Классификация систем единого логического входа

Описанная схема допускает различные реализации в зависимости от применяемых технологий и протоколов аутентификации, типов операционных систем и сервисов, а также организационной принадлежности ее элементов.

В зависимости от применяемых криптографических технологий аутентификации системы единого логического входа делятся на два класса:

- *системы на основе разделяемого секрета*: многоразовых и одноразовых паролей, биометрических данных и другой информации, которая имеется как у пользователя, так и в базе учетных данных провайдера идентичности;
- *системы на основе технологии открытых и закрытых ключей*, использующей цифровые сертификаты; в этом варианте провайдером идентичности является центр сертификации, выдавший цифровой сертификат пользователю, а сам сертификат используется в качестве токена доступа.

В свою очередь системы на основе разделяемого секрета могут далее подразделяться в зависимости от применяемого протокола аутентификации. Наиболее популярными протоколами этого типа являются протоколы Kerberos, RADUIS, TACACS.

В зависимости от типа сервиса, к которому пользователь получает доступ, системы единого логического входа делятся на:

- *системы входа на основе веб-сервисов*. Эти системы рассчитаны на широкий класс веб-сервисов, к которым доступ осуществляется с помощью веб-браузера. Эти системы используют специфику веб-сервисов – протокол HTTPS, языки XML, SAML. Примером SSO этого типа является система *Shibboleth*, разработанная сообществом Internet2;
- *системы входа на основе корпоративных сервисов*. Здесь под корпоративными сервисами понимаются все сервисы, не использующие веб-браузер в качестве пользовательского интерфейса, например сервисы мейнфреймов, баз данных и других корпоративных приложений. В частности к этому типу систем единого логического входа относится система Kerberos.

В зависимости от организационной принадлежности системы единого логического входа делятся на корпоративные и федеративные:

- в *корпоративной системе* все элементы – пользователи, провайдеры идентичности и сервис провайдеры - принадлежат одной организации, возможно – разным ее структурным отделениям;
- *федеративную систему* составляют различные организации, которые договорились доверять друг другу в отношении аутентификации своих пользователей. В общем случае каждая организация выполняет функции как провайдера идентичности, так и сервис- провайдера. Каждая организация поддерживает базу учетных записей своих пользователей, которая не реплицируется в другие организации. При необходимости доступа пользователя одной организации к сервису другой организации выполняется вторичная аутентификация с помощью определенного протокола, например RADIUS или Shibboleth. Федеративная аутентификация достаточно популярна в академической среде, примером федерации такого типа является федерация Eduroam, членами которой являются многие университеты и исследовательские центры Европы и Америки. В Eduroam используется иерархия серверов RADIUS, а доступ ограничивается только доступом пользователей к Интернет через беспроводные сети.

Существуют также ряд систем манипулирования паролями, которые лишь очень условно могут быть отнесены к системам единого входа. Эти системы, представляющие собой надстройку над традиционной децентрализованной инфраструктурой локальных баз учетных записей, помогают пользователю управляться с большим количеством паролей для разных сервисов. Рассмотрим три типа таких систем:

- системы кэширования паролей на стороне клиента:
- системы кэширования паролей на стороне сервера;
- системы синхронизации паролей между серверами.

Система кэширования паролей на стороне клиента хранит в надежном зашифрованном виде все пароли, которые были использованы пользователем при входе в тот или иной сервер. При повторном обращении к этому серверу она сама автоматически выполняет логический вход от имени пользователя. Вы, конечно, сталкивались с такой функцией, встроенной во многие браузеры, когда браузер предлагает вам запомнить пароль. Считается, что кэширование паролей на стороне клиента является весьма опасной практикой, так как злоумышленник в случае получения доступа к вашему компьютеру, сразу получает доступ к всем серверам и сервисам, которыми вы пользуетесь, в том числе и вашему банковскому счету.

Кэширование на стороне сервера означает, что все пароли пользователя хранятся централизованно, например на выделенном сервере предприятия. При логическом входе пользователя в корпоративную сеть кэш паролей временно загружается в его клиентский компьютер, а после окончания сессии работы с ним кэш уничтожается. Считается, что это более защищенный способ по сравнению с постоянным хранением кэша паролей на клиентском компьютере.

Программы синхронизации паролей между серверами помогают уменьшить разнообразие паролей пользователей в корпоративной сети и свести их в крайнем случае к одному, действительному для всех серверов сети.

Все три разновидности программ манипулирования паролями не ликвидируют главную причину необходимости выполнения многочисленных логических входов в различные системы – наличие большого количества локальных баз учетной информации пользователей. Из-за этого обстоятельства такие системы и не относят к системам единого логического входа специалисты-пуристы.