گزارش در مورد نحوه پیاده سازی LDAP برای SSO – قسمت تئوری

تهیه و تنظیم: مبین خیبری

شماره دانشجویی: 994421017

استاد راهنما: دکتر تاجبخش

چکیده:

هدف از این تمرین، گزارشِ نحوه‌ی پیاده‌سازیِ استفاده از سرویسِ LDAP برای ارائه‌ی خدماتِ SSO جهت احراز هویت کاربرانِ سرویس‌هایی نظیرِ Email، Git و ... می‌باشد. در گزارش‌کارِ پیش‌رو قصد داریم صرفا به مبانیِ نظریِ طراحیِ چنین سیستمی اشاره کنیم و به زبانِ ساده نیازمندی‌های فنیِ این سیستم را بررسی کرده و در نهایت سیستمی با چنین ویژگی‌هایی را به‌صورت تئوری طراحی کنیم.

از آنجا که کار با چنین سیستمی، آشناییِ همه‌جانبه با ساختار و نحوه‌ی عملکرد آن را می‌طلبد، در بخش‌های پیش‌رو ابتدا به معرفیِ کلیِ سرویس‌های LDAP، SSO و زیرساخت‌های لازم برای ساخت چنین سیستمی پرداخته و سپس مراحل طراحی را بررسی خواهیم کرد.

لازم به ذکر است که بسته به زیرساخت‌های فنیِ مورد استفاده، ممکن است جزئیاتِ پیاده‌سازیِ این سیستم بر اساسِ تغییراتِ مراجعِ ارائه‌دهنده‌ی این خدمات متفاوت باشند. به همین دلیل در طول این گزارش ما تا جای ممکن وارد جزئیات نشده و به تحلیلِ کلیِ کانفیگ‌های مورد نیاز برای پیاده‌سازیِ این سرویس، بسنده می‌کنیم.

SSO چیست؟

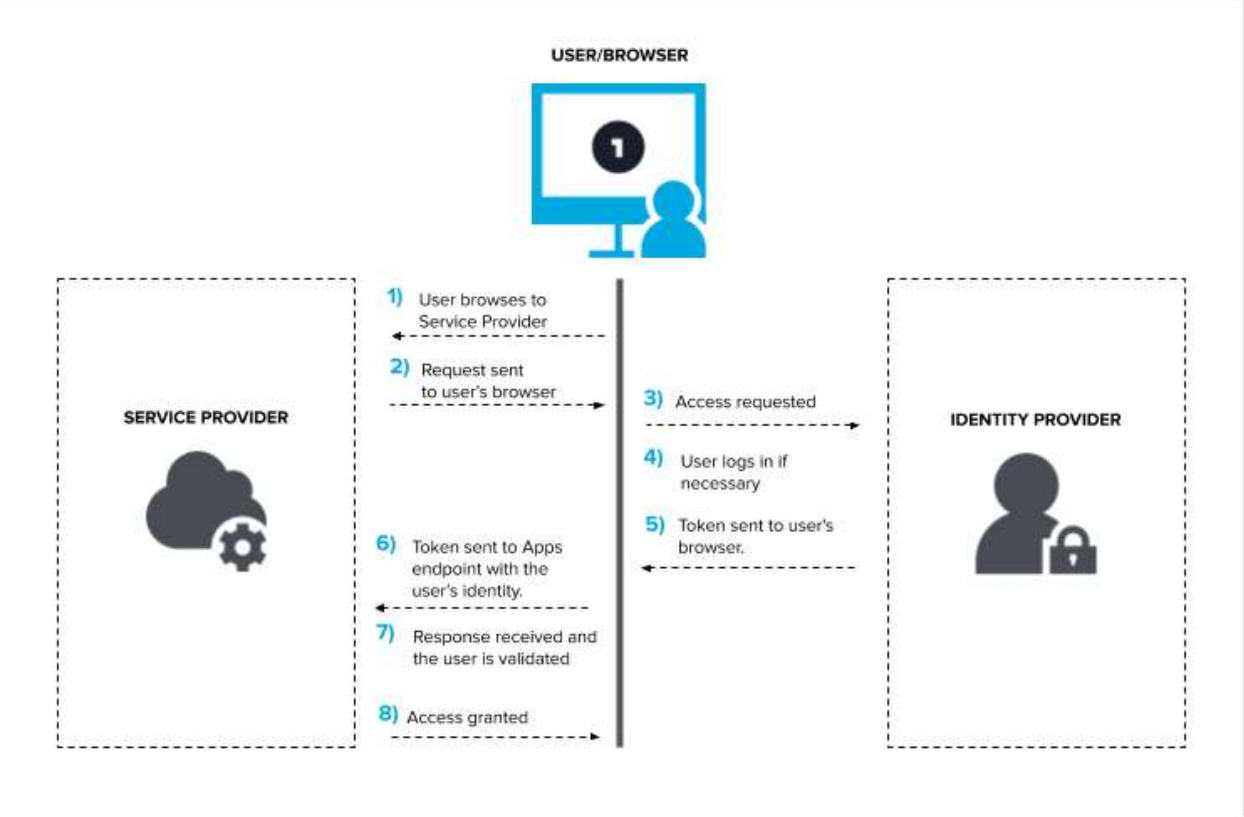
SSO یک روش احراز هویت است که به کاربران امکان می‌دهد با استفاده از تنها یک مجموعه داده‌های احراز هویت، به روشی امن در چند اپلیکیشن و وب‌سایت وارد شوند. در ادامه بررسی می‌کنیم SSO چیست، چه مزیت‌هایی دارد و روش پیاده‌سازی آن چگونه است.

