С. С. Агафьин

ОБЕСПЕЧЕНИЕ ДОВЕРЕННОСТИ КЛИЕНТСКОЙ СТОРОНЫ В СИСТЕМАХ ИНТЕРНЕТ-БАНКИНГА ПУТЕМ ИСПОЛЬЗОВАНИЯ ОТЧУЖДАЕМЫХ НОСИТЕЛЕЙ КЛЮЧЕВОЙ ИНФОРМАЦИИ

Все большее и большее число банков предлагают своим клиентам повысить безопасность совершения транзакций через Интернет путем использования электронных ключей (USB-токенов). Однако использование данных устройств в качестве обычных отчуждаемых носителей ключевой информации (ОНКИ) не позволяет исключить все проблемы безопасности.

В классической схеме реализации систем дистанционного банковского обслуживания (ДБО), использующих отчуждаемые носители ключевой информации, генерацию запроса к носителю, формирование APDU-команды и обработку ответа выполняет прикладное программное обеспечение клиентского терминала. В случае отсутствия доверия к нему, например, при наличии возможности заражения системы вредоносным программным обеспечением, данный подход не позволяет говорить о даже небольшом преимуществе над обычными парольными схемами аутентификации. Как показано в исследовании [1], вредоносное программное обеспечение способно самостоятельно проводить взаимодействие с электронным ключом, минуя системы защиты.

Таким образом, можно сделать вывод, что в системах ДБО следует использовать лишь носители ключевой информации, способные самостоятельно выполнять криптографические преобразования.

Ряд производителей ОНКИ предлагают в качестве решения данной проблемы использование защищенного обмена сообщениями. Однако такой обмен является протоколом низкого уровня, в то время как ключевая проблема безопасности находится на верхнем. Этот подход позволяет исключить лишь угрозы, связанные с находящимися в системе отладчиками APDU-команд, однако если предположить, что нарушитель способен запускать в системе клиента любое программное обеспечение, то ему ничего не помешает запустить активное вредоносное ПО, которое позволит выполнить операции более высокого уровня абстракции.

Единственным решением, не усложняющим схему системы безопасности и не требующим от пользователя длительных процедур (например, перезагрузки системы для использования модулей доверенной загрузки), является предельное сокращение участия клиентского терминала в процессе аутентификации и проведения платежа.

Простейшую схему, реализующую данный подход, можно представить в следующем виде.

ОНКИ хранит в защищенной памяти собственный закрытый ключ аутентификации и открытый ключ банка, к которому осуществляется подключение. Банковские центры обработки информации хранят открытые ключи выданных клиентам носителей ключевой информации и имеют доступ к закрытому ключу банка.

Работа с банком начинается с установления сеансового ключа симметричного шифрования по следующему протоколу.

1) Клиентский терминал отправляет на ОНКИ запрос о подключении к серверу.

2) ОНКИ передает аутентификационную информацию (например, параметры алгоритма Диффи—Хеллмана, случайное число и метку времени), подписанную собственным закрытым ключом.

3) Клиентская сторона прозрачно транслирует эти сведения на банковскую сторону, так как их целостность гарантируется использованием ЭЦП.

4) Банк выполняет проверку полученных сведений, генерирует собственные аутентификационные данные (например, согласие на использование заданных параметров Диффи—Хеллмана и результат выполнения первого шага данного протокола), подписанные собственным закрытым ключом.

5) Клиентская сторона прозрачно транслирует эти сведения на ОНКИ, так как их целостность гарантируется использованием ЭЦП.

6) ОНКИ завершает протокол установки сеансового ключа (возможно, потребуется отправка дополнительного сообщения банку).

При корректном завершении данного протокола между ОНКИ и банком устанавливается защищенный канал связи, который исключает возможность внешнего воздействия в силу использования симметричного алгоритма шифрования команд. Однако все еще остается проблема с передачей команд на носитель ключевой информации, а именно с аутентификацией дальнейших запросов пользователя.

Единственным решением данной задачи видится использование устройств визуального контроля подписи. В таком случае схема взаимодействия пользователя и банка после установления защищенного обмена сообщениями представляется в следующем виде.

1) Пользователь составляет в обозревателе Интернета запрос к банку (платежное поручение, запрос сведений о счете и т. п.).

2) Данный запрос передается на устройство визуального контроля, которое выводит основные реквизиты на собственный дисплей.

3) В случае достоверности приведенных сведений пользователь подтверждает дальнейшую обработку этой информации в ОНКИ.

4) ОНКИ на основе полученного запроса от средства визуального контроля генерирует запрос к банку, который зашифровывается по симметричному алгоритму и прозрачно передается на серверную сторону.

5) На банковской стороне происходит расшифрование полученных сведений, выполнение команды и генерация ответа.

6) Ответное сообщение прозрачно проходит на ОНКИ, где оно расшифровывается и возвращается в пользовательский интерфейс.

Однако, несмотря на кажущуюся эффективность решения, остается ряд нерешенных проблем. Все операции, выполняемые на аппаратной части клиентской стороны, исходят из предположения абсолютной доверенности данных компонентов. Тем не менее существуют исследования [2], показывающие, что реализации протоколов работы с устройствами визуального контроля в ряде случаев могут быть далеки от идеала и их роль путем определенных действий злоумышленника может быть сведена к тривиальным считывателям.

Также существенная проблема возникает при использовании отчуждаемых носителей ключевой информации. При определенных условиях злоумышленник может провести успешную атаку (например, при использовании побочных каналов утечки информации [3]), которая может привести к компрометации закрытого ключа аутентификации, на конфиденциальности которого строится вся предложенная схема.

Общее решение данных проблем аппаратных средств пока не представлено в открытых источниках и требует дополнительных исследований.

СПИСОК ЛИТЕРАТУРЫ:

1. *Mostowski W., Poll E.* Malicious Code on Java Card Smartcards: Attacks and Countermeasures // LNCS. 2008. Vol. 5189. P. 1–16.
2. *Blom A., Gans G., Poll E., Ruiter J., Verdult R.* Designed to Fail: A USB-Connected Reader for Online Banking // LNCS. 2012. Vol. 7617. P. 1–16.
3. *Wang D., Ma C.* On the security of two smart-card-based remote user authentication schemes for WSN // Cryptology ePrint Archive. Report 581. 2012. URL: http://eprint.iacr.org.