

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Reverse-engineering neznámého protokolu

Síťové aplikace a správa sítí

15. 11. 2021

Peter Urgoš
xurgos00

1. Analýza zachytenej komunikácie

Prednastavené hodnoty serveru sú: adresa je `localhost` IPv6, takže `::1` a port `32323`. Na komunikáciu sa používa TCP/IP stack. 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 dissektoru

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/>

Table of Contents

1. Analýza zachytenej komunikácie	2
2. Popis protokolu.....	2
2.1. Príkazy (commandy):.....	2
2.1.1. register	2
2.1.2. login.....	2
2.1.3. Logout.....	2
2.1.4. Send.....	2
2.1.5. List	3
2.1.6. Fetch.....	3
3. Návrh disektoru.....	3
4. Zdroje	3