کارگاه‌های آموزشی مرکز اطلاعات علمی

آموزش مهارت های کاربردی در تدوین و چاپ مقاله

اصول تنظیم قراردادها

مقاله نویسی علوم انسانی

دومین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردهای ایران
دانشگاه کاشان، ۲۳-۲۱ مهر ۱۳۹۴ (۱۵-۱۳ اکتبر ۲۰۱۵)، ص:۶۲-۵۹

سخنرانی

ارائه یک لایه رمزنگاری بروی مستند توصیف وب سرویس

آرزو میرطالبی
دانشکده برق و کامپیوتر، دانشگاه کاشان، mirtalebi@grad.kashanu.ac.ir

سید مرتضی بابامیر
دانشکده برق و کامپیوتر، دانشگاه کاشان، babamir@kashanu.ac.ir

چکیده

با افزایش روز افزون استفاده از معماری سرویس گرا در جهان امروز، وب‌سرویس‌ها به عنوان یک منبع با ارزش مدام در معرض حمله مهاجمین قرار دارند. تحقیقات انجام شده در این زمینه بصورت مدون در استانداردWS-Security آمده است. این استاندارد بروی امنیت پیام‌ها متمرکز است. این مقاله در ابتدا به توضیح چالش امنیتی موجود در مورد فایل WSDL می‌پردازد، سپس با استفاده از استانداردهای امنیتXML ، راهکاری برای تامین امنیت این فایل ارائه می‌دهد. روش ارائه شده به دلیل ایجاد محدودیت و کاهش سرعت دسترسی بهWSDL به عنوان یک روش عمومی پیشنهاد نمی‌شود و تنها برای وب سرویس‌هایی مناسب است که WSDL آنها حکم یک منبع با ارزش، حاوی اطلاعات مورد نیاز مهاجمین، جهت حمله به وب سرویس است.

واژه های کلیدی: امنیت وب سرویس، رمزنگاری XML ، امضایXML .

۱ مقدمه

استانداردهایXMLSignature و XMLEncryption در سال ۲۰۰۲ توسط W۳C برای امن کردن مستندات XML ارائه شدند. این دو استاندارد سعی داشتند با استفاده از رمزکردن مستندXML ، آن را از دسترسی مهاجمین مصون کرده و امنیتش را تا حد ممکن ایجاد کنند. در سال ۲۰۰۷ تلاش برای استفاده از این استانداردها در جهت امن سازی وب سرویس آغاز گردید و حاصل این تلاش‌ها در قالب

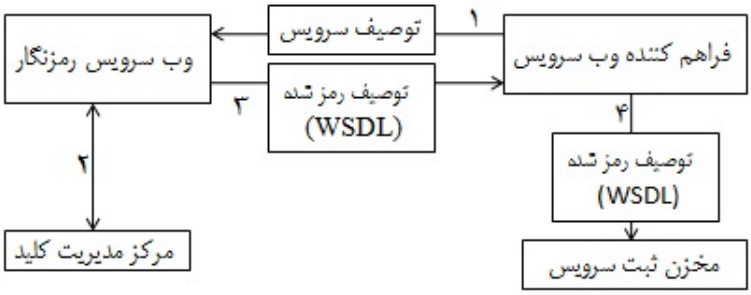
استاندارد WS-Security [1] به صورت مدون ارائه شد [۱]. این استاندارد تنها بروی امنیت پیام تمرکز کرده است و برای ایجاد امنیت آن از رمزنگاری و امضای XML استفاده می‌کند که وظیفه ایجاد یکپارچگی و محرمانگی را بر عهده دارند [۲]. یکی از نقاط ضعف وب‌سرویس که تا به حال اقدام خاصی در جهت امنیت آن صورت نگرفته، WSDL است. WSDL مستندی است که کلیه اطلاعات مورد نیاز جهت فراخوانی وب‌سرویس را در اختیار کاربران قرار می‌دهد و به فایل «توصیف وب‌سرویس» مشهور است[۳]. در برخی از وب‌سرویس‌ها این مستند می‌تواند منبع اطلاعاتی کاملی برای مهاجم‌ها باشد و مهاجم می‌تواند با پویش این مستند به اطلاعات لازم برای حمله به وب‌سرویس دست یابد. این مقاله به ارائه روشی برای امن کردن WSDL با استفاده از استانداردهای موجود در امنیتXML، پرداخته است. پیش از این نیز یک راهکار ابتدایی در رابطه با همین مسئله، توسط مولف در [۴] ارائه شده است.

