Управление сложными системами

УДК 338.12 + 338.24.01

В.Н. Графсков[1]
С.Е. Вечерская[2]

ИССЛЕДОВАНИЕ ПРОБЛЕМ, СВЯЗАННЫХ С ПЕРЕХОДОМ НА СТАНДАРТ PCI DSS 3.2, В КОМПАНИИ, ЗАНИМАЮЩЕЙСЯ ИНТЕРНЕТ-ЭКВАЙРИНГОМ

В работе проанализированы проблемы, связанные с переходом на обновленную версию стандарта безопасности PCI DSS одной из компаний, специализирующихся на электронной коммерции в городе Москве и занимающихся проведением платежей по банковским картам. В ходе данного исследования предложены варианты по устранению несоответствия стандарту безопасности PCI DSS.

Ключевые слова: *интернет-эквайринг, информационная безопасность, PCI DSS, SSL, TLS, антифрод.*

V.N. Grafskov
S.E. Vecherskaya

INVESTIGATION OF PROBLEMS ASSOCIATED WITH THE IMPLEMENTATION OF THE PCI DSS 3.2 IN A COMPANY ENGAGED IN THE INTERNET PAYMENT ACQUIRING

The work is the analysis of one of the Moscow companies readiness specialized in the electronic commerce in the city engaged into payments transfer on bank cards. In the course of this investigation were identified and resolved nonconformance standard of safety.

Keywords: *the Internet-acquiring, information security, PCI DSS, SSL, TLS, antifraud.*

В первые несколько десятилетий своего существования компьютерные сети в основном использовались учеными университетов для общения по электронной почте и корпоративными сотрудниками для печати на принтерах. В этих условиях о безопасности никто не задумывался. Но с каждым годом задачи сетевой безопасности становятся всё более всеобъемлющими и подразумевают проблемы.

Это, в частности, связано со средствами автоматизированной обработки данных и атаками на эти средства. Особую роль в противодействии потенциальным угрозам играет комплексный подход с использованием средств информационной защиты, в соответствии с их предназначением. Активная интеграция и использование открытых каналов связи значительно повысила уязвимость информации.

По официальным оценкам, от несанкционированного проникновения в информационные системы бизнес-сектор США теряет от 160 до 350 млрд долларов в год. Также в США ущерб от одного преступления, связанного с информационными технологиями, в среднем составляет около 10 миллионов рублей, а максимальный ущерб может составлять более 20 млрд рублей. Ущерб, наносимый преступниками информационной среды странам Евросоюза, оценивается более чем 30 млрд евро в год. Доход от этой дея-

[1] Кандидат технических наук, магистрант АНО ВО «Российский новый университет».

[2] Кандидат химических наук, доцент, доцент кафедры ИСвЭиУ АНО ВО «Российский новый университет».

тельности занимает третье место следом за торговлей оружием и наркотиками. Комитет ООН по предупреждению и борьбе с преступностью признал выход проблемы на международный уровень [1].

В России эта проблема стала актуальной в 1990-х годах, когда российские банки и финансовые структуры постепенно начали переводить свои расчеты и платежи в электронный вид

Для достижения безопасности информации важными задачами являются обеспечение таких ее свойств, как целостность, доступность, конфиденциальность и юридическая значимость. В настоящее время в нашей стране приобретает всё большую важность юридическая значимость информации, так же как и создание нормативно-правового законодательства в сфере информационной безопасности. Особенно остро этот вопрос встает при взаимодействии с системами автоматизации в различных коммерческих организациях. Юридическую значимость информации можно охарактеризовать как свойство или качество защищенной информации, которое позволяет обеспечить юридическую силу в соответствии с правовым режимом, установленным законодательством РФ в отношении документов или информационных процессов. Следует отметить, что для этого необходимо использовать сертифицированные средства защиты информации, разработанные организациями-лицензиатами, т.е. предприятиями, располагающими правом на разработку средств защиты информации.

Юридическая значимость также необходима для обеспечения строгого учета любых информационных услуг при создании Информационной системы платежного шлюза, при реализации политики безопасности на предприятии.

Интернет-эквайринг (англ. *internet acquiring*) – это технология, позволяющая принимать к оплате банковские карты через Интернет. Главное отличие от торгового и мобильного эквайринга состоит в отсутствии терминала для физического считывания данных карты. Таким образом, использовать интернет-эквайринг могут пользователи виртуальных банковских карт и электронных кошельков, у которых отсутствуют физические носители в виде пластиковых карт [2].

