فصلنامه علمی-ترویجی پدافند غیرعامل

سال سوم، شماره ۳، پاییز ۱۳۹۱، (پیاپی ۱۱): صص ۹-۱۸

چالش‌های امنیتی مدیریت اعتماد در وب‌سرویس‌ها

علی کریمی[۱]، محمود صالح اصفهانی[۲]، محمدرضا حسنی آهنگر[۳]

تاریخ دریافت: ۹۱/۰۸/۱۴
تاریخ پذیرش: ۹۱/۱۰/۰۴

چکیده

یکی از پیشرفت‌هایی که در سال‌های اخیر در شبکه‌های توزیع‌شده و محیط وب رخ داده است، معرفی وب‌سرویس‌ها به‌عنوان مولفه‌های نرم‌افزاری مستقل می‌باشد. وب‌سرویس‌ها توانایی تبلیغ شدن، قرار گرفتن در یک مکان و مورد استفاده قرار گرفتن در محیط وب بر اساس استانداردهایی از قبیل WSDL، UDDI و SOAP را دارند. هدف نهایی فناوری وب‌سرویس[۴] این است که استفاده از قابلیت‌های وب‌سرویس‌ها را به‌عنوان اجزای مستقل در سازمان‌های سرویس‌گرا امکان پذیر سازد. بنابراین وب‌سرویس‌گرا[۵] یک نمونه و الگوی بسیار جذاب برای تعاملات آینده در یک گستره وسیع از اقتصاد الکترونیکی تا علم الکترونیکی و حتی دولت الکترونیکی فراهم می‌سازد. در این میان با توجه به جنبه‌های مختلف امنیتی وب‌سرویس‌ها، مقوله مدیریت اعتماد در تعاملات کاربران با محیط‌های سرویس‌گرا از جایگاه ویژه‌ای برخوردار است. در سیستم‌های مبتنی بر اعتماد و اعتبارسنجی، از همتایان معتبر برای تبادل اطلاعات و انجام تراکنش استفاده می‌شود. این امر، به کاهش قابل توجه ارسال‌های مخرب در سیستم منجر می‌شود. توجه ویژه به جنبه‌های امنیتی مدیریت اعتماد و چالش‌های آن می‌تواند ما را در بهبود و گسترش تعاملات و توسعه کسب‌وکار الکترونیکی در شبکه‌های توزیع‌شده یاری رساند. در این مقاله ضمن معرفی کلی وب‌سرویس‌ها، به تعریف مبانی اعتماد و امنیت در این حوزه و چالش‌های فراروی آن خواهیم پرداخت.

کلیدواژه‌ها: مدیریت اعتماد، اعتبارسنجی، محیط‌های سرویس‌گرا، وب‌سرویس، چالش‌های امنیتی

۱- مربی و دانشجوی دکترای مهندسی نرم‌افزار- دانشگاه جامع امام حسین(ع) akarimy@ihu.ac.ir- نویسنده مسئول

۲- استادیار و عضو هیئت علمی دانشکده و پژوهشکده فناوری اطلاعات و ارتباطات- دانشگاه جامع امام حسین(ع) msaleh@ihu.ac.ir

۳- استادیار و عضو هیئت علمی دانشکده و پژوهشکده فناوری اطلاعات و ارتباطات- دانشگاه جامع امام حسین(ع) mahangar@ihu.ac.ir

4- Web Service Technology
5- Service-oriented Web

۱- مقدمه

ظهور فناوری‌های نو و پیشرفت وب، منجر به تولید سیستم‌های مستقل، خودمختار[1] و بسیار غیرمتمرکز شده است که می‌توان آن را شبکهٔ خدمات (service Web) غیرمتمرکز نامید؛ به‌گونه‌ای که در آن طیف وسیعی از برنامه‌ها در قالب «سرویس‌ها» در دسترس خواهند بود [۱]. وب به آرامی در حال تبدیل شدن به رسانه ممتاز برای فعالیت‌های انبوه کاربران می‌شود. محیط سرویس‌گرا به‌عنوان یک محیط باز، همیارانه، پویا و توزیع‌شده شناخته می‌شود که قادر است به‌موقع به نیازهای مشتری و پویایی کسب و کار پاسخ دهد [۲]. موجودیت‌های این محیط برای انجام فعالیت‌ها و تراکنش‌های مختلف، انتشار سرویس‌ها، و در خواست و ارائه سرویس، به سایر موجودیت‌ها نیاز دارند تا با یکدیگر ارتباط برقرار نمایند. با این حال، چنین تعاملاتی همیشه خالی از مخاطرات یعنی رفتار فریبکارانه نیست. هر دوی ارائه‌دهندگان سرویس و استفاده‌کنندگان آن با این خطر مواجه هستند.

امروزه کمتر کسی است که از مزایای محیط‌های برخط[2] و خدمات وب‌سرویس‌ها بهره‌مند نشده باشد و اکثر افراد به‌طور مستقیم یا غیر مستقیم با وب‌سرویس‌ها در ارتباط هستند. علاوه بر این، با رشد روزافزون دنیای مجازی، سازمان‌ها و شرکت‌ها نیز از امکانات و خدمات آنها به‌طور گسترده استفاده می‌کنند. این در حالی است که بیشتر افراد و حتی سازمان‌ها آموزش‌های لازم برای رویارویی با مخاطرات و چالش‌های این حوزه را ندیده‌اند. بنابراین، آیا می‌توان به این محیط‌ها اطمینان حاصل کرد و از مزایای بیشمار آن بهره‌مند شد؟ در اینجا، جایگاه و ضرورت یک زیرساخت پویایِ اعتماد که با ویژگی‌ها و نوسانات وب سازگار باشد، روشن می‌شود. سیستم‌های مدیریت اعتماد و روش‌های اعتبارسنجی می‌توانند برای احراز قابلیتِ اعتماد[3] وب‌سرویس‌ها و مقابله با چالش‌های امنیتی محیط پویا و توزیع‌شده وب، مناسب باشند.

۲- مفاهیم مبنایی اعتماد

با گسترش دامنه اینترنت و نیز توسعه روزافزون کسب‌وکار الکترونیکی در سطح جهانی، مفهوم اعتماد و مسائل مربوط به آن در چند سال اخیر به‌طور گسترده محور مطالعات اکثر سازمان‌ها قرار گرفته است. امروزه ارزش و اهمیت اعتماد در حوزه‌های مختلف به‌خوبی آشکار گردیده است؛ چرا که برقراری ارتباطات امن و تحقق تعاملات همیارانه میان افراد، نیازمند وجود اعتماد است. در عصری که روابط بین افراد و گروه‌ها هر روز ناپایدار و به سرعت در حال تغییر است، اعتماد و مدیریت آن که عمدتاً مبتنی بر استنتاج و تفاسیر در مورد انگیزه‌ها، شخصیت و صداقت افراد است، موضوع محوری محیط‌های سرویس‌گرا شده و حیات آنها را تضمین می‌نماید.

