استفاده از RPX برای شناسایی اعضای وب‌سایت

هویت ۲

امیربهاالدین سبط‌الشیخ

فرض کنید قرار است یک وب‌سایت مردمی درست کنید و اصلا هم قرار نیست طیف خاصی از کاربران را جذب کنید. از طرف دیگر، نمی‌خواهید خود را درگیر مسایلی مانند شناسه‌های کاربری، تعیین محدودیت‌ها و... بکنید. از همه مهم‌تر آنکه اطلاعات پروفایل شخص را نیاز دارید و نمی‌توانید همه کاربران را وادار کنید که نام و نام‌خانوادگی و دیگر اطلاعات فردی‌شان را کامل بنویسند. در واقع، تنبلی کاربران و مسایل مرتبط با ایجاد دسترسی و محدودیت در شناسه‌ها، از مهم‌ترین بخش‌های برنامه‌نویسی در ماژول کاربران به‌حساب می‌آید.

اما می‌توان به‌سادگی از شر تمام این دردسرها خلاص شد. با روش RPX، تعداد کاربران‌تان مشخص است: تمام کاربران جیمیل، یاهو، فیس‌بوک، اوپن‌آی‌دی، مای‌اسپیس، و ویندوز لایو، به‌طور پیش‌فرض جزکاربران شما به‌حساب می‌آیند. بنابراین، اقدامات دلفریب شما برای عضوشدن کاربران به‌حداقل ممکن کاهش خواهد یافت. همچنین، کاربران راحت‌تری خواهید داشت، هیچ کس توانایی به‌خاطر سپردن صدها گذرواژه برای صدها وب‌سایت را ندارد، بنابراین و طبق تحقیقات انجام شده، افراد معمولا از چند گذرواژه یک‌سان برای تمام وب‌سایت‌ها استفاده می‌کنند. درصورتی که از روش عادی ثبت نام در سایت بخواهیم پیش برویم، در این صورت کاربر تمایل خود را برای ثبت نام از دست می‌دهد، چراکه احتمالا گذرواژه وب‌سایت وی با گذرواژه آدرس ایمیلش یکی است و اطمینان لازم را ایجاد نکرده‌ایم. اما در صورتی که از RPX استفاده کنیم، این اعتماد خود به‌خود ایجاد خواهد شد.

RPX چطور کار می‌کند؟

این سرویس میان سرور شما و سرورهای تشخیص هویت فوق‌الذکر همانند پراکسی عمل می‌کند و بدون هیچ تلاش خاصی می‌توان با کمک RPX به راهبرد SingleSign-on (تک‌ورودی) رسید. راهبرد تک‌ورودی یعنی یک‌بار وارد یک‌سیستم شده، و در تمام وب‌سایت‌هایی که از آن سیستم استفاده می‌کنند، به‌طور خودکار داخل سیستم باشید. تک‌ورودی در واقع همان راه‌کاری است که ابرسایت‌هایی همانند مایکروسافت، یاهو، و جیمیل برای سرورهای مختلف خود در نظر گرفته‌اند.

دسترسی به توابع مربوطه RPX از طریق فراخوان‌های REST انجام می‌شود.

نکته: REST روشی برای انتقال وضعیت و توابع نرم‌افزاری در محیط‌های توزیعی و دور از هم، همانند محیط وب است.

کاربران خود انتخاب می‌کنند

اصلا نیاز نیست به‌دره سیلیکون سفر کنید و پای میز مذاکره گوگل و مایکروسافت بنشینید تا بخواهید از سیستم آنها استفاده کنید. کاربران شما می‌توانند خود انتخاب کنند که با کدام سرویس‌دهنده وارد وب‌سایت شما شوند. تنها کافی است که ظاهر نمایشی RPX را به‌آنها نشان دهید. آنها سرویس‌دهنده محبوب خود را انتخاب می‌کنند و بعد RPX باقی کارها را از جمله شناسایی کاربر و... انجام می‌دهد.

