УДК 336.717

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ РАСЧЕТОВ, СОВЕРШАЕМЫХ В ИНТЕРНЕТ-БАНКИНГЕ

Трембицкий Я.С.,
студент, Финансовый университет, Москва, Россия
ork-voodoo@inbox.ru

Аннотация. *На сегодняшний момент использование технологии безналичного расчета с применением пластиковых карт является одной из самых перспективных и востребованных технологий. Однако, как показывает практика, эти технологии должны быть надежно защищены. Целью данной статьи является изучение видов атак на кредитные организации и способы повышения безопасности расчетов.*

Ключевые слова: *расчеты; типы атак; 3D-Secure; SecurID; TLS; информационная безопасность.*

THE IMPROVEMENT OF THE SECURITY OF PAYMENTS MADE THROUGH INTERNET BANKING SYSTEM

Trembitskiy Y.S.,
student, Financial University, Moscow, Russia
ork-voodoo@inbox.ru

Abstract. *Nowadays cashless payment with the use of plastic cards is one of the most prospective and popular technologies. However, experience has shown that these technologies should be well protected. The present article aims to study the types of attacks on credit institutions and the ways to improve security of payments.*

Keywords: *payments; types of attacks; 3D-Secure; SecurID; TLS; information security.*

Введение

Нашу жизнь трудно представить без современных технологий. В любой сфере деятельности человека мы используем разные технологии, это касается и банковских операций, сделок и взаимных платежей, которые трудно представить без расчетов с применением пластиковых карт. Электронная платежная система — это система безналичных расчетов, в том числе и с помощью пластиковых карт. В настоящее время технология безналичного расчета с применением пластиковых карт весьма востребована и постоянно развивается. Следует отметить, что данный вид расчетов наиболее перспективный с точки зрения возможностей, удобства и простоты для физических лиц. По статистике, уже сегодня каждый 15-й житель России оплачивает различные услуги при помощи технологии безналичного расчета с применением пластиковых карт [1].

Научный руководитель: ***Курило А.П.,*** *доцент кафедры информационной безопасности, кандидат технических наук, факультет АРиЭБ.*

Классификация и проблемы

В связи с тем, что терминология считается неустоявшейся в этой сфере, четких рамок определений нет. Но на данный момент системы электронных платежей можно разделить на следующие:

- системы моментальных платежей;
- системы онлайн-банкинга (дистанционное банковское обслуживание);
- электронные платежные системы (ЭПС).

Главная отличительная черта электронных платежных систем от моментальных состоит в том, что в ЭПС в качестве расчетной единицы выступает электронная конвертируемая валюта, которую различные операторы конвертируют в реальные деньги по определенному курсу (например, система WebMoney, Яндекс.Деньги).

Для нормального функционирования электронная платежная система должна быть надежно защищена. С точки зрения информационной безопасности в системах электронных платежей для операций существуют следующие риски:

- использование незащищенных гаджетов;
- использование ненадежно защищенных каналов связи и другие [2].

Все это создает следующие проблемы:

- обеспечения целостности документов, передаваемых по каналам связи;
- обеспечения конфиденциальности;
- обеспечения взаимной аутентификации абонентов;
- обеспечения легальности операций, совершаемых в системе.

Методы решения проблем, деятельность FinCERT

Для решения изложенных проблем должны создаваться специальные структуры, центры. Роль данных структур, которые будут оповещать другие организации, будет достаточно высока.

FinCERT — это как раз центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, он является структурным подразделением Банка России. При создании данного подразделения предполагалось, что оно будет оказывать информационное взаимодействие Банка России, кредитных и некредитных финансовых организаций, разработчиков антивирусного ПО, провайдеров и операторов связи, а также для правоохранительных и иных государственных органов, занимающихся информационной безопасностью данной отрасли. Указанное взаимодействие направлено на обмен информацией о потенциальных компьютерных атаках в кредитно-финансовой сфере, актуальных угрозах и уязвимостях ПО.

