

## Безопасность платежных приложений и стандарт PA-DSS

11.06.2010

*В статье изложены проблемы безопасности приложений, в частности платежных приложений в рамках стандартов PCI DSS и PA-DSS, а также приведены основные предпосылки появления на свет стандарта PA-DSS, его особенности, назначение и преимущества соответствия.*

*Александр Поляков, руководитель направления аудита ИБ компании Digital Security, QSA, PA-QSA*

В данной статье прежде всего хотелось бы обратить внимание на важность безопасности приложений как таковых и платежных приложений в частности в рамках стандарта PA-DSS. Тема безопасности приложений давно входит в приоритетные направления деятельности нашей компании, и это не случайно. Последние годы вектор атак смещается вверх по модели OSI. Если раньше были актуальны проблемы безопасности сетевого уровня, атаки на сеть, платформы и операционные системы, то последние годы вектор заметно смещается в сторону приложений. Соответственного мнения придерживаются и западные компании, к примеру, в отчете инцидентов Verizon [1] за 2009 год 86% атак были направлены на WEB-приложения и только оставшиеся 14 – на инфраструктуру. С другой стороны, количество обнаруженных уязвимостей в программном обеспечении ежегодно растет. По данным лаборатории IBM X-Force [2] на 2009 год, в базе насчитывается порядка 44000 различных уязвимостей, и только исследовательским центром DSecRG [3] было обнаружено порядка 150 уязвимостей в 2009 году, а в мире существует десятки подобных центров. Кроме того, существует огромный черный рынок уязвимостей и исследователей, которые их продают, и информации об этих уязвимостях нет в публичном доступе. Таким образом, проблема безопасности приложений сегодня стоит довольно остро.

Если перейти от более общей проблемы к платежной среде и рассмотреть подробнее статистику того, какие системы чаще всего подвергаются атакам (Отчет Verizon), то это будут: POS-терминалы (32%), СУБД (30%), серверы приложений (12%), web-серверы (10%). На рабочие станции, серверы аутентификации, серверы резервного копирования, файловые хранилища и прочее выпадает только 10%. Из данной статистики также наглядно видна актуальность безопасности именно приложений, так как через их уязвимости чаще всего становится возможным получение доступа к данным.

Что же крадут злоумышленники и какие данные им интересны? Данный вопрос был освящен в двух различных отчетах: компании Verizon [3] и Trustwave [4]. По их данным, в 85% и 98% соответственно, целью атаки были именно карточные данные. Честно говоря, цифры шокирующие. Еще два интересных исследования были проведены данными компаниями. Компания Verizon [3] проводила поверхностную проверку на соответствие PCI DSS компаний, у которых произошел инцидент, связанный с кражей данных. В результате данных проверок была получена статистика, показывающая, на сколько процентов в среднем соответствовали компании различным требованиям стандарта PCI

DSS. Самым последним в этом списке было требование 6 («Безопасность приложений»), которому компании в среднем соответствовали на 5%. В отчете компании Trustwave [4] было показано что ни одна из компаний, в которой произошел инцидент, не соответствовала полностью пункту 6 стандарта PCI DSS, отвечающему за безопасность приложений. Что мы имеем в итоге, на самом деле парадоксально. С одной стороны, «Безопасность приложений» одно из наименее часто выполняемых требований, а, с другой стороны, через уязвимые приложения происходит большинство инцидентов, что странно со стороны компании, которая пытается защитить свои данные, но логично со стороны злоумышленника.

Если бы вы спросили у злоумышленника как украсть деньги, он бы без тени сомнения ответил: «Естественно через уязвимые приложения». Нельзя не согласиться с этим мнением, озвученным в статье на портале Pcworld [5], ведь, действительно, какой смысл придумывать какие-то сложные схемы, если через банальную SQL-инъекцию в платежном приложении можно получить базы номеров карт. Данная атака была не раз продемонстрирована в ряде отчетов по инцидентам, даже в тех компаниях, в которых были выполнены требования стандарта PCI DSS.

К слову об инцидентах, прямые потери финансовых структур в США от инцидентов составляют 7.5 млрд долларов в год. Для сравнения эти потери составляют стоимость порядка 50 крупных островов. В Англии потери от фрода, по данным APACS, составили порядка 500 млн долларов [6]. Что касается России, то цифры тоже существенные. По данным АРБР, годовой ущерб от действий кардеров составляет порядка 30 млн долларов [7]. Это все были прямые потери компаний, в которые не входят удар по репутации и потеря клиентов, а также возможная потеря бизнеса. Например, если вспомнить всем известный инцидент с Heartland, то стоимость акций этой компании на нью-йоркской бирже упала в 10 раз за 1 неделю, а такие падения даже в недавний кризис случались крайне редко.