مهم‌ترین چالش محیط‌های وب‌سرویس‌گرا، اطمینان از تعاملات مثبت و تراکنش‌های رضایت‌بخش است. افراد معمولاً از برخورد با غریبه‌ها که قبلاً آنها را نمی‌شناختند عقب نشینی می‌کنند. به همین دلیل، افراد، تعاملات و تراکنش‌های خود را به حداقل رسانده و تمایل دارند در ناحیه آسایش خود باقی بمانند. برای حل این مشکل، همتایان باید قادر باشند به منظور اجتناب از همتایان غیر قابل اعتماد و کاهش مخاطرات، در باره اعتماد استدلال کنند. مدیریت اعتماد[4] [۳] مکانیزمی است که اجازه می‌دهد، اعتماد متقابل[5] بین همتایان برقرار شود؛ اعتمادی که همکاری همتایان را امکان‌پذیر نموده و در درازمدت، افزایش مشارکت آنان را به ارمغان می‌آورد.

سیستم‌های اعتبارسنجی، بر اساس جمع‌آوری اطلاعات در مورد تعاملات گذشته همتایان و محاسبه میزان ارزش اعتبارسنجی آنها پایه‌گذاری می‌شوند. مقادیر اعتبارسنجی، اساس و مبنای شناسایی همتایان قابل اعتماد می‌باشد [۴].

اعتماد، جزء مفاهیمی است که در علوم مختلف از جمله روانشناسی و جامعه‌شناسی توسط صاحب‌نظران مورد بررسی قرار گرفته است و بنابر شرایط حاکم بر هر کدام از این حوزه‌ها، تعاریف متفاوتی از آن ارائه شده است. در اکثر تعاریف ارائه شده از اعتماد، سه متغیر: اعتمادکننده، اعتمادشونده و زمینه[6] به چشم می‌خورد.

ویژگی اعتمادکننده: از دیدگاه فرد اعتمادکننده، اعتماد، انتظاری است مبنی بر اینکه طرف مقابل از خود صداقت، صراحت، شایستگی، وفاداری و ثبات نشان دهد و فرصت‌طلبانه رفتار نکند.

ویژگی زمینه: هر اطلاعاتی که می‌تواند برای مشخص کردن وضعیت یک موجودیت مورد استفاده قرار گیرد، ویژگی زمینه (محیط) نامیده می‌شود. اعتماد می‌تواند چند بعدی و وابسته به متن (زمینه) باشد.

ویژگی اعتمادشونده: اعتمادشونده باید دارای پنج بُعد اعتماد باشد تا بتواند انتظارات اعتمادکننده را به‌خوبی برآورده سازد. همان‌طور که بیان شد این پنج بعد عبارتند از: صداقت، شایستگی، ثبات، وفاداری و صراحت.

۳- اعتماد و اعتبارسنجی[7]

۳-۱- تعریف اعتماد

تاریخچه اعتماد به قدمت وجود انسان در روی کره زمین برمی‌گردد. مفهوم اعتماد، نقش مهمی در بقای انسان دارد. ما درکارهای روزمره تجربه به‌دست می‌آوریم و بر اساس اعتماد به یکدیگر تکیه می‌کنیم. با این حال، ارائه تعریف دقیق و روشن از اعتماد، امری دشوار است.

1- Autonomous
2- Online Environment
3- Trustworthyness
4- Trust Management
5- Mutual Trust
6- Context
7- Reputation and Trust

مطابق فرهنگ لغات آکسفورد [۵]، اعتماد، عبارت است از «یک اعتقاد راسخ به قابلیت اطمینان، صداقت، توانایی یا قدرت کسی یا چیزی».

در سال ۲۰۰۰ گراندسیون و اسلومان[1] [۶] اعتماد را به‌عنوان «اعتقاد راسخ به صلاحیت و شایستگی یک نهاد در انجام یک عمل به‌طور مستقل، امن و قابل اطمینان در درون یک زمینه مشخص تعریف کرده‌اند».

در سال ۲۰۰۶ چانگ و همکاران[2] [۷]، اعتماد را به‌عنوان «اعتقادی که عامل اعتمادکننده به تمایلات و توانایی عامل اعتمادشونده برای تحویل یک خدمت توافق‌شده در یک زمینه خاص و در یک بازه زمانی مشخص تعریف کرده‌اند».

بر اساس تجربه‌ای که در دنیای فیزیکی کسب کرده‌ایم، اطلاعات ضروری را استخراج می‌کنیم که می‌توانند در ایجاد اعتماد در دنیای مجازی، با هدف افزایش قابلیت اطمینان کاربران و کاهش مخاطرات به ما کمک کنند.

مارش[3] [۹] یکی از اولین پژوهشگرانی است که به ارائه یک مدل رسمیِ (فرمال) اعتماد اقدام کرده است که می‌تواند در علوم کامپیوتر مورد استفاده قرار گیرد. این مدل بر ویژگی‌های اجتماعی اعتماد که از جامعه‌شناسی نشأت گرفته است مبتنی است.

۳-۲- تعریف اعتبارسنجی

همانطور که قبلاً اشاره شد، اعتبارسنجی به‌طور گسترده در حوزه‌های مختلف از جمله روانشناسی، جامعه‌شناسی، تجارت و اقتصاد مورد استفاده قرار می‌گیرد. بر اساس تعریفی که آکسفورد ارائه کرده، اعتبارسنجی عبارت است از «عقاید یا باورهایی که عموماً در مورد کسی یا چیزی بیان شده است». عبد الرحمان و همکارانش[4] [۱۰] اعتبارسنجی را به‌عنوان «یک انتظار و توقع در مورد رفتار یک عامل بر اساس اطلاعات مربوط به رفتار گذشته او» تعریف کرده‌اند. در محیط‌های سرویس‌گرا، چانگ و همکارانش اعتماد را به‌عنوان «تجمیع توصیه‌نامه‌هایی از جانب همه توصیه‌نامه‌های عوامل شخص ثالث و نظرات دست اول، دوم و سوم آنها و همچنین قابلیتِ اعتماد عامل توصیه‌کننده در ارائه توصیه‌های درست به عامل اعتمادکننده در باره کیفیت عامل اعتمادشونده» تعریف کرده‌اند.

۳-۳- ویژگی‌های اعتماد

اعتماد، مقوله شخصی و ذهنی[5] بوده و مبتنی بر عوامل مختلف از جمله درون زاد[6] و برون زاد[7] است. اعتماد را می‌توان به شکل عینی (قابل مشاهده) از طریق ردیابی مشارکت همتایان در سیستم اندازه‌گیری کرد. اعتماد، یک مقوله فازی است؛ زیرا مبهم و نادقیق می‌باشد. اعتماد، پویا است زیرا ثابت نیست و این تغییر با گذشت زمان صورت می‌گیرد. اعتماد هم‌چنین پیچیده است، زیرا روش‌های مختلفی برای تعیین اعتماد وجود دارد [۴].

رابطه اعتماد معمولاً نامتقارن است. تراکنش میان همتای اعتمادکننده و همتای اعتمادشونده به یک ارزش (مقدار) اعتماد منجر می‌شود که توسط همتای اعتمادکننده به همتای معتَمد تخصیص می‌یابد. این مقدار استحکام، رابطه اعتماد را نشان می‌دهد.

رابطه اعتماد می‌تواند انتقال‌پذیر (متعدی[8]) باشد. اگر علی به حسن اعتماد دارد و حسن به رضا اعتماد دارد، علی هم می‌خواهد با رضا تعامل داشته باشد. علی از حسن درخواست می‌کند، حسن رضا را به علی ارجاع می‌دهد. علی یک سنجش از اعتماد به رضا، براساس اعتماد حسن به رضا و اعتماد خودش به حسن استخراج می‌کند.