طرز کار SSO چیست؟

SSO بر مبنای یک رابطه اعتماد عمل می‌کند که بین اپلیکیشن که ارائه‌دهنده سرویس نامیده می‌شود و یک ارائه‌دهنده هویت مانند گوگل برقرار شده است. این رابطه اعتماد غالباً بر اساس یک گواهینامه است که بین ارائه‌دهنده هویت و ارائه‌دهنده سرویس مبادله می‌شود. این گواهینامه برای امضا کردن اطلاعات هویت از سمت ارائه‌دهنده هویت به ارائه‌دهنده سرویس عرضه می‌شود تا ارائه‌دهنده سرویس مطمئن شود کاربر که از منبع شناخته‌شده‌ای می‌آید. در SSO این داده‌های هویت به شکل توکن هستند که بخش‌های اطلاعاتی برای شناسایی کاربر از قبیل نشانی ایمیل یا نام کاربری را شامل می‌شوند.

فرایند لاگین به طور معمول شامل مراحل زیر است.

- کاربر به نشانی اپلیکیشن یا وب‌سایتی که می‌خواهد دسترسی یابد می‌رود که اینجا ارائه‌دهنده سرویس نامیده می‌شود.
- ارائه‌دهنده سرویس یک توکن به سیستم SSO یعنی ارائه‌دهنده هویت ارسال می‌کند که شامل اطلاعاتی در مورد کاربر از قبیل نشانی ایمیل می‌شود و برای احراز هویت کاربر استفاده می‌شود.
- ارائه‌دهنده هویت ابتدا بررسی می‌کند آیا کاربر قبلاً احراز هویت شده یا نه و در صورتی که چنین باشد امکان دسترسی به اپلیکیشن ارائه‌دهنده سرویس را فراهم ساخته و به گام پنجم می‌رود.
- اگر کاربر قبلاً وارد نشده باشد، با ارائه اطلاعات احراز هویت که از سوی ارائه‌دهنده هویت فراهم آمده از وی خواسته می‌شود که این کار را انجام دهد. این اطلاعات می‌توانند صرفاً یک نام کاربری و رمز عبور باشند و یا شامل اطلاعات دیگری از قبیل رمزهای عبور یک بار مصرف نیز باشند.
- زمانی که ارائه‌دهنده هویت، صحت اطلاعات احراز را تأیید کرد، یک توکن به ارائه‌دهنده سرویس بازگشت می‌دهد که نشانگر تأیید شدن فرایند احراز هویت است.
- توکنی که از سوی ارائه‌دهنده سرویس دریافت می‌شود، بر اساس رابطه اعتمادی تأیید می‌شود که بین ارائه‌دهنده سرویس و ارائه‌دهنده هویت در مرحله پیکربندی اولیه برقرار شده است.
- کاربر امکان دسترسی به ارائه‌دهنده سرویس را پیدا می‌کند.



زمانی که کاربر تلاش کند به وب‌سایت دیگری دسترسی یابد، این وب‌سایت جدید رابطه اعتماد مشابهی با SSO برقرار کرده باشد تا گردش کار احراز هویت به روش مشابهی انجام شود.

توکن SSO چیست؟

توکن SSO یک مجموعه داده‌ها یا اطلاعات است که در طی فرایند SSO از یک سیستم به سیستم دیگر ارسال می‌شود. این داده‌ها می‌توانند صرفاً شامل نشانی ایمیل و اطلاعاتی در مورد سیستم ارسال‌کننده توکن باشند. توکن‌ها باید به صورت دیجیتالی برای گیرنده توکن امضا شوند تا تأیید شود که توکن از یک منبع مورد اعتماد می‌آید. گواهینامه‌ای که برای این امضای دیجیتالی استفاده می‌شود در طی فرایند پیکربندی اولیه مبادله شده است.

