Равинская Т.Ю.
УО «Белорусский государственный экономический университет» (Минск)

БЕЗОПАСНОСТЬ ПЛАТЕЖЕЙ С ИСПОЛЬЗОВАНИЕМ ПЛАСТИКОВЫХ КАРТ В СЕТИ ИНТЕРНЕТ

Предоставление банковских услуг через Интернет является одним из наиболее динамичных сегментов электронной коммерции, который продолжает развиваться стремительными темпами вместе с ростом числа пользователей Сети. Одновременно с увеличением аудитории растет и количество клиентов, осуществляющих банковские операции через Интернет.

Лидирующее положение среди существующих платежных систем занимают системы на основе пластиковых карт. Успех применения пластиковых карт для расчетов в Интернете связан с привычностью такого вида оплаты, во многом схожего с оплатой в реальном мире.

Однако высокий уровень мошенничества в Интернете является сдерживающим фактором развития электронной коммерции, поскольку покупатели, торговля и банки боятся пользоваться этой технологией из-за опасности понести финансовые потери. Приведем классификацию возможных типов мошенничества через Интернет:

- транзакции, выполненные мошенниками с использованием правильных реквизитов карточки (номер карточки, срок ее действия и т. п.);
- компрометация данных (получение данных о клиенте через взлом баз данных торговых предприятий или путем перехвата сообщений покупателя) с целью их использования в мошеннических целях;
- магазины, возникающие на непродолжительное время, для того чтобы исчезнуть после получения от покупателей средств за несуществующие товары;
- злоупотребления торговых предприятий, связанные с увеличением стоимости товара по отношению к предлагавшейся покупателю цене или повтором списаний со счета клиента;
- магазины и торговые агенты, предназначенные для сбора информации о реквизитах карт и других персональных данных покупателей.

Обычно в рамках подобной классификации фигурирует еще пункт "Информационные сайты". Речь идет о сайтах, помогающих всевозможными рекомендациями и даже программными средствами совершить мошенническую транзакцию.

Первый тип мошенничества является наиболее массовым. Для совершения транзакции мошеннику обычно достаточно знать только номер карты и срок ее действия. Такая информация попадает в руки мошенников различными путями. Наиболее распространенный способ получения мошенниками реквизитов карт - сговор с сотрудниками торговых предприятий. Торговые предприятия, через которые проходят сотни и тысячи транзакций по пластиковым картам, зачастую хранят информацию о реквизитах карт в своих базах данных или на слипах (бумажных документах, подтверждающих факт совершения в торговых предприятиях транзакции). Результатом сговора становится передача

информации о реквизитах карт в руки криминальных структур.

Другой способ получения информации о реквизитах карт - кража баз данных карточек в торговых предприятиях.

Еще одним способом генерации правильного номера карты является программа CreditMaster, используемая мошенниками с 1995 года. Программа генерирует правильные номера карт, эмитированных некоторыми банками, используя для генерации номеров тот же алгоритм, что и банк-эмитент.

Достаточно распространенным является способ, когда криминальные структуры организуют свои магазины и торговые точки с главной целью получить в свое распоряжение значительные наборы реквизитов карт.

Нужно сказать, что с помощью Интернета вполне решаемой становится задача вычисления обоих основных параметров пластиковой карты - ее номера и срока действия. Например, если мошеннику известен номер карты, но не известен срок ее действия, то определить этот параметр карты не составляет большого труда. Пластиковая карта обычно выпускается сроком на два года. Параметр "срок действия карты" определяет месяц и последние две цифры года, когда действие карты заканчивается. Таким образом, мошеннику нужно отправить не более 24 авторизационных запросов для того, чтобы с вероятностью 1 определить верный срок действия карты. После этого можно совершить транзакцию в Интернете или изготовить поддельную карту.