С развитием интернет-торговли электронные платежи стали доступны с любого устройства, но требования информационной безопасности постоянно повышаются из-за нахождения уязвимостей в протоколах предыдущего поколения.

Стандарт безопасности платежной индустрии банковских карт PCI DSS разработан советом PCI SSC и является собирательным образом требований к обеспечению информационной безопасности международных платежных систем: MasterCard, Visa, AmericanExpress, Discovery и JCB [3].

В рассматриваемой компании была собрана статистическая информация по платформам, используемым для платежей (табл. 1). Информацией по платформам, использование которых не превышает 1% от общего количества, в приведенной статистике пренебрегли.

Таблица 1

Статистика по платежным платформам

Name	TLS1.0	TLS1.1	TLS1.2	%
TOTAL	98.19%	85.90%	84.09%	
MobileSafari 9	+	+	+	12,67
Android 4	+	–	–	9,87
YandexBrowser 15	+	+	+	8,89
Chrome 47	+	+	+	6,53
ChromeMobile 30	+	+	+	5,54
ChromeMobile 47	+	+	+	5,09
TV–browser	+	–	–	4,23
Chrome 46	+	+	+	4,02
Chrome 48	+	+	+	3,84
MobileSafari 8	+	+	+	3,95
ChromeMobile 46	+	+	+	3,92
YandexBrowser 16	+	+	+	3,84
IE 11	+	+	+	3,5
ChromeMobile 48	+	+	+	2,43
Chrome 49	+	+	+	2,38
MobileSafari 7	+	+	+	2,15
Opera 34	+	+	+	1,54
Firefox 43	+	+	+	1,54
ChromeMobile 49	+	+	+	1,16
Firefox 42	+	+	+	1,16
ChromeMobile 33	+	+	+	1

Как мы можем увидеть, большинство современных браузеров поддерживают рекомендуемый протокол TLS 1.2, но есть и устаревшие версии, которые поддерживают только версию 1.0. Это нативный браузер мобильной платформы Android 4, который берет за основу WebKit (WebKit – свободный движок для отображения веб-страниц, разработанный на основе кода библиотек KHTML и KJS) и WebOS, используемый в телевизионных устройствах для покупки контента (рис. 2).

