Предотвращение мошенничества в системах электронных платежей на основе мониторинга и анализа событий в POS-сетях

Д.В. Козлов, Н.П. Садовникова, Л.В. Дружинина и Д.В. Петрова

***Аннотация* — Предотвращение мошенничества в системах электронных платежей является актуальной задачей, решение которой позволяет предотвратить целый ряд схем краж, как со стороны сотрудников, так и со стороны клиентов. В статье рассмотрены существующие технологии для реализации системы контроля безопасности функционирования POS-сетей в реальном времени и дан их подробный анализ. Кроме того, предложена концепция системы мониторинга безопасности в POS-сетях, представлена ее архитектура, а также метод анализа потока событий и выявления угроз.**

Ключевые слова — POS-сети, realtime web, анализ угроз, проактивный мониторинг, информационная система, базы данных реального времени.

I. Введение

Система электронных платежей имеет сложную структуру, объединяющую разнородные элементы, распределенные на большой территории. Поддержка бесперебойной работы Pos-системы требует значительных затрат и связана с решением серьезных проблем, среди которых одновременная обработка данных большого объема, интеграция разнородных данных и проблема безопасности осуществления электронных платежей. Проблема предотвращения мошенничества в сфере электронных платежей становятся все более актуальной в связи с ростом безналичных расчетов, появлением новых угроз и способов несанкционированного доступа к информации в POS-сетях. Защита информации в процессе осуществления платежных операций требует более строго контроля и обнаружения угроз в оперативном режиме. От скорости обнаружения и реагирования на кибер-угрозу зависит то, сможет ли система предотвратить утечку критически важной информации или нет. Кроме того, размер ущерба в случае реализации угрозы, экспоненциально возрастает на протяжении времени обнаружения, реагирования и противодействия [1].

Одним из решений, позволяющих значительно снизить риски может стать внедрение единой информационной системы администрирования POS-сетей и ее интеграция с сервисом проактивного мониторинга. Сервис мониторинга позволяет оперативно обнаруживать угрозы безопасности личных данных владельцев карт и эффективно их устранять. Реализация сервиса мониторинга, позволяющего осуществлять сбор и предоставление оператору POS-сети информацию о существующих угрозах и параметрах сети в реальном времени, способна максимально сократить время обнаружения атак и даже предотвратить их появление [2]. Современные технологии, такие как: базы данных реального времени и realtime web, способны помочь при решении задачи оперативного мониторинга POS-сетей, а также существенно сократить время на анализ угроз, их выявление и предотвращение.

II. Тренды в управлении POS-сетями

Для управления POS-сетями, сегодня успешно внедряются системы администрирования сетей POS-устройств.

Такие системы позволяют:

1) Вести учет имеющихся POS-устройств и их конфигурации.
2) Удаленно обновлять ПО на POS-устройствах.
3) Удаленно конфигурировать параметры работы POS-устройств.
4) Удаленно доставлять ключи безопасности по защищенным каналам. При этом отдельно выделяется задача доставки первого ключа в устройство (мастер ключа, под которым, в дальнейшем, передаются все остальные ключи).

Наиболее распространенными из подобных систем являются: First Data, Networks POS, TransLink.iQ, решения компании INETCO для мониторинга POS и др. Рассмотрим каждую из приведенных систем, выделив ее

Статья получена 11 октября 2017.

Дмитрий Викторович Козлов – Волгоградский государственный технический университет, Факультет электроники и вычислительной техники, Кафедра системы автоматизированного проектирования и поискового конструирования, аспирант (e-mail: mrdiko4@gmail.com).

Наталья Петровна Садовникова – Волгоградский государственный технический университет, Факультет электроники и вычислительной техники, Кафедра системы автоматизированного проектирования и поискового конструирования, доктор технических наук, доцент (e-mail: sadovnikova@vstu.ru).

Дружинина Лидия Викторовна - Волгоградский государственный технический университет, Факультет электроники и вычислительной техники, Кафедра вычислительной техники, старший преподаватель (e-mail: deli_86@mail.ru).