۴- مفاهیم وب‌سرویس

بر اساس سند معماری وب سرویس‌ها که توسط کنسرسیوم جهانی وب[9] در سال ۲۰۰۴ منتشر شد، وب سرویس چنین تعریف شده است؛ وب سرویس عبارت است از: یک سیستم نرم‌افزاری که توسط یک URI تعریف می‌شود و از فناوری XML برای ارتباط با سایر نرم‌افزارها استفاده می‌کند. توصیفات وب سرویس‌ها توسط سایر سیستم‌های نرم‌افزاری قابل کشف است و امکان تعامل با آنها بر مبنای پیام‌های XML که قابل حمل با پروتکل‌های اینترنت (HTTP) می‌باشد، وجود دارد. مدل ساده وب سرویس شامل سه نهاد (موجودیت) زیراست [۱،۳]:

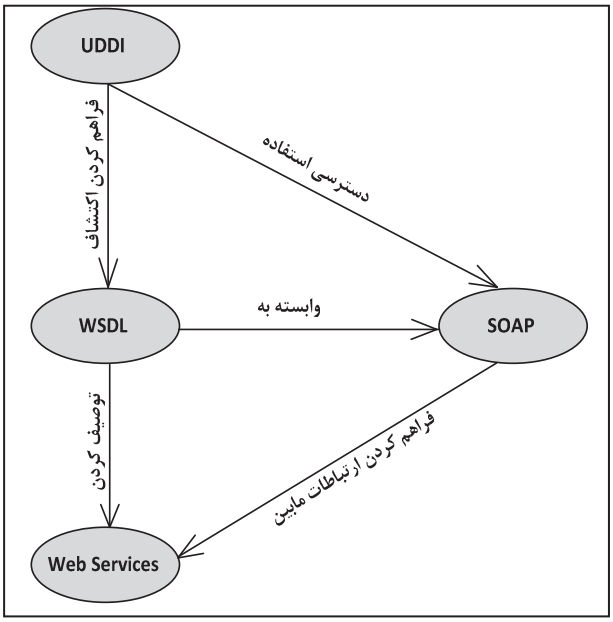
۱- فهرست (دفتر ثبت) سرویس[10]

۲- ارائه دهندهٔ سرویس[11]

۳- مشتری سرویس[12]

ارائه‌دهنده سرویس: نهادی است که سرویس مورد نظر را ایجاد و برای مشتریان دسترس‌پذیر می‌سازد. ارائه‌دهندهٔ سرویس ممکن است یک نهاد تجاری، دولتی و یا یک نهاد آکادمیک باشد و ممکن است یک سرویس و یا بیش از یک سرویس را ارائه دهد. ارائه دهندگان سرویس دارای شناسه‌های شناخته شده‌ای هستند. ارائه دهندهٔ سرویس مالک سرویس است و توصیفی از وب سرویس در قالب استاندارد (XML) ارائه کرده و آن را در فهرست سرویس مرکزی[13] منتشر می‌کند.

1- Grandison and Sloman
2- Chang et al.
3- Marsh
4- Abdul Rahman et al.
5- Subjective
6- Endogenous
7- Exogenous
8- Transitive
9- W۳C
10- Service Registry
11- Service Providers
12- Service consumer
13- Central service registry



شکل ۱- نقش اجزای مختلف در فناوری وب‌سرویس‌ها

فهرست سرویس: فهرست سرویس، یک فهرست قابل جستجو برای توصیفات سرویس است و مکانی است که ارائه دهندهٔ سرویس، توصیفات خود را در آن منتشر می‌سازد. این فهرست شامل اطلاعاتی در مورد ارائه دهندهٔ سرویس از قبیل آدرس، شماره تماس و نیز جزئیات فنی در مورد سرویس ارائه شده می‌باشد. فهرست سرویس شامل دو جزء است، یک پایگاه داده مربوط به توضیحات سرویس‌ها و یک موتور جستجو که به درخواست‌های مشتریان و ارائه دهندگان پاسخ می‌دهد. فهرست سرویس ممکن است عمومی یا خصوصی باشد. هر ارائه دهنده می‌تواند سرویس‌های خود را با منتشر کردن آن در یک فهرست عمومی تبلیغ کند. فهرست سرویس خصوصی توسط یک سری از ارائه دهندگان خاص و شناخته شده مورد استفاده قرار می‌گیرد.

مشتری سرویس: اطلاعات سرویس را از فهرست سرویس استخراج کرده و از توصیف آن برای تعامل با وب سرویس‌ها استفاده می‌کند. روش تعامل در شکل (۱) با کلمات کلیدی «**انتشار**»، «**اتصال**» و «**یافتن**» به تصویر کشیده شده است. به منظور دستیابی به ارتباط بین برنامه‌های کاربردی که بر روی سکوهای مختلف اجرا می‌شوند و با زبان‌های برنامه‌نویسی متفاوت نوشته شده‌اند، برای هر یک از عملیات فوق‌الذکر استانداردهای خاصی مور نیاز است.

۵- ابعاد امنیت در وب‌سرویس‌ها

ابعاد امنیت در وب‌سرویس‌ها را می‌توان در پنج بعد اصلی زیر مورد بررسی قرار داد [۳]:

- پیام رسانی امن (Secure Messaging)
- حفاظت از منابع (Resource Protection)
- امنیت در مذاکرات و قراردادها (Negotiation and Contracts)
- روابط اعتماد (Trust Relationships)

نیازمندی‌های نرم‌افزار امن (Requirements for secure software) ابعاد مذکور، اصول اصلی امنیت در وب‌سرویس‌ها را تشکیل می‌دهند و هر بعد به تنهایی جزئی ضروری و لازم در توسعه وب‌سرویس‌ها و تکمیل‌کننده لایه‌های مختلف امنیتی در آنها به حساب می‌آید.

۵-۱- پیام‌رسانی امن

وب‌سرویس‌ها برای تعاملات خود از شاهراه اینترنت بهره می‌گیرند و از پروتکل SOAP و سایر پروتکل‌های انتقال (اغلب HTTP) برای ایجاد ارتباط استفاده می‌کنند. با توجه به اینکه طراحی پروتکل SOAP از ابتدا با دیدگاه امنیتی انجام نشده است، لذا مستعد حملات مختلف از طرف خرابکاران اینترنتی می‌باشد. بنابراین برای پوشش ضعف‌های امنیتی این پروتکل ارتباطی در وب‌سرویس‌ها، راهکارهای مختلفی ارائه شده است که از مهم‌ترین آنها می‌توان به موارد زیر اشاره کرد:

- HTTP از طریق SSL / TLS: با توجه به اینکه پیام‌های SOAP از طریق پروتکل HTTP منتقل می‌شوند، لذا به‌کارگیری پروتکل SSL/TLS برای امن‌سازی ارتباطات می‌تواند یکی از راهکارهای امنیتی تلقی گردد.
- XML Encryption و XML Signature: این دو استاندارد برای امضاء و رمزنگاری فایل‌های XML توسط کنسرسیوم جهانی وب ارائه شده است. نظر به اینکه تمام پیام‌های SOAP با فرمت XML نوشته می‌شوند، لذا توسعه‌دهندگان وب‌سرویس‌ها با بهره‌گیری از استانداردهای فوق می‌توانند عملیات امضای دیجیتال یا رمزنگاری پیام‌های SOAP را انجام دهند.
- WS - Security: این استاندارد نیز در راستای ارائه مکانیزم‌هایی برای ایجاد امنیت لازم در پیام‌های SOAP از طریق XML Encryption و XML Signature تعریف شده است.

