УДК 621.391

С.П. Евсеев, О.Г. Король

Харьковский национальный экономический университет имени Семена Кузнеца, Харьков

ИССЛЕДОВАНИЕ МЕТОДОВ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

В статье рассматриваются основные методы построения систем двухфакторной аутентификации, оценивается риск различных методов онлайн-атак против системы двухфакторной аутентификации PassWindow. Проводится сравнительный анализ различных систем двухфакторной аутентификации с системой PassWindow в сфере противостояния различным интернет-сценариям атак.

Ключевые слова: *двухфакторная аутентификация, онлайн-атаки, социальная инженерия.*

Вступление. Существующие системы аутентификации базируются на предъявлении пользователем компьютеру статической пары идентификатор/пароль. Однако в таком случае пары могут быть скомпрометированы из-за халатности пользователей или возможности подбора паролей злоумышленником [11 – 14]. Значительные интервалы времени, в течение которых пароль и идентификатор остаются неизменными, позволяют применить различные методы их перехвата и подбора. Для повышения защищенности компьютерной системы администраторы ограничивают срок действия паролей, но в типичном случае этот срок составляет недели и месяцы, что вполне достаточно для злоумышленника. Радикальным решением является применение двухфакторной аутентификации, когда система просит пользователя предоставить ей «то, что ты знаешь» (имя и, возможно, некий PIN-код), и «то, что у тебя есть» – какой-либо аппаратный идентификатор, ассоциирующийся с этим пользователем [11, 12].

Целью статьи является исследование основных методов построения систем двухфакторной аутентификации, анализ рисков различных методов онлайн-атак против систем двухфакторной аутентификации на основе системы PassWindow. Проводится сравнительный анализ различных систем двухфакторной аутентификации в сфере противостояния различным интернет-сценариям атак.

Основная часть.

В настоящее время Интернет превратился в основной метод связи нашей современной жизни. Он, несомненно, будет основным инструментом для осуществления покупки и других финансовых операций. Появление этих технологий создало сопутствующей спрос на методы аутентификации, основанные не только на традиционных криптографических способах (шифрование, хеширование, цифровая подпись), но и на методах, основанных использовании нескольких факторов обеспечения подлинности лица, осуществляющего финансовую операцию. Двухфакторная система безопасности основана на том, что пользователь, кроме того, что знает пароль доступа к определенному имени пользователя (“логину”), – владеет и инструментом для получения соответствующего ему ключа доступа. Последним может служить сохраненный на компьютере электронный сертификат безопасности либо пришедший на личный телефон СМС с кодом подтверждения, либо же отпечаток пальца, снятый считывающим электронным устройством [11].

Методы строгой (двухфакторной) аутентификации чаще всего используются в финансовой сфере, но в принципе могут применяться практически в любой другой области. Основные способы построения систем двухфакторной аутентификации приведены на рис. 1 и подразделяются [13]:

1. *ПО для идентификации конкретного ПК*. В компьютер инсталлируется специальная программа, устанавливающая в нем криптографический маркер. Тогда в процесс аутентификации будут вовлечены два фактора: пароль и маркер, встроенный в ПК. Так как маркер постоянно находится на данном компьютере, пользователю для входа в систему нужно будет лишь ввести логин и пароль.

2. *Биометрия*. Использование биометрии в качестве вторичного фактора идентификации осуществляется путем идентификации физических характеристик человека (отпечаток пальца, радужная оболочка глаза и т.п.).

3. *Одноразовый e-mail- или sms-пароль*. Использование в качестве вторичного фактора идентификации такого пароля возможно путем отправки второго одноразового пароля на зарегистрированный адрес электронной почты или на мобильный телефон.

4. *Токен с одноразовым паролем*. Пользователю выдается устройство, которое генерирует постоянно изменяющиеся пароли. Именно эти пароли и вводятся

пользователем в дополнение к обычным паролям при аутентификации.

5. *Контроль извне.* Этот метод предполагает звонок из банка на предварительно зарегистрированный телефонный номер. Пользователь должен ввести пароль по телефону, и только после этого он получит доступ к системе.

6. *Идентификация с использованием гаджетов.* Такого рода идентификация осуществляется путем помещения криптографической метки на какое-нибудь устройство пользователя (например, на USB-накопитель, iPad, карту памяти и т.п.). При регистрации пользователь должен подсоединить данное устройство к ПК.

7. *Карточка с соскабливаемым слоем.* Пользователю выдается карточка с PIN-кодом, который используется лишь однажды.

Рис. 1. Основные системы двухфакторной аутентификации

Проведенный анализ показал, что в банковских системах, как правило, применяются системы двухфакторной аутентификации, основанные на одноразовых e-mail- или sms-паролях и различные типы токенов.