رابط کاربری ورود را می‌توانید هم به‌صورت Pop-up و هم به‌صورت داخل صفحه‌ای به کاربر نشان بدهید، حتی می‌توانید برای خود رابط کاربری خاصی ایجاد کنید.

کاربران قدیمی، با یک کلید وارد می‌شوند

کاربرانی که یک‌بار وارد سیستم شده‌اند، از بار دوم، با یک صفحه تک دکمه‌ای روبه‌رو می‌شوند که بعد از تائید مشخصات توسط RPX، تمام اطلاعات لازم برای ورود یک کاربر به‌سیستم به‌شما ارسال می‌شود.

استفاده راحت وسودسریع

با استفاده از فناوری‌های آزادی همچون اوپن‌آی‌دی (OpenID)، RPX می‌تواند هویت شخص را تایید کند و داده‌هایی که برای پروفایل هر کاربر نیاز دارید را به شما ارسال کند. ضمن آنکه RPX داده‌هایی که از منابع مختلف دریافت می‌شود را نرمال‌سازی کرده و شما نیازی به تشخیص فرمت‌های گوناگون داده ندارید. تنها یک نوع داده به‌شما ارسال می‌شود و از همان یک‌نوع داده هم استفاده خواهید برد.

مزیت‌ها

با قبول کردن وب‌سایت‌هایی چون AOL، گوگل، یاهو یا فیس‌بوک برای ثبت‌نام و ورود به سیستم، می‌توانید دسترسی وب‌سایت خود را برای کاربران سریع‌تر کنید و حرکت از قطب «کاربر مهمان» تا «کاربر عضو» را سریع‌تر بپیمایید. استفاده از RPX این زمان صرفه‌جویی شده را به‌شما می‌بخشد تا صرف اصل نرم‌افزار تحت وب خود بکنید و روی هدف اصلی‌تان متمرکز شوید.

تشخیص هویت

RPX از OpenID و دیگر پروتکل‌ها برای تشخیص هویت کاربران استفاده می‌کند. RPX یک API (رابط برنامه‌نویسی کاربردی) ساده مبتنی بر REST دارد که در واقع شکلی انتزاعی از فرم اطلاعات هر سرویس‌دهنده را در خود دارد. با پیاده‌سازی RPX API، به‌سرعت قادر خواهید بود Single Sign-on را در سیستم خود پیاده‌سازی کنید.

ظاهر مدیریت‌شده

با یک تکه کد می‌توانید تمام رابط کاربری را تعیین کنید. RPX فهرستی از سرویس‌دهنده‌ها را در همان یک تکه کد نشان خواهد داد و کاربران به سیستم وارد می‌شوند. رابط مدیریت‌شده RPX کاربر را خوب به یاد دارد. وقتی کاربر به سیستم بازگشت، تنها یک کلیک با لاگین کردن فاصله دارد. از آنجایی که رابط کاربری این سرویس ورود، قابل انعطاف است، می‌توانید رابط کاربری خود را هم به‌جای رابط پیش‌فرض قرار دهید.

انطباق با حساب‌ها و کاربران فعلی

با RPX، می‌توان ورود از سرویس‌دهنده‌های معروف را برای هر دو وب‌سایت تازه‌کار و با عضو قبلی پیاده‌سازی کرد. همچنین می‌توان برای هر حساب کاربری، چندین OpenID در نظر گرفت. بنابراین کنترل کامل هویت را به‌کاربر واگذار خواهیم کرد.

ارتقا خودکار

از آنجایی که RPX یک وب‌سرویس است، تنها پیش‌نیازی که دارد، ارسال درخواست‌های HTTPS از سوی سرور مبدا (سرور شما) است. هیچ کتابخانه، هیچ نرم‌افزار جانبی و هیچ ابزاری برای استفاده از این سرویس نیاز نیست. بنابراین، در صورت ارتقا، سیستم خودبه‌خود به‌روز می‌شود.

همخوانی داده‌ها

وقتی کاربران شما در سایت‌های شبکه اجتماعی‌ای همچون فیس‌بوک و مای‌اسپیس نام خود را تغییر می‌دهند، همخوانی داده‌ها، نام آنها را هم در سیستم‌تان تغییر می‌دهد.