Петрова Дарья Владимировна - Московский технологический университет, Институт комплексной безопасности и специального приборостроения, Кафедра прикладная и бизнес-информатика, студент (e-mail: darina200896@mail.ru).

особенности:

1) First Data (Clover® Apps) – глобальная система в области администрирования POS-устройств. Предоставляет широкий набор инструментов администрирования POS-терминалов и периферийных устройств. Поддерживает стандарт безопасности инфраструктуры платежных карт PCI [3]. TransArmor от First Data использует комбинацию технологий шифрования и токенизации для полной защиты и удаления данных платежной карты из среды торгового предприятия, поэтому системы никогда не будут содержать фактические номера карт в транзакциях, которые обрабатывают. Это решение избавляет от необходимости хранить данные карт, заменяя их случайным номером, называемым «токеном». При этом решение TransArmor минимизирует риски за счет сокращения объема соответствия PCI, тем самым перекладывая «бремя» защиты данных держателях карт с пользователя на First Data.
2) TransLink.iQ - обеспечивает удобное управление POS-терминалами в режиме реального времени, безопасную и быструю передачу финансовых транзакций с POS-терминалов, а также возможности интеграции с внешними системами для передачи электронных платежей. Программное обеспечение было разработано в соответствии с требованиями международных компаний VISA International и MasterCard International и соответствует стандартам EMV. С 2007 года компания сертифицирована согласно требованиям уровня 1 PCI.

   Возможности TransLink.iQ включают в себя: управление сетью POS-терминалов; реализация карточных операций в POS-терминалах; безопасный и оперативный перевод карточных операций для банков-приобретателей; интеграция с внешними системами; удаленное обновление программного обеспечения POS-терминалов; мониторинг сети POS-терминалов.
3) Networks POS – система обеспечивает надежное управление POS-терминалами в режиме реального времени. Это самый быстрорастущий поставщик аппаратного и программного обеспечения точек продаж (POS) в индустрии розничной торговли. Система предоставляет выбор аппаратного / программного обеспечения, осуществляет внедрение и обучение сотрудников.
4) Mercury Processing Services International - предлагает полные и гибкие POS-услуги - от выбора POS-терминала и лизинга (услуги по закупкам) и обработки транзакций до разработки и интеграции программного обеспечения, настройки сервисов и обучения. Данная система работает на надежных и гибких платформах и позволяет поддерживать: нескольких поставщиков; различные типы связи (IP, Lease Line IP, Dial-UP / GSM); различные протоколы авторизации; интеграцию с торговыми кассовыми системами; мультивалютные транзакции между POS-серверами; бесконтактные транзакции (включая решение HCE).
5) INETCO Solutions for POS Monitoring and Retail Application Management. Решения INETCO для мониторинга POS и анализа каналов фиксируют данные транзакций в режиме реального времени и обеспечивают централизованное отображение всех POS и других розничных приложений с помощью легко настраиваемых информационных панелей, отчетов по запросу и аналитики взаимодействия с потребителями.

   Достоинствами данной системы являются:

   – возможность анализа поведения потребительских расходов и данных о продажах с градацией по времени, хранению, региону, типу карт / цифровых платежей, статусу завершения транзакции, POS-терминалам или типам регистра (например, самообслуживание, киоск и др.);

   – прогнозирование очередей, движение денежных средств, а также повышение рентабельности целевых маркетинговых компаний за счет лучшей сегментации рынка;

   – снижение зависимости от хостов авторизации и сторонних поставщиков коммутаторов (фиксация всех цифровых транзакции в сети розничных платежей и независимое отслеживание производительности транзакций, контроль покупательской способности);

   – возможность проактивного мониторинга жизненного цикла каждого взаимодействия с потребителями, снижение риска сбоев в работе службы, быстрое выявление проблем с авторизацией узлов и изоляция производительности или мошеннических угроз в любой точке розничной сети платежей.

На основе проведенного анализа систем администрирования сетей POS-устройств были сделаны следующие выводы. Функционал большинства систем ограничивается только возможностью удаленного обновления и конфигурирования POS-устройств. В некоторых системах, таких как TransLink.iQ и система мониторинга INETCO, реализованы функции мониторинга POS-сетей в реальном времени. Однако весь мониторинг в этих системах сводится к мониторингу аппаратных ресурсов, нагрузки на сеть передачи данных, а также отображению интегральных оценок по осуществленным транзакциям (количество и скорость обработки).