Сегодня несколько компаний предлагают системы двухфакторной аутентификации, основанные на генерации одноразовых паролей (One-Time Password – OTP), в числе которых RSA Security, VASCO Data Security и ActivIdentity.

Для ее реализации используются различные виды генераторов OTP. Генератор OTP представляет собой автономный портативный электронный прибор, способный генерировать и отображать на встроенном ЖК-дисплее цифровые коды. Для семейства устройств Digipass компании VASCO механизм генерации одноразовых паролей основан на криптографическом TripleDES-преобразовании набора данных, состоящего из 40 бит текущего времени и 24-битового вектора данных, уникальных для каждого идентификатора доступа. Полученный результат преобразования виден на дисплее в виде шести или восьми десятичных цифр, визуально считывается пользователем и вручную вводится как пароль в ответ на запрос прикладных программ об аутентификации. Периодичность смены паролей при этом составляет 36 с, таким образом, пользователь получает действительно одноразовый пароль для входа в систему [14].

На серверной части компьютерной системы этот пароль сравнивается с паролем, сгенерированным самим сервером по такому же алгоритму с использованием показаний текущего времени часов сервера и уникальных данных устройства, которые хранятся в специальной БД. При совпадении паролей разрешается доступ пользователя в систему. Принцип работы системы двухфакторной аутентификации фирмы VASCO представлен на рис. 2.

Рис. 2. Принцип работы системы двухфакторной аутентификации фирмы VASCO

Аутентификация на основе PassWindow. PassWindow является способом обеспечения двухфакторной аутентификации в онлайн среде. Она включает в себя две части матрицы – физический ключ с печатным рисунком на переносной пластиковой пластине и цифровой шаблон штрих-кода представленный в виде изображения на обычном электронном экране, например, на дисплее ноутбука или мобильного устройства. Они генерируют пользователю уникальный одноразовый пароль и набор цифр для отдельной транзакции, когда накладываются друг на друга. Этот пароль затем используется для онлайн-аутентификации и проверки подлинности транзакций. Информация о конкретной транзакции включена в эти цифры, такая как номер предполагаемого счета или суммы транзакции, что позволяет пользователю визуально подтвердить подлинность принятого запроса на аутентификацию.

Эти особенности делают PassWindow одним из очень немногих доступных в настоящее время механизмов аутентификации, которые предлагает надежную и достоверную защиту от новейших сетевых угроз безопасности «атак посредника» (Man-In-The-Middle (MITM)) [14].

Технология PassWindow базируется на уникальной способности части матриц передавать информацию таким образом, что она расшифровывается только при наложении физического шаблона знаков предполагаемого получателя (эту информацию пользователь имеет) после чего отображается шаблон штрих-кода (challenge pattern) на электронных сетевых устройствах пользователя, таких, как компьютер, смартфон и т.д. Сочетание ключа и шаблона штрих-кода показывает закодированную информацию только единственному пользователю, причем полный просмотр шаблона возможен только с прямого ракурса. Любой перехват штрих-кода через электронные устройства означает, что информация при утечке не будет достаточной для того, чтобы злоумышленник узнал секретный ключ шаблона пользователя в течение всего срока деятельности карты.

Шаблоны штрих-кода PassWindow могут существовать в виде уникальных статических изображений последовательности символов или в виде более расширенной анимационной версии, которая является основной темой этого документа. Эти анимированные штрих-коды состоят из последовательности статических шаблонов, каждый из которых содержит закодированные символы или же ничего не означают и просто динамически добавляют энтропию в весь шаблон. Последовательности шаблонов штрих-кода генерируются динамически сервером аутентификации таким образом, что каждый является уникальным (и, следовательно, имеющим смысл) только при использовании вместе с ключом к которому они подходят. Любое вмешательство или подделка шаблона штрих-кода будет пассивно представлена пользователю в виде появления комбинаций в шаблоне, который не соответствуют ожиданиям, например, случайно размещенные сегменты, которые не содержат никаких символов, случайные цифры, недостающие или избыточные цифры, появляющиеся в пределах одного шаблона, или проведение проверки информации, которая не относятся к активной транзакции.

Любой буквенно-цифровой код может быть надежно передан с помощью метода PassWindow, однако текущая реализация метода направлена на передачу коротких строк случайных цифр для использования их в качестве одноразового пароля в сочетании с цифрами, идентифицирующими уникальность транзакции проверки подлинности пользователя. Как только пользователь подтверждает, что уникальная информация в рамках транзакции – закодированная в штрих-кодах соответствует желаемой, он может завершить транзакцию, введя соответствующий одноразовый пароль. Основные этапы системы PassWindow представлены на рис.3.