آیا SSO امن است؟

پاسخ به این سؤال بستگی به موارد مختلفی دارد. SSO از جهات مختلف می‌تواند موجب ارتقای امنیت بشود. یک راهکار «ثبت نام منفرد» (single sign-on) اجازه می‌دهد که مدیریت رمز عبور و نام کاربری برای کاربران و همچنین مدیران به صورت ساده‌تری انجام یابد. بدین ترتیب دیگر لازم نیست کاربران رمزهای عبور مختلف را ذخیره کرده یا به خاطر بسپارند و تنها یک رمز عبور منفرد پیچیده را به خاطر می‌سپارند. SSO در اغلب موارد به کاربران امکان می‌دهد که سریع‌تر به اپلیکیشن‌هایشان دسترسی یابند.

SSO همچنین موجب می‌شود که زحمت‌های بخش پشتیبانی هر شرکت برای کمک به کاربرانی که رمز عبورشان را فراموش کرده‌اند کاهش یابد. مدیران می‌توانند الزاماتی مانند پیچیدگی رمز عبور و احراز هویت‌های چندمرحله‌ای (MFA) را به روش متمرکزی مدیریت کنند. همچنین مدیران می‌توانند در صورت ترک سازمان از سوی یک کارمند با سرعت بالاتری دسترسی‌های وی را قطع کنند.

ثبت نام منفرد برخی معایب نیز دارد. برای نمونه ممکن است بخواهید برخی اپلیکیشن‌ها به روش محافظه‌کارانه‌تری عمل کنند. به این جهت بهتر است یک راهکار SSO انتخاب شود که این امکان را در اختیار شما قرار می‌دهد مثلاً پیش از ورود کاربر به یک اپلیکیشن خاص یک عامل احراز هویت دیگر نیز بخواهد یا این که پیش از دسترسی کاربر به یک شبکه امن از دسترسی وی به برخی اپلیکیشن‌های خاص جلوگیری کند.

شیوه پیاده‌سازی SSO چیست؟

خصوصیات شیوه پیاده‌سازی یک راهکار SSO تا حدود زیادی به نوع راهکاری که انتخاب می‌کنید وابسته است. اما مراحل کار هر چه که باشد، باید اطمینان پیدا کنید که اهداف و ایده‌های روشنی در مورد پیاده‌سازی چنین راهکاری دارید. برای نمونه باید پاسخ سؤالات زیر را یافته باشید.

- انواع متفاوت کاربرانی که به آن‌ها خدمت می‌دهید کدام هستند و الزاماتشان چیست؟
- آیا به دنبال یک راهکار داخل سازمانی هستید یا یک راهکاری ابری برای شما مناسب است؟
- آیا راهکاری که انتخاب کرده‌اید همراه با رشد نیازها و مقیاس‌بندی سازمانتان رشد خواهد کرد؟

- چه ویژگی‌هایی نیاز دارید تا مطمئن شوید که تنها کاربران معتمد می‌توانند وارد شوند. MFA، احراز هویت تطبیقی، اعتماد بر مبنای دستگاه، وایت لیست کردن نشانی IP و غیره از جمله این ویژگی‌ها هستند.
- با چه سیستم‌هایی تجمیع خواهد شد؟
- آیا نیاز به دسترسی API دارید؟

سیستم مناسب SSO چه ویژگی‌هایی دارد؟

نکته مهم این است که تفاوت بین SSO و سیستم‌های مدیریت رمز عبور را بدانید. این سیستم‌ها نیز گاهی SSO نامیده می‌شوند که اختصاری برای عبارت «ثبت نام مشابه» (Same Sign-on) است. در سیستم‌های مدیریت رمز عبور شما یک نام کاربری و رمز عبور واحد دارید، اما هر بار که به اپلیکیشن یا وب‌سایت دیگری مراجعه می‌کنید باید مجدداً آن را وارد نمایید. سیستم مدیریت رمز عبور تنها کاری که انجام می‌دهد این است که رمز عبور شما را برای اپلیکیشن‌های مختلف نگهداری می‌کند و در مواقع لازم آن‌ها را به جای شما وارد می‌کند. هیچ رابطه اعتمادی بین اپلیکیشن و سیستم مدیریت رمز عبور وجود ندارد.

از سوی دیگر در SSO پس از این که به وسیله راهکار SSO وارد شدید، می‌توانید به همه اپلیکیشن‌ها و وب‌سایت‌های تأیید شده از سوی راهکار بدون نیاز به ورود مجدد دسترسی داشته باشید. این موارد شامل اپلیکیشن‌های ابری و همچنین اپلیکیشن‌های سازمانی هستند.

