

ZAŠTITA WEB SERVISA**Gojko Grubor****Angelina Njeguš**

Univerzitet Singidunum

Danijelova 32, Beograd.

e-mail: ggrubor@singidunum.ac.rs

e-mail: anjegus@singidunum.ac.rs

Sažetak: Web servisi (WS) se baziraju na XML, SOAP i OSI standardu računarskih mreža. Organizacije koriste SOA za podršku aplikacija kritičnih za misiju. SOA ističe otkrivanje dinamičkih servisa, kompoziciju i interoperabilnost. Tehnologija WS se sve više koristi za implementaciju SOA, iako se SOA može implementirati korišćenjem drugih tehnologija. Da bi SOA postigla svoje ciljeve, aplikacije moraju biti pouzdane i bezbedne. Za zaštitu WS predložen je veliki broj standarda zaštite. Cilj ovog rada je pregled bezbednosnih izazova WS i raspoloživih standarda za njihovu zaštitu.

Ključne reči: web servisi, SOA, dimenzije zaštite, servisi zaštite, kontrole zaštite.

Abstract : The Web services are based on XML, SOAP and computer network OSI model. The SOA's are used by organizations for mission critical applications. A SOA emphasizes dynamic service discovery, composition, and interoperability. Web services technology are increasingly becoming the SOA implementation of choice, albeit a SOA could be implemented by another technology. To truly meet its goals, applications must be secure and reliable. A large number of security standards have been proposed for Web services. The main goal of this paper is to provide an overview of Web services associated security challenges, and the standards available for securing them.

Key words: web services, SOA, security dimensions, security services, security controls.

1. UVOD

Glavne funkcionalnosti WS-a su otkrivanje, prenos poruka, portali, uloge i koordinacija (orkestracija, koreografija). Za otkrivanje WS razvijen je standard UDDI¹, [6], koji omogućava međusobno dinamičko pretraživanje WS. Svaki WS kreira deljivi WSDL interfejs za dinamičko povezivanje sa novim servisima bez dodatnog programiranja, izmene konfiguracije i intervencije korisnika. Poruke WS-a se šalju u XML formatu. U većini WS-a postoje dva tipa SOAP poruka: zahtevi i odgovori. WS-i međusobno mogu komunicirati serijski, paralelno ili asinhrono, zavisno od aplikacije ili protokola koji ih podržavaju. Web portal obezbeđuje čitljiv interfejs za funkcionalnosti WS-a i pristup većem broju izvora podataka nego sam WS. Uloge podnosioca zahteva, provajdera odgovora i servisa i posrednika su sastavne komponente web baziranih SOA. Podnosilac zahteva inicira transakciju WS-a, provajder prihvata zahtev, obezbeđuje odgovor i uspostavlja standardne servise za zaštitu- autentifikaciju, autorizaciju, šifrovanje i neporecivost. WSDL i servis otkrivanja ne obezbeđuju standardno pregovaranje, ako neki zahtevi to traže. Ovi standardi su u toku razvoja. Posredni WS je onaj koji je pozvan u lancu transakcije. Primer posrednog WS-a je XML kapija (gateway). Iz perspektive podnosioca zahteva postoji samo jedan provajder servisa, ali ih može biti više. Koordinacija je orkestracija u SOA organizacije i koreografija između SOA više organizacija kada u WS-u učestvuje više uloga. Iako se

¹ Akronimi i skraćenice su date u poglavlju 4. Akronimi i skraćenice

standardi zaštite WS-a ubrzano razvijaju i poboljšavaju i dalje su nerešeni neki bezbednosni izazovi.

2. ZAŠTITA WEB SERVISA

2.1. Taksonomija pretnji WS-a

Upotrebljiva taksonomija pretnji za WS-e prikazana je u tabeli T. 1, [5].

T.1. Taksonomija pretnji za WS-e

	Pretnja	Opis
1.	Izmena poruke (IP)	napadač ubaci, ukloni ili modifikuje informaciju u poruci
2.	Gubitak poverljivosti (GP)	neovlašćeni korisnik otvori informacije u poruci
3.	Falsifikovanje poruke (FP)	napadač šalje lažnu poruku u ime validnog pošiljaoca
4.	Čovek u sredini (ČS)	napadač je između pošiljaoca i provajdera i menja poruke
5.	Lažno predstavljanje principala (LPP)	napadač šalje naizgled validne poruke sa stvarnim podacima legitimnog korisnika (principala)
6.	Lažno predstavljanje (LP)	napadač pravi naizgled validne poruke sa lažnim podacima
7.	Ponovljeno slanje delova poruke (PSDP)	napadač uključuje delove jedne ili više prethodno poslatih poruka u novu poruku
8.	Ponovljeno slanje poruke (PSP)	napadač ponovo šalje prethodno poslatu poruku
9.	Odbijanje izvršavanja servisa (DoS)	napadač troši resurse sistema koji ne izvršava validni zahtev
10.	Implementacija defektnog softvera	može dovesti do iskoristivih ranjivosti za udaljeni pristup

2.2. Taksonomija napada na web servise

Taksonomija napada na web servise prikazana je u tabeli T. 2, [3], [5].

