**Безопасность электронных платежных систем.**

Платеж обычно состоит из транзакций с картой. В основном используется международный стандарт для операций по банковским картам с чипом EMV (Europay + MasterCard + VISA). Преимуществом карт с чипом по сравнению с картами с магнитной полосой является возможность аутентификации. Анализ [1, 10] показал отсутствие безопасного метода проверки подлинности карт с чипом. Используются различные атаки на карты EMV. Несмотря на то, что смарт-карта является защищенным от несанкционированного доступа устройством, а также удобна для переноски, она имеет не достаточно надёжного пользовательского интерфейса. Ему не хватает возможности ввода / вывода для взаимодействия с владельцем карты. Отсутствие возможности ввода PIN-кода напрямую допускает возможность его перехвата между клавиатурой и картой. С другой стороны, отсутствие надежного дисплея приводит к невозможности узнать реальную сумму транзакции. Нет также возможности проверить информацию о том, кто находится на другой стороне транзакции. Что, следовательно, приводит к возможности ретрансляции данных в другое место. Согласно [18] возможны несколько вариантов такой атаки POS-терминала: перехват скиммером, использование камеры, Double-Swipe(повторное несанкционированное считывание), “взломанный” терминал или поддельный терминал.

При нынешней криптосистеме на основе RSA возможен взлом защиты от копирования HDCP(«защита широкополосного цифрового содержимого») с помощью MitM(«человек с середине») атаки на основе дешевой платы с FPGA. Такая плата представляет собой вéнтильную мáтрицу, программи́руемую по́льзователем. Согласно решению консорциума EMV международный стандарт EMV переходит на криптосистему на основе ECC вместо RSA. Это асимметричная криптосистема, основанная на эллиптических кривых над конечными полями [2, 11]. Предлагается также использование обоих криптосистем RSA и ECDSA [12]. Спецификация для ECC, доступная в [13], определяет использование EC-DSA и EC-IES для подписей и шифрования, соответственно. В другом предложении [14] рассматривается криптосистема EC-Schnorr, которая минимизирует количество вычислений, необходимых для

генерации подписи, что важно из-за ограниченности вычислительной мощности процессоров смарт-карт [15]. Основной причиной миграции в ECC является ограничение по размеру открытых ключей действующей EMV на основе RSA, которые не могут быть больше чем 1984 бит [16]. Различия между криптосистемами с открытыми ключами существуют в нескольких параметрах [12]. Классические криптосистемы с открытым ключом, такие как RSA (Rivest, Shamir, Adleman), основаны на различной сложности выполнения прямого и обратного расчета, например, “умножения” и “факторизации” [17].

В настоящее время EMV подключают 3D Secure (Three-Domain Secure) защищенный XML протокол авторизации пользователей для CNP-операций (без присутствия карты), который используется как дополнительный уровень безопасности проведения платежей по покупкам товаров и услуг в интернете [3]. Для ряда стран базовым становится протокол 3D Secure Electronic Transactions (SET) [4]. Интеграция SET с EMV - это возможный путь для облегчения более широкого использования SET в транзакциях в интернет торговле, поскольку это может упростить регистрацию пользователя. Оценивается эффективность интеграции SET / EMV для снижения мошенничества в электронной торговле. Кроме того, рассматривается возможность реализации SET / EMV [5]. Транзакции без карты выполняются через Интернет и по телефону. Из-за отсутствия физического POS-терминала в этом типе транзакций нет стандартного процесса аутентификации владельца карты [1]. Это является основной проблемой безопасности таких транзакций. Для аутентификации используют либо протоколы на основе EMV, при которых клиент в момент совершения транзакции должен иметь свою карту. Аутентификацию такого типа (SET / EMV и EMV / CAP) называют двухфакторной, так как используются смарт-карта и пароль. При другом подходе (3D SET, другое называние 3D Secure, и 3D SSL) при оплате не нужно иметь свою карту. Банки и продавцы предпочитают онлайн-аутентификацию карт с помощью протокола 3D Secure [6], несмотря на недостатки этой технологии. Транзакции осуществляются через Интернет, телефон или почту в отсутствие физического POS-терминала, карты и владельца карты в одном и том же месте, что приводит к