Сегодня, на рынке не существует систем, способных осуществлять сбор и отображение информации в реальном времени, о критических параметрах безопасности функционирования POS-устройств. Перечень всех необходимых параметров можно найти в стандарте безопасности платежных приложений (PA-DSS). Соблюдение требований этого стандарта позволяет минимизировать риски компрометации данных. Реализация сервиса мониторинга POS-сетей, обеспечивающего возможность контроля за выполнением требований PA-DSS в реальном времени, позволила бы существенно сократить время реагирования на угрозы и повысить защищенность системы в целом.

III. Подходы к построению системы мониторинга работы POS-сетей в реальном времени

В процессе мониторинга безопасности POS-сетей субъект (оператор системы администрирования) в оперативном режиме получает всю необходимую информацию об объекте наблюдения (POS оборудование, его состояние, конфигурация и выполняемые им действия) от самого устройства и других субъектов, взаимодействующих с устройством. Каждая операция, выполняемая устройством или выполняемая над устройством логируется, анализируется и информация о ней сообщается оператору в реальном времени. Собранная информация анализируется на наличие в ней инцидентов, свидетельствующих о наличии угрозы безопасности системе. Инциденты как правило проранжированы по степени угрозы. В зависимости от степени угрозы реакция на инцидент варьируется. Он может быть проигнорирован, а в некоторых случаях его обнаружение приведет к частичной или полной блокировке системы. Для поиска инцидентов используют продукционные модели, методы сопоставления с известными прецедентами и пр. [4].

При обнаружении инцидента, система должна выполнить действия, определенные для реагирования на этот инцидент. Это в первую очередь информирование оператора о произошедшем событии. Кроме того, возможны такие действия как: рассылка уведомлений другим ответственным субъектам, полное или частичное блокирование выполнения некоторых функций (как отдельного устройства, так и всей системы) и др.

Проиллюстрировать описанный процесс можно примером работы с ключами безопасности в POS-устройствах. При компрометации одного из ключей безопасности в системе, он должен быть заменен во всех использующих его устройствах. При этом, если скомпрометирован транспортный ключ, то замене также подлежат все ключи, которые были доставлены под ним. Ключ может быть скомпрометирован при утере самого устройства, содержащего этот ключ. Обнаружить потерю устройства можно, в том числе, наблюдая в системе мониторинга, тот факт, что устройство долго не информировало систему о своем статусе работы. В этом случае оператор должен поставить соответствующий признак данному устройству. В свою очередь система, должна определить ключи, которые использовались в утерянном устройстве и пометить их как небезопасные. Система также обнаруживает все устройства, которые содержат небезопасные ключи, блокирует их работу, до момента замены ключей, а также инициирует создание работы по замене необходимых ключей.

IV. Поиск инцидентов в потоке событий POS-сетей

Преимущественно система мониторинга должна отслеживать события (event), инициированные устройствами POS-сети или ее пользователями. Каждого инициализатора событий мы будем назвать Actor.

Каждое событие выполняется в рамках того или иного процесса (process). Простейший процесс состоит из линейной последовательности событий. Зачастую, процессы можно поделить на несколько подпроцессов, выполняемых последовательно или параллельно.

В большинстве кейсов достаточно анализа потока событий только одного Actor-а. В более сложных случаях для эффективного анализа состояния системы необходимо рассматривать события от нескольких Actor-ов.

Каждое событие системы описывается следующими параметрами:

1) Уникальный идентификатор события (e_{id}).
2) Тип/класс события.
3) Идентификатор процесса, к которому относится событие (p_{id}).
4) Идентификатор Actor-а, инициализировавшего событие.
5) Множество пар <Key, Value> - набор конкретных параметров события, зависящий от класса события. Например, дата-время возникновения события.
6) Строковое представление события $S(e_{id})$.