۵-۲- حفاظت از منابع

به‌طور کلی وقتی منابع به‌صورت عمومی در دسترس هستند، مهم‌ترین مسئله، اطمینان از تامین امنیت آنهاست. برای حفاظت و کنترل دسترسی به منابع، وب‌سرویس‌ها نیاز دارند کاربران خود را شناسایی نمایند. متدهای شناسایی مختلفی در این راستا معرفی شده‌اند که مهم‌ترین آنها عبارت‌اند از:

- متدهای شناسایی از طریق لایه انتقال
- توکن‌های امنیتی
- سرآمد (Header) شناسایی پیام SOAP

۵-۳- امنیت در مذاکرات و قراردادها

برای ارائه تسهیلات ویژه در تراکنش‌های کسب‌وکار، وب‌سرویس‌ها باید قادر باشند ایجاد، اجرا و تداوم خود را از طریق قراردادهای بین سازمانی تداوم بخشند. به‌عنوان مثال، یک وب سایت خرید برخط، از طریق قرارداد خود با بانکی که خدمات وب‌سرویس ارائه می‌دهد، به مشتریانی که از طریق وب‌سرویس بانک تأییدشده و اجازه دسترسی به منابع دارند، اجازه خرید از فروشگاه خود را می‌دهد. یعنی قرارداد منعقده بین دو بنگاه این اطمینان را به‌وجود می‌آورد که تمام وب‌سرویس‌ها، بین دو بنگاه طبق انتظار عمل کرده و تمام اطلاعات بین بنگاه‌ها به‌صورت امن رد و بدل خواهد شد.

۵-۴- روابط اعتماد در وب‌سرویس‌ها

هدف از مدیریت اعتماد در جوامع برخط، ایجاد اعتماد بین همتایان با استدلال قوی و با قابلیت اطمینان بالا است که با جمع‌آوری و تجزیه و تحلیل اطلاعات کافی مبتنی بر اعتماد و تصمیم‌گیری همراه است. استانداردهای وب‌سرویس‌ها ذاتاً انعطاف‌پذیرند و امکان توسعه مدل‌های معماری مختلف برای تکامل آنها وجود دارد. مهم‌ترین مدل‌های اعتماد در حوزه وب‌سرویس‌ها عبارتند از [۳]: مدل اعتماد واسطه‌ای[1]، مدل اعتماد جفت[2]، مدل اعتماد یکپارچه[3] و مدل دفاع محیطی[4]. وقتی این مدل‌ها از واژه *اعتماد* استفاده می‌کنند، آنها صرفاً به توانایی اعتماد به هویت سرویس محدود می‌شوند. توانایی شناسایی هویت یک وب‌سرویس به این معنی نیست که سرویس خود ذاتاً قابل اعتماد است. همیشه این احتمال وجود دارد که یک وب‌سرویس در یک حالت نادرست وارد شده یا مورد مصالحه قرار گیرد. بر اساس تعاریفی که از اعتماد ارائه شده است، احراز هویت یک وب‌سرویس ممکن است برای تشخیص قابل اعتماد بدون آن کافی نباشد. وقتی روابط اعتماد به محدوده چند سازمان گسترش می‌یابد، نیازمندی‌های هر یک از وب‌سرویس‌ها متفاوت خواهد بود. به این دلیل، صرف نظر از اینکه ارائه‌دهنده سرویس از لحاظ هویتی قابل اعتماد است یا خیر، درخواست‌کننده نباید فرض کند که اطلاعات غلط یا محتوای بدخواهانه در پاسخ به درخواست او ارسال نخواهد شد. به‌طور مشابه، به جهت اینکه ارائه‌دهندگان سرویس (مانند یک سرور) درخواست‌های درخواست‌کنندگان مختلف را پذیرا هستند، آنها نیز نباید فرض کنند که داده‌های غلط یا محتوای بدخواهانه به‌جای درخواست‌های معتبر ارسال نخواهد شد. با این وجود، شناسایی و احراز هویت وب‌سرویس‌ها یک مرحله اساسی در برقراری اعتماد محسوب می‌شود. هر مدل اعتماد دارای مزایا و معایبی است و پشتیبانی از اعتماد را در محیط‌های گسترده متنوعی امکان‌پذیر می‌سازد.

۵-۴-۱- مدل اعتماد واسطه‌ای

در این مدل، بین سرویس‌دهنده و سرویس گیرنده، عنصر قابلِ اعتماد سوم قرار دارد و به‌عنوان میانجی برای ارائه خدمات مختلف امنیتی عمل می‌کند. در این مدل، ارتباطات بین وب‌سرویس‌ها به راحتی تسهیل می‌شود، چرا که هر وب‌سرویس به‌جای شناسایی هویت تمام وب‌سرویس‌ها، تنها نیاز دارد هویت عنصر قابل اعتماد سوم را شناسایی کند.

۵-۴-۲- مدل اعتماد جفت

این مدل که ساده‌ترین مدل اعتماد است، دارای کمترین قابلیت توسعه‌پذیری است. در این روش، هر وب‌سرویس از طریق تنظیمات امنیتی سایر وب‌سرویس‌ها که با آنها ارتباط دارد، اعتماد را شکل داده و در نتیجه، کلیه تراکنش‌ها با اطمینان کامل انجام می‌شوند. در صورت اضافه شدن وب‌سرویس جدید به سیستم، تمام اطلاعات جدید باید بر روی تمام وب‌سرویس‌های موجود اضافه گردد که این معضل در مورد سیستم‌های بزرگ به‌خوبی مشهود بوده و مقیاس‌پذیری سیستم را دچار مشکل می‌کند.

۵-۴-۳- مدل اعتماد یکپارچه

در این مدل به وب‌سرویس‌های سازمان‌های مختلف اجازه داده می‌شود به‌طور یکپارچه بر اساس مکانیزم‌های مختلف اتحاد با یکدیگر تعامل کنند. در واقع این روش، تلفیقی از دو روش قبلی است. هر سازمان که بخواهد با سازمان دیگر متحد شود باید روش‌ها و پروتکل‌های پیچیده کسب‌وکار را اجرا کند، اما نتیجه نهایی امکان می‌دهد وب‌سرویس‌های هر سازمان با تعداد کمی از وب‌سرویس‌ها یا با آنهایی که تغییری در پیکربندی اولیه آنها رخ نداده است تعامل کنند.

۵-۴-۴- مدل دفاع محیطی

در این مدل، دستگاه‌ها تحت عنوان دروازه XML بین سرویس‌دهنده و سرویس‌گیرنده قرار می‌گیرند. در واقع می‌توان گفت دروازه XML از طریق اجرای عملکردهای امنیتی مرتبط، نقش یک پراکسی را برای وب‌سرویس‌ها ایفا می‌کند. اگرچه این راه‌کار به‌عنوان ابزاری مفید برای استراتژی‌های امنیتی یک سازمان مطرح است؛ اما نقش یک نوشدارو را ایفا نمی‌کند. اگر حمله‌کننده بتواند از دروازه XML عبور کند، تمام وب‌سرویس‌های داخلی نسبت به حمله آسیب‌پذیر خواهند بود. وب‌سرویس‌های داخلی باید به‌طور امن طراحی، توسعه و پیکربندی شوند.

