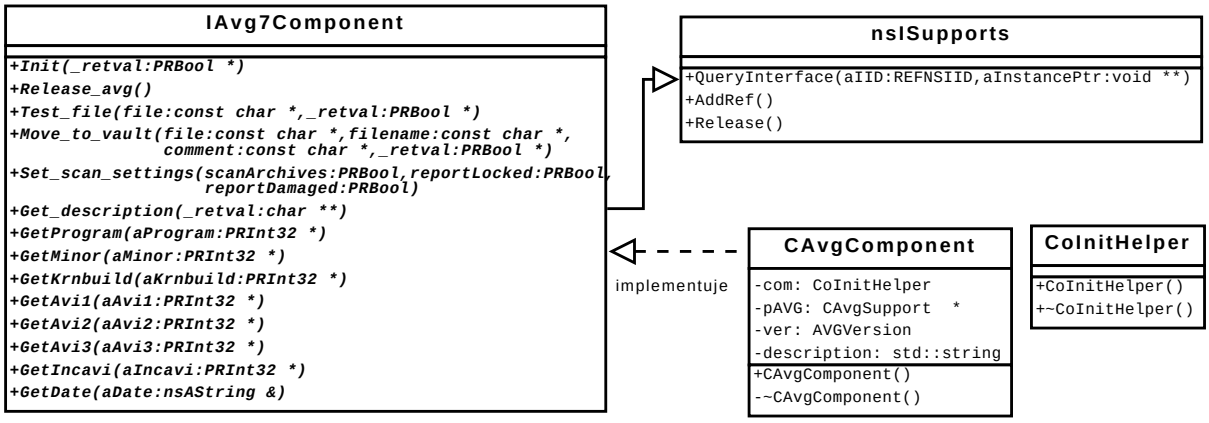
2.1 XUL ROZHRANIE

XUL [1] je značkovací jazyk založený na XML, ktorý slúži na popis užívateľského grafického rozhrania. Týmto jazykom sú popisané užívateľské rozhrania aplikácií založených na platforme Mozilla a podporuje prenositeľnosť. XUL používa známe webové technológie CSS, JavaScript a DOM.

Prvky UI sú definované XML tagmi. Základom býva okno určitého typu, ktoré obsahuje ďalšie prvky, ktoré tvoria jeho obsah. Interakcia s užívateľom je naprogramovaná pomocou javascriptu a vyvoláva sa na základe udalostí. Podporovaná je aj lokalizácia, čo bude využité v module.
V tomto jazyku bolo popísané okno s nadstaveniami modulu a výstražné dialógy. Okrem toho jazyk umožňuje pomocou *overlays* pridávať ďalšie prvky do prostredia cieľovej aplikácie, tým sa zabezpečí integrácia skriptov do prostredia a pridanie položiek do menu.

2.2 XPCOM KOMPONENTA

XPCOM – Cross Platform Component Object Model [2] je multiplatformový komponentový objektový model. Obsahuje podobné princípy ako model CORBA a model COM od firmy Microsoft. Pomocou tejto technológie je možné rozdeliť funkcionalitu do menších častí, tzv. *komponentov*.
V modeli je rozdelená implementácia a rozhranie. Implementácia býva obsiahnutá v dynamickej knižnici a rozhranie je popísané pomocou XPIDL – interface description language pre XPCOM. Na pripojenie sa ku konkrétnej komponente je potrebné uviesť jej ContractID, čo je jej jednoznačný reťazcový identifikátor. Komponenta sa pripája metódou `getService()` alebo `getInstance()`. Tieto metódy majú parameter názov požadovaného rozhrania.
Pomocou XPCOM je potrebné prepojiť modul s AVG, pričom sa použije AVG API. Na základe popisu rozhrania v xpidl bol vygenerovaný hlavičkový súbor, ktorý je podkladom pre návrh komponenty zobrazený na obr.1. Komponenta zabezpečuje inicializáciu a uvoľnenie kernelu AVG. Okrem metódy na testovanie súborov umožňuje presun súboru do antivírovej truhly, nadstavenie parametrov testu a zistenie popisu posledne nájdenej infekcie. Pre modul sú vytvorené dve komponenty z dôvodu podpory AVG 7 aj AVG 8.