فرق بین نرم‌افزار SSO و راهکار SSO چیست؟

هنگامی که به بررسی گزینه‌های مختلف SSO می‌پردازید، ممکن است متوجه شوید که گاهی اوقات از آن‌ها به نام نرم‌افزار SSO و گاهی با عنوان راهکار SSO یاد می‌شود. در اغلب موارد این تفاوت از شیوه دسته‌بندی گزینه‌ها از سوی سازمان‌ها ناشی می‌شود. نرم‌افزار چیزی است که روی یک سیستم نصب می‌شود. نرم‌افزار در واقع برای انجام برخی وظایف خاص و نه بیشتر طراحی شده است. اما عنوان راهکار نشان می‌دهد که امکان بسط یا سفارشی‌سازی ظرفیت‌های محصول اصلی وجود دارد. یک ارائه‌دهنده ممکن است به شرکتی ارجاع بدهد که راهکار تولیدی را میزبانی می‌کند.

آیا انواع مختلفی از SSO وجود دارند؟

زمانی که بحث در مورد SSO است، اصطلاحات جدید زیادی وجود دارد که باید بلد باشید.

- مدیریت بخشی هویت (FIM)
- OAuth (امروزه نسخه دوم آن مطرح است)
- اتصال OpenID (OIDC)
- زبان نشانه‌گذاری دسترسی امنیتی (SAML)

- ثبت نام مشابه (SSO)

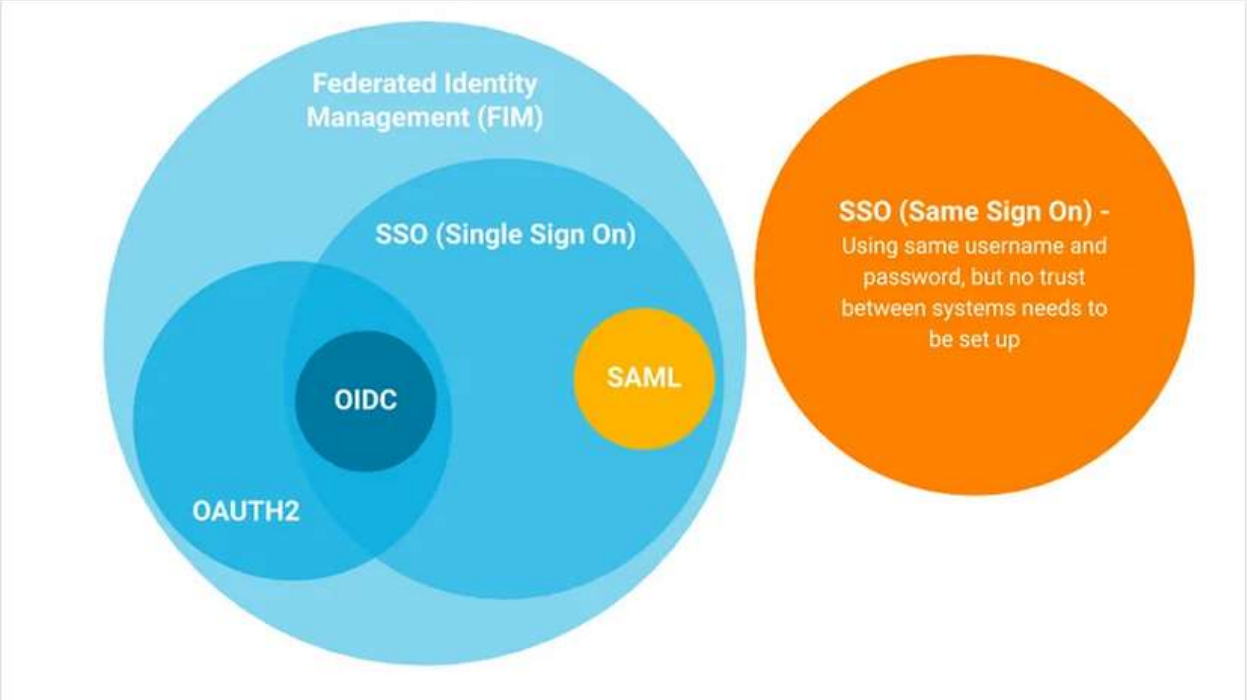
SSO در واقع بخشی از یک مفهوم بزرگ‌تر به نام «مدیریت بخشی هویت» (Federated Identity Management) است و از این رو گاهی اوقات SSO به نام «SSO بخشی» نیز نامیده می‌شود. FIM در واقع به رابطه اعتماد ایجاد شده بین دو یا چند دامنه یا سیستم‌های مدیریت هویت اشاره دارد. SSO در اغلب موارد یک ویژگی است که درون معماری FIM ارائه می‌شود.

