



TEHNOLOGIJA, INFORMATIKA I OBRAZOVANJE ZA DRUŠTVO UČENJA I ZNANJA

6. Međunarodni Simpozijum, Tehnički fakultet Čačak, 3–5. jun 2011.

TECHNOLOGY, INFORMATICS AND EDUCATION FOR LEARNING AND KNOWLEDGE SOCIETY

6th International Symposium, Technical Faculty Čačak, 3–5th June 2011.

UDK: 004.9:796.323

Stručni rad

PRENOS OSNOVNIH STATISTIČKIH PARAMETARA U KOŠARCI KORIŠĆENJEM INTERNETA

Branko Markoski¹, Zdravko Ivanković², Predrag Pecev³, Zoran Milošević⁴, Višnja Istrat⁵

Rezime: Rad opisuje dva načina zaštite podataka koji se razmenjuju u B2B aplikacijama, upotrebom web servisa. Podaci se prosleđuju između dve različite baze podataka, putem strukturiranog XML dokumenta. Opisano softversko okruženje se koristi za prikupljanje i evidenciju podataka sa košarkaških utakmica (prve savezne muške i ženske lige Srbije), koji se u trenutnom režimu šalju ka centralnom web serveru gde se ažurira stanje svih trenutno odigranih utakmica i na web sajtu omogućuje praćenje utakmica koje su u toku, takozvani online prenos. Program za slanje statistike na internet je realizovan u programskom jeziku C#. Za enkripciju podataka zadužen je SHA (Secure Hash Algorithm)-256. Zaštita web servisa koja je primenjena ovde implementirana je na dva načina, upotrebom SSL (Secure Socket Layer) protokola za implementaciju sigurnosti na transportnom nivou, i upotrebom XML-Security standarda za implementaciju sigurnosti na nivou poruke.

Ključne reči: Web Servisi, SSL, WS-Security, Java, J2EE, XML-Signature

TRANSFER OF BASIC BASKETBALL STATISTICAL PARAMETERS VIA INTERNET

Summary: This paper describes two ways to protect data that is exchanged in B2B applications using Web services. The data is passed between two different database through a structured XML document. Described software environment is used to collect and record data from basketball games (the first male and female federal league of Serbia),

¹ Branko Markoski, University of Novi Sad, Vojvodina - Serbia, Technical Faculty "Mihajlo Pupin", Zrenjanin, e-mail: markonins@yahoo.com

² Zdravko Ivanković, University of Novi Sad, Vojvodina - Serbia, Technical Faculty "Mihajlo Pupin", Zrenjanin, e-mail: ivankovic.zdravko@gmail.com

³ Predrag Pecev, University of Novi Sad, Serbia, Faculty of Sciences, Dept. of Mathematics and Computer Sciences, e-mail: predrag.pecev@gmail.com

⁴ Zoran Milošević, University of Novi Sad, Vojvodina - Serbia, Faculty of Sport and Physical Education, Novi Sad, e-mail: zoranais@eunet.rs

⁵ Višnja Istrat, University of Novi Sad, Vojvodina - Serbia, Technical Faculty "Mihajlo Pupin", Zrenjanin, e-mail: visnja.istrat@gmail.com

which are, in the current regime, sent to a central web server where the status of all currently played games are updated, and via web site it is enabled to track games that are in progress, the so-called online transmission. Program to send statistics to the Internet is realized in C#. Data encryption is provided by SHA (Secure Hash Algorithm) -256. Web service security that was used here was implemented in two ways, using SSL (Secure Socket Layer) protocol to implement security at transport level, and use of XML Security standards for implementing security at the level of a message.

Key words: Web Services, SSL, WS-Security, Java, J2EE, XML-Signature.

1. UVOD

„Ja ne verujem u vođenje statistike. Jedina statistika koja je bitna je konačan rezultat.“ Ovo je bilo tačno nekada, uglavnom iz razloga što i njihovi protivnici takođe nisu vodili i koristili statistiku. Međutim, vremena su se zasigurno promenila. Konačan rezultat je i dalje najvažniji, ali i način na koji je taj rezultat postignut je danas od velike važnosti.

