Занимательные факты из биографии ПИН-кода, *или Теория вероятностей в индустрии платежных карт*

Игорь Голдовский, генеральный директор ЗАО «Платежные Технологии»

Предлагаемая вашему вниманию статья написана в жанре эссе – свободного размышления на заданную тему. Тема в данном случае – персональный идентификационный номер держателя карты, или ПИН-код. Статья построена в форме ответов на вопросы, представляющиеся интересными как для ее автора, так и, надеемся, для читателей журнала «ПЛАС». Интересными хотя бы потому, что ответы на них, как вы сами убедитесь по прочтении данного эссе, далеко не всегда тривиальны, а иногда просто неожиданны.

Каждому держателю карты, не говоря уже о специалистах в области карточного бизнеса, известно, что такое ПИН-код. Держатель карты знает, что ПИН-код требуется вводить на клавиатуре банковского терминала при выполнении некоторых карточных операций (например, всегда при снятии наличных в банкоматах) и что ПИН-код является величайшим в мире секретом, который необходимо держать в строжайшей тайне и лучше всего – просто хранить в памяти, нигде не записывая.

Специалисту, кроме того, известно, что до сегодняшнего дня ПИН-код остается самым надежным и эффективным среди наиболее распространенных на практике методов верификации держателя карты (учитывая, что массового внедрения биометрических технологий следует ожидать не раньше, чем через десятилетие). ПИН-код – это секрет, определенный для держателя конкретной карты и известный только держателю этой карты и, в некоторых случаях, о которых будет рассказано ниже, ее эмитенту. При выполнении ряда так называемых PIN-based транзакций эмитент должен иметь возможность проверить соответствие ПИН-кода используемой при проведении транзакции карте (точнее, номеру карты). Другими словами, между номером карты и значением ПИН-кода должно существовать соответствие, наличие которого, собственно, и проверяется эмитентом карты. Именно в проверке этого соответствия и заключается верификация держателя карты, являющегося владельцем соответствующего карте ПИН-кода.

Какие же требования предъявляются к проверяемому эмитентом соответствию между ПИН-кодом и номером карты? Должно ли, например, соответствие быть взаимно однозначным? Здесь ответ очевиден – нет! Действительно, в соответствии со стандартом ISO 9564-1 ПИН-код – это последовательность десятичных цифр длиной от 4 до 12 цифр, в подавляющем большинстве случаев – длиной 4 цифры. Количество же десятичных цифр в номере карты обычно равно 16. Так что говорить о взаимно однозначном соответствии ПИН-кода и номера карты не приходится.

Тогда возникает другой вопрос: определяется ли ПИН-код однозначно по номеру карты, т. е. является ли он функцией от номера карты? В общем случае ответ также отрицательный – одному номеру карты могут соответствовать разные значения ПИН-кода.

В таком случае, в чем же, собственно, состоит требование к соответствию между номером карты и ПИН-кодом? Требование заключается в следующем: для любого заданного номера карты количество значений ПИН-кода, соответствующих этому номеру карты, должно быть «небольшим», т. е. вероятность угадать соот-

ветствующее номеру карты значение ПИН-кода должна быть невысокой. Что подразумевается под «небольшим» и «невысокой», мы поясним ниже, после рассмотрения двух наиболее широко используемых видов соответствия ПИН-кода и номера карты.

Вопрос 1. Наиболее распространенные методы генерации/верификации ПИН-кода: в чем заключаются их принципиальные различия и какое отражение они находят на практике? Какой из этих методов надежнее с точки зрения обеспечения безопасности?

На сегодняшний день наиболее распространенные методы генерации/верификации ПИН-кода, устанавливающие соответствие между ПИН-кодом и номером карты, основаны на использовании алгоритмов IBM 3624 и VISA PVV. Не вдаваясь в детали, кратко напомним читателю о сути этих алгоритмов.

Вначале коснемся описания алгоритма IBM 3624 (случай ПИН-кода длиной 4 цифры):

1. Берется номер карты (16 самых правых цифр) PAN.
2. Вычисляется значение Encrypt3DES (PGK, PAN), представляющее собой значение 3DES-функции от номера карты PAN и двойного ключа генерации ПИН-кода PGK.
3. К полученному результату применяется процедура децимилизации (Decimalization Table).
4. Из полученного на предыдущем шаге результата, представляющего собой последовательность из 16 десятичных цифр, выбираются 4 цифры, расположенные в каких-либо наперед заданных 4 позициях. Полученное в результате значение называют PIN Natural.
5. Для получения значения ПИН-кода цифры значения PIN Natural складываются по модулю 10 с соответствующими цифрами величины PIN Offset, представляющей собой произвольную последовательность из 4-х десятичных цифр. Значение PIN Offset может храниться на магнитной полосе карты и/или в БД карт на хосте эмитента.

