Стандарти и технологии за защита използвани при Web услугите

М. Шопов, И. Станков, Н. Каканаков

Въведение

Web услугите използват технологии, за които се предполага, че ще променят и определят начина на комуникиране в световната мрежа през следващите години. Стандартизираният интерфейс на Web услугите, позволява работата на предлаганата услуга в разнородна среда, правейки я платформено независима. Стандартите за Web услуги дефинират само външния интерфейс на услугите, но не и как се реализира самата услуга вътрешно. Това дава възможност за лесно и бързо трансформиране на съществуващите бизнес решения и предлагането им като Web услуги. За да стане това реалност обаче е необходимо Web услугите да отговарят на високите изисквания за сигурност на бизнеса.

Сигурността не е включена първоначално в архитектура на Web услугите. С навлизането им изниква необходимостта от добавяне на разширения, които да дефинират правила за сигурност и надеждност при Web услугите.

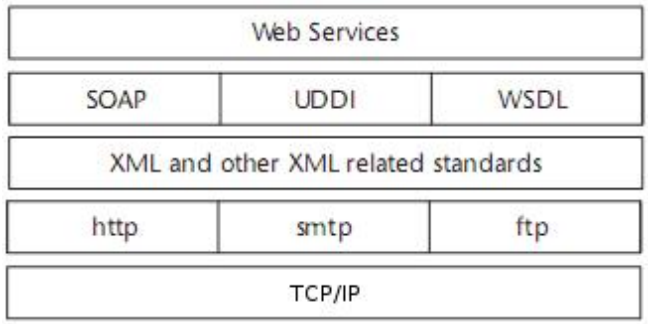
Архитектура на Web услугите

Web услугите предоставят възможност за достъп, както до бизнес логиката, така и до логиката на приложенията, използвайки стандартни протоколи като HTTP, SMTP, FTP. Поради повсеместното разпространение и използване на тези протоколи, както и кодирането на данните в XML формат, Web услугите се считат, че отговарят на всички изисквания за осъществяване пренос на данни през различни среди и платформи. Web услугите преодоляват различните среди за разработка на приложения, платформи върху които работят тези приложения, както и езиците на които са написани тези приложенията. Всички тези особености и характеристики на Web услугите скриват разпределената работа на споменатите технологии, за да предоставят една завършена система за нуждите както на бизнеса, така и на разпределената автоматизация [8], [10].

При разглеждане на сигурността при Web услугите, трябва да се насочим към архитектурата и протоколния стек или по-точно, да обърнем внимание на протоколите, които осъществяват комуникацията. Могат да бъдат откроени три базови такива:

- Simple Object Access Protocol (SOAP);
- Web Services Definition Language (WSDL);
- Universal Description, Discovery and Integration (UDDI).

Всички останали протоколи прибавят допълнителна функционалност и възможности към основните характеристики на ядрото протоколи.



Фиг. 1: Протоколен стек на Web услугите

Както се вижда от фиг. 1, протоколният стек е съвкупност от конвенционални мрежови протоколи, които осъществяват комуникацията между отделните Web услуги. В него могат да се обособят пет области [8], [10]:

- Транспортна услуга: грижи се за обмен на съобщения между отделните приложения и включва протоколи като HTTP, SMTP, FTP, BEEP (Blocks Extensible Exchange Protocol).
- Обмен на XML съобщения: тази услуга се грижи за кодирането на съобщенията в стандартен формат, така че те да бъдат разбрани от другата страна в комуникацията.
- Описание на услугата: описва се дадена услуга, като това включва семантиката на общуване. Използва се WSDL.
- Регистриране на услуга: публикува се услугата в даден общоизвестен регистър (Universal Description Discovery and Integration – UDDI).
- Откриване на услуга: позволява търсене в регистър с публикувани услуги (UDDI) по определени критерии.