1- Brokered Trust Model
2- Pairwise Trust Model
3- Federated Trust Model
4- Perimeter Defense Model

۵-۴-۵- نیازمندی‌های نرم‌افزارهای امن

تمام نرم‌افزارها، از جمله وب‌سرویس‌ها، نیاز دارند الزامات مربوط به عملکرد، هزینه، قابلیت استفاده مجدد و امنیت را برآورده سازند. مثال‌هایی از الزامات احتمالی برای نرم‌افزارهای امن عبارت‌اند از؛ قابل پیش‌بینی بودن، صحت عملکرد و قابلیت دسترسی.

۶- انواع حملات در سیستم‌های مدیریت اعتماد

در این قسمت، رایج‌ترین تهدیدات امنیتی به‌کاررفته در حوزه مدیریت اعتماد و اعتبارسنجی در محیط‌های توزیع‌شده، معرفی و توضیح داده می‌شود. علاوه بر این، رویکردی به‌منظور مقابله و حل این تهدیدات پیشنهاد خواهد شد.

توجه به این نکته مهم است که اگرچه همه این تهدیدات را می‌توان در برخی از مدل‌های اعتماد و اعتبارسنجی عملی کرد، اما همه آنها در هر مدلی عملی نیست، زیرا برخی تهدیدات خاص، یک نوع از مدل اعتماد و اعتبارسنجی است.

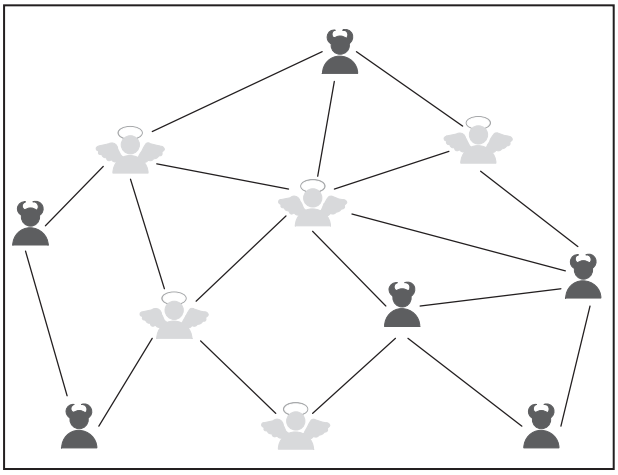
۶-۱- حمله یک عامل بدخواه منفرد[1]

حمله یک عامل بدخواه و دارای انگیزه خصومت‌آمیز، یکی از رایج‌ترین حملات روی اعتماد و اعتبارسنجی وب‌سرویس‌ها می‌باشد. رفتار یک عامل بدخواه خطرناک است، زیرا همیشه منجر به ارائه خدمات نامطلوب وب‌سرویس‌ها می‌گردد. همچنین این عامل می‌تواند باعث خدشه دار شدن اعتبار و شهرت شماری از عامل‌ها در وب‌سرویس‌هایی با چندین عامل گردد. این عامل معمولا با سایر عوامل در این زمینه همکاری ندارد و خود به صورت کاملاً انفرادی و اختصاصی عمل می‌کند.

از جمله راه‌های پیشگیری از این‌گونه رفتارهای بدخواهانه، کاهش سطح اعتماد به همتایانی است که همیشه دارای خدمات نامطلوب و رتبه‌بندی نامناسب در میان وب‌سرویس‌ها هستند که ممکن است یک عامل بدخواه باشند [۷].

۶-۲- حملات playbook

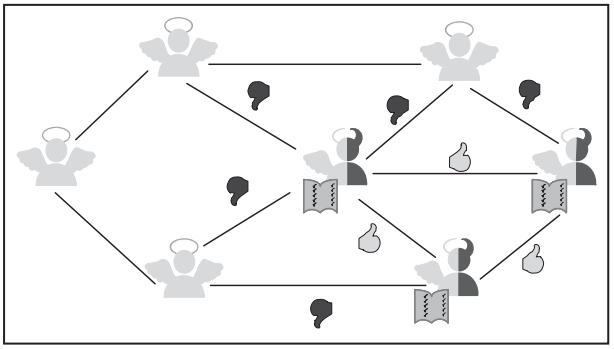
در این حمله، یک عامل یا گروهی از عامل‌ها برای به‌دست آوردن اعتبار بالا و جایگاه مناسب در میان سایر کاربران، در یک دوره زمانی معین به ارائه خدمات مطلوب و عملکرد مناسب می‌پردازند. بر پایه شهرت بالای کسب شده، به مرور زمان عامل می‌تواند بر خلاف رفتار قبلی خود عمل کند و به ارائه خدمات نامطلوب و با کیفیت پایین بپردازد. به عبارت دیگر، عامل مورد نظر با استفاده از یک کتابچه (*book*) که شامل تمام حملات (play) ممکن است، متناظر با زمان و شرایط خاص خود، حمله‌ای متناسب با آن را انجام می‌دهد. از جمله نکات مهم در این رابطه این است که انتخاب نوع حمله و زمان اجرای آن می‌تواند تاثیر زیادی در اثربخشی آن داشته باشد. با این حال، این تغییر رفتار از سوی برخی از وب‌سرویس‌ها لزوماً غیر اخلاقی محسوب نمی‌شود.



شکل ۲- حمله یک عامل بدخواه منفرد [۷]

علاوه بر این، به دلیل پویا بودن ماهیت اعتبارسنجی، این تغییر رفتار عامل همیشه غیر اخلاقی شمرده نمی‌شود. همه عوامل در محیط وب بر عملکرد یکدیگر نظارت کرده و برازندگی و شایستگی را افزایش می‌دهند.

از جمله راه‌کارهای مقابله با این نوع حملات، شناخت به‌روز از سرویس‌دهنده و آگاهی کامل کاربران در مورد مدت اعتبار و جزئیات سرویس مورد نظر خود است که باید از طرف سرویس‌دهنده در مورد آن اطلاعات کافی را به‌دست آورند [۱۲و۱۱].