Проверка значения ПИН-кода, представленного держателем карты при выполнении операции, осуществляется по номеру карты и значению PIN Offset (поскольку ключ генерации ПИН-кода и таблица децимилизации являются фиксированными величинами, мы их здесь не упоминаем).

Очевидно, что при использовании алгоритма IBM 3624 значение ПИН-кода полностью определяется номером карты и величиной PIN Offset. Вероятность угадать значение 4-цифрового ПИН-кода с одной попытки равна 0,0001 (поскольку в данном случае ровно одно значение ПИН-кода соответствует каждому номеру карты).

Теперь рассмотрим алгоритм VISA PVV (случай ПИН-кода длиной 4 цифры):

1. Вычисляем TSP = PAN11+PVKI+PIN, где PAN11– двоичное представление последних 11 цифр номера карты без цифры Luhn Check Parity, PVKI – двоичное представление индекса, определяющего 3DES-ключ эмитента карты, PIN – двоичное представление 4-цифрового значения ПИН-кода, + – знак операции конкатенации бинарных последовательностей.
2. По индексу PVKI извлекается пара ключей Key A, Key B, формирующая 3DES-ключ эмитента (используется ключ двойной длины).
3. Вычисляется Result = EncryptDES (Key A, DecryptDES(Key B, EncryptDES(Key A, TSP))), где EncryptDES и DecryptDES – операции, соответственно, шифрования и расшифрования, выполненные с помощью алгоритма DES.
4. Выполняется двухпроходная децимилизация значения Result слева направо (проходом слева направо выписываются

КАЛЕЙДОСКОП

Новый контроллер NFC от NXP уже на подходе

Компания NXP (Голландия) выпустит новый чип NXP PN544 технологии NFC на рынок в III квартале 2009 г. Чип отвечает всем требованиям спецификаций Single Wire Protocol (SWP), выпущенным European Telecommunications Standard Institute (ETSI). Телефоны, оснащенные данным чипом и дополненные SIM-картой SWP, позволяют пользователям получать доступ к бесконтактным приложениям, таким как мобильные и транспортные платежи, покупка билетов и т.д.

Чип PN544 полностью согласуется со всеми выпущенными спецификациями NFC в соединении SWP. Кроме того, гарантировано взаимодействие интерфейса SWP с поддержкой технологии MIFARE. Чип PN544 полностью совместим с существующей бесконтактной платежной инфраструктурой. Ранее, в 2008 г., ассоциация операторов мобильной связи GSMA рекомендовала изготовителям мобильных телефонов объединить функциональные возможности NFC с коммерчески доступными мобильными телефонами к середине 2009 г.

MoneyGram эмитирует предоплаченную карту Visa

Компания MoneyGram Int., оператор системы денежных переводов MoneyGram, объявила о выпуске предоплаченной карты Visa Inc., выдача которой начнется в ряде точек обслуживания MoneyGram в США с июня 2009 г. Эмиссия карт осуществляется совместно с системой AccountNow и банком MetaBank (Сторм Лейк, США). Держатели карты смогут использовать ее в рамках системы AccountNow, предназначенной для частных лиц, не имеющих банковских счетов и не обладающих доступом к традиционным кредитным банковским продуктам, таким как кредитные карты, а также в банкоматах сети Plus и в сетях ReadyLink и Interlink.

все десятичные цифры значения Result в порядке их следования, а затем вторым проходом в порядке следования выписываются оставшиеся шестнадцатеричные цифры, из которых предварительно вычитается число 10).

5. Значение PVV равно четырем самым левым цифрам полученного результата.

Проверка ПИН-кода, представленного держателем карты при выполнении транзакции, выполняется по номеру карты и значению PVV, которое может храниться как на магнитной полосе карты, так и в БД карт на хосте эмитента.

Принципиальные различия алгоритмов VISA PVV и IBM 3624 состоят в следующем. Алгоритм IBM 3624 является алгоритмом генерации/верификации ПИН-кода, в то время как алгоритм VISA PVV определяет только процедуру верификации ПИН-кода. Алгоритм VISA PVV не определяет значения ПИН-кода для карты. В то же время часто при использовании метода VISA PVV предполагается, что ПИН-код генерируется по случайному равновероятному закону. Это требование не является обязательным, но в подавляющем большинстве случаев при использовании метода VISA PVV в качестве ПИН-кода используется случайная величина, представляющая собой последовательность из 4-х цифр, распределенную по равновероятному закону в диапазоне значений от 0000 до 9999. Везде ниже, говоря о методе VISA PVV, мы по умолчанию будем рассматривать именно случай равновероятного распределения значения ПИН-кода для конкретной карты.