T. 2. Taksonomija napada na web servise

Napadi prepoznavanja		
1.	Templejt kôda	informacije o razvoju web aplikacije mogu ukazati na potencijalne <i>bagove</i>
2.	Nasilan napad pretraživačem	otkriva neobjavljen WS ponavljanjem zahteva za WS pomoću URL obrazaca, npr., CGI (<i>Common Gateway Interface</i>) programom
3.	Transverzalni napad na direktorijum	napadač pristupa restriktivnim fajlovima unutar WS-a u cilju otkrivanja pasvorda servera ili izvršnih fajlova za skrivene komande
4.	Skeniranje WSDL	vešt napadač locira WS, uklonjen iz ranije generisanih WSDL i pristupa WS-u
5.	Napad otkrivanjem registara	ako su loše konfigurisani (npr. LDAP, X.500, UDDI, ebXML itd.), registri sadrže autentifikacione i druge informacije o WS-u
6.	Napad na kontrole zaštite	identifikacija, autentifikacija i autorizacija korisnika pre davanja prava pristupa, koje obezbeđuje UDDI standard
Napad za povećanje privilegija		
1.	Napad rečnikom	moгуć na sisteme sa slabom pasvord zaštitom
2.	Napad na format linije programskog kôda	ranjivost formata linije programskog kôda nastaje zbog greške programera; bag može omogućiti napadaču da preuzme kontrolu nad programom i hostom na kojem program radi
3.	Plavljenje bafera	ranjivost prepunjenog bafera u komponentama WS-a, omogućava kompromitovanje/preuzimanje kontrole nad WS i obaranje servisa (DoS napad).

2.3. Uobičajeni faktori rizika web servisa

Web servisi imaju većinu istih faktora rizika kao i ostali programi, ali tradicionalne tehnologije zaštite - *firewalls*, *IDS/IPS*, *SSL/TLS* nisu adekvatne, zato što *firewalls* obično propuštaju HTTP, a *SSL/TLS* ne štiti od posrednika koji izvršava napad „čovek u sredini“. Uobičajeni faktori rizika WS-a odnose se na pet *dimenzija zaštite WS-a*: *razmene poruka*, *resursa*, *pregovaranja*, *upravljanja poverenjem* i *funkcija kontrola zaštite*. Glavni faktori

rizika SOAP i osnovni bezbednosni problemi WS-a su, što SOAP ne obezbeđuje, [15]: *autentifikaciju, zaštitu integriteta i poverljivosti, detekciju ponovljenog slanja poruka, robusni mehanizam za autentifikaciju ulaza u registar, otpornost na DoS napade* itd.

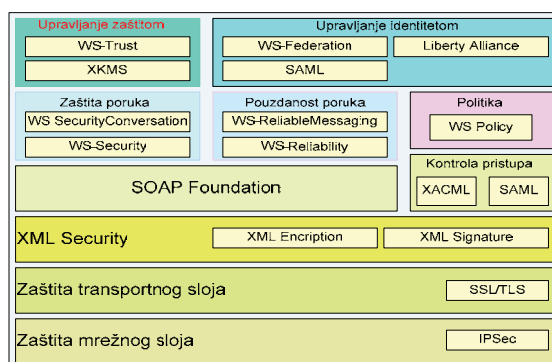
2.4. Standardi, servisi i tehnologije zaštite web servisa

Značajniji koncepti zaštite WS-a uključuju, [5], [1]: *identifikaciju i autentifikaciju, autorizaciju, integritet, neporecivost, poverljivost i privanost*. Od većine navedenih rizika mogu zaštititi WS-i i HTTP standardi (W3C). Pokrivanje pretnji servisima zaštite prikazano je u tabeli T. 3.

T. 3. Pokrivanje pretnji standardima zaštite

	IP	GP	FP	CS	LPP	LP	PSDP	PSP	DoS
XML šifrovanje (WS-security)		X		X	X	X	X		
XML digitalni potpis	X		X		X	X	X	X	
Token zaštite WS			X		X	X			
Adresiranje WS								X	
SSL/TLS	X	X	X*	X	X*	X*	X		
SSL/TLS sa sertifikatom klijenta	X	X	X	X	X	X	X		
HTTP autentifikacija			X		X	X			
*Pretnje se ublažavaju samo za poruke provajdera pošiljaocu zahteva, a ne obrnuto									