Каждый процесс анализируемый системой описывается следующим набором параметров:

1) Уникальный идентификатор процесса (p_{id}).
2) Тип/класс процесса.
3) Множество пар <Key, Value> - набор конкретных параметров процесса, зависящий от класса процесса.
4) Связанный список событий (e_i) процесса.
5) Массив подпроцессов (p_i) процесса.
6) Строковое представление процесса $S(p_{id})$.

   В случае если процесс не имеет подпроцессов, то строковое представление процесса представляет собой, последовательную конкатенацию строковых представлений событий, принадлежащих данному процессу (т.е. последовательная конкатенация всех $S(e_i)$).

   В случае если процесс имеет подпроцессы, то строковое представление процесса представляет собой массив строковых представлений его подпроцессов (т.е. массив всех $S(p_i)$).

Процессы, не имеющие подпроцессов, далее будем называть «простыми».

Таким образов, анализ простого процесса на наличие угрозы (инцидента), сводится к анализу его строкового представление.

Каждый инцидент, который необходимо выявить в общем потоке событий, также представляет собой, конечный набор событий. Однако, нахождение конкретного инцидента может быть осложнено присутствием шума из других событий также принадлежащих общему потоку событий и конкретному процессу. Этот шум может возникать, как в случае наличия «незначащих» событий в процессе, с точки зрения его анализа на наличие того или иного инцидента, так и в случае попыток злоумышленника, замаскировать свои действия. Также, зачастую, инцидент моет включать несколько итерационных последовательностей из однотипных событий. Таким образом, сведение задачи нахождения инцидента в

процессе, к задаче поиска подстроки (всех событий инцидента) в строковом представлении процесса, является не эффективным.

Для наиболее эффективного поиска инцидента в процессе, необходимо каждый инцидент сопоставить с конкретным шаблоном поиска. Таким шаблоном, может стать регулярное выражение, организованное таким образом, что если поиск совпадений регулярного выражения по строковому представлению процесса вернет ненулевой результат, то инцидент присутствует в процессе, в противном случае, данного инцидента в процессе не существует.

Рассмотрим данный метод на примере авторизации пользователя в системе. Предположим, что последовательный трехкратный ввод неверного пароля является инцидентом, который необходимо обнаружить. Пусть все действия пользователя в процессе авторизации A порождают некоторый конечный набор событий <a, b, c, d, s, f>, где:

– a – вход пользователя на страницу авторизации;

– b – попытка восстановить пароль с помощью телефона;

– c - попытка восстановить пароль с помощью электронной почты;

– d – неудачная попытка смены пароля при помощи старого пароля;

– s – пароль введен верно и пользователь авторизован в системе;

– f - пароль введен неверно.

Процесс A инициализируется при возникновении события «a» для конкретного пользователя и закрывается при возникновении события «s». Если пользователь уже имеет открытый процесс A, то все события из группы <a, b, c, d, s, f> при их возникновении добавляются в текущий процесс A.

Для поиска описанного инцидента необходимо составить для него регулярное выражение, которое будет проверятся при добавлении каждого нового события в процесс A. В данном случае корректным регулярным выражением, описывающим инцидент, является выражение – /([^f]*f){3}/ .

Описанное регулярное выражение найдет инцидент для всех возможных последовательностей A, которые его содержат. Например, в последовательностях «afbcdcdff» или «abcdfcdfcf» инцидент будет успешно обнаружен.

Стоит заметить, что подобный подход, позволяет анализировать только те события, которые находятся в области видимости конкретного процесса, что существенно сокращает сложность регулярных выражений, описывающих инцидент и увеличивают скорость его поиска.

Использование инструмента регулярных выражений, в конечно счете позволяет быстро построить и эффективно применить автомат для поиска инцидентов конкретного типа.

Концептуальная архитектура системы мониторинга работы POS-сетей

На сегодняшний день каждый клиент, внедряющий систему администрирования POS устройств, предъявляет требования к простоте доступа к актуальной информации, отдавая предпочтение облачным решениям. При этом к самим системам предъявляются требования высокой производительности, безопасности, разделения информации между разными уровнями ответственности пользователей, а также надежности и понятности.