Другое различие алгоритмов VISA PVV и IBM 3624 заключается в следующем. При использовании алгоритма IBM 3624 каждому номеру карты соответствует единственное значение ПИН-кода. Это легко следует из описания алгоритма IBM 3624, определяющего функциональную зависимость ПИН-кода от номера карты.

При использовании метода VISA PVV функциональной зависимости ПИН-кода от номера карты не существует. ПИН-код является случайной величиной! Соответствие ПИН-кода номеру карты в данном случае проверяется по номеру карты и значению величины PVV, как это было описано выше.

С помощью теории вероятностей легко показать, что в случае, когда ПИН-код для каждого номера карты выбирается по случайному равновероятному закону, известному значению PVV соответствует не менее двух значений ПИН-кода с вероятностью, равной:

$$1-\frac{Np(1-p)^{N-1}}{1-(1-p)^{N}}\approx 41.8\%$$

где N – число возможных значений ПИН-кода (при длине ПИН-кода, равной 4 цифрам, N=10000), p=0.0001 – величина, обратная мощности множества возможных значений PVV.

При этом среднее число значений ПИН-кода, соответствующих известному значению PVV, равно:

$$\frac{Np}{1-(1-p)^{N}}\approx 1{,}58$$

Таким образом, при использовании метода VISA PVV для верификации ПИН-кода вероятность угадать допустимое значение ПИН-кода с одной попытки примерно в 1,58 раза выше, чем в случае использования алгоритма IBM 3624! Однако, несмотря на то, что алгоритм VISA PVV не обеспечивает единственности значения ПИН-кода для каждого номера карты при фиксированном значении PVV, необходимый объем перебора возможных значений ПИН-кода по порядку остается в данном случае тем же, что и при использовании алгоритма IBM 3624. Поэтому с точки зрения безопасности (необходимого объема перебора возможных значений ПИН-кода до угадывания соответствующего значения ПИН-кода карты) оба метода генерации/верификации ПИН-кода являются эквивалентными.

Вопрос 2. Известно ли эмитенту значение ПИН-кода держателя карты, т.е. может ли эмитент только на основании хранимых на его хосте данных вычислить значение ПИН-кода карты?

Вначале обратим внимание читателя на то, что в соответствии с требованием международных платежных систем, определенным в п.3.2.3 стандарта PCI Data Security Standard (PCI DSS), значение ПИН-кода не должно храниться, даже в защищенном виде, на терминальных устройствах и в процессинговых центрах торгово-сервисных предприятий, в процессинговых центрах третьесторонних процессоров и банков, включая хост эмитента карты.

Как станет ясно ниже, ответ на поставленный вопрос полностью зависит от используемого метода генерации/верификации ПИН-кода, места хранения значений величин PIN Offset/PVV и используемой карточной технологии (карта с магнитной полосой или микропроцессорная карта).

Начнем со случая, когда значения PIN Offset/PVV хранятся на магнитной полосе. Очевидно, в этом случае при любом методе генерации/верификации ПИН-кода восстановить ПИН-код у эмитента не получится. Именно поэтому общая рекомендация платежных систем заключается в хранении значений PIN Offset/PVV на магнитной полосе карты, что снижает вероятность компрометации ПИН-кода в результате мошеннических действий персонала банка.

Теперь рассмотрим случай, когда значения PIN Offset/PVV хранятся в БД карт хоста эмитента. В этом случае при использовании алгоритма IBM 3624 эмитент легко вычисляет значение ПИН-кода карты. При использовании алгоритма VISA PVV эмитент может найти значение ПИН-кода, соответствующее известному ему значению PVV, методом перебора всех 10000 возможных значений. Как ранее отмечалось, при этом эмитент найдет одно значение ПИН-кода с вероятностью, примерно равной 58,2%, и более одного значения ПИН-кода – с вероятностью 41,8%.

Если карта эмитента является картой с магнитной полосой, то применение любого значения, соответствующего PVV, даст положительный результат верификации держателя карты при проведении

транзакции. Поэтому в этом смысле эмитенту известно значение ПИН-кода карты.

Если карта эмитента является микропроцессорной, поддерживающей метод верификации держателя PIN Offline, то угадать одно из значений ПИН-кода, соответствующее PVV, мало. Необходимо знать значение ПИН-кода, записанное в секретную область памяти чипа! Таким образом, в случае микропроцессорной карты с вероятностью 41,8% эмитент не знает точного значения ПИН-кода, даже если PVV хранится на хосте эмитента.