شکل ۳- حملات Playbook

۶-۳- رتبه‌بندی‌های ناعادلانه[2]

این حمله شامل ارائه رتبه‌بندی‌هایی است که رأی و نظر واقعی ارزیاب را منعکس نمی‌کند. این رفتار در اکثر جوامع، غیراخلاقی

1- An Individual Malicious Agent

2- Unfair Ratings

تلقی می‌شود و از این‌رو نشان‌دهنده یک حمله می‌باشد. با این حال، تشخیص اینکه این حمله چه زمانی رخ می‌دهد بسیار دشوار است؛ زیرا عوامل موجود در یک جامعه، دسترسی مستقیم به نظرات واقعی یکدیگر را ندارند. آنها فقط آنچه را که عوامل دیگر بیان می‌کنند برای انتخاب، مشاهده می‌کنند. راهبردی که اغلب برای تشخیص رتبه‌بندی‌های ناعادلانه احتمالی پیشنهاد می‌شود، مقایسه رتبه‌بندی‌های ارائه‌شده توسط عوامل مختلف دربارهٔ یک وب‌سرویس و استفاده از عوامل مورد اعتماد قبلی به‌عنوان یک محک می‌باشد. با این حال، این روش در سناریوهای خاص منجر به نتایج غلط می‌شود؛ به‌عنوان مثال، در حالت تبعیض که در زیر توضیح داده می‌شود: شرایطی که تشخیص رتبه‌بندی‌های ناعادلانه نسبتاً آسان است، و نیز حالتی که کیفیت وب‌سرویس رتبه‌بندی شده به‌طور عینی (قابل مشاهده) ارزیابی شود. به این معنی که رتبه‌بندی می‌تواند با معیار کیفیتی قابل مشاهده به‌طور مستقیم مقایسه گردد [۱۲].

۶-۴-تبعیض[1]

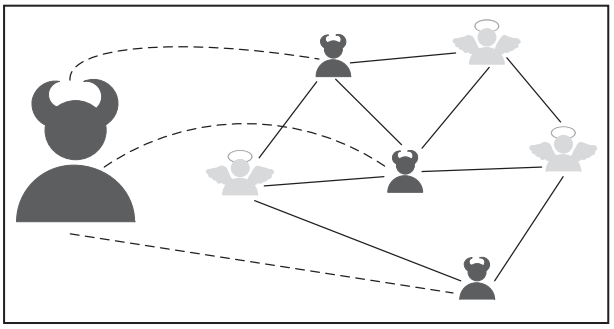
تبعیض بدان معنی است که یک نهاد ارائه‌دهنده سرویس، هم زمان برای یک گروه اعتمادکننده، سرویس‌های با کیفیت بالا و برای گروه دیگر، سرویس‌هایی با کیفیت پائین فراهم می‌کند. این رفتار می‌تواند اثرات بسیار متفاوت بر امتیاز نهاد ارائه‌دهنده سرویس- بسته به نوع سیستم اعتماد و اعتبارسنجی خاصی که استفاده می‌کند - داشته باشد. همچنین برخی از این نهادها برای کاربران مورد اعتماد پیشین خود، خدمات با کیفیت بالا و برای کاربران ناشناس خود، خدماتی با کیفیت پایین ارائه می‌کنند. برای مثال، اگر یک سیستم مدیریت اعتماد و اعتبارسنجی، روشی برای تشخیص رتبه‌بندی‌های غیرمنصفانه بر اساس مقایسه رتبه‌بندی‌های عوامل ناشناخته با رتبه‌بندی‌های عوامل مورد اعتمادِ قبلی استفاده می‌کند، کافی است که حمله‌کننده برای عوامل مورد اعتمادِ قبلی، سرویس‌های باکیفیت بالا فراهم نماید. این روش برای تشخیص رتبه‌بندی‌های غیرمنصفانه اثر متناقض خواهد داشت زیرا رتبه‌بندی‌های منفی واقعی توسط سیستم رد خواهد شد، به‌طوری که حمله‌کننده برای ارایه سرویس بی‌کیفیت تحریم نخواهد شد [۱۱و۱۰].

۶-۵- تبانی[2]

تبانی بدین معنی است که گروهی از عوامل، رفتارشان را به‌گونه‌ای هماهنگ می‌کنند که همانند *playbook*های در حال اجرا، رفتارهای غیرمنصفانه یا تبعیض‌آمیز فراهم می‌کنند. تبانی هوشمندانه می‌تواند تأثیر قابل توجهی بر امتیازات و در نتیجه، افزایش سود یا صلاحیت عوامل خاص داشته باشد. تبانی لزوماً غیراخلاقی نیست؛ برای مثال، در حالتی که این کار برای کنترل کیفیت خدمات ارائه‌شده با یک روش هماهنگ، توسط یک گروه انجام گیرد. با این حال، اگر تبانی شامل هماهنگی برای رتبه‌بندی‌های غیرمنصفانه باشد به‌طور واضح یک اقدام غیراخلاقی خواهد بود [۱۱].

۶-۶- حمله Sybil[3]

یک موجودیت که در حوزه سیستم مدیریت اعتماد و اعتبارسنجی، چندین هویت مستعار ایجاد می‌کند قادر است چندین رتبه‌بندی برای یک سرویس مشابه فراهم نماید. این مسئله نمایانگر یک حمله است که می‌تواند برای مهاجم این فرصت را فراهم کند تا بر روی امتیازات محاسبه‌شده به‌طور نامتناسب و غیرمنصفانه تاثیرگذار باشد. این حمله، حمله فالگیری نیز نامیده می‌شود و در پی کتابی که با همین نام توسط فلورا رتا شریب[4] در مورد یک زن که از اختلال شخصیتِ چندگانه رنج می‌برد نوشته شده است.



شکل ۴- حمله Sybil

یکی از راه‌حل‌های رایج برای مقابله با این‌گونه تهدیدات امنیتی، صَرف هزینه برای ایجاد هویتی جدید در این اجتماع می‌باشد. صَرف این هزینه، لزوماً اقتصادی نیست اما با توجه به زمان و منابع موجود، این کار می‌تواند اقتصادی باشد.

روش پیشنهادی دیگر برای مقابله با این مشکل، استفاده از یک مدیریت نهاد مرکزیِ هویت در سیستم، یا حتی یک مجموعه از فراهم‌کنندگان هویت برای تضمین اینکه هر شرکت‌کننده در اجتماع دارای هویت منحصربه فرد و تغییر ناپذیر باشد، می‌باشد [۱۰و۷].

۶-۷- اقدامات فریبکارانه[5]

در یک محیط سرویس‌گرا، همتایان به طرق مختلفی از قبیل تبادل اطلاعات، انتقال مقادیر و... با یکدیگر تعامل دارند. در حین تعامل با همتایانِ سیستم، یک همتای فریبکار ممکن است سهم خود را از

1- Discrimination
2- Collusion
3- The Sybil Attack
4- Flora Rheta Schreibe (1973)
5- Deceptive Practices

تراکنش به‌طور کامل تکمیل نکند، یا در دسترس بودن خدمات مسلمی را وعده دهد که لزوما عرضه نکرده است. یک مدلِ اعتماد باید:

۱- پیش از تعامل، در شناسایی چنین همتایان فریبکاری به سایر همتایان کمک کند.

۲- پس از تعامل، همتایان را قادر سازد تا در مورد این همتایان فریبکار به دیگران آگاهی رسانند.

۶-۸- حمله جعل هویت[1]

حمله جعل هویت، به تهدید مطرح‌شده توسط همتای بدخواه اطلاق می‌شود که خود را به‌عنوان همتای دیگر جا می‌زند. هدفی که در پس این تهدید وجود دارد می‌تواند سوء استفاده از مزایای همتای جعل هویت شده، یا بد نام کردن همتای جعل هویت شده از طریق تعاملات فریب‌آمیز با همتایان دیگر باشد. جعل هویت نوعاً از طریق: **۱)** امضاء پیام‌های صادر شده و **۲)** احراز هویت فرستندگان در سمت گیرنده، مورد توجه قرار می‌گیرد.

