УДК 004.056.53 + 004.031.42 + 004.031.43

# БЕЗОПАСНОСТЬ ПОЛЬЗОВАТЕЛЯ ВЕБ-ОРИЕНТИРОВАННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

Щербаков А.С., Аноприенко А.Я.

*Донецкий национальный технический университет*

*Рассматриваются потенциальные угрозы безопасности пользователей веб- и интернет-ориентированных компьютерных систем (КС). Выполнен обзор частых ошибок пользователей и потенциальных уязвимостей, которые ведут к серьёзным потерям.*

## Введение

Сегодня, когда множество устройств, от персонального компьютера до телефона, подключены к Интернету, безопасность пользователя является очень важным вопросом. В одно мгновение можно потерять многое — от личной переписки до коммерческой тайны или денег на кредитной карте.

## 1 Авторизация пользователя

Наиболее распространённый механизм аутентификации пользователя опирается на использование паролей. Пароль достаточной сложности должен обеспечить сложность атаки перебором по словарю или полного перебора. На практике администраторы пользователи систем часто вдаются в крайности: либо используются типичные пароли («qwerty», «111», «p@ssw0rd») для привилегированных учётных записей, либо политики сложности паролей настроены таким образом, что пользователи не могут запомнить пароль, записывают его на бумаге и хранят рядом с консолью [1,2].

Следующей ошибкой в отношении паролей является использование одного пароля для нескольких ресурсов. Автору известны случаи, когда недобросовестный администратор веб-сайт проверял, подходят ли пароли пользователей ресурса к их почтовым ящикам.

В случае, если пользователь забыл пароль, обычно предусматриваются различные процедуры восстановления доступа. Наиболее распространённый — восстановление через e-mail. Поэтому следующим объектом интереса кибер-преступников является почтовый ящик. Для минимизации рисков взлома почтового ящика следует использовать уникальный пароль и проверить способы восстановления доступа к ящику: они должны быть удобными для пользователя, однако при этом не должны позволять злоумышленнику выдать себя за пользователя. Например, в случае утери пароля пользователю предлагается восстановить доступ по ответу на «секретный» вопрос. Часто в роли такого вопроса выступает один из стандартных, например: «Ваше любимое блюдо?» Очевидно, что вариантов ответа на такой вопрос не так уж и много [3].

Перечисленные аспекты являются вполне очевидными, однако продолжают часто встречаться на практике.

Кроме указанных вариантов, почтовый ящик может быть скомпрометирован через XSS-уязвимости. Это особенно актуально для веб-интерфейсов почтовых сервисов, в меньшей степени — для desktop-клиентов [4].

Дополнительной защитой учётной записи могут являться восстановление пароля только через мобильный телефон и двухфакторная авторизация. Полагается, что телефон всегда под рукой у пользователя, и похитить его достаточно сложно. В случае восстановления забытого пароля через мобильный телефон пользователю отправляется SMS-сообщение с уникальным кодом, который он должен будет предоставить системе для аутентификации. В случае с двухфакторной авторизацией для доступа к системе одновременно используются как стандартная связка логин-пароль, так и SMS-код, повышая надёжность аутентификации [5].

В то же время украинские провайдеры мобильной связи предоставляют услуги абонентам анонимно (на условиях предоплаты) — идентификация абонента производится по его требованию. Это является серьёзным компрометирующим фактором для использования мобильного телефона в качестве средства аутентификации. Для идентификации владельца номера провайдеры используют информацию о последних звонках, пополнениях мобильного счета — эти данные можно легко подделать: заставить пользователя перезвонить на номера злоумышленника, самостоятельно пополнить мобильный счёт пользователя. После этого можно сообщить провайдеру об утере телефона и заказать услугу восстановления sim-карты. Sim-карта текущего абонента блокируется, а злоумышленник может получить новую карту с номером «утерянной».

**2 Безопасность при совершении платежей**

В свете описанной уязвимости особую опасность представляет привязка он-лайн банкинга к мобильному телефону. Некоторые банки предоставляют возможность снятия денег со счета клиента без наличия платёжной карты, авторизовывая клиента через его мобильный телефон. В этом случае, заполучив новую sim-карту, злоумышленник может снять деньги с карточного счета владельца.

Следующим аспектом безопасности, о котором следует упомянуть, являются защищённые соединения. Многие сетевые протоколы передают данные — в том числе и пароли — в открытом виде. Перехватить трафик пользователя, особенно в публичных сетях, не составляет трудностей, поэтому для передачи чувствительных данных следует использовать только шифрованные соединения — https, sftp, ssh.