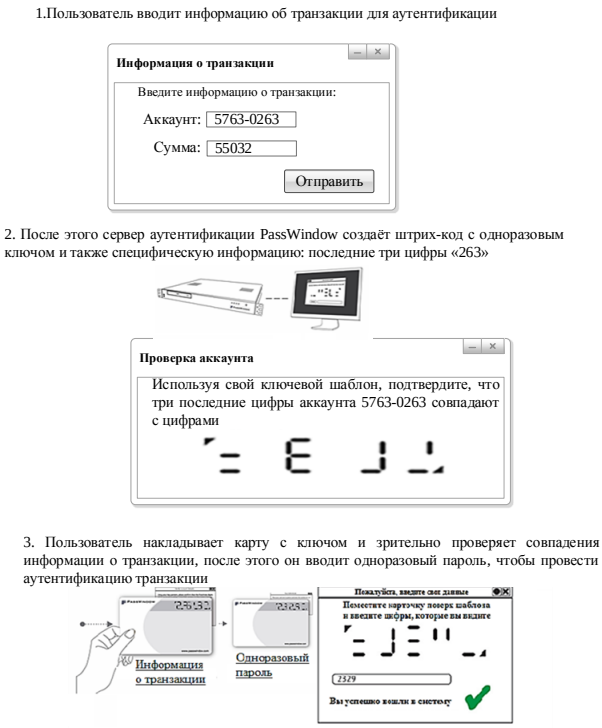

Рис. 3. Основные этапы работы PassWindow

Конструкция и профиль безопасности кодов аутентификации транзакций может быть изменен динамически для того, чтобы соответствовать широкому спектру конкретных задач онлайн-аутентификации.

Оценка безопасности систем двухфакторной аутентификации.

Анализ современных систем аутентификации показал, что их безопасность измеряется путем деления разности между стоимостью атак и выгоды для атакующего на стоимости защиты от них. Таким образом, дорогие, хотя и более безопасные методы, такие как криптографические PKI-устройства с собственными защищенными каналами связи, экранов и клавиатур оцениваются так низко по шкале безопасности, в то время как банковские системы все еще преимущественно опираются на самый дешевый и, казалось бы, наименее защищенных способ использования PIN-кодов и паролей. Общая стоимость и сложность развертывания таких устройств часто перевешивает пользу от их сверхвысокой безопасности.

Угрозы безопасности в сети можно разделить на сетевые атаки (информация, поступающая с удаленного агента) и локальные атаки, которые происходят от вредоносных программ уже, установленных на системе клиента, например, троянов, руткитов, и так далее. Часто оценки

безопасности аутентификации сосредоточены главным образом на сетевых атаках предполагая, что пользовательский терминал (т.е. настольный компьютер, ноутбук или мобильное устройство) является защищенной платформой [11 – 14]. Тем не менее, часто злоумышленник получает полный доступ к ПК жертвы через скрытые процессы связи, которые остались от вредоносных программ, использующие неисправленные дыры в безопасности лицензионного программного обеспечения.

Типичными методами атак являются:

• *Взламывание онлайновых баз данных* – похищение информации, хранящейся в торговых базах, данных.

• *Человек посередине / фишинг* – третья сторона вмешивается и олицетворяет клиента и сервера, заставляя записывать и/или изменять сообщения друг друга.

• *Атаки в области социнженирии* – клиентов обманываютс целью выведать их личные данные для последующей передачи хакеру.

• "*Человек в браузере*" – вредоносная программа, установленная на компьютере жертвы, для сообщения о сетевой активности, нажатий клавиш, а также данных захваченных с экрана хакеру, позволяя ему перехватывать данные перевода средств, в которых средства могут быть невольно искажены путём изменения отображаемой информации в браузере пользователя.

• *Атака полным перебором паролей пользователей* – сервер опрашивается со всеми возможными комбинациями паролей.

• *Простая кража* – подробности об аутентификации записаны или на карточке могут быть физически приняты и скопированы.

• *Наблюдение со спины* – злоумышленник может незаметно наблюдать, как пользователь вводит детали своей сделки.

Проведем *анализ методов двухфакторной аутентификации по сравнению с системой PassWindow* и их противостоянию различным типам атак.