Отметим, что перебор значений ПИН-кода в рамках описанной выше процедуры поиска значения ПИН-кода, соответствующего известному значению PVV, не займет много времени. Проверка одного значения ПИН-кода (вычисление соответствующего ему значения PVV) занимает порядка 10 мс (в зависимости от модели используемого банком модуля HSM). Таким образом, перебор всех возможных значений ПИН-кода займет примерно 100 секунд или, с учетом загрузки модуля HSM другими задачами, – несколько минут.

Вопрос 3. В каких случаях можно восстановить забытое держателем карты значение ПИН-кода без перевыпуска карты?

Итак, держатель карты вместе со своей картой прибывает в банк-эмитент и просит банк восстановить забытое им значение ПИН-кода без перевыпуска карты (перекодировка магнитной полосы по нашему определению входит в понятие «перевыпуска карты»).

При использовании эмитентом метода IBM 3624 эмитент считывает с карты или из БД карт хоста эмитента значение PIN Offset и вычисляет значение ПИН-кода для карты держателя. Это значение печатается в ПИН-конверте и передается клиенту.

При использовании метода VISA PVV эмитент считывает с карты или из БД карт хоста эмитента значение PVV. Далее методом перебора всех значений ПИН-кода эмитент находит значения, соответствующие значению PVV. При этом в случае карты с магнитной полосой любое из соответствующих PVV значений ПИН-кода можно передать клиенту в качестве нового значения ПИН-кода. В случае же микропроцессорной карты среди соответствующих VISA PVV значений ПИН-кода придется выбрать (с помощью команды Verify) единственное значение, записанное в памяти чипа. Можно не выбирать старое значение ПИН-кода, а использовать первое попавшееся соответствующее PVV значение, перезаписав его на чипе с помощью команды PIN Change/Unblock.

Таким образом, и в случае использования метода VISA PVV можно восстановить значение ПИН-кода без перевыпуска карты. Однако на практике эмитенты предпочитают не пользоваться описанной выше процедурой восстановления ПИН-кода, а вместо нее просто перевыпускают карту с новым значением ПИН-кода. Вполне вероятно, что некоторые банки просто не знают про процедуру восстановления ПИН-кода при использовании метода VISA PVV. Кроме того, реализацию процедуры восстановления ПИН-кода придется заказывать у поставщика программного обеспечения процессингового центра эмитента (ни одно известное на рынке ПО такую функцию в готовом виде не поддерживает), оснащать отделение специальным рабочим местом, используемым для восстановления забытого ПИН-кода. А это дополнительные финансовые затраты. Поэтому на практике оказывается проще перевыпустить карту забывчивому клиенту.

Вопрос 4. В каких случаях держатель карты может самостоятельно поменять ПИН-код в банкомате своего эмитента, а в каких – нет?

Сам вопрос предполагает, что эмитент карты поддерживает функцию смены значения ПИН-кода на своих банкоматах. Тогда легко видеть, что если значения PIN Offset/PVV хранятся на магнитной полосе карты, то изменить значение ПИН-кода в банкомате не получится, поскольку изменение ПИН-кода влечет за собой изменение значений PIN Offset/PVV.

В случае же, когда значения PIN Offset/PVV хранятся в БД карт хоста эмитента, изменить значение ПИН-кода не составляет проблемы. В этом случае значения PIN Offset/PVV будут вычислены для нового значения ПИН-кода и помещены в БД карт вместо прежних значений. Кроме того, при использовании микропроцессорной карты, поддерживающей метод верификации держателя PIN Offline, эмитент карты в скрипт-процессинге отправит карте команду PIN Change/Unblock, записав в микросхему новое значение ПИН-кода.

Таким образом, с точки зрения безопасности (уменьшения вероятности компрометации ПИН-кода инсайдером) значения PIN Offset/PVV предпочтительнее хранить на магнитной полосе карты. Однако, если эмитент желает предоставить держателям своих карт возможность смены значения ПИН-кода, величины PIN Offset/PVV необходимо хранить в БД карт хоста эмитента.

Вопрос 5. Обычно эмитентами используется ПИН-код длиной 4 цифры. Как изменяется вероятность взлома/подбора ПИН-кода, если мошеннику каким-либо образом известно, что в значении ПИН-кода используется $k \le 4$ различных цифр?

С помощью элементарной комбинаторики легко показать, что количество возможных значений $S(k)$ ПИН-кода при условии, что в ПИН-коде используется k различных цифр, равно:

- $S(1) = 10;$
- $S(2) = C_{10}^{2} \times (C_4^1 + C_4^2 + C_4^3) = 630;$
- $S(4) = C_{10}^{4} \times 4! = 5040;$
- $S(2) = 1000 - 10 - 630 - 5040 = 4320$

Шанс угадать ПИН-код, не выходя за рамки трех возможных попыток его ввода (обычный лимит, устанавливаемый эмитентом, после превышения которого эмитент требует задержать карту), соответственно, равен:

- при $k = 1$ 1:3,33;
- при $k = 2$ 1:210;
- при $k = 3$ 1:1440;
- при $k = 4$ 1:1680

Таким образом, знание злоумышленником k позволяет существенно изменить вероятность отгадывания ПИН-кода (в случае, если он не знает значения k, вероятность отгадывания примерно равна 1:3333).