### **После такого отнюдь не радужного вступления встает резонный вопрос - Что делать?**

Первым на помощь пришел документ Visa PABP, который являлся набором лучших практик по безопасности платежных приложений и состоял из различных требований к платежным приложениям. Тем не менее, множество действительно важных требований, относящихся к безопасности, через которые и осуществляются атаки на приложения, не были освещены в данном стандарте. К таким требованиям можно отнести: удаление критичных данных после истечения максимально допустимого срока хранения данных, хранение и передача паролей в зашифрованном виде, ряд требований по безопасному программированию, аудит управления изменениями и прочее.

Следующим этапом в повышении безопасности платежных систем было появление стандарта PCI DSS, который, в отличие от PABP, стал обязательным и регламентировал выполнение требований по безопасности для систем, обрабатывающих карточные данные. В нем уже достаточно четко были прописаны требования, относящиеся к любым приложениям и системам, которые обрабатывают карточные данные. Тем не менее, данный стандарт был направлен на компании, осуществляющие обработку карточных данных, а не на приложения, что на практике породило множество проблем, мешающих компаниям достичь соответствия PCI DSS из-за приложений, которые не поддерживают эти требования или напрямую им противоречат. Ведь в случае если у приложения, которое использует компания, передаются пароли в открытом виде, необходимо «накручивать» дополнительные средства защиты в виде шифрования и оформлять компенсирующие меры; если не был проведен

аудит на наличие программных уязвимостей, то необходимо приобрести и установить межсетевой экран уровня приложений, а если приложение, не дай Бог, хранит TRACK после авторизации, то компания и вовсе лишается возможности получить сертификат соответствия PCI DSS.

Учитывая важность требований безопасности к платежным приложениям с одной стороны, и совместимость этих приложений с требованиями стандарта PCI DSS с другой стороны, советом PCI SSC был разработан стандарт PA-DSS. Стандарт призван обеспечить безопасность приложений и совместимость с требованиями PCI-DSS и перенести ответственность за это на производителей программного обеспечения, у которых до этого момента руки были развязаны.

На самом деле, производитель, проходя аудит, получит ряд преимуществ. Во-первых, это возможность оставаться на рынке, так как после 1 июля 2012 года использование не сертифицированных приложений компаниями, попадающими под действие стандарта PCI DSS, будет запрещено. Во-вторых, это повышение защищенности приложения, что само по себе стоит не малых денег, и гораздо выгоднее его осуществить в связке сертификацией по PA-DSS, чем в рамках отдельной работы. В-третьих, это конкурентное преимущество на рынке, так как компании, выбирающие платежные приложения или собирающиеся поменять поставщика услуг, уже сейчас будут смотреть в сторону сертифицированных приложений. Ну и наконец, громкий пресс-релиз и листинг приложения на сайте PCI SSC в списке сертифицированных приложений – это еще один шаг для повышения “веса” приложения на рынке.

Преимущества использования сертифицированных по PA-DSS приложений компаниями, попадающим под действие стандарта PCI DSS очевидны. Во-первых, они так же получают возможность оставаться на рынке после начала даты действия стандарта, во-вторых, компания уменьшает количество необходимых для выполнения требований PCI DSS, перенося их на разработчика приложений и сокращая расходы на соответствие PCI DSS, в-третьих, компания получает руководство по безопасному внедрению (Implementation Guide), которое также помогает привести систему в соответствие стандарту PCI DSS и, наконец, в-четвертых, что наиболее важно – они получают безопасное приложение, тем самым существенно уменьшая риск компрометации данных.

Причем следует отметить, что эта безопасность не формальна. За ней стоит реальный аудит безопасности с применением общепризнанных методик, таких как OWASP и WASC на наличие программных уязвимостей. Стоит отметить, что аудит на наличие программных уязвимостей – это далеко не только статический анализ кода стандартными утилитами на наличие типовых строк, таких как `strcpy`, указывающих на возможное наличие уязвимости переполнения буфера, и не только `blackbox fuzzing` с использованием типовых программных средств, это еще и глубокий интеллектуальный анализ бизнес-логики приложения и поиск соответствующих уязвимостей в процессе реальной работы приложения. Как следует из опыта DSecRG по анализу защищенности бизнес-приложений, значительная доля уязвимостей относится именно к классу логических ошибок, которые не обнаруживаются стандартными утилитами, что также подтверждается известными западными компаниями в их отчетах. В списке TOP 10 уязвимостей, составленном компанией Cenzic [8] (производитель сканера для поиска уязвимостей в WEB-приложениях), на 2 месте (22% уязвимостей) находятся логические уязвимости, связанные с контролем доступа, а в аналогичном списке компании Trustwave логические ошибки занимают второе место, а третье и четвертое

принадлежит ошибкам авторизации и аутентификации. Для поиска ошибок такого класса в отличие от переполнений буфера и различных инъекций кода, не существует программных средств, полностью автоматизирующих данный процесс, поэтому уповать можно только на опыт конкретного эксперта в области анализа защищенности приложений.