Razvoj informacionih tehnologija i njihove integracije u sve oblasti našeg društvenog i privrednog života nije zaobišao ni sport. Sve veći profesionalizam i konkurencija uslovljavaju klubove da sve sistematičnije pristupaju svim aktivnostima. Poseban napredak se primećuje u sistemu treninga i analizi protivničkih timova i igrača, tj. skautiranju. U prošlosti, košarkaška statistika je bila luksuz dostupan samo velikim profesionalnim klubovima [1]. Za prosečnog trenera, statistika je predstavljala pravu noćnu moru, zahtevajući veliku količinu vremena i truda, najpre u samom prikupljanju statističkih podataka, a zatim i u ručnom izračunavanju različitih zbirnih statističkih parametara. Za većinu trenera statistika jednostavno nije bila vredna tolikog truda. Međutim, računari su sve to promenili. Oni su skinuli veliki teret i odgovornost za vođenje statistike sa trenera, istovremeno im pružajući pregršt informacija o kojima su oni do pre samo petnaestak godina mogli da sanjaju. I, najbolje od svega, rasprostranjenost i relativno niska cena računara i softvera omogućuje dostupnost ovih informacija svima. Danas živimo u svetu informacija. Osnovna obeležja informacije, koja definišu njen kvalitet, a samim tim i vrednost, su : tačnost, potpunost, razumljivost i pravovremenost. Bolje je nemati informacije uopšte nego imati netačne, nepotpune, nerazumljive ili nepravovremene informacije [15].

Arhitektura aplikacije (čija implemen-tacija je razmatrana u radu) se sastoji iz više klijenata koji rade nad Interbase-ovom bazom podataka, na lokalnoj mašini. Klijentske aplikacije prikupljaju i evidentiraju podatke sa košarkaških utakmica u trenutnom režimu, i isto-vremeno putem web servisa šalju podatke prema centralnom web serveru na kojem je postavljena web aplikacija koja radi nad MySQL bazom podataka[3]. Slanje i ažuriranje podataka o utakmi-cama odvija se putem web servisa. Podaci o jednoj utakmici strukturirani su u okviru XML dokumenta, u koji se podaci prvo izvoze iz Interbase baze podataka. Potom se XML dokument šalje u okviru SOAP zahteva web servisu na web serveru. Web servis čita dokument i ažurira novo stanje o utakmici koja je u toku. Kako web servis omogućuje modifikacije nad bazom podataka spoljašnjim korisnicima, to je potrebna i zaštita u slučaju eventualnih zloupotreba. Validacija ispravnosti implementirane zaštite web servisa je izvršena kroz osnovne sigurnosne zahteve koji su dati kao [7]:

- **poverljivost** (eng. reliability) – sadržaj poruke koja se razmenjuje u komunikaciji je dostupan samo učesnicima

- ❑ **integritet** (integrity) – zaštita od izmene sadržaja poruke u toku prenos, kao i na na mestu gde se poruka skladišti
- ❑ **autentifikacija** (authentication) – učesnici u komunikaciji su sigurni da komuniciraju sa učesnikom za koga veruju da je taj za koga se predstavlja.
- ❑ **autorizacija tj. kontrola pristupa** (access control) – specifikacija prava pristupa delovima poruke učesnicima komunikacije
- ❑ **neporečivost** (nonrepudiation) – učesnik ne može poreći svoje učešće u komunikaciji nakon samog čina