На конец мая 2016 в информационном обмене с FinCERTом участвовали 275 различных кредитных организаций и филиалов. Также FinCERT осуществляет информационный обмен с правоохранительными органами. При необходимости сотрудники FinCERT выступают в качестве экспертов, если просят правоохранительные органы. При получении сообщения об угрозе FinCERT проводит анализ, по результатам которого выполняет рассылку информационного бюллетеня[1]. Статистика по количеству разосланных бюллетеней приведена на *рис. 1*.

Какие же существуют типы атак?

- Целенаправленные атаки, связанные с подменой входных данных для АРМ КБР.
- Рассылки электронных сообщений, содержащих вредоносное ПО.
- Атаки, направленные на устройства самообслуживания.
- DDoS-атаки.
- Reversal-атаки.

Также отдельно стоит выделить атаку на самого клиента путем социальной инженерии. Прекрасно понимая, что многие обладатели пластиковых карт, владельцы электронных кошельков не совсем компетентны в этой сфере, мошенники смещают вектор атак именно в эту сторону. Как известно, против социальной инженерии практически нет эффективных технических способов противодействия, следовательно, атаки на клиента путем социальной инженерии очень серьезная проблема.

Приведем краткую информацию об атаках данного типа.

1. Целенаправленные атаки, связанные с подменой входных данных для АРМ КБР.

[1] FinCERT. (2016). Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России.

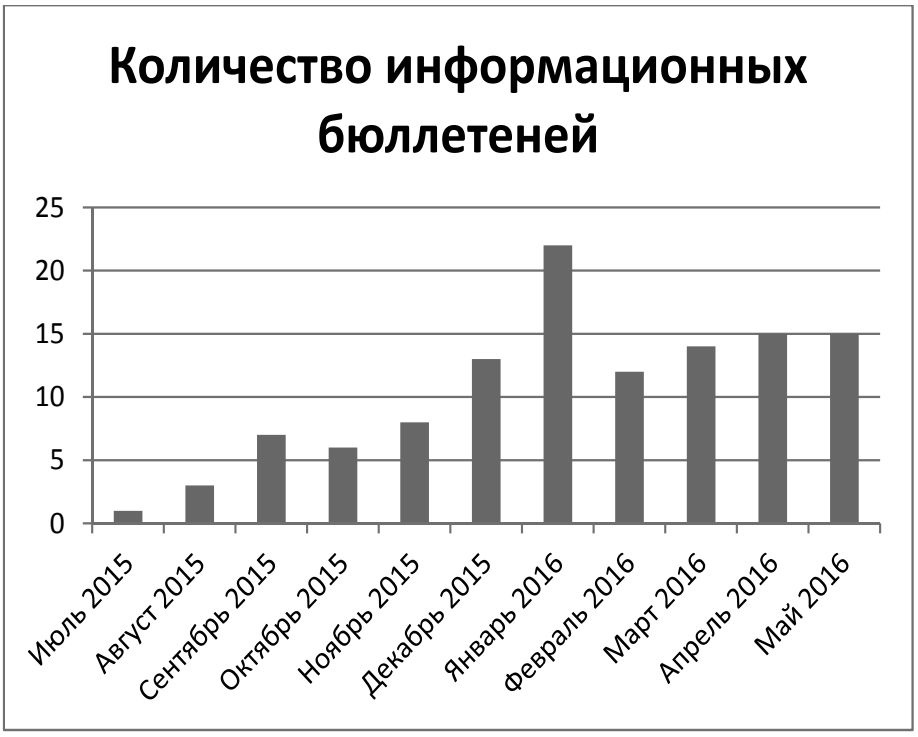

Рис. 1. **Статистика FinCERT по информационным бюллетеням**

Под целенаправленной атакой понимается компьютерная атака, ориентированная на использование конкретных, известных злоумышленникам уязвимостей в информационной инфраструктуре организаций.