Следует помнить, что публичные wi-fi сети могут быть не только прослушаны, но и быть специально созданными злоумышленником для сбора данных. Это также касается различных прокси-серверов и «зеркал» для популярных ресурсов в Сети.

Ещё одна частая ошибка пользователей — разглашение реквизитов платёжной карты. Например, часто в ресторанах или кафе карта передаётся официанту, который удаляется с ней для оплаты через POS-терминал. В этот момент могут быть скопированы реквизиты карты, достаточные для совершения в будущем злоумышленником платежей этой картой: номер карты, срок действия, CVV2/CVC2-код [6]. Другой ошибкой владельцев платёжных карт является сообщение PIN-кода кассиру: злоумышленнику достаточно заполучить карту или сделать её копию и поторопиться к банкомату.

Никогда не следует передавать свою платёжную карту в чужие руки.

При платежах в Интернет лучше пользоваться специально выпущенной картой — многие банки выпускают виртуальную (только реквизиты) карту для Интернет-платежей — на счёт такой карты переводится требуемая сумма перед совершением

платежа, если карта будет скомпрометирована, вероятность получения денег злоумышленником будет мала, так как на этой карте не хранятся средства.

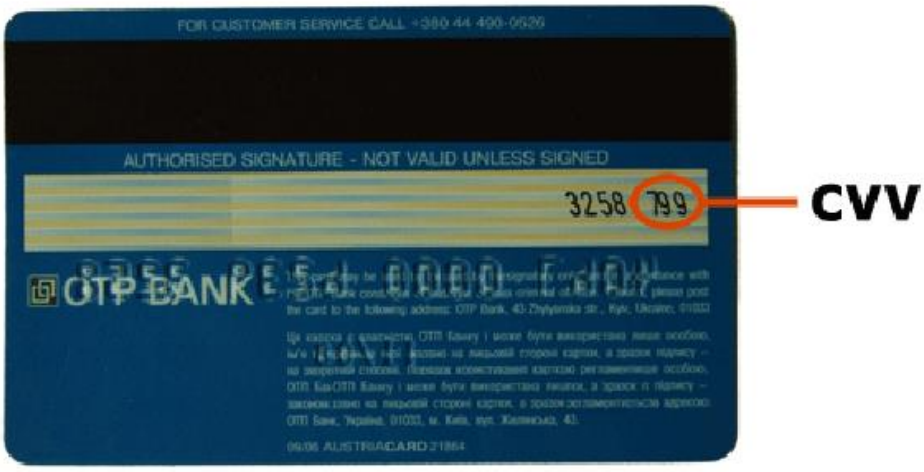


Рис. 1 — CVV2-код на платёжной карте VISA

**Выводы**

В докладе приведён краткий обзор наиболее частых и критичных по безопасности ошибок пользователей компьютерных систем и сетей, представляющих опасность в случае, если этими ошибками воспользуется злоумышленник.

Для предоставления удобного доступа к своим сервисам поставщики различных услуг вынуждены упрощать меры безопасности, поэтому на пользователя ложится задача сохранения в тайне идентифицирующих его данных. Эта задача отнюдь не проста, в основном из-за недостаточной грамотности пользователей в технических вопросах обеспечения безопасности.

**Литература**

[1] Mazurek M. L. et al. Measuring password guessability for an entire university //Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. – ACM, 2013. – С. 173-186.

[2] Top 100 Adobe Passwords with Count // электронный ресурс // название с экрана, - режим доступа: http://stricture-group.com/files/adobe-top100.txt

[3] Bonneau J., Just M., Matthews G. What’s in a Name? //Financial Cryptography and Data Security. – Springer Berlin Heidelberg, 2010. – С. 98-113.

[4] Grossman J. XSS Attacks: Cross-site scripting exploits and defense. – Syngress, 2007. - С. 1-13

[5] Suoranta S., Andrade A., Aura T. Strong authentication with mobile phone //Information Security. – Springer Berlin Heidelberg, 2012. – С. 70-85.

[6] DeGennaro R. P. Merchant Acquirers and Payment Card Processors: A Look Inside the Black Box: A Reprint from the" Economic Review". – DIANE Publishing, 2008. - С. 40.

**Как правильно ссылаться на данный доклад:**

Щербаков А.С., Аноприенко А.Я. Безопасность пользователя веб-ориентированных компьютерных систем // Информатика и компьютерные технологии / Сборник трудов IX международной научно-технической конференции 4-6 ноября 2013 г., Донецк, ДонНТУ. – 2013. С. 510-512.