

Система усиленной аутентификации по отпечатку пальца

Постановка проблемы

- При обращении к публичным интернет-сервисам (web-почта, депозитарии файлов, социальные сети, и т.п.), имеющих традиционную систему входа Логин-Пароль, в ряде случаев у пользователей могут возникать проблемы, связанные с несанкционированным доступом посторонних к их персональным данным, хранящимся на удаленных серверах.
 - Модель угрозы: нарушитель знаком с пользователем и каким-либо образом похищает его пароль, не используя при этом изощренных средств.
 - Требования, предъявляемые к «защите от своих»:
 - простота в использовании, возможность выбора альтернативных способов усиления аутентификации;
 - возможность простого подключения в уже работающий сервис.
-

Предлагаемое решение с точки зрения пользователя

- 1) Легко устанавливаемый клиент, запускается вместе с Windows



- 2) Пользователь регистрируется на сайте: вводит пароль, который использовался до внедрения системы, логин и нажимает кнопку регистрации

Регистрация сервиса веб-аутентификации

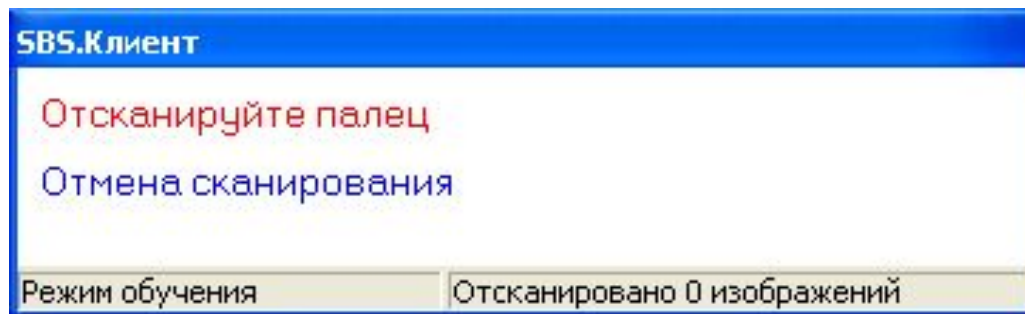
Введите логин, пароль и отсканируйте палец (клиент должен быть запущен!)

Логин

Пароль

Предлагаемое решение с точки зрения пользователя

- 3) Активируется клиент и предлагает отсканироваться



- 4) После сканирования модель отпечатка по защищенному каналу отправляется на сервер, регистрация успешно произведена

Регистрация

Регистрация прошла успешно!

Предлагаемое решение с точки зрения пользователя

5) При аутентификации работа сходная. Пользователь вводит свой логин. Логин может быть сохранен в cookies. И нажимает ссылку для входа

Вход по отпечатку

Введите ваши данные:

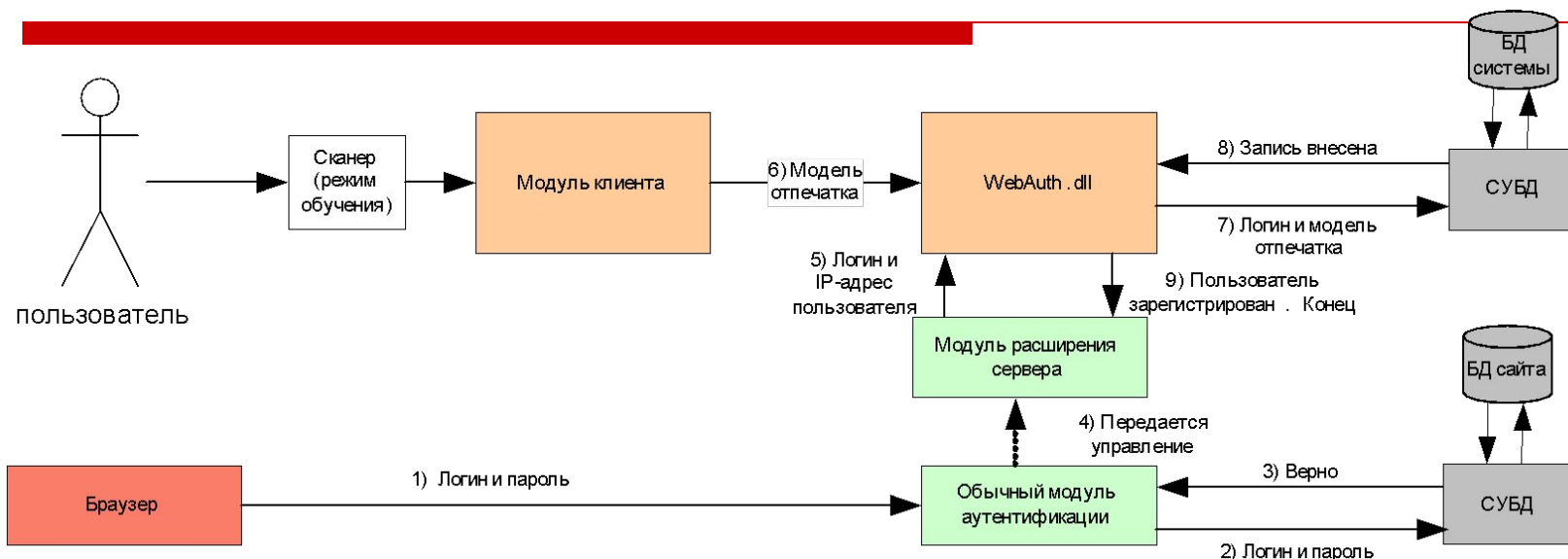
Login

6) Снова активируется клиент, вход успешно выполнен

Вход в систему

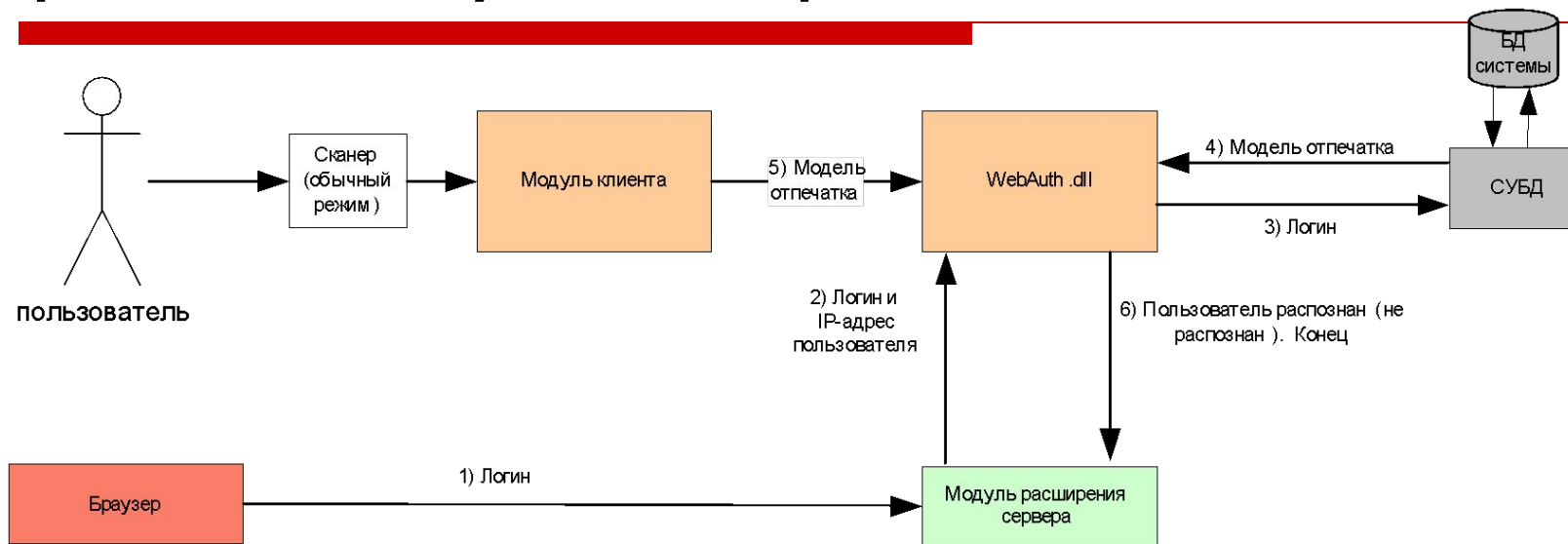
Добро пожаловать!

Предлагаемое решение, работа в режиме регистрации



- **Режим регистрации:**
- **1) Браузер передает логин и пароль, введенные пользователем, обычному модулю аутентификации сервера**
- **2,3,4) Модуль аутентификации сравнивает их с ранее сохраненными, и только в случае удачного результата разрешается подключать данный сервис (управление передается в модуль расширения сервера, работающий с WebAuth)**
- **5) Модуль расширения передает логин и IP-адрес пользователя в WebAuth (вызывая функцию регистрации)**
- **6) Модуль WebAuth.dll устанавливает связь с модулем клиента и принимает от него модель отпечатка**
- ~~**7,8,9) В БД вносится новая запись с логином и моделью отпечатка. Сервис подключен.**~~

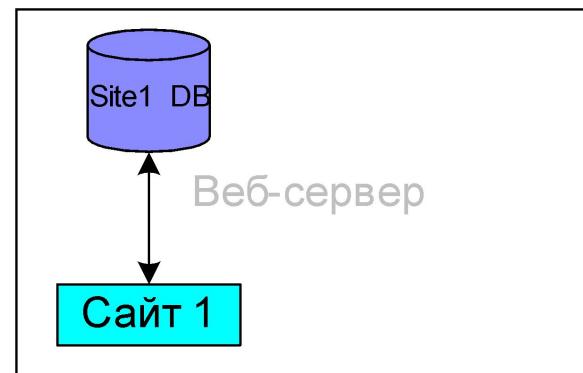
Предлагаемое решение, работа в режиме аутентификации