FinCERT смог зафиксировать значительное число атак, связанных с подменой входных данных для АРМ КБР. За период с октября 2015 г. по март 2016 г. организацией FinCERT была зафиксирована 21 атака на инфраструктуру кредитных организаций. Злоумышленники попытались похитить денежные средства на общую сумму порядка 2,85 млрд руб. При этом предотвращено хищение порядка 1,6 млрд руб.

2. Рассылки электронных сообщений, содержащих вредоносное ПО, наиболее распространенный тип атак. Во вложении к письму обычно прикрепляют исполняемый файл, который замаскирован под документ, или файл, который содержит макровирусы. По данным на май 2016 г., наиболее массовая доля рассылок приходится на вредоносное программное обеспечение типа Trojan.Downloader,

3. Атаки, направленные на устройства самообслуживания.

FinCERT также зафиксировал рост интереса мошенников к устройствам самообслуживания, не только к банкоматам, но и POS-терминалам. При реализации данных атак, которые были направлены на банкоматы, злоумышленники попытались похитить денежные средства на общую сумму свыше 99 млн руб.

4. DDoS-атаки.

Для DDoS-атак главной целью является отказ в обслуживании легитимных клиентов, вплоть до полной невозможности работы с сервисом. В некоторых случаях DDoS-атака используется для того, чтобы скрыть факт целенаправленной атаки.

5. Reversal-атаки.

FinCERT зафиксировал атаку с использованием подложных сообщений об отмене платежной операции (reversal). Атака связана с особенностью обработки сообщений об отмене авторизации переводов денежных средств процессинговым центром. В основном процессинговые центры не проверяют подлинность подобного запроса в связи с отсутствием контроля ряда полей указанной операции[2].

[2] FinCERT. (2016). Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России.

Предлагаемые способы решения проблемы

Все эти атаки в основном программно-аппаратного происхождения, поэтому и противодействия им немного проще и более известны, нежели в случае атак на клиента. Что же мы можем предложить?

В-первую очередь это, конечно, обучение держателей карт минимальным навыкам для обеспечения собственной безопасности. Самое главное, что надо помнить — это никогда и никому не передавать данные о своей карте.

Кроме такого простого метода защиты от мошенников, безусловно, необходимо использовать и технологические средства.

Весьма удобным способом повышения безопасности является постановка клиента на SMS-оповещения совершаемых операций. Это дает возможность информировать клиента о всех операциях по его карточным счетам, в том числе и об операциях, совершаемых без его ведома, т.е. мошеннических операциях. Тогда возникает вопрос надежности передачи сведений по каналу оповещений, так как SMS-канал не является доверенным. Он не шифруется, и факт передачи информации не подтверждается отправителем, поэтому возможны мошеннические действия, связанные с подменой адреса. Это отдельная задача, требующая своего решения.

Другим способом повышения безопасности в случае взаимосвязи клиента с банком по IP протоколу использование протокола SSL — он надежно защищает информацию, передаваемую через Internet. Протокол SSL использует технологию шифрования с открытым ключом и цифровые сертификаты для опознания сервера, участвующего в транзакции, и защиты информации в процессе ее передачи от одной стороны к другой по каналам Интернета. Данный протокол SSL использует импортные алгоритмы шифрования, не считающиеся надежными, что создает риски утраты конфиденциальности. В связи с этим лучше использовать протокол TLS, который использует российские алгоритмы шифрования.

Также, помимо использования протокола шифрования, используют такие известные способы идентификации держателя карты, как проверка CVV2/CVC2-кодов. Следует отметить, что этот метод обеспечивает высокий уровень безопасности клиента только в том случае, если канал закрыт протоколом SSL или TLS, а также организация строго следует стандарту PCI DSS[3]. К сожалению, все эти меры безопасности недостаточны для обеспечения высокого уровня безопасности расчетов в сети Internet. Доля мошеннических операций растет, и пока не будет хорошей защиты, эта доля уменьшаться не будет.