سرویس‌دهنده‌ها

در حال حاضر، گوگل، یاهو، فیس‌بوک، مای‌اسپیس، بلاگر، وردپرس، اوپن‌آی‌دی، توییتر، AOL، ویندوز لایو و وری‌ساین از این سیستم پشتیبانی می‌کنند.

پروفایل

RPX داده‌های کاربر را برای هر یک از حساب‌های مرتبط با خود نمایش می‌دهد: نام، آدرس ایمیل، جنسیت، تاریخ تولد، اختلاف‌زمانی با گرین‌ویچ، وب‌سایت، شماره تلفن، تصویر پروفایل و آدرس. البته هر یک از سرویس‌دهنده‌ها روش خودش را برای ارسال داده‌ها دارند، اما RPX از روش خودش استفاده می‌کند.

تجهیز با شبکه‌های اجتماعی

با کمک API موجود در RPX می‌توان نسبت به ارسال مطالب و وضعیت‌ها در وب‌سایت‌های فیس‌بوک، مای‌اسپیس، توییتر، و یاهو اقدام کرد. عملیات اجتماعی را می‌توان درست همزمان با ورود کاربر به سیستم آغاز کرد.

منابع:

http://www.RPXnow.com
https://rpxnow.com/docs

نشت حافظه

نشت حافظه یعنی مصرف بیش از اندازه حافظه در جهت اجرای دستورات یک برنامه. از مهم‌ترین ضعف‌هایی که باعث نشت حافظه می‌شود، نبود Garbage Collection (جمع‌آوری آشغال) خودکار در زبان برنامه‌نویسی است. زبان‌هایی مثل C و C++ در معرض مستقیم نشت حافظه قرار دارند. عموما زمانی نشت حافظه روی می‌دهد که حافظه تخصیص داده شده به یک نرم‌افزار، غیرقابل آدرس‌دهی باشد. این مشکلات که ازآن به‌عنوان باگ‌های نرم‌افزاری سیستم یاد می‌شود، باعث ایجاد نرم‌افزارهای دیباگی شد که روی حافظه فعالیت می‌کردند و این نشت‌ها را تشخیص می‌دادند.

نرم‌افزارهایی چون BoundsChecker، Valgrind، Insure++ و memwatch برخی از همین ابزارهای دیباگ بودند.

زبان‌های جاوا، سی‌شارپ، لیسپ و VB.NET قابلیت جمع‌آوری خودکار آشغال را دارند، اما در مقابل نشت حافظه مصون نیستند. برای مثال ممکن است یک برنامه در یک حلقه نامتناهی، اشیایی با رفرنسی از جنس خود بسازد که باعث می‌شود بخش زیادی از حافظه از دسترسی خارج گردد.

نشت حافظه، به‌طور کلی با الگوریتم زیر به‌سادگی قابل درک خواهد بود:

فرض کنید که ما اکنون روی پله‌شماره X ایستاده‌ایم و هدف، پله‌شماره Y است. الگوریتم به‌این صورت انجام می‌شود که وقتی دکمه‌ای فشار داده شد.

تکه‌ای حافظه تخصیص داده شود و برای به‌خاطر سپردن شماره پله استفاده شود.

شماره پله داخل آن بخش از حافظه قرار داده شود.

آیا روی پله هدف ایستاده‌ایم؟

اگر چنین است، کاری برای انجام دادن نیست. پایان.

در غیر این صورت:

تا زمانی که پاها آزاد شوند باید صبر کنیم.

به پله مورد نظر برویم و حافظه‌ای که دریافت کرده‌ایم را آزاد کنیم.

در نگاه اول الگوریتم بدون نقص به‌نظر می‌رسد، اما وقتی دقت کنیم، در صورتی که ۲۰۰ بار پیغام درخواست به ماندن در همان پله اعلام شود، از آن‌جایی که در حالت درستی شرط، حافظه را آزاد نکرده‌ایم، ۲۰۰ خانه حافظه، بدون رفرنس باقی خواهد ماند و نشت عظیمی رخ خواهد داد.