Разгледаният по-горе протоколен стек на Web услугите е направен с цел да се подчертае механизма на сработване на този вид

технология за комуникация, както и да се очертаят насоките, в които трябва да се търси някакъв вид защитено предаване. Това е технология базирана на обмен на съобщения, поради което информацията може да се криптира преди да се предаде или да се въведе даден потребителски маниер за обмен на тази информация [8].

Общи изисквания към сигурността за Web приложенията

Съществуват няколко основни елемента на сигурността, които са фундаментални за постигане на пълна защита на комуникацията между двете крайни приложения в многослойните системи [7],[8],[10]:

- ***удостоверяване на автентичност*** – удостоверява се, че отсрещната страна е тази за която се представя. В резултат се отпускат множество документи, които описват атрибути като идентичност, роля, група, пропуски. При удостоверяването за автентичност може да се използва надеждна трета страна като посредник. Получените документи се включват по-късно в заглавната част на съобщенията.
- ***определяне правата на достъп*** – различните потребители/приложения могат да имат различно ниво на достъп. Тук се определят правата на достъп до определени ресурси, както и до определени операции и приложения.
- ***осигуряване на конфиденциалност и интегритет*** – посредством криптиращи алгоритми и протоколи за защита на данните и съобщенията от прочитане и модифициране. Криптирането осигурява нужната конфиденциалност на предаваните данни, които могат да бъдат разчетени само от притежателя на декриптиращия ключ. Цифровия подпис от друга страна осигурява цялостност на данните и гарантира, че не са били променяни по пътя си, без да ги защитава от директно прочитане.
- ***наличност*** – въпреки, че не е толкова очевидно изискване към сигурността колкото изброените по-горе, осигуряването на наличност на предлаганите услуги е критичен етап в изграждането на сигурни системи. Освен да предпазва наличните ресурси от несанкциониран достъп системата за сигурност трябва да гарантира достъпа до предлаганите услуги на оторизираните клиенти.

Традиционните техники за изграждане на сигурност като виртуални частни мрежи (VPN), Secure Socket Layer (SSL) и Transport Layer Security (TLS) са приложими само за ограничен набор от силно контролирани приложения, използващи Web услуги. Те не могат да се справят с динамичното създаване на канали, който Web услугите изискват. Опити да се приспособи някои от тези методи са сложни и недостатъчно универсални [1]. Необходимо е разработването на нови механизми за сигурност, които отчитат специфичните характеристики на Web услугите. В резултат се появяват много стандарти за XML и WS (Web услуги) сигурност.

Специфични изисквания към сигурността за Web услуги

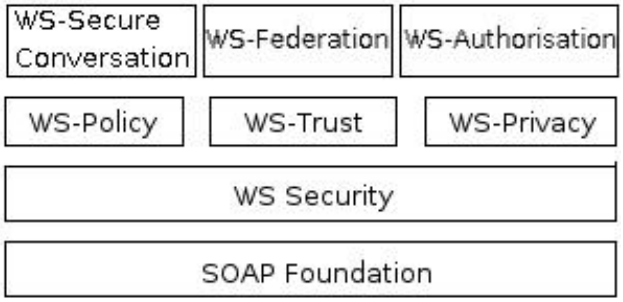
Web услугите са силно динамични и разпределени по характер. Въпреки, че използват същите транспортни механизми и протоколи както и Web базирания трафик те имат допълнителни изисквания за осигуряване на минимални нива на сигурност. Широко използваните и поддържани протоколи за защита на Web трафик – SSL и TLS не са приложими за комплексните и в големи обеми транзакции типични за Web услугите. Причината е необходимостта от декриптиране и последващо криптиране на данните на всеки от междинните сървъри.

Web услугите са проектирани да преминават през защитните стени като по този начин компрометират използването им като защита на приложния слой. Те се явяват интерфейс към приложения и по този начин откриват много повече функционалност към вътрешни и външни заплахи. Тяхната хетерогенност и платформена независимост ги прави уязвими към проблемите в сигурността на всички типове интерфейси използвани в една система използваща Web услуги. Мрежите използващи Web услуги най-често са равностойни (peer-based) с децентрализирано администриране, което ги прави трудни за единен и стандартизиран контрол и наблюдение [7].