Более того, перебор может быть значительно сокращен, если мошеннику известна дополнительная информация о характере совпадений цифр в ПИН-коде. Например, если мошеннику известно, что в ПИН-коде используются только две разные цифры, причем каждая цифра встречается по два раза, то перебор сократится до 270 вариантов, и вероятность отгадать ПИН-код за три попытки уменьшается до 1:90! Если мошеннику известно, что в ПИН-коде используются две разные цифры, одна из которых встречается трижды, то перебор сокращается до 360 вариантов, и вероятность отгадать значение ПИН-кода за три попытки составляет 1:120.

Известны случаи, когда мошенники для выяснения цифр ПИН-кода тщательно протирали клавиатуру банкомата и после ввода держателем цифр ПИН-кода по жировым отпечаткам фиксировали нажатые держателем клавиши. В этом случае мошеннику становятся известны конкретные цифры ПИН-кода, не известен только порядок их следования. Если обозначить через m (m = 1,…,4) число различных нажатых держателем цифр, тогда очевидно, что количество возможных вариантов ПИН-кода $R(m)$ определяется равенством:

$$R(m) = S(m) / C_{10}^{m}$$

Тогда:

- $R(1) = 1$;
- $R(2) = (C_4^1 + C_4^2 + C_4^3) = 14$;
- $R(4) = 4! = 24$;
- $R(3) = S(3) / C_{10}^{3} = 36$

Вероятность угадать ПИН-код при трех возможных попытках его ввода в случае известных цифр ПИН-кода равна:

- при $m = 1$ 1:1;
- при $m = 2$ 3:14;
- при $m = 3$ 1:12;
- при $m = 4$ 1:8

Вопрос 6. Насколько критично, чтобы все 4 цифры ПИН-кода (наиболее распространенная длина значения) были разными? Нужно ли вводить ограничения на количество различных цифр в ПИН-коде держателя карты?

Иначе вопрос звучит следующим образом: требуется ли исключить из возможных значений ПИН-кода те значения, в которых число различных цифр k невелико (k = 1, 2, 3)?

Сразу заметим, что если потребовать, чтобы k = 4 (т. е. все цифры ПИН-кода были разными) для любого допустимого значения ПИН-кода, то перебор возможных значений ПИН-кода сокращается примерно в два раза (до 5040), что не оказывает существенного влияния на безопасность метода верификации с помощью ПИН-кода. В то же время, конечно, хотелось бы понять – стоит ли все-таки «городить огород», ограничивая множество допустимых значений ПИН-кода, или считать любое возможное значение ПИН-кода допустимым? Чтобы ответить на этот вопрос, нужно понять, откуда исходит угроза в случае, когда число различных цифр в ПИН-коде ограничено (не равно 4).

Представляется, что модель угрозы компрометации ПИН-кода выглядит следующим образом. Злоумышленник, обнаруживший повторение цифр значения ПИН-кода, может существенным образом сократить объем перебора возможных значений ПИН-кода. Например, если злоумышленник, подглядывающий из-за спины держателя, обнаруживает, что последний набирает одну и ту же цифру при вводе ПИН-кода (а на практике это можно визуально обнаружить), объем перебора значений ПИН-кода сокращается до 10. В этом случае вероятность компрометации

КАЛЕЙДОСКОП

«РуссКом-Кард плюс» расширяет ассортимент сублимационных принтеров-кодировщиков

Компания «РуссКом-Кард плюс» предложила клиентам специальные односторонние модели принтеров SunLightK3 Single (CIM, Италия) с возможностью установки дополнительных опций, таких как кодировщики/считыватели контактных и бесконтактных чипов (в том числе Em-marine и Mifare), в стандартный корпус принтера. Ранее для доукомплектации односторонней модели принтера требовался специальный «модуль опций»: иными словами, принтер-кодировщик поставлялся в «удлиненном» корпусе, в котором, при тех же функциональных возможностях, стоимость принтера была несколько выше стандартной.

