**SVEUČILIŠTE U ZAGREBU, FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA**

36. Chat

**WEB PRIKLJUČNICE I SIGURNA KOMUNIKACIJA**

Matija Šekrst

**Zagreb, prosinac 2016.**

# Uvod

Tema ovog izvješća je su Web priključnice (engl. *Web sockets*), sigurna komunikacija između više priključnica, te mogućnosti ostvarenja takve komunikacije korištenjem *Node.js* platforme.

*Node.js* je platforma koja omogućuje izradu skripti koje se izvode na poslužitelju. Sigurna komunikacija u ovom radu odnosi se na nemogućnost nekog napadača da sazna sadržaj poruka koje razmjenjuju klijent i poslužitelj.

U prvom poglavlju bit će objašnjena tehnologija Web priključnica, u drugom poglavlju dan je pregled mogućnosti izvedbe sigurne komunikacije između priključnica. Treće poglavlje bavi se implementacijom sigurne komunikacija za Node.js platformu.

# Web priključnice

Web priključnice su tehnologija koja omogućuje interaktivno slanje poruka s klijenta na poslužitelj. Interaktivno ovdje znači da je s klijentske strane moguće poslati poruku na poslužitelj korištenjem priključnica, te nastaviti neki drugi posao. Isto tako je moguće da poslužitelj primi poruku, obradi je i da po potrebi pošalje odgovor klijentu. Važno je napomenuti da tehnologija Web priključnica omogućuje i da poslužitelj obavještava klijenta o promjenama. Upravo će se ova ideja upotrijebiti u izradi projekta. Naime klijent će se registrirati kod poslužitelja poruka koji će primati poruke, pohranjivati ih u bazu podataka, te obavještavati klijenta kojemu je namijenjena poruka o novoj poruci. Druga važna napomena je da će se cijela komunikacija odvijati u stvarnom vremenu (engl. *real time*), što znači da će klijent primati poruke i prikazivati ih bez potrebe za osvježavanjem stranice (engl. *refresh*).

Web priključnice se mogu izvesti korištenjem oba transportna protokola: UDP i TCP.