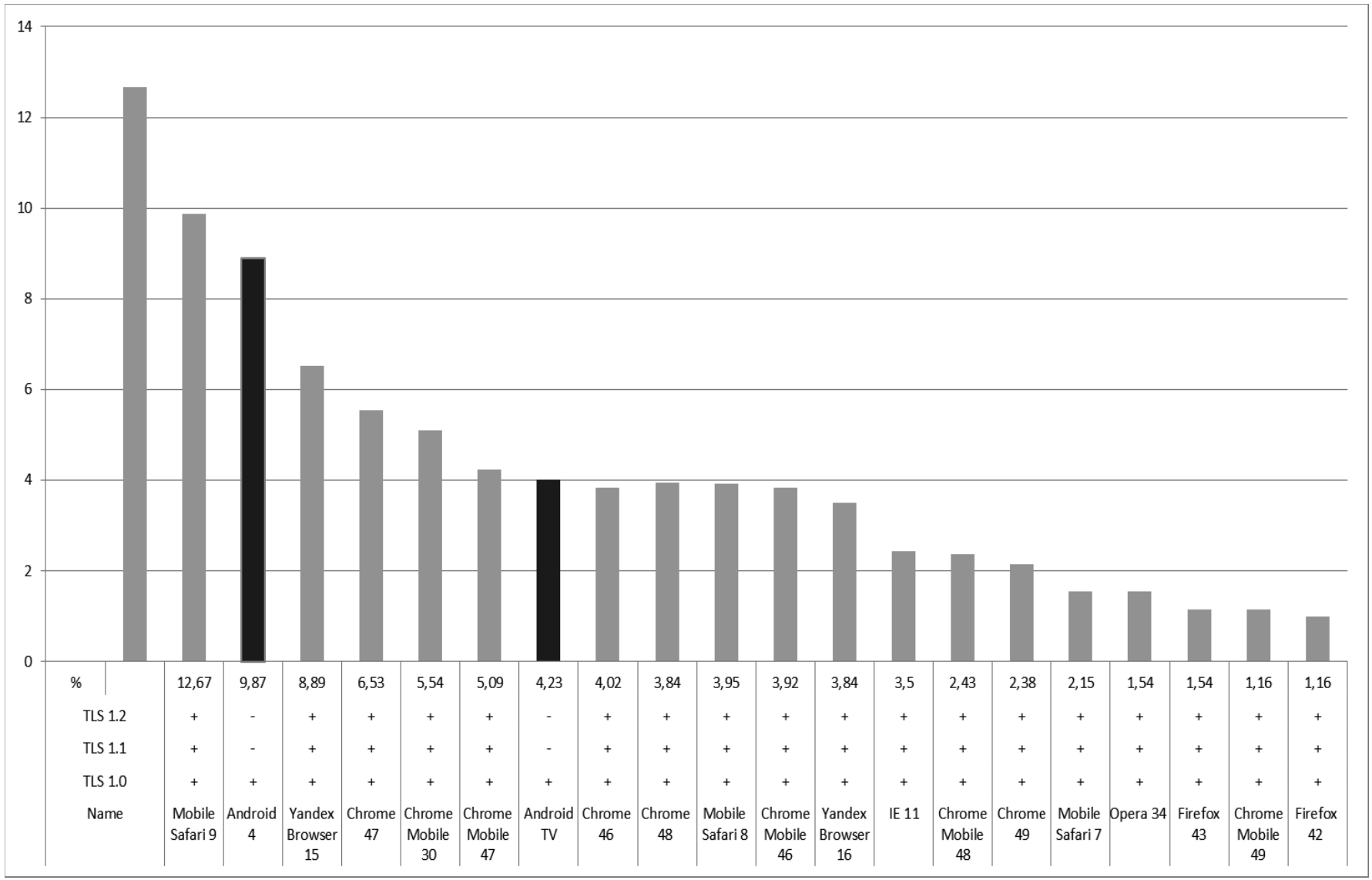

Рис. 1. Платформы, используемые для платежей

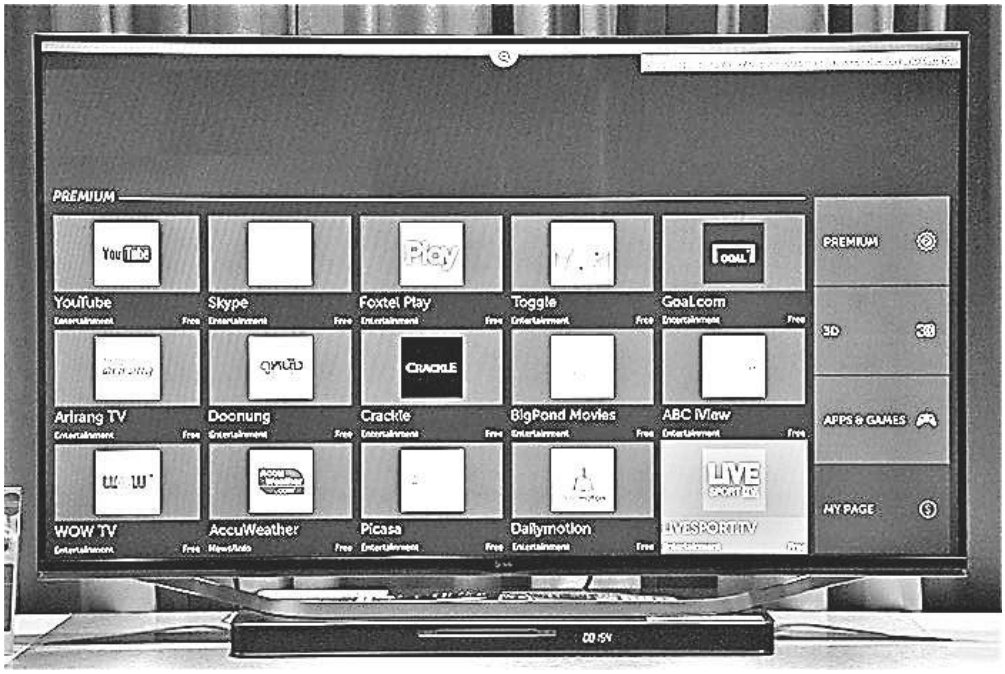

Рис. 2. WebOS

Для обеспечения безопасности платежа используется сервис для противодействия мошенническим операциям – антифрод (antifraud). Он анализирует информацию о покупателе и покупаемом товаре на базе статистики платежей и настроек для данного продавца. Результатом является решение проводить или не проводить платеж и давать или не давать уведомления департаменту борьбы с мошенничеством.

