Západočeská univerzita v Plzni
Fakulta aplikovaných věd
Katedra informatiky a výpočetní techniky

Simple Mail Transfer Protocol

Analýza a syntéza protokolu

Semestrální práce z předmětu KIV/PSI

Petr Zelenka, pzeli@students.zcu.cz

Zadání

- Protokolová analýza

  “Vytvořte programové vybavení pro zachycování a analýzu SMTP paketů. Soustřeďte se zejména na SMTP protokol a ve zprávách na zobrazování obsahu záhlaví. Zachovávejte diskrétnost.”

- Protokolová syntéza

  “Dále realizujte klienta SMTP, který bude schopen vytvořit a korektně odeslat zprávu.”

Stručná charakteristika protokolu (1)

- Základní protokol pro přenos elektronické pošty
- Používán od 80. let minulého století
- Textově orientovaný protokol
  - Nejčastěji přenášený pomocí protokolu TCP
  - Může být přenášen i pomocí dalších protokolů (NCP, NITS, X.25)

- Server běží standardně na portu 25 (SMTP) nebo 465 (SMTP/SSL)

Stručná charakteristika protokolu (2)

- Simple Mail Transfer Protocol může být jednoduchý
  - RFC 0821 – 72 stran
  - RFC 2821 – 79 stran
  - RFC 2822 – 51 stran
- Pro porovnání: OSI IS-IS Intra-domain Routing Protocol
  - RFC 1142 – 653 stran

- Simple Mail Transfer Protocol může být složitý
  - Existuje řada různých rozšíření

Formát přenášených zpráv

- Zprávy obsahující požadavky klienta
  - Řídící příkazy (DATA, EXPN, HELO, HELP, MAIL FROM, NOOP, QUIT, RCPT TO, RSET, VRFY a další)
    - <příkaz> [<mezera> <parametry příkazu>] <CRLF>
  - Data
    - <datový řetězec> <CRLF>

- Zprávy obsahující odpovědi serveru
  - Kód a zpráva označující stav poslední provedené operace
  - <kód> <zpráva> <CRLF>

Příklad komunikace

- 220 smtp.ceskypes.cz ESMTP Postfix; Mon, 12 Apr 2006 11:10:00 +0200 (CEST)
- HELO bouda.ceskypes.cz
- 250 smtp.ceskypes.cz Helo kokrspanel@ceskypes.cz, pleased to meet you
- MAIL FROM: kokrspanel@ceskypes.cz
- 250 kokrspanel@ceskypes.cz... Sender ok
- RCPT TO: ratlik@ceskypes.cz
- 250 ratlik@ceskypes.cz... Recipient ok
- DATA
- 354 End data with <CR><LF>.<CR><LF>
- From: Kokrspanel <kokrspanel@ceskypes.cz>
- To: Ratlik <ratlik@ceskypes.cz>
- Subject: Co kupuji kocky
- Kocky kupuji WHISKAS!!!
- .
- 250 EAA20455 Message accepted for delivery
- QUIT
- 221 Bye.

Návrh implementace (1)

- SMTP analyzátor (smtpa)
  - Program pro zachytávání a analýzu přenášených zpráv elektronické pošty
  - Možnost využití pro monitorování přenášených zpráv
  - Možnost využití pro vytváření přehledů a statistik

- Odposlech obsahu zpráv porušuje současnou legislativu
  - Využívání samotných hlaviček
- Nutnost indentifikace příslušnosti paketů k relaci

Návrh implementace (2)

- SMTP syntezátor (smtps)
  - Program pro sestavení a odeslání zprávy elektronické pošty umožňující zadat uživateli libovolné parametry
  - Možnost využití pro odesílání falešných zpráv (fakemailer)
  - Nutnost vést uživatele procesem sestavení zprávy
    - Uživatelské rozhraní ve stylu průvodce (např. instalátor Linuxové distribuce Debian)

Závěr

- Implementace SMTP analyzátoru/syntezátoru není obtížná, pokud se implementuje základní varianta protokolu
- Obě části semestrální práce jsou užitečné :-)
- Obě části semestrální práce jsou na sobě nezávislé, není tedy žádný rozumný důvod integrovat je do jednoho celku

Použité zdroje

- RFC 0821 – Simple Mail Transfer Protocol (1982)
- RFC 2821 – Simple Mail Transfer Protocol (2001)
- RFC 0822 – Format of ARPA Internet Text Messages (1982)
- RFC 2822 – Internet Message Format (2001)
- zkušenosti s programem telnet a otevřenými SMTP servery

Děkuji za pozornost

Prostor pro dotazy