В допълнение, засилената работа по защитата на Web услугите довежда до появата на голям брой стандарти и спецификации, което затруднява ясния поглед върху проблемите и решенията. Липсва и синхронизация между различните спецификации които често се препокриват [7]. Голяма част от тези спецификации са все още в процес на разработка.

Архитектура на сигурността при Web услугите

През 2002 година Microsoft и IBM съвместно създават модел за прилагане на политики за сигурност при Web услугите. Тяхната стратегия включва набор от спецификации, способни да осигурят надеждна среда за предаване на данните, повишена работоспособност при между-платформена комуникация, която се осъществява през Интернет.



Фиг. 2: Спецификация на сигурността при Web услугите

Спецификацията на сигурността, както е показано на фиг. 2. се основава на WS-Security (Web Services Secutity). Тази методология е разгледана подробно в следващата част от статията. На фиг.2 са показани и два допълнителни слоя, които надграждат WS-Security и предоставят специфична функционалност с предварително дефиниран набор от правила. В тези два слоя се включват набор от спецификации за отделни елементи на сигурността [3], [10]:

- *WS-Policy* е разширение към WS-Security спецификацията, в което се описват политиките на деклариране и използване на дадена функционалност;
- *WS-Trust* спецификацията дефинира рамките за настройка и поддържане на взаимоотношенията на сигурност между страните, участващи в комуникционния процес;
- *WS-Privacy* позволява да се добавят организационни модели към дадени Web услуги, за да се позволи имплементирането на конкретни политики.
- *WS-Authorization* предоставя процедури и определя изискванията при конфигурирането на комуникацията от *край-до-край* – определянето на политиките от предходния слой, както и маркерите на сигурността;
- *WS-SecureConversation* конкретизира предоставянето на определена функционалност за определянето на идентичността на участниците в комуникацията;
- *WS-Federation* позволява да се определят задачите за създаването на сигурна среда за взаимодействие, които ще използват Web услуги.

Методи за защита на Web услуги

Съществуват три основни механизми за осигуряване на защита [5]:

- на ниво транспорт;
- на ниво съобщение;
- на ниво роли.

Съществуват три механизма за защита на ниво транспортен слой: SSL/TLS, първично определяне на идентичността, клиентско определяне на идентичността (two way SSL). Защитата на данните се осигурява само докато се транспортират от една входна точка до друга.

На ниво съобщение защитата се осигурява като самите съобщения се криптират. Тук е възможно различни части от съобщението да бъдат криптирани с различни ключове за различните получатели на съобщението. Могат да бъдат използвани цифрови подписи за осигуряване на интегритет на съобщението. Три от механизмите които могат да се използват тук са: XML криптиране, XML подписване и използване на маркери.

При наличие на потребители изграждането на сигурност включва определяне на идентичността и оторизация. Определянето на идентичността е свързано с идентификация чрез потребителско име и парола или сертификат. Оторизацията е свързана с определяне на правата които отделните потребители имат на различните системи. Най-често използваният механизъм за осигуряване на оторизация е посредством използване на роли.

Стандарти и спецификации за сигурност при Web услуги

Съществуващите технологии и стандарти като LDAP, PKI, SSL/TLS, IPSec и VPN все още изпълняват важна роля при подсигуряването на Web услугите поради широкото им приложение и доказаните предимства. За да се отговори обаче на специфичните нужди на Web услугите се появяват редица допълнителни стандарти.

Основните стандарти за Web услуги – XML, SOAP, WSDL и UDDI представляват основните блокове върху които се изграждат и имплементират Web услугите. Въпреки, че са широко приети от индустрията, тези стандарти

не включват никакви механизма за защита. Нещо повече, самите те притежават проблеми със сигурността [2], [7]. Въпроси, които трябва да намерят отговор са: На надеждно място ли е разположен UDDI регистъра? Как да се провери дали информацията не е била подправяна? Може ли да се разчита на организацията предоставяща услугата?