По требованиям PCI DSS, запрещается хранить полную информацию о банковской карте (PAN) или код проверки подлинности карты (CVV). Разрешено хранить «маску карты» из первых 6 и последних 4 цифр карты. Также разрешается присваивать клиентам внутренний ID. Имя держателя и срок действия карты можно передавать исключительно по защищенным каналам.

В основе архитектуры антифрода лежит множество фильтров, которые могут быть подключены к клиенту. Ниже приведена схема подключения фильтров antifraud на уровне базы данных.

На ранних этапах необходимо проверить правильность внесения имени держателя карты (тире и цифры в имени неприемлемы), является ли карта действующей (у карты есть срок действия), проходит ли номер карты проверку алгоритмом Луна.

Проверка номера кредитной карты представляет собой вычисление контрольной цифры, закодированной алгоритмом Луна. Алгоритм Луна – это не криптостойкий алгоритм, а алгоритм проверки целостности информации, заключается он в том, что каждая нечетная цифра номера удваивается, и если произведение больше или равно 10, из него вычитается 9; полученные таким образом цифры суммируются, а полученная сумма должна быть кратна 10, на основании этого делается вывод о верности номера.

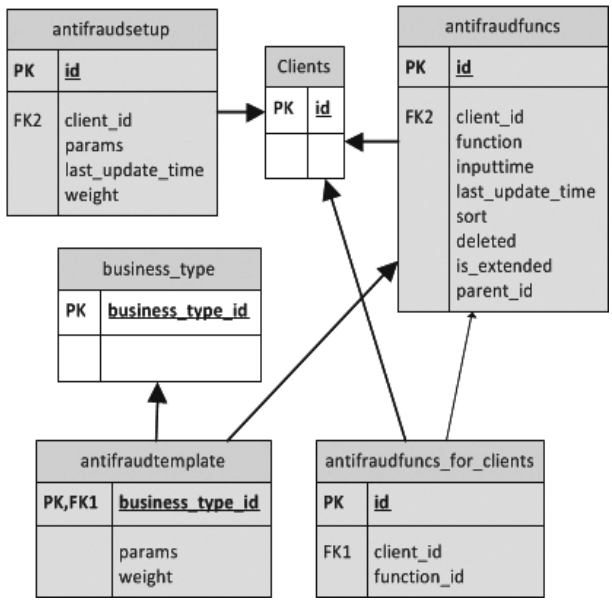

Рис. 3. Таблицы в базе и их взаимосвязь

Таблица 2

Форма расчета контрольной цифры по алгоритму Луна

4	5	8	1	2	6	1	2	1	2	7	4	8	4	5	7
8		16		4		2		2		14		16		10	
8		7		4		2		2		5		5		1	

$8 + 5 + 7 + 1 + 4 + 6 + 2 + 2 + 2 + 2 + 2 + 4 + 5 + + 4 + 5 + 1 = 60$

Фильтры имеют балльную систему; в результате анализа система оценивает каждую транзакцию, присваивая ей определенное количество баллов за соответствие каждому паттерну. Оценки варьируются от 0 (безопасно) до 100 (мошенничество).

Как компенсационная мера для канала, использующего слабый протокол шифрования, была перестроена система анализа.

При анализе применяется алгоритм «Сходство Джаро – Винклера», который рассчитывает числовую величину схожести между двумя заданными строками,

$$d_w = d_j + \left(lp\left(1 - d_j\right)\right),$$

где d_j – расстояние Джаро для строк;

l – длина общего префикса от начала строки до максимума 4-х символов;

p – постоянный коэффициент масштабирования, использующийся для того, чтобы скорректировать оценку в сторону повышения для выявления наличия общих префиксов; p не должен превышать 0,25, поскольку в противном случае расстояние может стать больше, чем 1.

$$d_j = \begin{cases} 0 \\ \frac{1}{3}\left(\frac{m}{|s_1|} + \frac{m}{|s_2|} + \frac{m-t}{m}\right), \end{cases}$$

где $|s_i|$ – длина s_i;

m – число совпадающих символов;

t – половина числа транспозиций [4].