۶-۹- حمله On – Off[2]

حمله On – Off به رفتار خاکستری یک عامل اشاره دارد که برای یک مدت زمانی رفتار خوب و سپس رفتار بدی از خود ارائه می‌دهد. این تغییر رفتار، اثراتی بر روی فاکتورهای اعتماد و بهره‌برداری از وب‌سرویس‌ها می‌گذارد. باید گفت حمله On – Off اشاره به سناریویی دارد که یک همتای مخرب، مقادیر قابل توجهی دادهٔ پاک و آلوده را به‌طور متناوب برای همتایان درخواست‌کنندهٔ داده ارسال می‌کند. با انجام این کار، همتای مخرب می‌تواند ارزش اعتماد خود را بالاتر از آستانه از پیش تعیین شده نگه‌داشته و در نتیجه، از شناخته شدن خود به‌عنوان یک عنصر مخرب جلوگیری نماید. در حقیقت، حمله On – Off به سوء استفاده از این واقعیت می‌پردازد که اکثر مکانیزم‌های مدیریت اعتماد برای تحمل سطح خاصی از مقادیر آلوده (مانند اطلاعات ناقص و داده اشتباه) با توجه به شرایط نامطلوب شبکه طراحی شده‌اند.

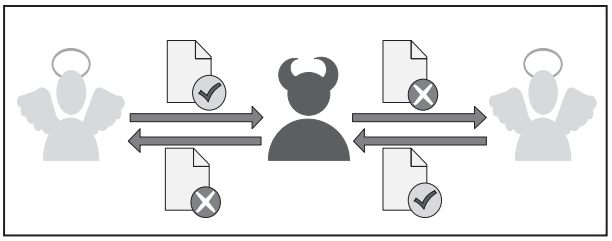
برای مقابله با حمله On – Off، یک راه موثر عبارت است از طراحی یک سیستم مدیریت اعتماد که در آن، نرخ افت مقدار اعتماد، بزرگ‌تر از نرخ رشد آن باشد. اگر مکانیزم مدیریت اعتماد، ارضاءکننده این وضعیت باشد می‌تواند به مقابله با این حمله بپردازد [۱۳].

۶-۱۰- حمله مردی در میانه[3]

یک همتای بدخواه می‌تواند میان پیغام‌هایی که از یک همتای ارائه‌کننده سرویس خیرخواه به سوی درخواست‌کننده سرویس ارسال می‌شود، قرار گرفته و به بازنویسی آنها با خدمات نامطلوب بپردازد که در این صورت، باعث کاهش سطح اعتماد و شهرت همتای خیرخواه می‌گردد. حتی این همتای بدخواه می‌تواند به صورت کینه‌جویانه به تغییر پیشنهادات و درخواست‌های یک همتای صادق بپردازد که حتی ممکن است نفعی برای خود نداشته باشد. اگر پاسخ مناسبی به این عمل داده نشود، این حمله می‌تواند باعث ایجاد آسیبی بزرگ به سیستم گردد.

یک راه ساده برای اجتناب از این خطر، استفاده از سازوکارهای رمزنگاری به‌منظور احراز هویت هر کاربر در سیستم است (شاید با امضاء دیجیتال یا هر مکانیزم مشابه دیگر).

با این حال، متاسفانه همیشه این راه‌حل امکان‌پذیر نیست، مخصوصاً در محیط‌های بسیار توزیع شده مانند شبکه‌های حسگر بی‌سیم [۱۰و۷].



شکل ۵- حمله مردی در میانه

۶-۱۱- حمله مداوم[4]

حمله مداوم، اشاره به سناریویی دارد که یک همتای مخرب اقدام به ارسال مداوم مقادیر قابل توجهی دادهٔ آلوده به سایر درخواست‌کنندگان داده می‌کند. این نوع حملات به‌راحتی قابل کنترل هستند.

بر اساس سازوکارهای سیستم‌های مدیریت اعتماد، زمانی که یک همتای مخرب اقدام به حمله مداوم می‌کند، مقدار اعتماد آن به‌سرعت کاهش می‌یابد. هنگامی که مقدار اعتماد آن کمتر از حد آستانه از پیش تعیین‌شده شود، سیستم آن را به‌عنوان یک عنصر آلوده‌کننده تشخیص داده و مانع از اشتراک و انتشار داده‌های آلوده می‌گردد [۱۳].

۶-۱۲- حمله گزافه‌گویی[5]

حمله گزافه‌گویی اشاره به سناریویی دارد که یک یا گروهی از

1- Impersonation Attack
2- On-Off Attack

3- Man in the Middle Attack
4- Persistent Attack
5- Bad-Mouthing Attack

همتایان بدخواه عمداً اقدام به تولید پیشنهادات یا نظرات منفی برای انجام توطئه بر علیه همتایان ممتاز می‌کنند. اگر فقط یک کاربر بدخواه وجود داشته باشد اثر این حمله تا حد زیادی محدود است و بنابراین می‌توان از آن صرف نظر کرد.

این واقعیت ناشی از این علت است که نظر و پیشنهاد یک همتای بدخواه، به تنهایی قادر به تغییر بزرگی در مقدار اعتماد غیر مستقیم نمی‌باشد؛ زیرا اعتماد غیر مستقیم، از پیشنهادات و نظرات یک گروه از همتایان به‌دست آمده است. با این حال، زمانی که یک گروه از همتایان بدخواه اقدام به تبانی و ارائه نظرات منفی می‌کنند اثر زیادی روی مقدار اعتماد غیر مستقیم خواهند گذاشت.

در سیستم‌های مدیریت اعتماد، دو راه حل به صورت کلی برای برخورد با این حملات مطرح شده است:

۱- فیلتر کردن توصیه‌های بالقوه همتایان بدخواه.

۲- کاهش وزن اعتماد غیر مستقیم. حملات گزافه‌گویی تا زمانی که توصیه‌نامه‌ها مورد توجه هستند، اجتناب ناپذیرند. بنابراین، کاهش وزن اعتماد غیرمستقیم در محاسبات اعتماد، روش مناسبی برای دفاع در برابر این حملات است [۱۳].

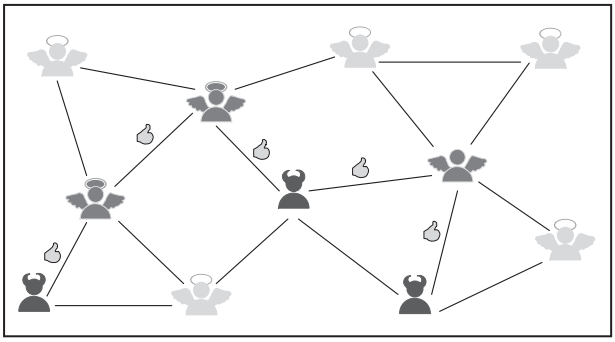
۶-۱۳- حمله جاسوسان بدخواه[1]

برخی از همتایان بدخواه، زمانی که به‌عنوان ارائه‌دهندگان خدمات انتخاب می‌شوند همیشه خدمات نامطلوبی ارائه می‌کنند. این همتایان بدخواه با تخصیص حداکثر مقدار اعتماد به سایر همتایان بدخواه در شبکه، جمعی از همتایان بدخواه را تشکیل می‌دهند. سایر همتایان بدخواه متمایز از دیگران، مشهور به جاسوسان بداندیش - که همیشه خدمات خوبی را به‌عنوان ارائه‌کننده خدمات از خود نشان می‌دهند، لکن آنها هم حداکثر مقدار رتبه‌بندی را برای سایر همتایان بداندیش که همیشه خدمات بدی را ارائه می‌کنند - فراهم می‌کنند (شکل ۶).