OAuth 2.0 یک فریمورک خاص است که آن را نیز می‌توان بخشی از معماری FIM در نظر گرفت. OAuth روی ایجاد امکان اشتراک اطلاعات هویت کاربر میان دامنه‌های مختلف بر مبنای رابطه اعتماد استوار است.

اتصال OpenID یا به اختصار OIDC یک لایه احراز هویت است که بر مبنای OAuth 2.0 ساخته شده تا کارکرد Single Sign-on را عرضه کند.

«زبان نشانه‌گذاری دسترسی امنیتی» یا به اختصار SAML یک استاندارد باز است که برای عرضه کارکرد SSO طراحی شده است.

این موارد را می‌توانید در نمودار زیر به طور خلاصه مشاهده کنید.



منظور از نرم‌افزار SSO به عنوان یک سرویس چیست؟

دقیقاً مانند هر اپلیکیشن دیگری که امروزه روی اینترنت اجرا می‌شود، کارکرد SSO نیز می‌تواند به فضای ابری جابجا شود. پلتفرم‌های مختلفی امروزه سرویس‌های SSO را بر روی کلود و به شکل SaaS عرضه می‌کنند.

منظور از SSO اپ به اپ چیست؟

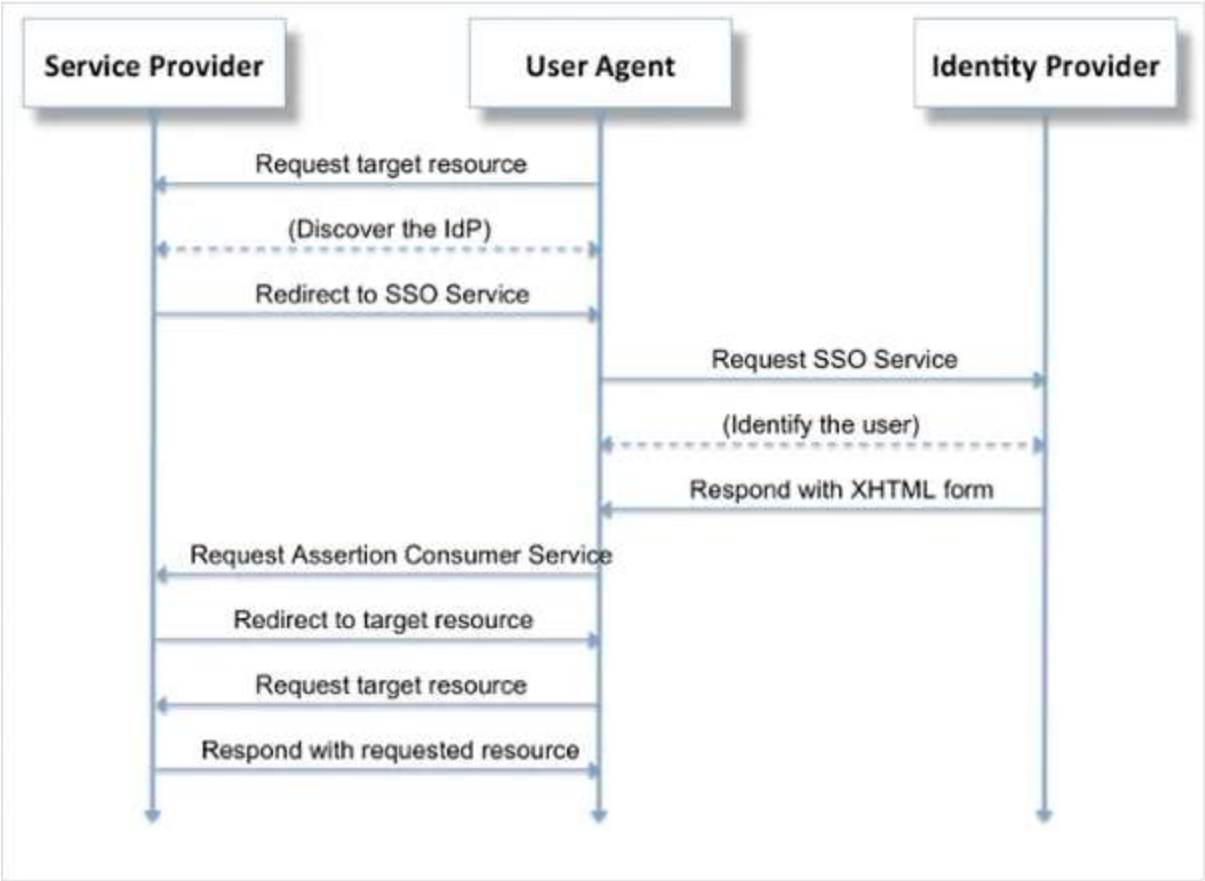
SSO بین اپلیکیشن هنوز به یک استاندارد تبدیل نشده است. در واقع این اصطلاحی است که برای ارسال هویت یک فرد از یک اپلیکیشن به اپلیکیشن دیگر درون یک اکوسیستم منفرد استفاده می‌شود. این فرایند تا حدودی شبیه OAuth 2.0 است اما یک روش یا پروتکل استاندارد محسوب نمی‌شود و در حال حاضر صرفاً از سوی SAPCloud مورد استفاده قرار می‌گیرد.