По-долу са изброени редица стандарти и спецификации разработвани от различни организации и компании [6], [9].

SAML (Security Assertion Markup Language) е XML-базирана рамкова спецификация за обмяна на информация за удостоверяване на автентичност и определяне на права на достъп. Може да се използва между приложения използващи различна инфраструктура или платформа (Windows vs. Java). Друго възможно приложение е за изграждане на система за еднократно вписване (Single Sign-On – SSO) между различни системи и платформи. Самия протокол не осигурява конфиденциалност и интегритет. За тази цел се използват XML Enc и XML DSig или протоколи от по-ниските нива.

XKMS (Xml Key Managment Specification) – е стандарт, който дефинира интерфейс към Web услуги за управление на инфраструктура с публичен ключ. Състои се от два протокола XML Key Information Service Specification (X-KISS) за откриване и извличане на публични ключове и XML Key Registration Service Specification (X-KRSS) за регистриране, отстраняване и възстановяване на ключове на сървъра за публични ключове.

XML Encryption – стандарт за криптиране на XML документи, който позволява криптирането както на целия документ така и само на части от него. Криптираното съдържание заедно с допълнителна служебна информация се представя също във XML формат за да може допълнително да се обработва от XML инструменти. За разлика от SSL и VPN, където криптирането е от типа сървър-до-сървър, респективно мрежа-до-мрежа, този стандарт позволява криптиране от тип край-до-край.

XML DSig (XML Digital Signatures) – стандарт за гарантиране на интегритет и удостоверяване на автора на документа. Разликата му с другите стандарти за цифрови подписи е в това, че позволява подписване само на част от XML документа.

XACML (eXtensible Access Control Markup Langualge) – представлява XML базирана спецификация за задаване на правила за контрол на достъпа. Спецификацията дефинира методи за кодиране на правила, свързването на правила с политики и задаване на алгоритми за обединяването им в случай на използване на различни политики и правила между двете страни. Тя дефинира също и политики, които да бъдат включени в изпращаното съобщение, за да опишат правата на достъп и да докажат самоличността на изпращащата страна.

WS-Security (Web Services Security) може да се разглежда като шаблон за добавяне на маркери за сигурност в заглавната част на SOAP съобщението и как тези маркери да бъдат защитени чрез някои от спецификациите изброени по-горе. WS-Security е първото от серия правила, предоставящи сигурност при системи базирани на Web услуги. Този стандарт се разработва съвместно от IBM, Microsoft, и VeriSign. Понастоящем този стандарт е известен като WSS. Той включва и подробности за употребата на SAML, Kerberos и сертификата X.509. Поради начина на имплементиране на стандарта, сигурността се гарантира в заглавната част на SOAP съобщението, т.е. на приложно ниво. Оттук може да се направи и извода, че като цяло сигурността при този метод е от типа *край-до-край*.

Модерни средства за защита на Web услуги

Наред с множеството стандарти за мрежова сигурност и специфични за Web услугите, се появяват и нови разработки, базирани на семантиката на комуникацията и контекста на съобщенията. Тези разработки все още не са наложени като стандарти, но се налагат като практики от бизнеса. Пример за такава разработка е проекта за *Semantic Firewall*. Той се представя като услуга, работеща заедно с традиционните защитни стени, като отчита контекста на входящите и изходящи съобщения, както и семантиката на последователността им като разговор. Предимството на тази разработка е, че се интегрира с модерните насоки в разработката на Web услуги, като описание на бизнес процесите, потока на работа на услугите, взаимодействието и онтологията им [11].