Obrázek 1: Objektový návrh AVG XPCOM komponenty

Pre jednoduchý prístup ku komponente slúži javascriptový objekt, ktorý zabezpečuje zistenie nainštalovanej verzie AVG, automatické zavedenie príslušnej komponenty, inicializovanie a uvoľňovanie. Vďaka tomu stačí na všetky operácie s AVG zavolať konkrétnu metódu tohoto objektu.

2.3 REAKCIE NA INFIKOVANÝ E-MAIL

Hlavnú časť modulu tvorí kontrola prijatej pošty. Testujú sa všetky e-maily s prílohami, ktoré môžu byť nebezpečné. Po nalezení infekcie v doručenom e-maily je potreba na ňu reagovať.

Navrhol som niekoľko možností, ktoré by mali vyhovieť väčšine užívateľov. Hrubo zobrazené možnosti je možné ľubovoľne kombinovať, ale mať vybranú jednu z operácií je povinné.

Výstražný dialóg – Zobrazený dialóg zobrazí e-mailovú adresu odosieľateľa, konto, kde bol doručený e-mail, predmet správy a výpis pozitívne testovaných príloh s popisom infekcie.

Poznámka v predmete – Do predmetu bude pridaný užívateľom definovaný textový reťazec.

Operácia – vykoná sa práve jedna z nasledujúcich

- Presun do špeciálnej zložky – Celý e-mail sa presunie do zložky *AVG infected*.
- Odstránenie príloh – Infikované prílohy budú odstránené.
- Zmazanie e-mailu – Celý e-mail bude zmazaný.

Pri kontrole odosielanej pošty je užívateľ upozornený, že odosiela infikovaný obsah s bližším popisom, a môže pokračovať v odosielaní bez týchto príloh alebo sa vrátiť k vytváraniu správy. Modul umožní aj manuálnu kontrolu cez kontextové menu, ktorá pri nájdení infekcie ponúkne možnosť dané prílohy odstrániť. Pre každý typ kontroly je možné nadstaviť parametre, ktoré povoľujú testovanie vo vnútri archívov, oznamovanie zamknutých a poškodených archívov.

3 VÝSLEDKY

Modul bol úspešne implementovaný pomocou spomenutých technológii, podporuje obe aktuálne verzie AVG a je ho možné inštalovať do vývojovej rady Thunderbirdu 2.
Doba trvania kontroly je priamo úmerná veľkosti príloh. Pri menších prílohách (do 0,5 MB) je spomalenie aplikácie na dnešných počítačoch ťažko pozorovateľné. Pri rádovo väčších prílohách je spomalenie výraznejšie, ale výkonové problémy s takými prílohami má aj Thunderbird.

4 ZÁVER

Modul úspešne kontroluje správy prijaté cez protokol IMAP. V dôsledku zložitej implementácie tohoto protokolu nemôžem vylúčiť výskyt problémov na niektorých serveroch, ale implementácia modulu bola zameraná tak, aby bolo takéto správanie minimalizované a hrozí v špecifických prípadoch, ktoré sa často ani neporadí opäť reprodukovať. Protokol POP3 je o poznanie jednoduchší, takže kontrola je v jeho prípade bezproblémová.
Modul bude prínosom k bezpečnejšej e-mailovej komunikácií. Hlavnou výhodou je kontrola správ cez zašifrované protokoly, ktoré bežné súčasti antivírových programov nie sú schopné kontrolovať, avšak toto si často užívateľ neuvedomuje.

REFERENCE

[1] McFarlane, N.: Rapid application development with Mozilla, Prentice Hall 2003, ISBN 0-13-142343-6

[2] Turner, D, Oeschger, I.: Creating XPCOM components, [Online], [cit. 2008-02-18], Dostupné z WWW `http://www.mozilla.org/projects/xpcom/book/cxc/`

[3] AVG Technologies: AVG API dokumentácia, 2008