Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК004.031.43-049.65

Бердимырадов
Керим Мыратович

Защита транзакций в системах электронных платежей интернет-магазина

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-98 80 01«Методы и системы защиты информации, информационная безопасность»

_____
_____

Научный руководитель
Пулко Татьяна Александровна
кандидат технических наук, доцент
_____

Минск 2016

ВВЕДЕНИЕ

Узкоспециальная, мало кому интересная еще лет 10 назад тема электронных платежей и электронных денег в последнее время стала актуальной не только для бизнесменов, но и конечных пользователей. Модные слова "e-business", "e-commerce" знает, наверное, каждый второй, кто хоть изредка читает компьютерную или популярную прессу. Задача дистанционной оплаты (перевода денег на большие расстояния) из разряда специальных перешла в повседневные. Однако обилие информации по этому вопросу вовсе не способствует ясности в умах граждан. Как из-за сложности и концептуальной не проработанности проблемы электронных расчетов, так и в силу того, что многие популяризаторы работают зачастую по принципу испорченного телефона, на бытовом-то уровне все, конечно, понятно каждому. Но это до тех пор, пока не настанет черед практического освоения электронных платежей. Вот тут-то и обнаруживается непонимание того, насколько уместно использование электронных платежей в тех или иных случаях.

Между тем задача приема электронных платежей становится все более актуальной для тех, кто собирается заниматься коммерцией с использованием Интернета, а равно и для тех, кто собирается совершать покупки через Сеть. Эта статья предназначена и тем, и другим.

Основной проблемой при рассмотрении систем электронных платежей для новичка является многообразие их устройства и принципов работы и то, что при внешней похожести реализации в их глубине могут быть сокрыты достаточно разные технологические и финансовые механизмы.

Стремительное развитие популярности глобальное сети Интернет привело к возникновению мощного импульса развития новых подходов и решений в самых различных областях мировой экономики. Новым течениям поддались даже такие консервативные системы, как системы электронных платежей в банках. Это выразилось в появлении и развитии новых систем платежей - систем электронных платежей через Интернет, главное преимущество которых заключается в том, что клиенты могут осуществлять платежи (финансовые транзакции), минуя изнурительные и иногда технически трудноосуществимый этап физической транспортировки платежного поручения в банк. Банки и банковские учреждения также заинтересованы во внедрении данных систем, так они позволяют повысить скорость обслуживания клиентов и снизить накладные расходы на осуществление платежей.

В системах электронных платежей циркулируют информация, в том числе и конфиденциальная, которая требует защиты от просмотра, модификации и навязывании ложной информации. Разработка

соответствующих технологий защиты, ориентированных на Интернет, вызывает серьезные затруднения в настоящее время. Причина этого в том, что архитектура, основные ресурсы и технологии сети Internet ориентированы на организацию доступа или сбора открытой информации. Тем не менее, в последнее время появились подходы и решения, свидетельствующие о возможности применения стандартных технологий Интернет в построении систем защищенной передачи информации через Интернет.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является исследование методов защитытранзакций в системах электронных платежей интернет-магазина, выявление ихдостоинств и недостатков, и предложение мер по их усовершенствованию.

Задачи, решаемые в диссертационной работе:

− провести анализ литературно-патентных источников информации;

− описать существующие методы и протоколы защиты транзакций в системах электронных платежей интернет-магазин;

− на основе существующих методов предложить метод повышения эффективности защиты транзакций инициализируемых интернет-магазинами;

− оценить эффективность предложенного метода.

Основным методом, применяемым в диссертационной работе, является улучшение недостатков современного протокола защиты данных при передачи уязвимых данных кредитной карты во время транзакции, и на его основании разработать информационную систему эмулирующую данные улучшения.

Объектом исследования выступают протоколы защиты данных при осуществлении транзакций через интернет-магазины. Предметом исследования являются методы защиты транзакций, осуществляемых через интернет магазины.

Тема диссертационной работы соответствует приоритетным научным направлениям фундаментальных и прикладных исследований в сфере информации и инженерно-технической безопасности создания современных систем защиты информации.

Личный вклад магистранта

Содержание диссертации демонстрируют личный вклад автора. Основные научные и практические результаты были получены лично автором.

В работах, опубликованных совместно, автор фокусируется на способах улучшения недостатков современных протоколов защиты данных кредитной карты для транзакций осуществляемых интернет магазинами, а также алгоритме шифрования данных кредитной карты.

Научный руководитель Пулко Т.А., кандидат технических наук, доцент, является соавтором основных публикаций. Он сформулировал цели и задачи исследования, выбрал методы исследования, участвовал в планировании работы и обсуждении результатов, интерпретировал и обобщал полученные результаты.

Теоретическая и методологическая основа исследования

В основу диссертации легли результаты известных исследованийроссийских и зарубежных учёных в области информационнойбезопасности, концептуальных и методологических основ защиты информации.Для получения теоретических результатов исследования применялись методы защиты, используемые протоколах при передаче уязвимых данных кредитной карты.

Защищенная передача данных кредитной карты по сети Интернет осуществлялась на основе протокола SET. Система эмулирующая передачу данных кредитной карты реализована при помощи таких технологий как: HTML, CSS, JavaScript, MySql, PHP.

Апробация результатов диссертации

Теоретические и практические результаты диссертационных исследований докладывались и обсуждались на следующих научных конференциях:XVI научно-техническаяконференция студентов и молодых специалистов Белорусской государственной академии связи«Новые информационные технологии в телекоммуникациях и почтовой связи», Минск: БГАС, 24-25 мая 2016г.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликованы 1 печатные работы в сборнике «Тезисы докладов XVI научно-технической конференции студентов и молодых специалистов Белорусской государственной академии связи»

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, основной части из четырех глав, заключения, библиографического списка. Полный объем диссертационной работы составляет 76 страниц, включая 9 иллюстраций, библиографический список из 19 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы, сформулирована цель диссертации, изложены основные положения, выносимые на защиту.