۲ رویکرد پیشنهادی

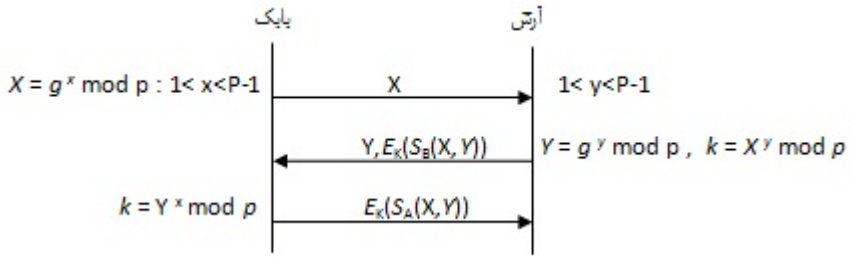
برای ایجاد این دیوار امنیتی بروی فایل WSDL [2] باید برخی برچسب‌هایXML موجود در آن را با استفاده از الگوریتم‌های رمزنگاری ارائه شده در XMLEncryption رمزکنیم، سپس به جای مستند اصلی، مستند رمز شده را در دسترس عموم قرار دهیم. به منظور ایمن کردن WSDL ، این مستند باید پیش از ثبت وب سرویس در UDDI [3] رمز شود. UDDI استانداردی برای ثبت و یافتن وب سرویس‌ها است و کلیه وب سرویس‌ها موظفند اطلاعات خود را در UDDI ثبت کنند. متقاضی وب‌سرویس نیز جهت یافتن اطلاعات مربوط به وب‌سرویس موردنظر خود به این مخزن مراجعه می‌کند[۵]. برای این کار فراهم کننده وب سرویس[4] ابتدا توصیف خود را به سرویس رمزنگار[5] می‌فرستد. وظیفه این سرویس تولید کلید برای رمز نگاری، ثبت کلید در مرکز مدیریت کلید[6] و در نهایت تولید توصیف رمز شده است. با رمز شدن فایل WSDL ، سطح امنیتی مورد نظر روی آن ایجاد شده است. در این مرحله درخواست ثبت این مستند به UDDI فرستاده می شود. زمانی که کاربر نیاز به فراخوانی وب سرویس داشته باشد، به UDDI مراجعه می‌کند تا آدرس WSDL آن را بدست آورد. با مراجعه به WSDL ، اگر با یک مستند رمز شده مواجه شود قادر نخواهد بود به اطلاعات درون آن دست یابد مگر اینکه آن را رمزگشایی کند. این مراحل در شکل ۱ نشان داده شده است. کاربر می‌تواند کلید مورد نیاز برای رمزگشایی را از مرکز مدیریت کلید بگیرد. اما این مرکز تنها در صورتی کلید را در اختیار کاربر قرار می‌دهد که اصالت وی اثبات شده باشد. نحوه احراز هویت کاربر وابسته به زیرساختی است که در معماری سرویس‌گرا استفاده شده است. ساده‌ترین راه برای احراز هویت استفاده از LDAP [7]. می‌باشد. در این روش اطلاعات کلیه کاربران مجاز در یک پایگاه داده که نزد سرویس LDAP است ، ثبت می‌شود. هنگامی که کاربری از سرویس مدیریت کلید درخواست کلیدی برای رمز گشایی می‌کند، سرویس مدیریت کلید یک درخواست بررسی اصالت به سرویس LDAP ارسال می‌کند و در صورت دریافت جواب مثبت کلید را در اختیار وی قرار می‌دهد. مراحلی که نیازمند ارتباط مستقیم دوطرفه بصورت ایمن هستند، از کلید اشتراکی برای ایجاد این کانال امن بین طرفین استفاده می‌کنند و دو طرف پیام‌هایشان را با کلید اشتراکی رمز می‌کنند. برای تبادل کلید مشترک بین طرفین از روش STS استفاده می‌شود و مطابق شکل ۲ عمل می‌کنند. احتمال فاش شدن کلید مشترک وجود دارد که در ساده

---

[1] Web Service Security
[2] Web Service Definition Language
[3] Universal Discovery and Description Integration
[4] Web Service Provider
[5] Encriptor Web Service
[6] XKMS
[7] Lightweight Directory Access Protocol