Вклады населения Белоруссии достигли почти 5,6 млрд долл. США

Согласно данным Национального банка Республики Беларусь (НБРБ), в январе–апреле 2009 г. рублевые и инвалютные вклады населения в банках страны увеличились более чем на 2,3 трлн белорусских рублей (827 млн долл. США), или на 17,6%. В предыдущем месяце они возросли почти на 427 млрд белорусских рублей (153 млн долл. США), или на 2,8% (рублевые – на 380,5 млрд белорусских рублей (136 млн долл. США), или на 6%, инвалютные – на 29,7 млн долл. США, или на 1%). На начало мая вклады населения достигли почти 15,6 трлн белорусских рублей (5,6 млрд долл. США). Депозиты в национальной валюте составили свыше 6,7 трлн белорусских рублей (2,4 млрд долл.), а в иностранной – свыше 3,1 млрд долл. США.

ции ПИН-кода при трех возможных попытках ввода ПИН-кода составляет примерно 0,333. Это очень высокая вероятность компрометации, и потому нежелательно, чтобы в ПИН-коде все цифры были одинаковыми. Поэтому разумно исключить из области допустимых значения ПИН-кода со всеми одинаковыми цифрами.

В случае присутствия двух различных цифр в ПИН-коде при использовании каждой цифры в ПИН-коде два раза вероятность компрометации за три попытки ввода ПИН-кода, как отмечалось ранее, равна 1:90. Это невысокая вероятность, но в случае, когда мошенник может дополнительно определить, какие именно две цифры входят в состав значения ПИН-кода (например, с помощью описанного выше приема с использованием отпечатков пальцев держателя), вероятность компрометации за три попытки возрастает до недопустимо высокого значения 0,5. Поэтому значения ПИН-кода, состоящие из двух одинаковых цифр, желательно не допускать.

Что касается использования трех или четырех различных цифр в ПИН-коде, то вероятность компрометации ПИН-кода в этом случае невелика. Резюмируя вышесказанное, можно утверждать, что имеет смысл ограничить множество допустимых значений ПИН-кода значениями, в которых не менее 3 цифр являются разными.

Вопрос 7. Насколько безопасно разрешать клиенту использовать один и тот же ПИН-код для разных карт?

Для ответа на этот вопрос в качестве критерия оценки схемы будем рассматривать среднее время до компрометации значений ПИН-кода карт. Сравниваются две схемы – все карты клиента имеют один ПИН-код; для каждой карты клиент использует разные значения ПИН-кода.

Пусть ζ и η – случайные величины, представляющие собой время до компрометации всех значений ПИН-кода в случае, когда ПИН-код один на все карты держателя, и в случае, когда он разный для каждой карты, соответственно. Время выражается в количестве операций до компрометации ПИН-кода.

Тогда, очевидно, имеют место равенства:

$$\xi = \min\{\xi_j, j = 1,...,K\};$$

$$P\{\xi = k\} = \sum_{i=1}^{K} C_K^i \cdot (P\{\xi_j = k\})^i (P\{\xi_i > k\})^{K-i} =$$

$$= \sum_{i=1}^{K} C_K^i \cdot (p^{k-1}q)^i (p^k)^{K-i} = p^{(k-1)K}(1-p^K)$$

где ξ_j– время до компрометации j-й карты держателя, $(j = 1,...,K)$, $q = 1 - p$ – вероятность компрометации ПИН-кода при выполнении одной операции.

Отсюда легко получить, что:

$$M\xi = \frac{1}{1-p^K}$$

Далее, очевидно:

$$\eta = \max\{\xi_j, j = 1,...,K\};$$

$$M\eta = \sum_{i=0}^{K-1} \frac{1}{1-p^{K-i}}$$

Отсюда получаем, что при использовании различных значений ПИН-кода для каждой карты выигрыш во времени до компрометации всех значений ПИН-кода составляет:

$$\Delta = M\eta - M\xi = \sum_{i=1}^{K-1} \frac{1}{1-p^{K-i}}$$

При $K = 3$ и $(p = 0{,}999)$ получаем $\Delta \approx 1500$

Таким образом, при выбранном значении вероятности компрометации ПИН-кода за одну операцию $(q = 0{,}001)$ держатель трех карт сделает в среднем на 1500 операций больше до компрометации всех ПИН-кодов его карт, чем в случае, когда для всех карт держателя использовалось одинаковое значение ПИН-кода. Но при этом держателю карты придется помнить различные значения ПИН-кода для каждой из трех своих карт.

Вопрос 8. В связи с проблемами защиты карточных данных, включая ПИН-код, в торговых POS-терминалах возникает вопрос: а стоит ли внедрять получающую в последние годы все большее распространение технологию Chip&PIN? Ведь рост числа компрометаций значений ПИН-кода в торговой сети увеличивает объем мошеннических операций через банкоматы!

