УДК 004.056.5

К ВОПРОСУ ОБЕСПЕЧЕНИЯ КОМФОРТНОСТИ ЗАЩИТЫ ПРИ УПРАВЛЕНИИ БИЗНЕС-ПРОЦЕССАМИ

С.С. Владимирова
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: vss@ipu.ru

Е.А. Курако
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: kea@ipu.ru

В.Е. Москальков
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: mve@ipu.ru

В.Л. Орлов
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: ovl@ipu.ru

Ключевые слова: защита информации, безопасность, пароль, аутентификация, комфортность защиты

Аннотация: Рассмотрена необходимость обеспечения комфортности защиты информационных систем, использующихся в малом и среднем бизнесе. Показана возможность организации удобного взаимодействия пользователей с программными комплексами при минимальных усилиях без снижения уровня безопасности.

1. Введение

По мере развития информационных технологий происходит повышение роли защиты. Действительно, первоначально программы работали на изолированной машине, доступ к которой обеспечивался посредством системного пароля, что во многих случаях было достаточным. В процессе эволюции информационные системы становились распределенными, строились на локальной сети, и уже такая конфигурация требовала повышенных мер защиты. Ввиду широкого распространения сети Интернет проектируемые программные комплексы стали использовать ее ресурсы, то есть передача данных начала производиться по общедоступным сетям. В этом случае, работа без серьезных мер обеспечения безопасности становилась фактически невозможной.

Вместе с тем, при возрастании роли защиты перед пользователем ставились все более сложные задачи. Он должен был формировать, запоминать, вводить длинные пароли, включающие различные типы символов (большие и малые буквы, цифры, другие знаки). Необходимо было получать закрытую ключевую информацию для формирования своей электронной подписи и открытую - для шифрования сообщений, направляемых своим корреспондентам. Пользователь должен был также обеспечивать другие меры безопасности, например, надежное хранение ключевой информации в то время, когда с ней не проводится работа.

Все это вместе становилось непростой задачей. Тем более, что в сферу обеспечения безопасности включались все новые участники, в том числе из среднего и малого бизнеса, которым было тяжело освоиться в этой новой для них области. Нужно также учитывать то обстоятельство, что дополнительные обязанности просто осложняли основную работу.

Поэтому появилась необходимость упрощения работы клиентов при организации управления бизнес-процессами без ущерба для безопасности, а в ряде случаев, когда это возможно – допустимого снижения требований, предъявляемых к защите. Некоторые из этих способов «удобной» (комфортной) защиты были рассмотрены в [1].

Рассмотрим некоторые дополнительные аспекты повышения комфортности работы средств обеспечения безопасности в системах малого и среднего бизнеса.

2. Отсутствие ввода пароля при входе

Отсутствие ввода пароля при входе, казалось бы, идеальный вариант в смысле комфортности, при котором не требуется ввода пары логин-пароль. Тогда становится непонятным, какой пользователь подключается к системе. Так как эта информация в большинстве случаев необходима, то вводится допущение, в соответствии с которым клиент ассоциируется с пользователем компьютера, то есть считается, что с данного рабочего места входить в систему могут только определенные лица, которые соответствуют пользователям компьютера и представились при входе. Программно всегда можно определить системные учетные данные пользователя и IP-адрес для входа данную сеть. А это значит, что при первом обращении всегда можно спросить логин и пароль сотрудника, входящего в информационную систему и запомнить эту пару вместе с парой IP-адрес и данные пользователя компьютера. Естественно, эту информацию необходимо хранить в закрытом виде. При обращении сотрудника к информационной системе всегда можно вычислить IP и идентификатор пользователя и по ним определить нужный логин и пароль.

Таким образом, при последующих обращениях к информационной системе вводить логин и пароль не потребуется. Но при этом нужно иметь уверенность, что доступ к данному компьютеру от имени определенного пользователя имеет только данное лицо.

3. Упрощенный пароль

Действительно, отсутствие пароля дает определенную комфортность. Вместе с тем, пользователь, стремящийся к комфорту может настроить свой компьютер таким образом, что и пользовательский пароль можно будет не вводить. Но тогда любой человек может загрузиться и осуществить вход в информационную систему от имени отсутствующего сотрудника. Также возможна ситуация, когда несколько человек работают за

одним компьютером. Чтобы избавиться от этого недостатка, возможно применение упрощенных паролей.

Упрощенный пароль может использоваться, так как он не передается по сети, не нужен при шифровании и подписании сообщений. Он, фактически, является ключом доступа к определенной информационной системе, но вместе с тем область его действия не выходит за пределы данного компьютера. Так как этот компьютер по определению не представляет собой общедоступное средство, то использование упрощенных паролей оправдано.

Упрощенный пароль для удобства обычно формируется из четырех-пяти цифр, не требует частого изменения и реализует доступ к информации, обеспечивающей сетевую безопасность.