مزیت استفاده از SAML برای SSO چیست؟

SAML تنها استانداردی است که هم از احراز هویت (authentication) و هم احراز دسترسی (authorization) پشتیبانی می‌کند. این بدان معنی است که کاربران نه تنها می‌توانند با استفاده از ترکیب شناسه/رمز عبور خود لاگین کنند، بلکه می‌توانند پروفایل، نقش‌ها و مجوزهای خود را نیز از طریق همین پروتکل به اشتراک بگذارند.

SAML علاوه بر همه گزینه‌های دیگر کنترل بیشتری در اختیار شرکت‌ها قرار می‌دهد تا با پشتیبانی از امضا کردن و رمزگذاری داده‌ها از هر دو سمت ارائه‌دهنده سرویس و ارائه‌دهنده احراز هویت، لاگین‌های خود را به مراتب امن‌تر سازند. بنابراین در صورت نیاز می‌توان داده‌ها را در کل فرایند رمزنگاری کرد و هیچ حمله‌ای نمی‌تواند آن‌ها را رمزگشایی کند، مگر این که از قبل به هر دو کلید خصوصی سمت سرویس و احراز هویت دسترسی داشته باشد. این پروتکل در سال 2005 معرفی شده و از این نظر پیاده‌سازی‌های زیادی برای سیستم‌ها و زبان‌های مختلف عرضه شده است.

گردش کار کاربر در SSO-های مبتنی بر SAML بسیار شبیه انتقال داده‌ها در درخواست‌های HTTP-Redirect و HTTP-POST است.



فرایند کار چنین است:

- کاربر درخواست آغاز SSO را به ارائه‌دهنده سرویس می‌دهد.
- ارائه‌دهنده سرویس یک درخواست احراز هویت رمزگذاری شده base64 ایجاد کرده و به ارائه‌دهنده هویت ارسال می‌کند.
- ارائه‌دهنده هویت درخواست احراز را دریافت کرده، تأیید کرده و از کاربر می‌خواهد که احراز (لاگین) کند.
- ارائه‌دهنده هویت فرم XHTML را به همراه پاسخ رمزگذاری شده base64 به کاربر ارسال می‌کند.
- کاربر پاسخ SAML را به ارائه‌دهنده سرویس ارسال می‌کند.
- ارائه‌دهنده سرویس پاسخ SAML را تأیید کرده و کاربر را به منبع هدف ریدایرکت می‌کند.

پیاده‌سازی SSO مبتنی بر SAML

چنان که در بخش قبل دیدیم برای پیاده‌سازی SSO مبتنی بر SAML به دو «نقطه انتهایی» (endpoint) نیاز داریم.

- یک نقطه انتهایی اقدام به ساخت درخواست احراز هویت کرده و کاربر را به فرم لاگین ریدایرکت کرده و داده‌های درخواست لاگین را که به صورت base64 رمزگذاری شده ارسال می‌کند.
- نقطه انتهایی دیگر یک پاسخ SAML را پس از موفقیت فرایند لاگین پذیرفته و دریافت می‌کند.

شیوه انتقال داده‌ها از یک موجودیت به موجودیت دیگر به سه روش می‌تواند باشد:

- اتصال HTTP-Redirect داده‌ها را به شکل پارامتر دریافتی بسته‌بندی می‌کند.
- اتصال HTTP-Post داده‌ها را به شکل درخواست HTTP ارسال می‌کند. این روش معمولاً از طریق ساخت یک فرم XHTML انجام می‌شود.

هیچ دخالتی از سوی پروتکل HTTP از سمت کاربر یا مرورگر صورت نمی‌گیرد، بلکه یک اتصال مستقیم بین دو نقطه انتهایی صورت می‌گیرد.

درخواست‌های احراز هویت به طور معمول با استفاده از اتصال HTTP-Redirect یا HTTP-Post ارسال می‌شوند زیرا payload داده‌ها کم است. اما از آنجا که پاسخ SAML معمولاً برای قرار گرفتن در یک URL بیش از حد بزرگ است، بهتر است از اتصال HTTP-Post برای انتقال داده‌های پاسخ SAML استفاده شود.