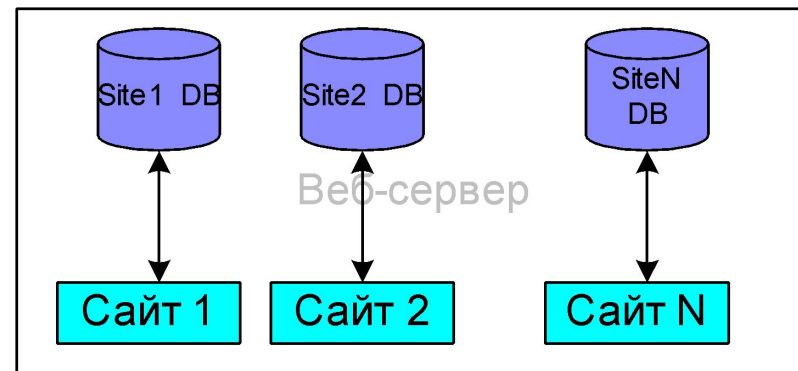
- ❑ **1) Браузер передает логин, введенный пользователем, модулю расширения сервера**
- ❑ **2) Модуль расширения сервера вызывает функцию из WebAuth.dll для аутентификации пользователя с данным логином и IP**
- ❑ **3,4) Модуль WebAuth.dll проверяет, что данный пользователь зарегистрирован, и читает ранее его сохраненную модель из БД**
- ❑ **5) Модуль WebAuth.dll устанавливает связь с модулем клиента и принимает от него модель отпечатка**
- ❑ **6) Модуль WebAuth.dll сравнивает две модели и возвращает результат модулю расширения сервера. Последний в зависимости от результата открывает пользователю вход или показывает страницу с сообщением об ошибке**

Варианты внедрения системы

- **Вариант 1.** На одном веб-сервере (и физическом и программном) размещен один сайт. Самый простой способ внедрения в этом случае – установить СУБД на ту же машину, БД сайта хранится также локально

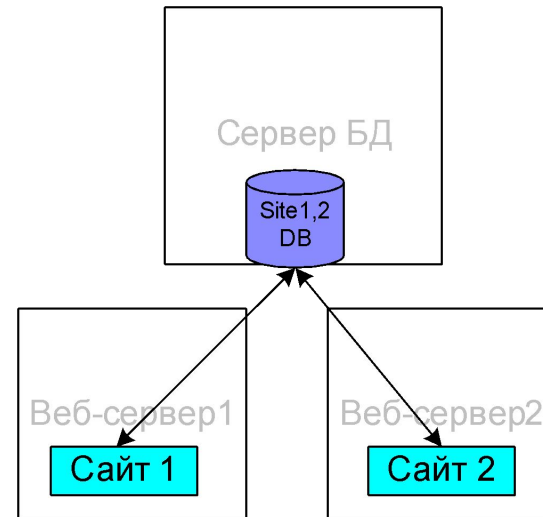
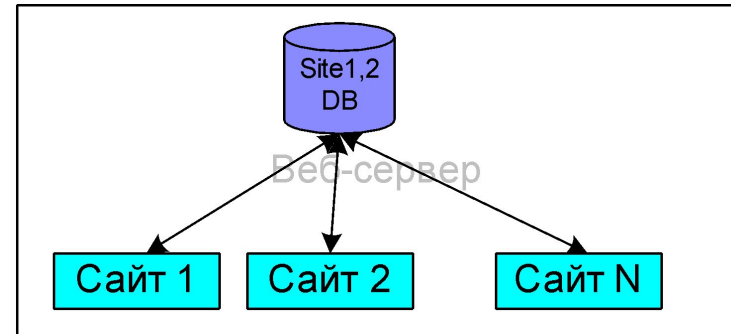


- **Вариант 2.** На одном веб-сервере размещено несколько сайтов. Сайты независимы, каждый использует свою БД. Достаточно установить одну СУБД локально, через нее обеспечить доступ к отдельным БД сайтов.



Варианты внедрения системы

- **Вариант 3.** На одном веб-сервере размещено несколько сайтов. Они образуют портал и компания, поддерживающая этот портал, желает, чтобы можно было использовать единственную учетную запись на всех. Устанавливаем локальную СУБД и всем сайтам обеспечиваем доступ к одной БД.
- **Вариант 4.** Сайты уже на физически разных машинах. Здесь используется сервер БД.



Достоинства системы

- Простота внедрения на сайте
 - Масштабирование средствами СУБД
 - Администрирование БД системы с помощью стандартных СУБД
 - Поддержка наиболее популярных СУБД
 - Простота установки и использования клиента
 - Надежность
 - Кроссплатформенная серверная часть
 - Совместимость с абсолютно любыми браузерами
 - Возможность применения в Internet и Intranet, в том числе для аутентификации не на сайтах
-

Области применения

Электронные платежные системы



Форумы

Доступ к ресурсам Инtranет

Социальные сети



Почта



Депозитарии файлов