В общей характеристике работы сформулированы ее цель и задачи, показана связь с научными программами и проектами, даны сведения об объекте исследования и обоснован его выбор, представлены положения, выносимые на защиту, приведены сведения о личном вкладе соискателя, апробации результатов диссертации и их опубликованность, а также, структура иобъем диссертации.

В первой главе кратко рассматриваются основные понятия Интернет-коммерции. Отмечается важность задач обеспечения информационной безопасности при осуществлении финансовых взаиморасчетов через сеть Интернет, Одним из важнейших элементов Интернет-коммерции являются системы электронных платежей в сети Интернет. Производится анализ проблематики современных электронных платежных систем

Во второй главе рассматриваются протоколы участвующие при платежных операциях в сети Интернет. Более детально исследован протокол SET – протокол для проведения операций по кредитной/банковской карте через небезопасные сети. Описаны преимущества применения протокола SET над другими протоколами, которые обеспечивают более надежное и защищенное проведение транзакций по кредитной карте через Интернет. Производится процесс сравнения протоколов и осуществляется выборка одного протокола для дальнейшего исследования.

В третьей главе исследуются технологии, средства и языки программирования, необходимые для реализации информационной системы эмулирующей процесс обмена данными между участниками финансовой транзакции. В процессе сравнения инструментов разработки, осуществляется выборка наиболее оптимальных, для дальнейшей работы с ними.

В четвертой главе исследуется на практике протокол обмена данными SET, на основе которого была разработана система наглядно отображающая процесс оплаты через Интернет с детальным исследованием объектов взаимодействующих в транзакции. Описывается разработанные прототип интернет магазина и процессинговой системы для эмулирования процесса транзакции.

Представлена реализованная программа для шифрования уязвимых данных кредитной карты. Описывается метод двух этапный метод шифрования, осуществляемый данной программой (номер карты шифруется закрытым ключом владельца + открытым ключом банка/платежного шлюза).

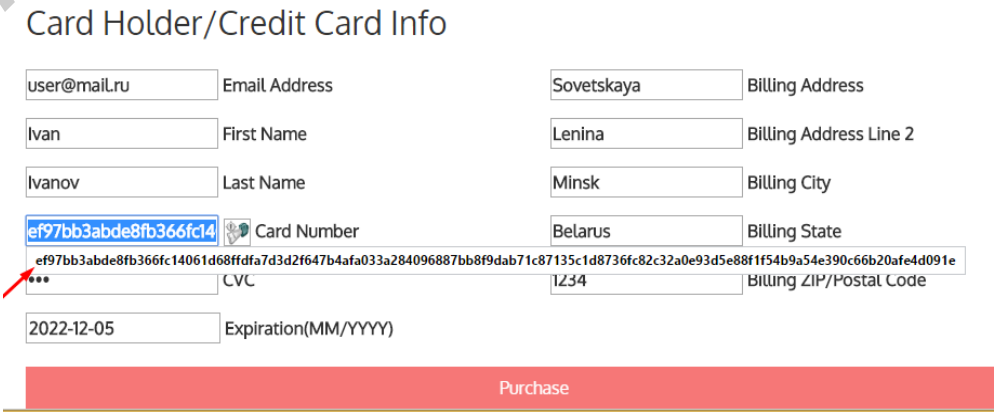

Рисунок 1 - Результат шифрования номера кредитной карты.

ЗАКЛЮЧЕНИЕ

Полученные в рамках диссертационной работы теоретические и практические результаты направлены на совершенствование защиты обмена данных кредитной карты в транзакции.

1. Проанализировав особенности передачи экономически ценных данныхкредитных карт в сети Интернет, можно сказать, что существующие сейчас протоколы защиты данных характеризуются имеющими недостатками.

Изучив протоколы, используемые при передаче данных, их характеристики, выявив их достоинства и недостатки, можно сделать вывод, что наиболее лучшим протоколом для проведения операций по кредитной/банковской карте через небезопасные сети (например Интернет), является SET. Он гарантирует защиту от компрометации данных, мошеннических транзакций по «правильным» картам, злоупотребления магазинов и от фиктивных банков. Так же был проведён анализ методов защиты в существующих протоколах, который позволил поставить цель и задачи исследования, которые необходимо решить при написании магистерской диссертации.

2. Анализ возможностей исследуемого протокола показал, что методы защиты применяемы в протоколе имеют ряд изъянов. Дорогое решение и высокие эксплуатационные расходы, сложное внедрение протокола, влекущее за собой существенные изменения в уже работающих программных обеспечениях в магазинах и эквайерах не являются единственными недостатками.

Очень существенный минус в том, что владельцу карточки требуется установить на свой компьютер довольно сложный в настройке CardholderWallet. Поэтому с целью улучшения показателей протокола, была разработана система обеспечивающая шифрование данных кредитной карты двух этапным шифрованием в среде web-браузера.

3. Анализ результатов показал, что разработанная система позволяет покупателям и банкам обмениваться данными кредитных карт в сети Интернет избегая посредников (платежные шлюзы) и дает уверенность в конфиденциальности и целостности данных.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1–А] БердимырадовК.М. Защита транзакций в системах электронных платежей интернет-магазина/ К.М. Бердимырадов, Т.А. Пулко // Новые информационные технологии в телекоммуникациях и почтовой связи: Тезисы докладов XVI научно-технической конференции студентов и молодых специалистов Белорусской государственной академии связи, 24-25 мая 2016г., Минск: БГАС.