4. Минимизация подготовки к шифрованию

Если раньше шифрование применялось в наиболее важных системах, относящихся к государственному сектору, то теперь в силу того, что информация обычно передается по общедоступным сетям, это средство практически используется во всех программных комплексах, даже относящихся к малому бизнесу. Но проблема состоит не в том, чтобы провести шифрование, а в том, чтобы провести подготовительную работу, которая во многом ложится на пользователя. Действительно, даже если взаимодействие идет между двумя точками, то необходимо для каждой из точек провести генерацию открытых и закрытых ключей, сохранить их, обеспечивая безопасность хранения, провести обмен открытыми ключами и также сохранить их. Обычно это делалось с использованием различных процедур, обеспечиваемых пользователем и структурами, его курирующими.

Рассмотрим упрощенный подход, основанный на том, что пользователь практически ничего не знает о подготовительном периоде. Естественно, этот процесс должен быть ориентирован в основном на коммерческие структуры и организации малого бизнеса, так как здесь могут не использоваться ограничения, характерные для систем государственного назначения.

При упрощенном подходе целесообразно использовать сеансовый способ обращения. Обычно сеанс начинается с сетевого соединения и завершается разъединением. На начальной стадии каждого сеанса проводится генерация пары ключей: закрытый и открытый ключи шифрования. Причем эта пара может храниться, зашифрованная на пароле, вычисляемом на основе упрощенного пароля. Далее открытый пароль шифрования посылается на сервер, а сервер, возвращает свой открытый пароль каждому обратившемуся к нему клиенту. Весь дальнейший процесс обмена информацией между любой парой «клиент-сервер» будет защищен. А нежелательные клиенты будут отсечены на основе использования механизмов аутентификации [1]. Например, для систем, использующих сервис-браузеры, аутентификация проводится в соответствии с [2,3].

Здесь важно то, что пользователь в процессе выполнения этого достаточно сложного алгоритма никак не задействован и его обязанности сводятся к вводу упрощенного пароля.

5. Пример использования упрощенного подхода в сервис-браузерной архитектуре

Для примера рассмотрим информационную систему, основанную на сервис-браузерной архитектуре [3]. Сервис-браузер при запуске аутентифицирует пользователя. Аутентификация может происходить с использованием упрощенного подхода. В результате сервис-браузер получает от сервера данные о созданном сеансе, например, идентификатор, время создания и период активности. Так же сервис-браузер устанавливает режим работы с сервером, по умолчанию это режим с шифрованием сообщений. Все дальнейшие обращения из прикладных программ к серверу происходят с использованием полученных параметров. Таким образом, средства защиты с одной стороны унифицируются для разных прикладных систем, с другой стороны становятся более простыми как для пользователей, так и для программистов прикладных систем.

При организации взаимодействия с сервером, клиентское программное обеспечение, как правило, помещает техническую информацию о сеансе в заголовке отправляемого запроса.

Приведем пример формирования заголовков передаваемых пакетов к прикладному сервису на языке C# с использованием платформы WCF[4]. В момент открытия соединения с сервером в заголовок встраивается информация о сеансе, полученная от сервис-браузера (или самостоятельно):

```
var ea = new EndpointAddress("http://Server/Service/service.svc");
var eab = new EndpointAddressBuilder(ea);
eab.Headers.Add(AddressHeader.CreateAddressHeader("ClientId",
string.Empty, info));
var ourService = new ServiceClient(new WSHttpBinding(),
eab.ToEndpointAddress());
```

На стороне сервера полученная информация разбирается и проверяется на корректность.

Как уже сказано, все передаваемые данные шифруются в соответствии с настройками. Сервис-браузер обеспечивает работу со средствами защиты в различных режимах, например, режим зашифрованных данных или полностью открытый режим. Прикладное программное обеспечение, которое обеспечивает выдачу запросов и обработку ответов, остается неизменным.

6. Заключение

Таким образом, даже при существующих непростых методах защиты информации возможно обеспечение достаточно комфортного способа взаимодействия с пользователями при организации управления бизнес-процессами без снижения уровня обеспечения безопасности. При этом основными из них являются методы использования упрощенного пароля и минимизации процесса подготовки к шифрованию.

Список литературы

1. Козлов А.Д., Орлов В.Л. Методы и средства обеспечения информационной безопасности распределенных корпоративных систем. М.: ИПУ РАН, 2017. 156 с.

2. Курако Е. А., Орлов В. Л. Способ организации взаимодействия клиента с сервером приложений с использованием сервис-браузера: Патент на изобретение RU 2656735 C1; Зарегистрирован 06.06.2018. Заявлено 17.05.2017. Опубликовано: 06.06.2018. Бюллетень № 16.
3. Курако Е.А., Орлов В.Л. Сервис-браузеры для информационных систем // Программная инженерия. 2017. Т. 8, № 9. С. 413-421.
4. Сибраро П., Клайс К., Коссолино Ф., Грабнер Й. WCF 4: Windows Communication Foundation и .NET 4 для профессионалов. М.: Диалектика, 2011. 464 с.