Друго модерно средство за осигуряване на защита при Web услугите представлява XML защитната стена. Целта на защитната стена от този тип е да извършва филтриране на XML съобщения, анализирайки съдържанието им и прилагайки предварително зададени правила за контрол на достъпа. Даден клиент или приложение може да извърши достъп до

дадена услуга само ако съществува правило, което позволява това и съдържанието на съобщението се счита за безопасно за приложението. Този тип защита има следните предимства [4]:

- правилата за контрол на достъпа се съхраняват централизирано и следователно са лесни за администриране;
- събиране на журнална информация за входящи и изходящи съобщения;
- може да бъдат комбинирани със система за откриване на нарушители;
- добавянето на ново приложение е лесно, просто се добавят нови правила; добавянето на нов потребител изисква добавяне на правило в съответния набор.

Възможни недостатъци на подхода с XML защитна стена са: зависимост на ефективността на приложенията от натоварването на защитната стена; разчита се на сигурността на операционната система, на която се изпълнява защитната стена.

Изводи и бъдещо развитие

В статията са разгледани проблемите при реализиране на сигурни Web услуги заедно с наличните стандарти и модерни решения, които са в процес на разработка и изследване. Същността на този тип приложения съществено се различава от тази на стандартните Web приложения поради навлизането на семантиката на документите като параметър в администрирането и търсенето им. Предимствата на Web услугите се явяват като слаби места на сигурността им. Текст базираните документи (XML), включващи описание на типовете данни и интерфейсите за достъп (WSDL) увеличават уязвимостта. Имплементацията на SOAP върху популярни мрежови протоколи ги прави неуловими за стандартните защитни стени. Появява се необходимост от защити, които са интегрирани с архитектурата на Web услугите и се интересуват от семантиката и онтологията на обменяните съобщения и документи.

Благодарности

Изследванията в настоящата работа са финансирани от Фонда за научни изследвания към МОН – проект „МУ-МИ-1602/2006”, договор „Д01-777/26.10.06”.

Литература

[1] Alchaal, L., V. Roca, M. Habert, "Managing and Securing Web Services with VPNs," p.236, IEEE International Conference on Web Services (ICWS'04), 2004.

[2] Barbir, A., “Web Services Security: An Enabler of Semantic Web Services,” Proc. Business Agents and the Semantic Web, held in conjunction with the 16th Canadian Conf. Artificial Intelligence (AInbsp'03), 2003.

[3] Chou, D. and K. Yurov, “Security Development in Web Service Environment,” Computer Science and Interfaces, vol.27, pp. 233-240, 2005.

[4] Fernandez, E., "Two patterns for web services security", Proc. International Symposium on Web Services and Applications (ISWS'04), Las Vegas, NV, 2004.

[5] Ganesan, H., “Web Services: Interoperability and Security,” Arizona State University, Students Report, 2004.

[6] Geer, D., "Taking Steps to Secure Web Services," *Computer*, vol.36, no. 10, pp. 14-16, Oct., 2003.

[7] Gutierrez, C., E. Fernandez-Medina, M. Piattini, „Web Services Security: Is the problem solved?,” INFORMATION SYSTEMS SECURITY, vol.13; part 3, pp. 22-31, 2004, ISSN 1065-898X.

[8] Hratmann, B., J. Flinn, B. Konstantin,S. Kawamoto, “Mastering Web Services Security,” Wiley Technology, Indianopolis, 2003, ISBN: 0471267163.

[9] Naedele M., “Standards for XML and Web Services Security,” *Computer,* vol. 36, no. 4, pp.96-98, Apr., 2003.

[10]O'Neil, M., “Web Services Security,” McGraw-Hill/Osborne, 2003, ISBN: 0072224711.

[11]Ronald Ashri, T. Payne, D. Marvin, M. Surridge, S. Taylor, “Towards a Semantic Web Security Infrastructure,”Proc. of Semantic Web Services, California, 2004.

За контакти:

Инж. **Митко Шопов**
e-mail: mshopov@tu-plovdiv.bg

Инж. **Иван Станков**
e-mail: istankov@tu-plovdiv.bg

Инж. **Николай Каканаков**
e-mail: kakanak@tu-plovdiv.bg

Лаборатория по Компютърни мрежи и Разпределени системи.
Технически Университет София, Филиал Пловдив