Интернет-банкинг Беларуси: проблемы безопасности данных

Шавель О. А., студ. II к. БГЭУ,
науч. рук. Вашкевич Ю. Б., магистр эк. наук, ассистент

Система интернет-банкинга стала неотъемлемой частью услуг, предоставляемых сегодняшними банковскими системами. Данный вид сервиса отличает очевидное удобство в использовании: совершение платежей доступно в режиме онлайн. В то же время он имеет серьезнейший недостаток — отсутствие гарантий конфиденциальности передаваемых данных в web-сети. Следовательно, банк, предоставляя услуги интернет-банкинга, «играет в рулетку»: либо обеспечивает надежный сервис, либо теряет доверие клиентов в случае утечки их персональных данных.

Под персональными данными подразумеваются логин и пароль, используемые клиентом для входа в систему. Если они становятся доступными для хакера, взломщик может от имени легального пользователя распоряжаться его денежными средствами. Существует множество способов взлома пользовательских данных. Наиболее популярные из них: снифинг, фишинг, и как разновидность последнего скаминг. Суть снифинга состоит в перехвате трафика «жертвы», а точнее генерируемых браузером HTTP-запросов, содержащих данные клиента: логин и пароль. Фишинг заключается в подделке страниц авторизации: пользователь, попав на фальшивую страницу, принимает ее за настоящую и вводит свои данные. Отличие скаминга от фишинга в том, что подделывается не одна страница, а весь сайт, в точности копирующий оригинал. Использование одноразовых паролей в описываемых случаях не обеспечивает сохранности данных.

Безусловно, современные банки оснащены средствами защиты от перечисленных выше способов атаки. В первую очередь, это передача данных с использованием криптографического SSL — протокола. Он предотвращает попытки перехвата сетевого трафика, так как информация передается в зашифрованном виде. Сегодня большинство интернет-банков Беларуси использует протоколы защищенной передачи данных.

Однако приведенного способа защиты может оказаться недостаточно. Проблема возникает в случае MitM-атаки (Man-in-the-middle attack) — ситуации, когда между сервером и клиентом в момент передачи данных оказывается некто посередине. Для того чтобы этого избежать, системы интернет-банкингов помимо шифрованного соединения устанавливают SSL-сертификаты, подтверждающие подлинность сервера. Их использование позволяет защитить данные не только от атаки «посередине», но также фишинга и его разновидностей.

SSL-сертификаты подписываются удостоверяющими центрами (certificate authority). На сегодняшний день лидером на рынке SSL-услуг является американская компания VeriSign, Inc. Среди белорусских систем интернет-банкинга

(Беларусбанк, Москва-Минск, Белагропромбанк, Белсвиссбанк) широко распространено сотрудничество с Thawte — дочерней компанией VeriSign. В среднем, белорусским банкам приобретение заверенного Thawte сертификата сроком на два года обойдется в $259-1199. Цена варьируется в зависимости от типа сертификата: от стандартного до принудительно высокого уровня шифрования (SGC). Последний используется, к примеру, в системе аутентификации сервера Белгазпромбанка.

В июле 2011 года хакерами был выпущен 531 поддельный сертификат удостоверяющего центра DigiNotar. Фальшивые сертификаты использовались как на ресурсах интернет-магазинов, так и спецслужб США, Израиля и Великобритании. Данный пример ошеломляющей атаки схож с продемонстрированной на конференции Chaos Communication Congress в 2008 году 100% уязвимостью сертификатов SSL, имеющих корректную подпись удостоверяющего центра (Central Authority). Оба случая доказывают отсутствие гарантированной защиты данных даже при использовании SSL-сертификата. Возможность его взлома объясняется проблемами хеширования данных еще до шифрования. Так, компания VeriSign отказалась от использования алгоритма хеширования MD5 для подписи сертификатов именно по причине его нестойкости к коллизиям — ситуациям, когда два разных сообщения дают одинаковый хеш. К счастью, ведущие банки страны заверены сертификатами, подписанными более надежным алгоритмом SHA-1. Это уменьшает риск взлома системы, однако также не дает стопроцентной гарантии, так как MD5 и SHA-1 реализуют одинаковую структуру построения хеш-функции и, вероятно, в скором времени SHA-1 окажется не менее уязвим.

Также сохранность сертификата обеспечивается использованием аппаратных ключей eToken (Белгазпромбанк) в виде смарт-карт или USB-устройств, необходимых для проверки его валидности. Этот способ защиты предотвращает не только возможность подделки сертификата, но и частично вирусные атаки.

К сожалению, на сегодняшний день не существует фундаментальной защиты от вирусных атак. В отличие от остальных приемов взлома, вирусы способны обойти любой защитный механизм! Единственным решением может послужить полная изоляция системы от внешней сети, однако такой исход событий мало приемлемый для обеих сторон: клиентов и банка.

Уровень защищенности современных банковских систем Беларуси можно считать варьируемым: одни используют схему «по умолчанию» (логин, пароль, сеансовый ключ), другие прибегают к более надежным средствам. При выборе банка, предоставляющего услуги интернет-банкинга, необходимо учитывать, каким центром подписан сертификат, вид сертификата, использование дополнительных средств защиты. На данный момент сотрудничество с надежным центром сертификации является максимально эффективным методом обеспечения безопасности данных.