Očigledno je da nema kontrola zaštite koji sprečavaju DoS i DDoS napade, a detaljna specifikacija *standardnih kontrola zaštite SOA* data je u literaturi [5]. *PKI infrastruktura* podržava većinu WS-a, zato što se najveći deo zaštite WS-a zasniva na *šifrovanju i digitalnom potpisu XML* i/ili *SSL/TLS*, koji koriste X.509 digitalni sertifikat za skladištenje kriptografskih parametara, [4]. Osnovni bezbednosni izazovi koji nisu adekvatno rešeni u zaštiti WS-a su: *poricanje, poverenje, eksploatacija tajnih kanala, kompromitovani servisi, širenje malicioznih programa, DoS napadi i nekorektna implementacija servisa*. Glavno težište razvoja *metodologije za zaštitu WS-a* (perspektivna je *metodologija S-vektora*) usmereno je na PKI, protokole zaštite, sigurne programske jezike i zrele procese za proizvodnju softvera, [2], [3]. *Referentni model zaštite WS-a* u OSI modelu mreža (ali ne striktno hijerarhijski), prikazan je na slici Sl. 1. Servisi na OSI i XML bezbednosnim slojevima štite SOAP razmenu poruka u prenosu, sa mehanizmima zaštite *IPsec*, *SSL/TLS*, *XML Encryption* i *XML Signature* na različitim slojevima, [7], [8]. Iznad *XML security* sloja su samostalni standardi izgrađeni na SOAP, *WS-Security* i *WS-SecureConversation*, *XACML* (može definisati politiku pristupa za svaki sistem) i *SAML* (može definisati potvrdu pristupa u svakom okruženju, [5]).



Sl. 1. Referentni model zaštite web servisa

3. ZAKLJUČAK

Primarni cilj SOA je da napravi kolekciju softverskih servisa dostupnih preko standardnih protokola, čija se funkcionalnost može automatski otkriti i integrisati u aplikaciju. Standardi zaštite WS-a ne obezbeđuju razvoj robusnih i pouzdanih WS-a. Zahteva se sistem inženjerski pristup i slojeviti sistem zaštite WS-a. Za upravljanje identitetom koriste se PKI sertifikati unutar SOA. Bezbednosne zahteve dimenzija zaštite SOA može podržati veći broj standarda zaštite, ali ne i za kontrolisanu odgovornost (*accountability*) i od D/DoS napada.

4. AKRONIMI I SKRAĆENICE:

1. **DoS/DDoS** (*Dianil of Service/Distributed Dianil of Service*): odbijanja servisa/distriburani napad odbijanja izvršavanja servisa.
2. **ebXML** (*Electronic Business XML*): modularan set specifikacija za B2B transakcije sa XML.
3. **Federation**: kolekcija međusobno poverljivih domena
4. **HTTPS** (*HyperText Transfer Protocol over SSL/TLS*): HTTP prenošen preko SSL/TLS.
5. **IDS/IPS** (*Intrusion Detection Systems/ Intrusion Protection Systems*): detektori upada/zaštite od upada u sistem.
6. **Kerberos**: algoritam za verifikaciju identiteta principala na otvorenoj mreži (NT Win OS).
7. **LDAP** (*Lightweight Directory Access Protocol*): aplikativni protokol za zahteve i modifikaciju servisa PKI direktorijuma koji rade preko TCP/IP protokola.
8. **PKI** (*Public Key Infrastructure*): infrastrukturna komponenta zaštite sa javnim ključem.
9. **SAML** (*Security Assertions Markup Language*): okvir za autentifikaciju i autorizaciju razmene informacija u XML formatu (tzv., *assertions*).
10. **SOA** (*Service-Oriented Architecture*): kolekcija servisa, koji međusobno komuniciraju preko podataka ili dva i više servisa koji koordiniraju neke aktivnosti.
11. **SOAP**: protokol na XML za razmenu struktuiranih informacija u mrežnom okruženju.
12. **SSL/TLS** (*Secure Socket Layer/Transport Layer Security*): zaštitni protokoli između aplikativnog i transportnog sloja.
13. **UDDI** (*Universal Description, Discovery, and Integration*): zatvorni servis na XML za otkrivanje WS-a i provajdera WS-a.
14. **WSDL** (*Web Services Description Language*): XML format za opisivanje mrežnih servisa za prenos poruka; komplementaran je UDDI standardu.
15. **Web Service**: softverska komponenta/sistem za podršku interakcije inoperabilnih mašina ili aplikacija preko mreže.
16. **WS-Security** (*Web Services Security*): okvir za ugradnju mehanizam zaštite u SOAP poruke.
17. **XML Encryption**: proces za šifrovanje/dešifrovanje XML dokumenata/delova dokumenata.
18. **X.509 sertifikat**: standard digitalnog sertifikata u PKI sistemu.

LITERATURA

1. Bishop, M., (2003), *Computer Security: Art and Science*, Pearson Education.
2. Grubor G., (2007), *Razvoj i upravljanje programom zaštite zasnovanim na modelu sazrevanja procesa*, doktorska disertacija, Univerzitet Singidunum, Beograd.
3. Milosavljević M., Grubor G., (2006), *Osnovi bezbednosti i zaštite IS*, Univerzitet Singidunum.
4. <http://csrc.nist.gov/publications/nistpubs/>, NIST SP 800-32, (2003), *Introduction to Public Key Technology and the Federal PKI Infrastructure*.
5. Singhal A., et al., (2007), *Guide to Secure Web Services*, NIST SP 800-95, <http://csrc.nist.gov/publications/nistpubs/>.
6. <http://www.oasis-open.org/specs/index.php#uddiv3.0.2>, (2006), *UDDI v3.0.2*.
7. <http://www.oasis-open.org/specs/index.php#wssv1.1>, (2007), *WS-Security v1.1*.
<http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>, (2008), *XML Encryption Syntax*