Для ответа на этот вопрос рассмотрим пример Великобритании. В 2001 г. на рынке этой страны уровень фрода типа Lost/Stolen (L/S, украденные/потерянные карты) составлял 5,07 базисного пункта, а в 2008 г. он опустился до значения 1,2 базисного пункта! Главная причина резкого падения уровня фрода L/S – практически повсеместное внедрение технологии Chip&PIN, предусматривающей использование ПИН-кода для подтверждения, в том числе, POS-терминальных транзакций.

Действительно, люди теряли, теряют и будут терять карты с примерно одинаковой интенсивностью как в 2001 г., так и в 2008-м и последующих годах. А в том случае, если держатель не склонен к рассеянности, «потерять» карту ему с удовольствием «помогут» злоумышленники. Однако в 2001 г. украденной картой можно было тут же воспользоваться в торговой сети до момента обнаружения держателем ее утраты (миграция на Chip&PIN началась в Великобритании в 2004 г.). В 2008 г. сделать это в Великобритании было уже не так просто (использовать украденную карту для выполнения CNP-операций для мошенников значительно менее выгодно), поскольку практически все POS-терминалы принимают чиповые карты и требуют от держателя ввода ПИН-кода, которого мошенник не знает по определению. Приходится передавать украденную карту британского банка для использования в других странах, где имеются POS-терминалы, не поддерживающие чип и/или не имеющие ПИН-пада. Как следствие, мошенники теряют время, клиент успевает опомниться/ заблокировать карту, и уровень мошенничества L/S значительно падает!

Как можно оценить, если бы в свое время в Великобритании не была принята программа Chip&PIN, размер потерь от фрода L/S составил бы в 2008 г. около 257 млн фунтов стерлингов (без учета фрода NRI – Not Received Items) при уровне в 5,07 базисного пункта. Однако благодаря Chip&PIN в 2008 г. размер этого ви-

НОВЫЙ ВЗГЛЯД НА ИНТЕГРАЦИОННЫЕ КАССОВЫЕ РЕШЕНИЯ

Подключение POS-терминалов и PIN-падов к кассовым системам по бессерверной технологии

Оптимизация затрат

Мы сокращаем Ваши расходы на покупку дорогостоящего серверного оборудования и обучение персонала работе с кассовыми системами.

Широкий потенциал для развития

Возможность подключения POS-терминалов и PIN-падов к кассовым системам различных производителей.
Реализация практически любого функционала решения для заказчиков.

Гарантированная надежность

Высокая отказоустойчивость оборудования за счет отсутствия единого управляющего сервера.

ЛАНИТ
Департамент Банковских Технологий

телефон : +7 (495) 967-6674
факс: +7 (495) 721-9155
e-mail: bankomat@lanit.ru
www.banking.lanit.ru

POS-терминалы и PIN-пады: HYPERCOM
программное обеспечение: TRANSACTION SYSTEMS

Три напряженных дня,
посвященных бизнесу, будущему
и инновациям!

СМАРТ-КАРТЫ БЕСКОНТАКТНЫЕ ТЕХНОЛОГИИ
ТЕРМИНАЛЫ И ИНТЕЛЛЕКТУАЛЬНЫЕ УСТРОЙСТВА
БИОМЕТРИЯ АУТЕНТИФИКАЦИЯ ТЕЛЕКОММУНИКАЦИИ
ПЛАТЕЖИ ТРАНСПОРТИРОВКА
MACHINE-TO-MACHINE
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

CARTES 2009 — 24 Years supporting the Smart Technologies Industry

iD

17–19 ноября 2009
Paris-Nord Villepinte Exhibition Centre – Франция

Событие № 1 в мировой индустрии цифровой безопасности и интеллектуальных технологий

500 экспонентов – 20 000 посетителей выставки – 30 000 кв. м. выставочных площадей – 200 докладчиков – 1 500 участников Конгресса

RUSSIA, COUNTRY OF HONOUR

www.cartes.com

Контакты:

Участие в выставке:	Посещение выставки:	Участие в Конгрессе:
Отдел продаж	Julie COCHET	Arnaud ROY
+33 (0)1 76 77 13 00	+33 (0)1 76 77 12 13	+33 (0)1 76 77 15 66
sales@cartes.com	julie.cochet@comexposium.com	arnaud.roy@comexposium.com

An event organized by comexposium

Cartes & IDentification 2009
70 avenue du Général de Gaulle
92058 Paris la Défense Cedex - France
cartes-id@comexposium.com

да мошенничества составил всего 54 млн фунтов стерлингов!