2. PROTOKOLI, STANDARDI I SPECIFIKACIJE ZAŠTITE WEB SERVISA

SSL je specifikacija koju je prvobitno dao Netscape 1994 godine kao verziju 2.0, a potom 1996 godine i kao verziju 3.0 [3], koja istovremeno predstavlja i poslednju SSL specifikaciju. SSL je kasnije standardizovan 1999 godine od strane IETF kao TLS (Transport Layer Security) verzija 1.0 [5]. Poslednja verzija TLS standarda je 1.1 i pojavila se kao RFC dokument 2006 godine [6]. TLS je sigurnosni protokol transportnog nivoa (eng. transport-level security), i kao takav radi na nivou toka bajtova. Koristi se za implementaciju sigurne komunikacije u platformski-nezavisnim, RPC (Remote Procedure Call) zasnovanim infrastrukurama. Mana SSL-a je u tome što ne pruža neporečivost, kontrolu pristupa poruci u komunikaciji između učesnika i šifrovanje samo određenih delova poruke.

WS-Security (Web Services Security Specification) [3] je standard za zaštitu SOAP poruka, koje predstavljaju XML format poruka koje se razmenjuju sa web servisima. Zaštita podataka u WS-Security standardu se odnosi na zaštitu integriteta i poverljivosti poruke, autentifikaciju i mogućnost pridruživanja sigurnosnih tvrdnji (token) poruci, i kao takav pruža sigurnost na nivou poruka (message-level security). WS-Security je standardizovan od strane OASIS-a (Organization for the Advancement of Structured Information Standards) organizacije koja se bavi razvojem i usvajanjem informacionih standarda elektronskog poslovanja [1]. U primeru je korišćena implementacija verzije 1.0 WS-Security standarda iz 2004 godine.

WS-Security okuplja specifikacije za zaštitu poverljivosti i autentičnosti XML dokumenata, XML-Encryption i XML-Signature, i daje niz preporuka za upotrebu tvrdnji radi autentifikacije pošiljaoca i zaštite integriteta poruke. XML-Signature obezbeđuje integritet, autentičnost i neporecivost poslate poruke [3,4].

Kako u ovom konkretnom primeru aplikacije za prikaz rezultata košarkaške utakmice, poverljivost sadržaja poruke nije neophodan zahtev, to XML-Encryption standard nije korišćen u implementaciji.

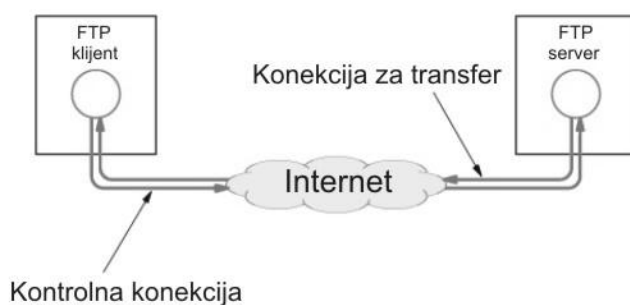
U poređenju sa SSL zaštitom, WS-Security je implementiran u višem aplikacionom sloju TCP/IP steka protokola, i garantuje end-to-end sigurnost poruci, dok SSL garantuje samo point-to-point sigurnost. Prvo se odnosi na mogućnost postojanja posrednika u komunikaciji između dva učesnika[6,8].

3. RAZMENA PODATAKA

Slanje košarkaške statistike se obavlja putem FTP (File Transfer Protocol) protokola. To je protokol za prenos podataka između dva računara koji koristi TCP/IP za mrežnu

komunikaciju. On se uspostavlja na zahtev klijentskog računara prema serverskom računaru, odnosno u našem slučaju program za slanje statistike šalje zahtev ka serveru na kojem dati podaci treba da se nalaze[9].

FTP sesija se sastoji iz sesije za transfer (DTP - Data Transfer Process) i kontrolne sesije (PI - Protocol Interpreter). Uvek se prva pokreće kontrolna sesija koja šalje zahtev za uspostavljanje veze. Kada kontaktirana mašina primi zahtev vrši se provera identiteta a nakon toga uspostavljanje dvosmerne komunikacije između datih mašina. Tek tada je moguće slanje podataka ka FTP serveru.