سخن پایانی:

پروتکل SSO مدت زیادی است که معرفی شده است. در این بخش با تاریخچه، انواع، کاربردها و مزیت و معایب آن آشنا شدیم. این فناوری همچنان در حال تکامل است و امروزه شاهد هستیم که دستگاه تلفن همراه کاربران به عنوان کلید احراز هویت آن‌ها برای لاگین کردن در پلتفرم‌های مختلف مورد استفاده قرار می‌گیرد. با این حال این فناوری نیز برخی معایب از نظر امنیتی و رعایت حریم خصوصی دارد و از هجمه انتقادات به دور نمانده است. از این رو باید در زمان تصمیم‌گیری برای استفاده از آن با چشم باز و با رعایت همه جوانب تصمیم‌گیری کنیم.

پروتکل LDAP چیست؟

پروتکل LDAP نسخه سبک تر شده پروتکل DAP می‌باشد و هر دو آن‌ها به عنوان بخشی از استاندارد X.500 هستند که استاندارد Directory Services می‌باشد. به زبان ساده LDAP پروتکلی است که به ما در پیدا کردن اطلاعات و پرونده های مربوطه و مورد نیازمان چه درون یک سازمان چه درون اینترنت کمک می‌کند و این فرایند را راحت تر می‌سازد.

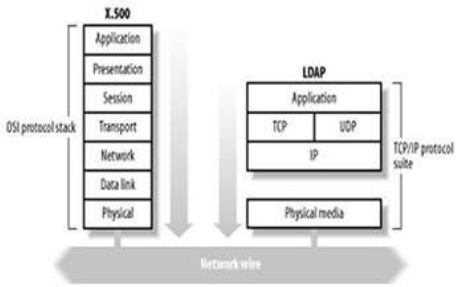
LDAP سرنام Lightweight Directory Access Protocol یک پروتکل استاندارد برای دسترسی به پوشه‌های مبتنی بر شبکه است. با این‌حال، با توجه به شناسایی رخنه های امنیتی در این پروتکل، امروزه LPDAPS به عنوان جایگزینی بهتر و ایمن‌تر که قادر به رمزگذاری ارتباطات است از سوی کارشناسان شبکه استفاده می‌شود. نکته‌ای که لازم است در ارتباط با این پروتکل به آن دقت کنید آشنایی با مفهوم پوشه است. یک پوشه یا در اصطلاح تخصصی دایرکتوری شبکه نوعی بانک اطلاعاتی ویژه است که اطلاعات مربوط به دستگاه‌ها، برنامه ها، افراد و سایر پارامترهای فنی یک شبکه کامپیوتری را نگه‌داری و ذخیره‌سازی می‌کند. از قدرتمندترین فناوری‌هایی که برای ساخت دایرکتوری‌های شبکه از آن‌ها استفاده می‌شود باید به LDAP و Microsoft Active Directory اشاره کرد.

LDAP روش استانداردی برای دسترسی و به روزرسانی فهرست‌های(دایرکتوری های) توزیع شده (Distributed) ارائه می دهد. LDAP مخفف Lightweight Directory Access Protocol است و مجموعه ای از پادمان ها (Protocols) و متدها، برای دسترسی به اطلاعات شاخه های توزیع شده است. متدهایی که در LDAP در اختیار دارید به شما این امکان را می‌دهد تا از اطلاعاتی که در درخت اطلاعات شاخه ها (Directory Information Tree – DIT) قرار دارد استفاده کنید. برای مثال در یک شبکه، این درخت شامل اطلاعاتی از اشیاء موجود در شبکه مانند کاربران، پرینترها، برنامه ها و ... است.

ال‌دپ از استانداردهای موجود در X.500 (استاندارد X.500 یک استاندارد جامع‌تر برای تعریف، نگهداری و مدیریت دایرکتوری های عمومی است. این استاندارد برای نگهداری اطلاعات عمومی (جهانی) استفاده می شود مانند آنچه در DNS استفاده شده است) پیروی می کند. اما LDAP از آن ساده‌تر و عملی تر است و برخلاف X.500، TCP/IP را نیز پشتیبانی می کند که برای استفاده در اینترنت نیز مفید است. ال‌دپ سبک‌تر از X.500 است و به همین دلیل گاهی به آن X.500 Lite نیز گفته می شود.

What is LDAP

- Lightweight Directory Access Protocol (LDAP)
  - LDAP v3: RFC 3377
  - RFC 2251-2256, 2829, 2830, 3377
- Why LDAP is lightweight
  - subset of X.500
  - X.500 base on OSI stack
  - LDAP base on TCP/IP
  - LDAP omits many X.500 operations that are rarely used
  - Providing a smaller and simpler set of operations



بررسی مفهوم Directory Services

به طور کاملا ساده Directory Services به کاربران در پیدا کردن اطلاعات و فایل های واقع شده در یک مکان کمک می‌کند.