увеличению доли банковских убытков [1]. Защитой от этого типа мошенничества является 3D Secure [7]. Например, Visa 3D Secure - это централизованная модель, включающая сервер каталогов (DS), который является центральной точкой для передачи информации о держателях карт между сервером эмитента (сервером управления доступом (ACS)) и продавцом, что приводит к увеличению, как числа сообщений, так и сложности [8]. Чтобы защитить владельца карты от атак с помощью спуфинга [9], 3D Secure использует подключаемые модули аутентификации (PAM), предоставляемые банком-эмитентом в момент аутентификации владельца карты [1, 8]. На первом этапе владелец карточки отправляет запрос продавцу, с информацией о карте. Затем web сайт продавца пересылает информацию владельца карты, используя либо сертификат, либо пароль, связываясь с банком-эмитентом в отношении номера счета. Эмитент затем отправляет сообщение на web сайт продавца, чтобы подтвердить регистрацию владельца карты. После подтверждения Access Control Server(ACS) от сервера торговому агенту передается подтверждение вместе с URL-адресом. Сервер Visa Directory Server (DS) отправляет подтверждение авторизации данных (необходимое для ACS) через браузер владельца карты. Сервер контроля доступа ACS отображает PAM, чтобы подтвердить владельца карты, а затем запросить информацию об аутентификации у владельца карты. В этом увлекательном процессе, в основном, участвуют всего четыре стороны. Кроме продавца и покупателя, это сервер консорциума Visa и сервер управления доступом ACS.

**Литература**


1. Siamak Solat. Security of electronic payment systems. https://arxiv.org/abs/1701.04556
2. Andrea Corbellini Elliptic curve cryptography: a gentle introduction. http://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/
3. https://cartoved.ru/tehnologii/bezopasnye-pokupki-v-internete-c-tehnologiej-3d-secure.html
4. B.Ratnakanth, P.S.Avadhani. A Review of Secure Authentication based e-Payment Protocol. IJACSA Vol. 8, No. 3, 2017.

5. Pita Jarupunphol, Chris J. Mitchell. Implementation Aspects of SET/EMV. https://link.springer.com/chapter/10.1007/978-0-387-35617-4_20
6. Murdoch, Steven J., and Ross Anderson. "Verified by visa and mastercardsecurecode: or, how not to design authentication." Financial Cryptography and Data Security.Springer Berlin Heidelberg, 2010. 336-342
7. http://www.visanet.com.pe/verified/demovisanet-web/resources/3DS_70015-01_System_Overview_external_v1.0.3.pdf
8. Pasupathinathan, Vijayakrishnan, et al. "Formal analysis of card-based payment systems in mobile devices."Proceedings of the 2006 Australasian workshops on Grid computing and e-research- Volume 54. Australian Computer Society, Inc., 2006.
9. Todd E. Humphreys, M. Ledvina, Mark L. Psiaki, Brady W. O'Hanlon, and Paul M. Kintner, Jr. Assessing the Spoofing Threat. https://gps.mae.cornell.edu/humphreys_etal_iongnss2008.pdf
10. Ильяшенко О. А. **Информационная безопасность индустриальных ИУС на FPGA: Нормативная база и SIS подход** / О. А. Ильяшенко, В. С. Харченко, Г. Ерван // Радіоелектронні і комп'ютерні системи. - 2013. - № 3. - С. 86–91. http://nbuv.gov.ua/UJRN/recs_2013_3_15.
11. Brzuska, Christina, et al. "An analysis of the EMV channel establishment protocol."Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013.
12. EMV Elliptic Curve Technical Report, Version 1.0, July 2001. https://www.emvco.com/specifications.aspx?id=72.
13. EMV Co. EMV Book 2 – Security and Key Management – Version 4.1z ECC – With support for Elliptic Curve Cryptography (May 2007).
14. www.emvco.com/faq.aspx?id=38
15. Schnorr, Claus-Peter."Efficient signature generation by smart cards." Journal of cryptology 4.3 (1991): 161-174.
16. Degabriele, Jean Paul, et al. "On the joint security of encryption and signature in EMV."Topics in Cryptology–CT-RSA 2012.Springer Berlin Heidelberg, 2012. 116-135.

17. Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21.2 (1978): 120-126.
18. Adida, Ben, et al. "Phish and chips." Security Protocols. Springer Berlin Heidelberg, 2009.