В то же время из-за повсеместного использования ПИН-кода и расширившихся возможностей для компрометации его значений злоумышленниками (банальное подглядывание, накладная клавиатура/видеокамера, установка malware в приложении банкоматов, фишинг/вишинг, подмена POS-терминала/ПИН-пада, закладки в POS-терминале, атаки на HSM и т. п.) в 2008 г. потери английских банков через ATM fraud возросли до 46 млн фунтов стерлингов. Для сравнения, в 2001 г. потери этого типа были настолько ничтожны, что даже не рассматривались в отчетах.

Таким образом, можно утверждать, что использование технологии Chip&PIN за 2008 г. позволило британским банкам сэкономить не менее 257 – (54+46) = 157 млн фунтов стерлингов (как вы помните, мы не учли снижение фрода вида NRI)!

Следует подчеркнуть, что для достижения такого эффекта необходима дружная миграция всех банков на технологию Chip&PIN. Именно в этом случае у мошенника, завладевшего картой без ПИН-кода, возникнет «спасительная» задержка с ее применением, связанная с поиском подходящего места для использования украденной карты, что приведет к падению размера мошенничества вида Lost/Stolen/NRI.

Если условие быстрой и дружной миграции банков на технологию Chip&PIN не выполняется (например, в России), то эффект может оказаться прямо противоположным – и ATM fraud, и Lost/Stolen/NRI-фрод будут расти одновременно.

Вопрос 9. На что именно в карточных технологиях влияет длина ПИН-кода?

В последние годы в индустрии безналичных платежей все чаще используется двухфакторная аутентификация держателя карты (MasterCard Chip Authentication Program и Visa Dynamic Passcode Authentication). Держатель карты должен знать значение ПИН-кода и иметь микропроцессорную карту, способную сгенерировать прикладную криптограмму. Только владея обоими факторами (картой и ПИН-кодом), держатель будет успешно аутентифицирован.

Как уже отмечалось, вероятность угадать ПИН-код карты, попавшей в руки мошенника, с помощью трех попыток равна примерно 1:3333. Наоборот, мошенник, знающий значение ПИН-кода, может попытаться отгадать нужные биты прикладной криптограммы. Чтобы при двухфакторной аутентификации оба фактора вносили примерно одинаковую лепту в безопасность схемы, достаточно выбрать из прикладной криптограммы для формирования CAP Token только 12 битов. Именно поэтому международные платежные системы рекомендуют выбирать не менее 16 битов (кратно числу байтов) из прикладной криптограммы, а стандартная длина CAP Token (одноразового пароля) при этом составляет 6–8 цифр.

P. S.

Очевидно, что список вопросов, возникающих вокруг ПИН-кода и его использования, может быть продолжен. В рамках же настоящего эссе автор рассмотрел только наиболее интересные с его точки зрения моменты, однако он выражает готовность ответить на новые вопросы читателей журнала «ПЛАС», связанные с данной увлекательной и актуальной темой. ПЛАС

КАЛЕЙДОСКОП

«Диасофт» в рейтинге крупнейших IT-компаний России 2008 г.

Согласно данным седьмого рейтинга CNews Analytics информационного портала CNews, в 2008 г. выручка сотни крупнейших отечественных IT-компаний по сравнению с предыдущим годом увеличилась на 16,7%. Это свидетельствует о том, что рост рынка информационных технологий продолжается. Впечатляющими на общем фоне являются показатели компании «Диасофт», бизнес которой в 2008 г. вырос на 40%.

В рейтинговой таблице крупнейших IT-компаний «Диасофт» занимает 52-е место. Почетная «золотая середина» сильнейших – свидетельство стабильности бизнеса компании, которая продолжает развиваться в соответствии с намеченным курсом.

По словам Александра Генциса, старшего вице-президента «Диасофт», кризис не внес сколько-нибудь серьезных изменений в стратегические планы компании. «Диасофт» продолжает интенсивно работать – ведет проекты с ключевыми клиентами, успешно обслуживает широкую клиентскую базу, заключает новые крупные контракты. «Уже эти факты вкупе с возможностью самофинансирования и, главное, конкурентоспособностью и востребованностью продуктов и услуг компании, позволяют «Диасофт» и ее клиентам с оптимизмом смотреть в будущее», – подчеркнул А. Генцис.

Банковскими картами расплачиваются около 100 тыс. пассажиров московского метро

Согласно заявлению начальника Московского метрополитена Дмитрия Гаева, около 100 тыс. пассажиров оплачивают проезд с помощью банковской карты. Стоимость разовой поездки по карте не отличается от цены простого билета. Но если владелец карты оплачивает проезд 60 раз в месяц, то ему компенсируется разница в цене. «Сначала оплачивать проезд можно было только картой Банка Москвы, с 2008 г. к проекту подключились еще 6 банков. Сегодня мы имеем заявки еще от 8 банков», – рассказал Д. Гаев.