И, естественно, самый главный мотиватор – это официальные сроки, установленные платежными системами. Условия Visa таковы: начиная с 1 июля 2010 года, вновь подключаемые к эквайерам торгово-сервисные предприятия должны использовать *только сертифицированные* по стандарту PA-DSS платежные приложения или быть проверены по PCI DSS. Начиная с 1 июля 2012 года, эквайеры должны гарантировать, что все торгово-сервисные предприятия и агенты используют *только сертифицированные* по стандарту PA-DSS платежные приложения. Условия MasterCard немного мягче. Они требуют, чтобы начиная с 1 июля 2012 года, все торгово-сервисные предприятия и поставщики услуг должны использовать *только сертифицированные* по стандарту PA-DSS платежные приложения.

#### Источники:

[1] Verizon. “Verizon 2009 Data Breach Investigations Report”

[http://www.verizonbusiness.com/resources/security/reports/2009\\_databreach\\_rp.pdf](http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf)

[2] DSecRG. Отчёт за 2008-2009 годы

[http://dsecrg.com/press\\_releases/?news\\_id=187](http://dsecrg.com/press_releases/?news_id=187)

[3] IBM X-Force Report

[http://www.risspa.ru/ibm\\_midyear\\_security\\_report\\_2009](http://www.risspa.ru/ibm_midyear_security_report_2009)

[4] TrustWave. Global Security Report 2010 Analysis of Investigations and Penetration Tests

[http://www.blackhat.com/presentations/bh-dc-10/Percoco\\_Nicholas/BlackHat-DC-2010-Percoco-Global-Security-Report-2010-slides.pdf](http://www.blackhat.com/presentations/bh-dc-10/Percoco_Nicholas/BlackHat-DC-2010-Percoco-Global-Security-Report-2010-slides.pdf)

[5] PCWORLD. PCI App Security: Who’s Guarding the Data Bank?

<http://pcworld.about.com/od/webbasedapplications/PCI-App-Security-Who-s-Guardi.htm>

[6] Денис Зенкин. Пластиковые войны

<http://www.itsec.ru/articles2/research/plastikovye-voiny>

[7] 7 Safe. UK Security Breach Investigations Report

[http://www.7safe.com/breach\\_report/Breach\\_report\\_2010.pdf](http://www.7safe.com/breach_report/Breach_report_2010.pdf)

[8] Cenzic. Web Application Security Trends Report Q3-Q4, 2009

[http://www.cenzic.com/downloads/Cenzic\\_AppsecTrends\\_Q3-Q4-2009.pdf](http://www.cenzic.com/downloads/Cenzic_AppsecTrends_Q3-Q4-2009.pdf)

## Об авторе

Александр Поляков. QSA, PA-QSA, Руководитель направления аудита ИБ компании Digital Security. Специализируется на проведении аудитов защищенности, тестов на проникновение, анализе защищенности бизнес-приложений и исследовательской деятельности в области информационной безопасности. Является известным экспертом по безопасности бизнес-приложений таких производителей, как Oracle и SAP, обнаружившим и опубликовавшим информацию о большом количестве уязвимостей в приложениях данных производителей. Один из основателей и руководитель исследовательского центра Digital Security Research Group [DSecRG], занимающегося поиском и анализом уязвимостей приложений и операционных систем. Автор ряда статей и исследований по информационной безопасности, автор книги «Oracle глазами аудитора: нападение и защита».

## О стандарте PA-DSS

Стандарт PA-DSS (Payment Application Data Security Standard) является, с одной стороны, развитием предписания Visa PABP (Payment Application Best Practices), а с другой стороны, адаптацией требований стандарта PCI DSS к приложениям.

Требования стандарта PA-DSS распространяются на приложения, обрабатывающие данные о держателях карт на этапе авторизации транзакции. При этом есть исключение – требования PA-DSS не распространяются на приложения собственной разработки и приложения, разработанные на заказ для одного единственного потребителя.

Все платежные приложения, выпускающиеся на рынок, должны проходить сертификацию по стандарту PA-DSS, которую могут выполнить только компании, обладающие статусом PA-QSA. Международные платежные системы предписывают торгово-сервисным предприятиям и поставщикам услуг использовать только сертифицированные по стандарту PA-DSS приложения, перечень которых опубликован и регулярно обновляется Советом PCI SSC.