به عنوان مثال پروتکل DNS به عنوان یک دفترچه تلفن حاوی اطلاعات آدرس IP و Domain Name است. کاربران زمانی که بخواهند وارد وب سایت KaliBoys.com شوند درصورتی که آدرس آن را در مرورگر خود وارد می‌کنند در پشت این آدرس، آدرس IP وب سرور کالی بویز قرار گرفته است و لود می شود تا آن ها را حفظ نکنیم.

یک نمونه کامل از یک Directory Service بسیار شبیه پروتکل DNS می‌باشد و پروتکل LDAP نیز به همین شکل است و به کاربران اجازه می‌دهد بدون اینکه از مکان یک کاربر یا یک فایل اطلاعی داشته باشند آن را پیدا کنند.

برای چه از LDAP استفاده کنیم؟!

بیشترین استفاده هایی که از پروتکل LDAP می‌شود احراز هویت می‌باشد. زیرا اکثر تجهیزات همچون فایروال های سخت افزاری، روترها و سرورها به راحتی از LDAP پشتیبانی می‌کنند و می‌توانیم با قرار دادن Username و Password فرایند احراز هویت خودمان را با استفاده از پروتکل LDAP به راحتی فراهم سازیم.

از جمله تجهیزات و نرم افزارهایی که از این پروتکل برای احراز هویت خود استفاده و یا پشتیبانی می‌کنند عبارتند از Docker, Jenkins, Kubernetes, Open VPN و پروتکل اشتراک گذاری فایل لینوکسی Samba. علاوه بر این مدیران سیستم و متخصصین از LDAP برای مدیریت و دسترسی بهتر به پایگاه های داده نیز استفاده می‌کنند.

بررسی LDAP Authentication

دو روش برای پیاده سازی احراز هویت در LDAPv3 وجود دارد.

- گزینه Simple
- گزینه SASL(Simple Authentication Security Layer)

احراز هویت Simple

اینگونه احراز هویت در LDAP به سه شکل ارائه می‌شود که به شرح زیر هستند:

- **Anonymous Authentication**: در این روش به شکل ناشناس کاربران در LDAP احراز هویت می‌کنند و وضعیت آنها را ارائه می‌دهند.
- **Unauthenticated authentication**: از این روش فقط برای اهداف خاص استفاده می‌شود و کاربر اجازه دسترسی به منابع و فایل هارا ندارد.

- **Username/Password Authentication**: این روش همانطور که از اسم آن‌هم پیداست از احراز هویت بر اساس Username و Password استفاده می‌کنند اما استفاده از این روش درصورتی که از پروتکل ایمنی برای رمزنگاری استفاده نشود کار معقولی نمی‌باشد.

احراز هویت SASL

روش احراز هویت برپایه SASL در واقع LDAP را به یک مکانیزم احراز هویت دیگر مانند Kerberos متصل می‌سازد. سرور LDAP ما از طریق پروتکل LDAP پیغام های LDAP را به سمت یک سرویس دیگر به منظور انجام احراز هویت انتقال می‌دهد.

بررسی LDAP Query

LDAP Query ها دستوراتی هستند که از Directory Services مورد نظر اطلاعات خاصی را درخواست می‌کنند. به عنوان مثال قصد داریم بفهمیم که یک کاربر در کدام یک از گروه های Directory Services ما وجود دارد LDAP Query ما به شکل زیر می باشد.

```
(&(objectClass=user)(sAMAccountName=yourUserName)
```

نصب و راه اندازی LDAP در سرورهای لینوکسی (Debian-Based)

برای راه اندازی و اجرای LDAP راه های بسیار زیادی وجود دارد از جمله آن‌ها نرم افزار OpenLDAP می‌باشد که یک نرم افزار رایگان و آزاد برای راه اندازی LDAP است. مراحل نصب و اجرا سازی OpenLDAP را بر روی یک سرور لینوکسی قدم به قدم پیش میبریم.

مرحله اول: آپدیت سیستم و مخازن آن

```
sudo apt update
sudo apt upgrade
```

مرحله دوم: نصب OpenLDAP

```
sudo apt install slapd ldap-utils
```

درحین نصب از شما سوالاتی مبنی بر پسورد سرور LDAP و آدرس سرور DNS پرسیده می‌شود که برحسب نیاز خودتان وارد کنید.

نصب و راه اندازی LDAP در سرورهای ویندوزی

برای نصب و راه اندازی LDAP در سرور های ویندوزی می‌بایستی سرویس Active Directory را در سرور ویندوز نصب کنید تا به همراه آن پروتکل LDAP نیز نصب شود.

پایان.