В большинстве случаев, номер карты представляет собой число, состоящее из шестнадцати десятичных цифр (хотя в соответствии со стандартом ISO 7812 "Идентификационные карты - система нумерации и процедура регистрации идентификаторов эмитентов" номер карты может состоять из 19 цифр). Из 16 цифр номера карты 6 первых представляют собой BIN (Bank Identification Number), предоставляемый банку международной платежной системой. Кроме того, достаточно часто крупные и средние банки используют 7-ю и 8-ю цифры номера для идентификации своих филиалов и отделений. Наконец, последняя цифра номера карты - цифра проверки на четность по алгоритму Luhn Check Parity, однозначно определяемая всеми остальными цифрами номера карты.

Таким образом, как правило, только 7 цифр номера карты являются независимыми переменными. Кроме того, чтобы выяснить значения зависимых переменных номера карты, мошеннику достаточно получить для себя в банке пластиковую карту. С учетом того, что средний банк выпускает под одним префиксом (первые 8-11 цифр карты) 50.000-500.000 карт, легко видеть, что, если банк генерирует номер карты по случайному закону, то плотность заполнения пространства возможных номеров карт (верхняя граница отношения количества выпущенных карт ко всему возможному множеству значений номера карты) составит 0,005-0,05. С учетом числа различных вариантов срока действия карты получается, что мошеннику требуется перебрать порядка 500-5000 различных вариантов для достижения своей цели.

Иногда помимо номера карты и срока ее действия требуется дополнительно сообщить торговому предприятию специальный цифровой код, называемый в системе VISA CVV2, а в системах Europay/MasterCard - CVC2. Этот цифровой код состоит из трех десятичных цифр, и получается с помощью

специального открытого алгоритма, применяемого к таким параметрам карты, как номер карты и срок ее действия. Алгоритм базируется на применении алгоритма шифрования DES и использует пару секретных ключей, известных только эмитенту карты. Таким образом, зная номер карты и срок ее действия, вычислить цифровой код без знания секретных ключей невозможно.

Сегодняшние оценки показывают, что когда обслуживающий банк передает в сеть значение цифрового кода CVC2/CVV2, лишь примерно в 30% случаев эмитент проверяет этот параметр). Некоторые эмитенты, даже определив, что значение цифрового кода неверно, дают положительный ответ на авторизационный запрос.

Использование цифрового кода CVV2/CVC2 в некоторой степени поможет борьбе с мошенничествами в Интернете, но не решит проблемы в целом.

Наиболее распространенными механизмами, призванными устранить указанные факторы и обеспечить безопасность проведения электронных платежей через Интернет сегодня являются:

· протокол SSL (Secure Socket Layer), один из существующих протоколов обмена данными, обеспечивающий шифрование передаваемой информации. В настоящее время это наиболее распространенный метод защиты;

· стандарт SET (Secure Electronic Transactions), разработанный компаниями Visa и MasterCard и обеспечивающий безопасность и конфиденциальность совершения сделок при помощи пластиковых карт.

Благодаря использованию цифровых сертификатов и технологий шифрования, SET позволяет как продавцам, так и покупателям производить аутентификацию всех участников сделки. Кроме того, SET обеспечивает надежную защиту номеров карт и другой конфиденциальной информации, пересылаемой через Интернет, а открытость стандарта позволяет разработчикам создавать решения, которые могут взаимодействовать между собой. Также важным фактором, обеспечивающим продвижение SET, является его опора на существующие карточные системы, ставшие привычным финансовым инструментом.

Для получения информации о распространении SET, включая информацию о банках, имеющих сертификаты Visa и Europay/MasterCard, и торговых и сервисных компаниях, принимающих платежи через SET, можно обратиться на сайт set-sites.com или сайты международных платежных систем.

Сегодня использование систем на базе SET является наиболее безопасным, но в силу различных причин он еще не получил достаточного распространения.

Вопросы организации безопасности при создании и эксплуатации систем банковского обслуживания через Интернет традиционно имеют важнейшее значение и привлекают большое внимание широких аудиторий. Защита системы как минимум должна обеспечивать однозначную идентификацию взаимодействующих субъектов (клиента и банка), шифрование передаваемой финансовой информации, защиту носителей информации. Сегодня все эти вопросы решаются большинством профессиональных средств защиты, которые используются как в западных, так и в отечественных системах.