Против социальной инженерии практически нет эффективных технических способов противодействия, следовательно, атаки на клиента путем социальной инженерии очень серьезная проблема.

Еще одним методом повышения безопасности может являться 3D-Secure. Данная технология позволяет обеспечивать более надежный уровень проверки подлинности пользователя по сравнению с многократно используемыми паролями. В качестве инструмента может быть использована SecurID — технология выработки синхронного одноразового пароля.

На мой взгляд, данная технология весьма хороша, поскольку, если наш логин и пароль скомпрометирован, то вероятность того, что еще дополнительный код будет скомпрометирован, очень мала. Как же работает данная технология?

При запросе пользователя доступа к ресурсу вместо стандартного приглашения на ввод логина и пароля запрашивается логин и дополнительный одноразовый код. Пользователю необходимо после ввода своих данных (логина и пароля) ввести дополнительный код,

[3] Payment Card Industry Security Standards Council, PCI SSC. Payment Card Industry (PCI) Data Security Standard (DSS). Получено из http://www.pcidss.ru/: http://www.pcidss.ru/files/pub/pdf/2_PCI_DSS_v3%20EN.pdf.

который генерируется в настоящее время и будет известен только нам.

Предоставленную пользователем информацию агент передает на сервер в зашифрованном виде. В сервере хранятся пин-коды пользователей и программные копии всех зарегистрированных токенов, соответственно он может проверить предоставленную пользователем информацию.

Весьма удобным способом повышения безопасности является постановка клиента на SMS-оповещения совершаемых операций.

В зависимости от результата проверки агент либо предоставляет пользователю доступ к ресурсу, либо отказывает ему в доступе.

Но и данная технология по генерированию дополнительного пароля не дает 100%-ной защиты. Возможные уязвимости данной технологии описаны ниже:

Технология не защищена от атак вида man-in-the-middle. Мошенник может заблокировать для пользователя доступ и подключиться к серверу, пока следующий токен-пароль не сгенерирован.

Другой проблемой является случайный подбор пароля. Данную проблему пытаются решить с помощью ограничения количества запросов на аутентификацию в течение определенного временного промежутка, на котором пароль не сгенерирован заново.

Самой опасной и почти неустранимой уязвимостью является потеря или кража токенов. В данном случае придется блокировать свою карту и восстанавливать не только карту, но и токен.

Несмотря на изложенные риски, на практике технология 3D-Secure является достаточно надежной и может быть использована, так как риски реализации приведенных угроз в настоящее время невысоки. Однако, помимо вышеуказанных процедур, которые, на мой взгляд, смогут повысить безопасность расчетов, совершаемых в интернет-банкинге, вполне возможно потребуется внесение некоторых изменений в законодательство.

Заключение

На сегодняшний день проблема повышения безопасности расчетов, совершаемых в интернет-банкинге, актуальна. Как мы видим, создаются структуры, отвечающие за безопасность, предлагаются различные способы повышения безопасности, происходит обмен данным между организациями. Но самый главный, на мой взгляд, путь решения проблемы — это повышение грамотности российских граждан в вопросах безопасности, а также повышение защищенности с помощью подтверждения операций и авторизации клиента одноразовым паролем. Инициатива обучения должна осуществляться со стороны оператора платежной системы, правительства и ЦБ РФ, а со стороны пользователя должно быть осознание рисков и желание обучаться. В таком случае решение будет эффективным, и, как следствие, уменьшится общий уровень мошенничества.

Список источников

1. *Васильев В.В.* (2013). О безопасности электронных платежей. PCWEEK. URL: https://www.itweek.ru/security/article/detail.php? ID=148477 (дата обращения: 10.05.2017).
2. *Колесников Д.Г.* Безопасность электронных платежных систем. URL: http://protect.htmlweb.ru/pcard.htm (дата обращения: 12.05.2017).
3. Пухарева Е. (2015). Безопасность электронных платежей как объект правового регулирования. Information Security // Информационная безопасность. № 6. С. 62–63.