در این تهدید، جاسوسان بدخواه ممکن است سطح بالایی از اعتماد و شهرت را به‌دست آورند، زیرا آنها همیشه سرویس خوب ارائه می‌کنند. در نتیجه، قادر هستند مکانیسم اعتماد و اعتبارسنجی مورد استفاده در سیستم را تغییر دهند. در بیشتر اوقات، این نوع حمله کم اهمیت نیست و یا راه ساده‌ای برای مقابله موثر با آن وجود ندارد.

مانند سایر تهدیدات امنیتی، مدیریت دقیقِ قابلیتِ اطمینان همتایان، نه فقط به‌عنوان ارائه‌کنندگان خدمات، بلکه به‌عنوان فراهم‌کنندگان توصیه‌نامه‌ها، ممکن است به‌طور موثر در جلوگیری از این گونه سوء استفاده‌ها کمک نماید؛ اگرچه، هم شناسایی همتایان بدخواه و هم جاسوسان بدخواه، به زمان، تلاش و منابع بیشتری نیاز دارد [۷].

1- Malicious Spies



شکل ۶- حمله جاسوسان بداندیش [۷]

۷- نتیجه‌گیری

مدیریت اعتماد مبتنی بر اعتبارسنجی در شبکه‌های توزیع‌شده و محیط وب‌سرویس‌ها، حوزه تحقیقاتی جالب و البته بسیار چالش برانگیز است. اعتبارسنجی به‌منظور ایجاد اعتماد میان همتایان، به حداقل رساندن ریسک مشارکت در تراکنش‌ها و افزایش اطمینان و رضایتمندی همتایان به‌کار می‌رود. اعتبارسنجی بر اساس ارزیابی تراکنش‌های انجام شده توسط همتایان می‌باشد. در این مقاله، اهمیت، مزایا و محدودیت‌های سیستم‌های مدیریت اعتماد و اعتبارسنجی بیان گردید. خصوصیات، ویژگی‌ها و چالش‌های امنیتی مهم این رویکردها مطرح و زمینه کاربرد آن‌ها در مدیریت وب‌سرویس‌ها شرح داده شد. همچنین بیان شد که این سیستم‌ها چگونه می‌توانند در توسعه کسب‌وکار الکترونیکی در سطوح گسترده موثر باشند.

موفقیت برنامه‌های تجارت الکترونیکی مبتنی بر اعتبارسنجی، باعث پیشرفت مدیریت اعتبارسنجی و استفاده گسترده از آن در برنامه‌های کاربردی شده است. مطالعه سیستم‌های مدیریت اعتماد و اعتبارسنجی، سازوکارهای مختلف برای برطرف‌سازی چالش‌هایی که در استفاده از این سیستم وجود دارند را به نمایش می‌گذارد. از آنجایی که مدیریت اعتبارسنجی یک ابزار ارزیابی ریسک است، هنگام طراحی یک سیستم اعتبارسنجی براساس مخاطرات موجود در تراکنش‌ها، لازم است محدودیت‌ها و پارامترهای مختلفی در نظر گرفته شوند. ثبات و پایداری این سیستم‌ها و توانمندی آنها در مقابل حمله‌های بدخواهانه و تهدیدات امنیتی از اهمیت ویژه‌ای برخوردار است و جهت‌های اصلی تحقیقات آینده را مشخص می‌کنند.

مراجع

1. Zaki Malik, Athman Bouguettaya "Trust Management for Service-Oriented Environments" , Springer, (**2009**).
2. Florian Skopik, "Dynamic Trust in Mixed Service-oriented Systems Models, Algorithms, and Applications", Dissertation, (**2010**).
3. A. Singhal, T.Winograd, K. Scarfone, "Guide to secure web services", NIST, (**2007**).

4. Loubna Mekouar, Youssef Iraqi, and Raouf Boutaba, "Reputation-Based Trust Management in Peer-to-Peer Systems: Taxonomy and Anatomy", Springer, (**2010**).
5. Oxford Dictionary. .Http://www.askoxford.com/
6. Grandisan, T., Sloman, M., "A survey of Trust in Internet Applications", In: IEEE Communications, Surveys, Vol. , (**2000**).
7. Chang, E., Dillon, T., Hussain, F.K., "Trust and Reputation for Service-Oriented Environments", Wiley, (**2006**).
8. Felix Gomez Marmol, Gregorio Martınez Perez, "Security threats scenarios in trust and reputation models for distributed systems", Elsevier, (**2009**).
9. Marsh, S., "Formalising Trust as a Computational Concept", Ph.D. thesis, University of Stirling, (**1994**).
10. Abdul-Rahman, A., Hailes, S., "Supporting Trust in Virtual Communities", In: Proceedings of the 33rd Hawaii International Conference on System Sciences, p. 6007. IEEE Computer Society, Washington, DC, USA, (**2000**).
11. Kedar Nath Singh, Suresh Kumar, "Attacks on Trust and Reputation System & its Defensive methods in Semantic Web", IJAEST, (**2011**).
12. Audun Jøsang , Jennifer Golbeck , "Challenges for Robust Trust and Reputation Systems", Saint Malo, France, (**2009**).
13. Xin Kang, Yongdong Wu, "Fighting Pollution Attack in Peer-to-Peer Streaming Networks: A Trust Management Approach", Institute for Infocomm Research, Singapore, (**2011**).

Trust Management Security Challenges in Web Services

A. Karimi[1]

M. Saleh Esfahani[2]

M. R. Hasani Ahangar[3]

Abstract

One of the advances made on distributed networks and web sites in the recent years is introducing web services as independent software parameters. Web services are capable of being advertised, placed in a location and utilized in the web site based on standards such as WSDL ،UDDI و SOAP.

The ultimate aim of the web service technology is to enable the utilization of the web services' capabilities in service-based organizations as independent elements. Therefore, a service-based web provides an attractive sample and example for future interactions in a wide range of e-business to e-science and even e-government. In this regard, considering different security aspects of web services, the issue of trust management in the users' interactions with the service-based domains is of special importance. In the systems which are based on trust and authentication, reliable counterparts are used for information exchange and interactions. This matter causes the reduction of destructive transmissions in the systems. Giving special attention to the security aspects of trust management and its challenges can help us in improving and developing interactions and development of e-business in the distributed networks. In this essay, while providing a general introduction of the web services, the definition of the principles of trust and security in this domain and the challenges they face are also provided.

Key Words: *Trust Management, Authentication, Service-based Domains, Web Service, Security*

1- Imam Hossein University, Instructor and Doctoral Candidate in Software Engineering (akarimy@ihu.ac.ir) - Writer in Charge
2- Imam Hossein University, Assistant Professor and Academic Member of the Faculty and Research Center of ICT (msaleh@ihu.ac.ir)
3- Imam Hossein University, Assistant Professor and Academic Member of the Faculty and Research Center of ICT (mahangar@ihu.ac.ir)