В последнее время активно развиваются технологии, способные помочь в построении облачных решений, отвечающих предъявленным выше требованиям. К таким технологиям можно отнести так называемые Real-time web технологии, Event Sourcing [5], а также базы данных реального времени [6, 7].

Real-time web это в первую очередь технологии поддерживающие протокол полнодуплексной связи WebSocket [8]. Подавляющее большинство современных браузеров поддерживают и активно его развивают. Кроме того, сегодня трендом является использование шаблона проектирования издатель-подписчик (англ. publisher-subscriber или pub/sub) [9], который становится очень мощным инструментом при использовании технологии WebSocket. Подобная архитектура позволяет открыть канал обмена сообщениями прямо из браузера, причем инициатором отправки сообщения может стать как сервер, так и клиент. Таким образом, появляется возможность подписываться из браузера клиента на события, рассылаемые сервером и отображать актуальную информацию пользователю в момент ее появления.

Для организации облачного мониторинга потока данных, наиболее эффективным является интеграция баз данных реального времени. При этом хранить в этой БД необходимо не все данные, а только события, возникающие в системе, имеющие необходимую информацию для предоставления ее пользователю. Базы данных реального времени (БДРВ) должны обеспечивать синхронизацию, репликацию данных и резервирование для обеспечения отказоустойчивости в реальном масштабе времени. Поскольку БДРВ поддерживают язык SQL-запросов, то для организации доступа к информации возможен стандартный подход как к обычным реляционным БД.

Описанную выше архитектуру можно проиллюстрировать UML диаграммой компонентов, представленной на рисунке 1 [10].

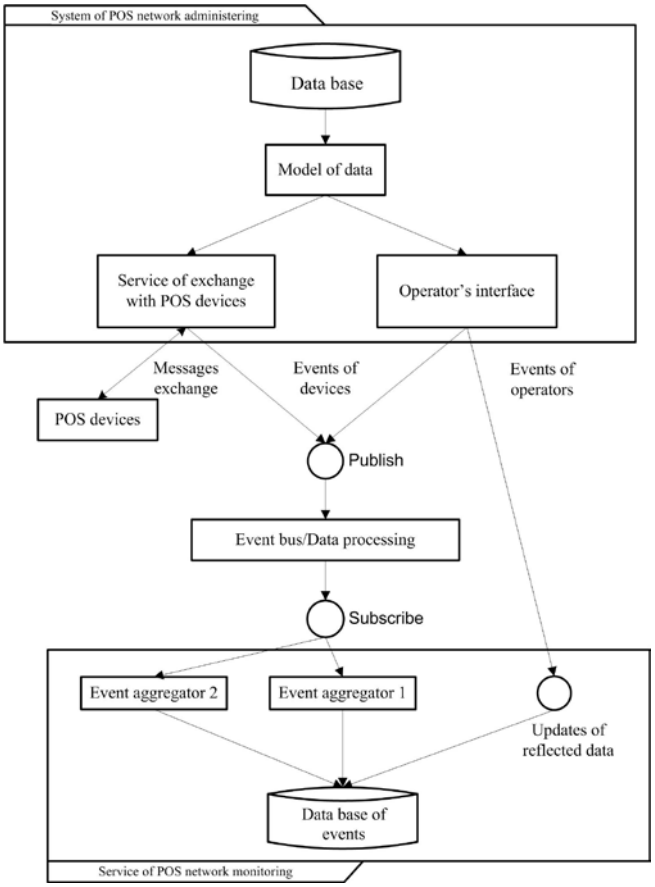

Fig. 1. Рис. 1 - Диаграмма компонентов системы мониторинга безопасности POS-сети

Из рисунка видно, что использование базы данных реального времени, хранящей события, возникающие в системе не отменяет наличие БД, хранящей в себе всю доменную область данных. Данная БД может быть в том числе и реляционной, для организации высокой скорости работы запросов и более строгого описания доменной области.

На сегодняшний день существует несколько баз данных реального времени, широко использующихся для решения подобного класса задач. К ним можно отнести: PipelineDB, CouchDB/PouchDB, Parse server и RethinkDB. Наиболее развитым и удачным решением на наш взгляд является использование базы данных RethinkDB [11].

