VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Reverse-engineering neznámeho protokolu

Síťové aplikace a správa sítí

Peter Urgoš

15. 11. 2021 xurgos00

# 1. Analýza zachytenej komunikácie

Komunikácia medzi referenčným serverom a klientom prebieha na prednastavenej adrese localhost a port 32323. Ak je to možné, použije sa IPv6, takže adresa bude ::1.

Na komunikáciu sa používa TCP/IP rámec. Jednotlivé správy sa posielajú v tele TCP segmentov.

# 2. Popis protokolu

Protokol podporuje 6 príkazov: register, login, logout, send, list a fetch. Za názvom príkazom nasledujú parametre.

Odpoveď môže mať status ok, alebo err. Za statusom nasleduje telo správy.

## 2.1. Príkazy a odpovede:

### 2.1.1. Register

Príkaz:

(register "<user>" "<pwd>")

Odpoveď(e):

(ok "registered user <user>")

(err "user already registered")

### 2.1.2. Login

Príkaz:

(login <user> <pwd>)

Odpoveď(e):

(ok "user logged in" "<token>")

(err "unknown user")

(err "incorrect password")

### 2.1.3. Logout

Príkaz:

(logout "<token>")

Odpoveď(e):

(ok "logged out")

### 2.1.4. Send

Príkaz:

(send "<token>" "<recipient>" "<subject>" "<body>")

Odpoveď(e):

(ok "message sent")

(err "unknown recipient")

### 2.1.5. List

Príkaz:

(list "<token>")

Odpoveď(e):

(ok ([message])), kde [message] môže byť ľubovoľný počet správ oddelených medzerou vo formáte (<id> "<sender>" "<subject>")

### 2.1.6. Fetch

Príkaz:

(fetch "<token>" <id>)

Odpoveď(e):

(ok ("<sender>" "<subject>" "<body>"))

(err "wrong arguments")

(err "message id not found")

# 3. Návrh disektoru

Disektor je implementovaný v zdrojovom súbore main.lua. Spracuváva pakety, ktoré boli odoslané, alebo prijaté z/do portu 32323.

Spracované pakety majú vo Wiresharku hodnotu v stĺpci Protocol nastavenú na ISA. Tieto pakety majú rozšírený strom s detailami o danom pakete, nazvaný ISA Protocol Data.

# 4. Zdroje

Kostra jednoduchého TCP klienta bola prevzatá z <https://beej.us/guide/bgnet/html/#client-server-background>

Implementácia base64 algoritmu bola prevzatá z - <https://renenyffenegger.ch/notes/development/Base64/Encoding-and-decoding-base-64-with-cpp/>

Obsah

[1. Analýza zachytenej komunikácie 2](#_Toc87913006)

[2. Popis protokolu 2](#_Toc87913007)

[2.1. Príkazy a odpovede: 2](#_Toc87913008)

[2.1.1. Register 2](#_Toc87913009)

[2.1.2. Login 2](#_Toc87913010)

[2.1.3. Logout 2](#_Toc87913011)

[2.1.4. Send 2](#_Toc87913012)

[2.1.5. List 3](#_Toc87913013)

[2.1.6. Fetch 3](#_Toc87913014)

[3. Návrh disektoru 3](#_Toc87913015)

[4. Zdroje 3](#_Toc87913016)