приложений. – URL: https://new-science.ru/huawei-privlekaet-razrabotchikov-v-svoj-magazin-prilozhenij/ (дата обращения 01.10.2022).

DOI: 10.25728/iccss.2022.52.24.018

Курако Е.А., Орлов В.Л.

Принципы обеспечения безопасности при использовании сервис-браузерной технологии

Аннотация: Рассматриваются вопросы защиты информации при использовании сервис-браузерной технологии. Выделяются уровни обеспечения безопасности. Определяется возможность использования сервис-браузера для защиты информационных систем.

Ключевые слова: сервис-браузер, клиент, сервер, средства защиты, безопасность, хранилище, аутентификация, авторизация

В качестве клиентов для информационных систем могут использоваться сервис браузеры [1, 2]. Сервис-браузер, в отличие от обычного браузера, имеет компонент, выполняющийся на клиенте (клиент браузера), и компонент (сервис браузера), выполняющийся на сервере (рисунок 1). Кроме того, на сервере (может быть отдельном) размещается хранилище данных браузера.

Причем каждый компонент включает три фрагмента.

- Фрагмент загрузки и обновления.
- Фрагмент обеспечения безопасности.
- Фрагмент организации запуска и завершения модулей.

В настоящей работе рассматривается фрагмент обеспечения безопасности, поэтому сосредоточимся на описании основных принципов, на которых базируется его разработка.

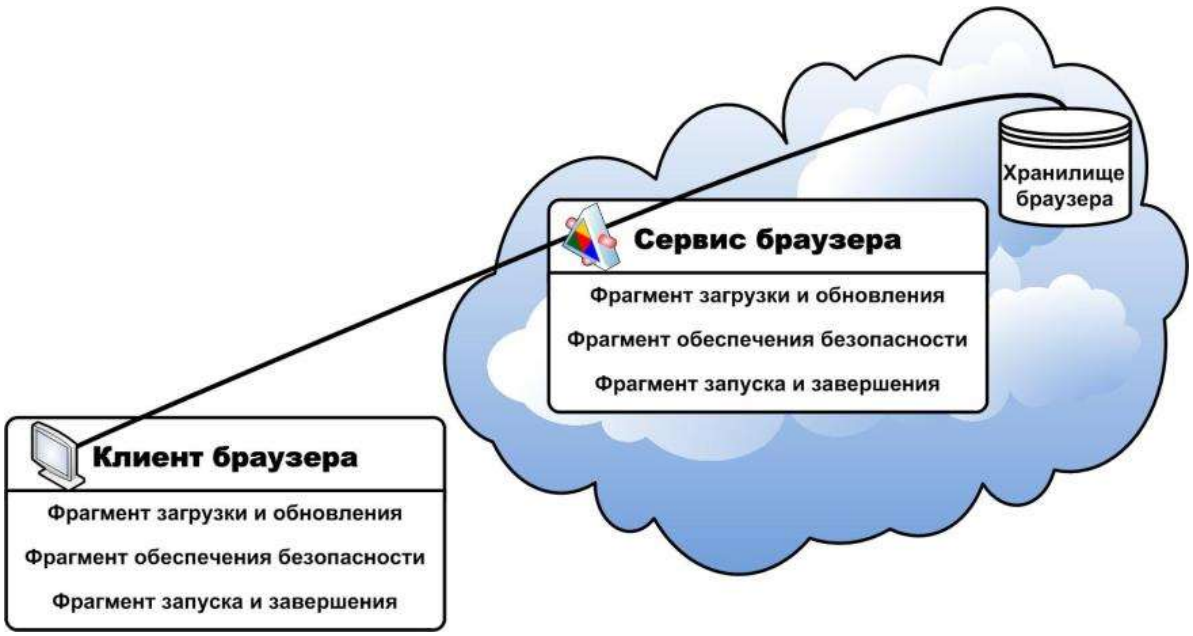

Рисунок 1 – Структура сервис-браузера

Ниже (рисунок 2) представлен краткий перечень базовых средств, использующихся при организации защиты информации в сервис-браузере.

Средства защиты клиента	Средства защиты сервера	Защита хранилища
Идентификация сеансов Авторизация Аутентификация HTTPS	Идентификация сеансов Авторизация Аутентификация HTTPS	Средства защиты БД

Рисунок 2 – Базовые средства защиты сервис-браузера

Так как фрагмент обеспечения безопасности присутствует как в клиентской, так и в серверной части, и более того, на клиенте и сервере существуют сопрягаемые средства, то для таких средств допускается различная реализация программного обеспечения. То есть, например, авторизация для различных сервис-браузеров может быть реализована по-разному, важно лишь то, что клиентские и серверные компоненты выполняют свои функции и хорошо сопрягаются друг с другом.

На нижнем уровне рекомендуется использовать HTTPS, так как существующие средства реализации протокола хорошо отлажены и обеспечивают высокий уровень защиты.