Slika 1. FTP komunikacija

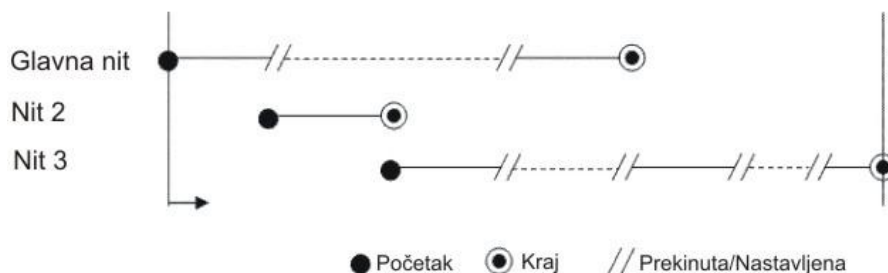
Kada FTP klijent uputi komandu ka FTP serveru, server vraća trocifreni broj koji predstavlja kod odgovora. Kodovi su određeni FTP standardom i koriste se radi brže i sigurnije razmene podataka. Na osnovu odgovora koji se dobija od servera znamo da li su podaci uspešno poslani i o tome se obaveštava korisnik preko poruke na korisničkom interfejsu.

Slanje htm fajla sa podacima o statistici se vrši na svakih 15 sekundi. Za slanje podataka odgovorna je posebna nit u aplikaciji. Na isteku tog intervala izvrši se tajmer koji kreira nit za slanje podataka[10].

Svaka aplikacija na Windows operativnim sistemima se tretira kao proces. Nit (thread) je "osnovna jedinica građe" procesa jer svaki proces mora imati najmanje jednu nit, ali po potrebi može sadržati i veše od jedne niti. Razlog za uvođenje više niti je potreba da se više stvari istovremeno izvršava u jednom procesu. Istovremeno izvršavanje u pravom smislu se dešava samo u računarima koji imaju više procesora (core2duo, core2quad, ...), pri čemu pojedinačni procesor izvršava određenu nit, dok drugi procesor izvršava neku drugu nit. Prilikom izvršavanja većeg broja niti dolazi do preključivanja procesora sa jedne niti na drugu, odnosno prvo se izvršava deo koda sa prve niti, zatim deo koda sa druge niti, pa ponovo deo koda sa prve niti itd. Na ovaj način simuliramo istovremeno izvršavanje više niti. Na slici broj 2 prikazano je istovremeno izvršavanje više niti.

Aplikacija za slanje statistike se sastoji iz dve niti. Prva nit je glavna nit programa koja pokreće aplikaciju i ostaje aktivna dokle god je i sama aplikacija aktivna. Druga nit služi za slanje podataka na server. Data nit se kreira na svakih 15 sekundi, pošalje podatke na server i nakon toga se automatski ubije. Aplikacija je razdvojena u dve niti da bi se omogućila

interakcija sa programom i u momentu kada on šalje podatke. U suprotnom program poslatu komandu, recimo za prestanak daljih slanja podataka, ne bi primio sve dok ne završi sa slanjem podataka. U slučaju dve niti on odmah registruje našu komandu i prestaje sa kreiranjem novih niti. Ukoliko je neka nit već kreirana ona će se izvršiti do kraji i poslati podatke.



Slika 2. Istovremeno izvršavanje više niti (multi threading)

Da bi se podaci slali na server neophodno je postojanje internet konekcije. U slučaju nestanka interneta, program nije u mogućnosti da pošalje podatke, a data pojava se tretira kao izuzetak. Izuzetak se hvata i obrađuje ali se izvršavanje programa ne prekida. Nit koja nije uspela da pošalje podatke se završava a brojač uspešno poslanih podataka se ne uvećava. Sledeća nit koja se kreira nakon 15 sekundi će ponovo pokušati da pošalje podatke. Ukoliko je u međuvremenu, internet konekcija obnovljena, data nit će poslati podatke na server i nakon toga se završiti. Kreiranje niti će se nastaviti sve dok iz korisničkog interfejsa ne zaustavimo aplikaciju. Na korisničkom interfejsu kao indikator slanja imamo brojač koji nam govori koliko su puta uspešno poslani podaci.