شکل ۱: مراحل اعمال لایه امنیتی در رویکرد پیشنهادی



شکل ۲: مراحل ایجاد کلید مشترک

ترین روش حمله، مهاجم می‌تواند با استفاده از امتحان کردن همه گزینه‌ها، به آن دست یابد. اما زمانی که باید صرف این کار شود بسیار بیشتر از طول عمر کانال‌های امن است. زیرا تبادل اطلاعات با استفاده از یک کانال ایمن تنها در مواردی استفاده شده است که ارتباطات کوتاه است. به منظور نشان دادن وضعیت امنیت WSDL به مراجعین، باید یک برچسب جدید به ابتدای مستند WSDL اضافه شود. هر یک از کاربران با چک کردن این برچسب متوجه می‌شوند که آیا این مستند نیاز به رمز گشایی دارد یا خیر . در ضمن هنگام رمز ،WDSL نباید این برچسب را رمز کرد تا کاربر به محض مراجعه به WSDL و بدون نیاز به رمز گشایی بتواند به وضعیت امنیتی آن پی ببرد.

۳ نتایج اصلی

با اعمال این سطح امنیتی، سرعت دسترسی کاربران کاهش می‌یابد، زیرا کاربر با مراجعه به WSDL ، به یک متن رمز شده برمی‌خورد و برای دسترسی به اطلاعات مورد نیاز خود، مجبور است آن را رمزگشایی کند. به همین خاطر این لایه امنیتی یک راهکار عمومی برای همه وب‌سرویس ها نیست، بلکه در جایی مناسب است که اطلاعات موجود در مستند توصیف وب‌سرویس به عنوان یک منبع ارزشمند اطلاعاتی برای مهاجمین تلقی شود. به عنوان مثال زمانی که یک وب سرویس بخواهد لیست سرویس‌های ارائه شده‌اش را به صورت محرمانه حفظ کند. برای ارزیابی مدل پیشنهادی، سیستمی با تعداد دلخواه سرویس‌دهنده و سرویس‌گیرنده در نظر گرفته شده است، سپس سناریوهای محتملی که ممکن است مدل پیشنهادی با آن روبرو شوند بررسی شده‌اند. شرح مختصر برخی از سناریوها در جدول زیر آمده است.

جدول ۱: ارزیابی برخی پارامترهای امنیتی

سناریو	نوع تقاضا	نتیجه تقاضا	دلیل	روش تشخیص توسط رویکرد پیشنهادی
سناریو۱	رمزگذاری WSDL توسط هویت نامشخص	ناموفق	عدم احراز هویت تامین‌کننده	توسط XKMS و لغو درخواست
سناریو۲	رمزگذاری WSDL توسط هویت معتبر	موفق	مهیا بودن شرایط لازم جهت رمزگذاری	طی مراحل تعریف شده در مدل پیشنهادی (شکل۱)
سناریو۳	رمزگشاییWSDL توسط هویت نامشخص	ناموفق	عدم احراز هویت مشتری	توسط XKMS و لغو درخواست
سناریو۴	رمزگشایی WSDL توسط هویت معتبر اما بدون اخذ حق دسترسی	ناموفق	عدم احراز صلاحیت مشتری	توسط سرویس LDAP و لغو درخواست
سناریو۵	رمزگشایی WSDL توسط هویت معتبر	موفق	مهیا بودن کلیه شرایط به برای رمزگشایی	طی مراحل تعریف شده در مدل پیشنهادی (شکل۱)

مراجع

[1] T. Erl and T. Boubez, “SOA Security,” ed: Pearson Education, 2011.

[2] M. P. Cristescu, E. A. Stoica, and L. V. Ciovica, “Web Services Specific Security Standards,” Procedia Economics and Finance, vol. 16, 2014, pp. 597-602.

[3] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, “A survey on trust and reputation models for Web services: Single, composite, and communities,” Decision Support Systems, vol. 74,2015, pp. 121-134.

[4] A. Mirtalebi and M. R. KhayyamBashi, “Enhancing Security of Web Services against WSDL Threats,” IEEE 2nd International Conference on Emergency Management and Management Sciences, pp. 920-923, 2011.

[5] M. I. P. Salas and E. Martins, “Security Testing Methodology for Vulnerabilities Detection of XSS in Web Services and WS-Security,” Electronic Notes in Theoretical Computer Science, vol. 302, 2014, pp. 133-154.

کارگاه‌های آموزشی مرکز اطلاعات علمی

آموزش مهارت های کاربردی در تدوین و چاپ مقاله

اصول تنظیم قراردادها

مقاله نویسی علوم انسانی