На следующем уровне проводится аутентификация, по существу, представляющая надежное определение пользователя. Обычно пользователь проверяется либо по сертификату, либо по паре «логин-пароль».

Если используется сертификат (чаще всего размещаемый на отдельном носителе), то обычно от сервиса получают случайную последовательность, подписывают ее электронной подписью и проверяют на сервисе. Если подпись верна, то из сертификата выбираются данные пользователя. Пользователь обычно имеет доступ к одной или нескольким информационным системам. Система может быть выбрана оператором из списка возможных.

Если на клиенте используется сочетание «логин-пароль» (вместе с идентификатором информационной системы), то эти данные следует проверить на сервисе. Для этого используется механизм хеширования. Как правило, на клиенте вычисляется хеш первого уровня, который определяется по значению строки, содержащей логин, пароль, константу. Затем формируется хеш второго уровня, где перед вычислением к хешу первого уровня добавляется значение текущего времени, и после вычисления – идентификатор информационной системы. Для передачи на сервер полученное значение обычно шифруется с использованием симметричного алгоритма.

На сервере путем расшифрования извлекается хеш. Из хранилища браузера также извлекается хеш первого уровня. Вычисляется хеш второго уровня с учетом времени и проводится сравнение хешей. Если сравнение прошло успешно, то по идентификатору системы определяется адрес системы. Таким образом, мы понимаем, какой пользователь к нам обратился, с какой информационной системой он хочет работать, и где располагается его система и пользовательская база данных этой системы.

То есть аутентификация завершена. Мы все, что необходимо, знаем о пользователе и его информационной системе.

Далее – авторизация. Мы на основании данных хранилища можем определить, какие пользовательские модули доступны обратившемуся к системе пользователю, какие действия он может

выполнять с использованием данных модулей. Таким образом, мы можем определить права данного пользователя относительно каждого приложения.

И наконец, очень важно, чтобы осуществленная аутентификация, проведенная авторизация действовали в течение определенного времени – сеанса пользователя. Отметим, что в рамках одного сеанса могут многократно вызываться сервисы, размещенные в серверной части. Если сеанс завершился, то для организации нового необходимо повторение процедур аутентификации и авторизации. И не только потому, что права пользователя за это время могли измениться. А главным образом потому, что каждое подключение к системе должно быть уникальным и санкционированным. То есть идентификатор сеанса должен формироваться с использованием криптосредств так, чтобы практически исключить возможность его вычисления со стороны злоумышленника. Идентификатор сеанса определяется в процессе проведении процедур аутентификации и авторизации и отменяется только при завершении сеанса.

Заметим, что для интеграции информационной системы с методами обеспечения безопасности сервис-браузера к каждому прикладному модулю должна подключаться клиентская библиотека, обеспечивающая взаимодействие со средствами защиты (получение параметров аутентифицированного пользователя, функции шифрования, дешифрования, обеспечения подписи). В каждом сервисе также происходит подключение к сервисной библиотеке, которая помимо обычных защитных функций обеспечивает строку подключения к хранилищу сервера, которое обычно реализуется как база данных.

Таким образом, сервис-браузер в процессе своей работы обеспечивает защиту информации для различных систем. Разработчики модулей таких систем не проектируют средства защиты, а только получают параметры при развертывании модуля для выполнения функций обеспечения безопасности и подключают соответствующие библиотеки сервис-браузера.

Литература:
1. *Курако Е.А., Орлов В.Л.* Сервис-браузеры для информационных систем // Программная инженерия. – 2017. – Том 8. №9. – С. 413-421.
2. *Курако Е.А., Орлов В.Л.* Организация защиты информации в системах, использующих сервис-браузеры / Материалы 26-й Международной научной конференции «Проблемы управления безопасностью сложных систем» (Москва, 2018). – М.: ИПУ РАН, 2018. – С. 109-112.

DOI: 10.25728/iccss.2022.61.68.019

Исхаков А.Ю.

Анализ запросов в протоколах прикладного уровня при реализации усиленной проверки подлинности субъектов доступа

Аннотация: При реализации эшелонированной защиты для критически важных объектов особое внимание уделяется снижению коэффициентов ложноположительных срабатываний средств защиты информации. В этой связи эффективным решением является разработка адаптивных многофакторных алгоритмов проверки подлинности, учитывающих особенности индикаторов компрометации и векторов предполагаемых атак в том числе в ходе инспектирования протоколов прикладного уровня. В рамках данного исследования рассматриваются признаки, доступные в ходе проведения инспекции HTTP-запросов при реализации усиленной проверки подлинности субъектов доступа.

Ключевые слова: протокол прикладного уровня, анализ запросов, индикатор компрометации, усиленная проверка подлинности, кибератака

В настоящее время в ходе инструментального анализа кибербезопасности различных объектов критической инфраструктуры исследователи продолжают фиксировать большое количество уязвимостей, связанных с интерфейсами доступа,