4. ZAKLJUČAK

Košarka je jedna od najpopularnijih sportskih grana kod nas, ali i ono što je najvažnije u savremenom sportu i jedan od najtrofejnijih sportova. Svakako da veliki broj klubova, mladih igrača i sportskih stručnjaka u Srbiji pokazuje da košarka ima značajno mesto u sportskoj industriji. Prikupljajući informacije o protivničkim igračima i njihovoj igri počinjemo da gradimo filozofiju igre, sistem i tehnologiju izviđanja protivnika. Gomilanjem informacija, njihovom analizom i sistematizacijom težimo ka modelu rada koji bi, pored prikupljanja informacija, bila uključena prezentacija informacija timu, uvežbavanje individualne i timske taktike u toku mikrociklusa između dve utakmice i kontrola uspešnosti i primene u toku same utakmice. Težnja za pobedama dovela je do saznanja da svaki detalj igre tima olakšava put do željenog trijumfa. Polako počinje da raste trka za informacijama o igri i igračima protivničkih timova da bi se sa što boljim poznavanjem protivnika bolje pripremili za utakmicu i time olakšali timu da nametne stil i tempo igre koji mi želimo da bi došli do željene pobede. Prednost upotrebe SSL-a za zaštitu web servisa je transparentost sa strane klijenta i jednostavnost konfiguracije aplikacionog servera. WS-Security standard nudi kompletnije rešenje za zaštitu podataka u XML formatu koji se razmenjuju na internetu, rad na nivou podelemenata poruke, mogućnost razdvajanja potpisivanja od šifrovanja poruke, i za razliku od SSL-a ispunjava sve sigurnosne zahteve.

5. LITERATURA

- [1] Slavko Trninić, *“Analiza i učenje košarkaške igre“*, 1996
- [2] FIBA *“FIBA RULES“*, Munich 2011.
- [3] Ivković D. *“Kako započeti utakmicu“*, Moska, 2006.
- [4] Markoski B., Ivetic D., Setrajčić J., Mirjanic D., Ivankovic Z. *“Košarkaški skauting“*, Infoteh Jahorina, Bih Vol. 8., 628-630, Mart 2009.
- [5] Jamie Angeli, *“Scouting America's Top Basketball Programs“*, Volume 2, 2004
- [6] Kumar P. , *“J2EE Security for Servlets, EJBs and Web Services: Applying Theory and Standards to Practice“*, Prentice Hall, 2003, 464 strana.
- [7] Chou W. , *“Inside SSL: the secure sockets layer protocol“*, IT Professional IEEE, Volume 4, Issue 4, July-August 2002, Page(s): 47-52
- [8] Rosenberg J., Remy D., *“Securing Web Services with WS-Security“*, Sams, 2004.
- [9] Dean Oliver, *“Basketball on paper – Rules and tools for performance analysis, Brassey's“*, Washington DC, 2004
- [10] Stalling W., *“Crypthography and Network Security Principles and Practices“*, Prentice Hall, 2005.
- [11] Jamie Angeli, *“Scouting America's Top Basketball Programs“*, Volume 1, 2003
- [12] Dierks T., Allen C., *“The TLS Protocol version 1.0 Internet RFC 2246 Proposed Standard“*, January 1999.
- [13] Dierks T., Rescorla E., *“The TLS Protocol version 1.1 Internet RFC 4346 Proposed Standard“*, April 2006.
- [14] Bhimani A., *“Securing the Commercial Internet“*, June 1996 Communications of the ACM, Volume 39 Issue 6 April 2006.
- [15] Ratgeber, L. *“Play from a game: (Head Coach)“*, Mizo Pecs 2010. 2007/2008. Mizo Pecs 2010 vs. Euroleasing Sopron