V. Заключение

Проблема предотвращения мошенничества в сфере электронных платежей становится все более актуальной в связи с ростом безналичных расчетов и появлением новых угроз и способов несанкционированного доступа к информации. Для совершенствования систем защиты информации в процессе осуществления платежных операций все более актуальной становится решение задачи мониторинга и обнаружения угроз в реальном времени. Одним из решений данной задачи может стать внедрение системы администрирования POS-сетей и ее интеграция с сервисом мониторинга. Сервис мониторинга сети POS-оборудования позволит оперативно обнаруживать угрозы безопасности личных данных пользователей, совершающих безналичный расчет при помощи платежных терминалов и эффективно их устранять.

На основе анализа аналогов и трендов развития систем администрирования Pos-сетей был сделан вывод о том, что наиболее удачным является облачное решение, позволяющее осуществлять не только удаленное обновление и настройку параметров оборудования, но и оперативный контроль системы в целом. Особенный интерес представляет мониторинг параметров безопасности сети, а именно решение задачи мониторинга требований группы стандартов PCI.

Предложенная концепция системы мониторинга безопасности функционирования POS-сетей в реальном времени предназначена для интеграции с системами администрирования POS-сетей. При успешном внедрении подобной системы предполагается существенное уменьшение рисков, связанных с эксплуатацией POS-оборудования, а также оперативный анализ текущего состояния сети.

Библиография

[1] Manworren, N., Letwat, J., Daily, O., Why you should care about the Target data breach, Business Horizons, Volume 59, Issue 3, 1 May 2016.

[2] Lodi, G., Aniello, L., Di Luna, G.A., Baldoni, R., An event-based platform for collaborative threats detection and monitoring, Information Systems, Volume 39, Issue 1, 2014.

[3] The PCI Security Standards [Электронный ресурс]. Режим доступа: https://www.pcisecuritystandards.org/pci_security/ (дата обращения: 01.05.2017).

[4] Aihua Shen, Rencheng Tong, Yaochen Deng, Application of Classification Models on Credit Card Fraud Detection, 2007 International Conference on Service Systems and Service Management, 2007, pp 1 – 4.

[5] Martin Fowler, Event Sourcing: Capture all changes to an application state as a sequence of events. 12 December 2005

[6] Buchmann, A. "Real Time Database Systems." Encyclopedia of Database Technologies and Applications. Ed. Laura C. Rivero, Jorge H. Doorn, and Viviana E. Ferraggine. Idea Group, 2005.

[7] Kanitkar, Vinay & Alex Delis (1997). "A Case for Real-Time Client-Server Databases.". Brooklyn, New York: Polytechnic University. Retrieved 13 December 2006.

[8] I. Hickson, The WebSocket protocol draft-hixie-thewebsocketprotocol-76. Google, Inc. May 6, 2010.

[9] Buschmann, F., Meunier, R., Rohnert, H., Sommerlad, P., & Stal, M. (1996). Pattern Oriented Software Architecture, Volume 1: A System of Patterns. John Wiley & Sons, 1996, pp. 339—343.

[10] Козлов Д.В., Анализ методов обнаружения и предотвращения угроз мошенничества в информационных системах, Известия Волгоградского государственного технического университета. 2017. № 1 (196). С. 112-115.

[11] Gianluca Tiepolo, “Getting Started with RethinkDB”. March 2016.

Fraud prevention in the system of electronic payments on the basis of monitoring and analysis events in POS-networks

D.V. Kozlov, N.P. Sadovnikova, L.V. Druzhinina and D.V. Petrova

***Abstract* — Fraud prevention in the banking sphere is a very important type of activity, which can cover a whole range of fraud schemes – both from employees and customers. The article studies the existing technologies for realization of the system of security control over functioning of POS networks in real time and analyzes them in detail. Besides, the concept of a security monitoring system in POS networks is presented, its architecture is proposed, as well as a method for analyzing the flow of events and detecting fraud.**

***Key words:* POS networks, realtime web, fraud analysis, proactive monitoring, information system, data bases of real time.**