Транзакционный анализ позволил увидеть отклонения по осям: x – количество покупок, y – частота оплат, z – сумма транзакции от типового поведения пользователя в части начислений и списаний по картам (рис. 4). Для этого нам необходимо выбирать общие статистические метрики: сумма транзакций, количество покупок по каждой карте (30-дневная выборка) и прочее. В среднем рабочая модель может опираться на множество показателей и учитывать уникальность каждого клиента. В таком случае 99% случаев мошенничества будут выбиваться из рядового поведения обычного клиента. Однако следует отметить, что создание персонального профиля для всех клиентов может плохо сказаться на скоростных характеристиках и в целом являться избыточной мерой.

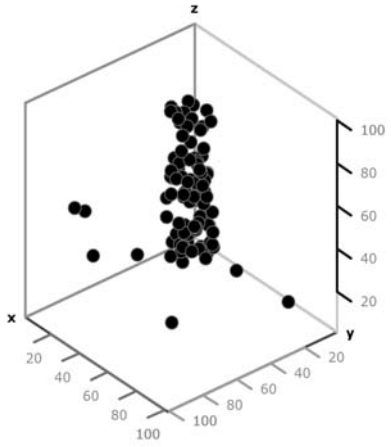

Рис. 4. Визуализация по активности использования распределения карт

Одним из таких моментов перехода к стандарту безопасности PCI DSS 3.2 является запрещение использовать для платежных страниц протоколы SSL и TLS ниже версии 1.2 из-за большого списка уязвимостей (Beast, Poodle, Logjam, Freak, Heartbleed).

В случае с Android 4 ситуацию можно изменить, установив сторонний браузер с поддержкой необходимых протоколов безопасности (например, Chrome). Ситуация с телевизорами гораздо сложнее – если версия стандарта PCI DSS 3.1 еще разрешала изолированное использование SSL для отдельных клиентов, то стандарт 3.2 однозначно это запрещает [3].

Обновить программное обеспечение на телевизионных устройствах со стороны клиента не представляется возможным. При отключении этих платежных страниц компания потеряет 4,23% от общего оборота, что составляет миллионы рублей в месяц.

Вариантом решения стало использование QuickResponseCode (матричный штрихкод).

QR-код был разработан японской компанией Denso-Wave [5] в 1994 году. Большое распространение штрихкодов в Японии привело к тому, что объём информации, зашифрованной в них, перестал устраивать промышленность. Вскоре японские компании представили новые современные способы кодирования небольших объёмов информации в графической картинке.

В отличие от старого штрихкода, который сканируют лазерным лучом, QR-код определяется датчиком или камерой как двумерное изо-

бражение. Три квадрата в углах изображения и меньшие синхронизирующие квадратики по всему полю кода позволяют нормализовать размер изображения, его ориентацию и угол расположения датчика к поверхности изображения. Точки переводятся в двоичные числа с проверкой по контрольной сумме.

При выборе контента на телевизионном устройстве и после формирования заказа на экране телевизионного устройства для пользователя отображается QR-код (рис. 5).

Рис. 5

Отсканировать его можно любым современным смартфоном, после чего в браузере, поддерживающем протокол TLS 1.2, открывается ссылка на персональную платежную страницу для оплаты заказа.

Таким образом, в результате внедрения новых схем взаимодействия, с учётом величины среднемесячного оборота в 2 млрд рублей, компания сможет сохранить клиентов, обеспечивающих доход около 80 миллионов в месяц.

В ходе данного исследования была рассмотрена деятельность компании – платежного провайдера на рынке интернет-эквайринга в городе Москве, занимающейся проведением платежей по банковским картам. Был проведён анализ проблем, связанных с переходом на PCI DSS версии 3.2, а именно: проведен срез статистики, учтены особенности оборудования, был перестроен алгоритм системы противодействия мошенничеству и введены компенсационные меры, позволившие обойти запрет на использование устаревшего протокола безопасности. Принятые меры помогли компании избежать потерь в миллиарды рублей в год.

Литература

1. Безмалый В.Ф. Тематическое издание Consumer Security. Microsoft Security Trusted Advisor.

2. Laudon, K.; Traver, C. E-Commerce Business, Technology, Society, 2007.

3. Интернет-портал: http://www.pcidss.com

4. William E. Winkler. Overview of Record Linkage and Current Research Directions. Research Report Series, 2006.

5. Интернет-портал: http://www.denso-wave.com