Обозначение *SMS-систем или систем двухфакторной аутентификации на основе мобильных телефонов* является ошибочным, более точный термин – это "внеполосная" аутентификация. Тем не менее, с распространениям GSM, смартфонов и планшетов подключенным к сети, даже это преимущество безопасности может быть утеряно, если аутентификация транзакции пользователя осуществляется на самом мобильном устройстве. Кроме того, рост нежелательного программного обеспечения для мобильных устройств теперь позволяет злоумышленнику получить доступ к кодам аутентификации, отправленных через SMS не только с помощью традиционного перехвата с помощью вредоносного ПО [1], но и путем перехвата и дешифрования данных, передаваемых через сеть GSM-телекоммуникаций [2]. Атаки аутентификации мобильных устройств успешно проводятся и без таких технологий. Вместо этого злоумышленник просто выдает себя за пользователя устройства и запрашивает, чтобы все SMS сообщения направлялись на другой номер телефона в течение всей атаки [3]. Другой метод проверки подлинности использует камеру мобильного устройства для чтения изображения штрих-кода на рабочей станции пользователя, который закодирован с OTP информацией о транзакции. Этот метод содержит ошибку, предполагая, что операционная система на мобильном устройстве пользователя не подвержена подобной уязвимости к вредоносному ПО, как и все другие формы программного обеспечения, работающего с сетью[4].

В случае использования *биометрической аутентификации* данные о пользователе предлагаются для онлайн-аутентификации. Однако биометрические устройства аутентификации не могут взаимодействовать с локальных устройств или сети не подвергаясь атакам вредоносных программ и/или атакам "посредника" [5]. Этот метод так же невозможно повторно изменить, после того, как злоумышленник выдал себя за пользователя, используя биометрическую аутентификацию.

Биометрическая аутентификация предоставляет пользователю удобный способ генерации онлайн имени пользователя, однако при прослушиваемой сети и зараженного мобильного устройства, общая производительность безопасности таких методов не лучше, чем при использовании обычного имени и пароля пользователя.

Электронные аппаратные маркеры бывают нескольких видов и включают в себя различные функции безопасности аутентификации. Наиболее часто аппаратные маркеры генерируют одноразовые пароли (OTP) используя криптографические алгоритмы с внутренним секретным ключом, или, чаще, секретный ключ генерируется на основе общего, синхронизированного значения системного времени. Пользователь читает отображённые устройством цифры и вручную вводит их в свои терминалы для перекрестной ссылки с сервером проверки подлинности.

Этот простой метод электронной генерации OTP остается уязвимым к атакам "посредника", так как пользователи обязаны разглашать OTP без средств проверки контекста аутентификации.

В ответ на это многие производители маркеров добавили небольшую цифровую клавиатуру, заметно увеличив размер маркера, но позволяя пользователю вводить информацию о конкретных транзакциях, зашифрованных с помощью секретного ключа, прежде

чем пользователь вводит результат в своем терминале. Это является одним из типов проверки или подписания транзакции, и действительно обеспечивает некоторую защиту от атаки “посредника”.

Тем не менее, этот метод по-прежнему уязвим для атак, при использовании трудоемкого процесса ручного подписания транзакции. Время и внимание, необходимое для выполнения ручной операции успешно используются для отвлечения пользователя от контекста информации о сделках, которые пользователь принимает, и, следовательно, атаки могут быть успешно совершены в массовом масштабе [6, 7].

Печатные списки OTP / сетки чисел. Более старый метод предоставления одноразовых паролей это печатные списки случайно сгенерированных кодов связи или кодов авторизации транзакций на листе бумаги или скетч-карте. Каждый код доступа, запрашивается в последовательности и используется для проверки подлинности одной транзакции.

В качестве альтернативы, может использоваться печатная таблица символов, и сервер аутентификации выдаст штрих-код, запрашивая символы, расположенные в определенных координатах.

Оба метода используют ключи и сигналы, которые могут быть сообщены вербально. Это позволяет злоумышленнику спросить пользователя о следующем действительном коде через вредоносные программы, используя социальную инженерию или фишинг-атаки. Кроме того, относительно низкая энтропия списков или сеток требует частого изменения ключей, чтобы предотвратить повтор запроса кода злоумышленником.

Эти методы остаются уязвимыми для полного спектра атак “посредника” по тем же причинам, что и все методы аутентификации с неизвестным контекстом.

Гипотетические атаки на средство аутентификации PassWindow

Атаки “посредника” и фишинг (MITM) происходят, когда злоумышленник находится между клиентом и сервером и выдает себя за обе стороны, осуществляет перехват, запись или изменение взаимодействия между ними [8].

Фишинг является примером атаки MITM, в результате чего пользователю показывается поддельная страница аутентификации, таким образом, он сообщает свои данные аутентификации злоумышленнику пока пользователь не знает, что эта информация была подделана и будет использоваться злонамеренно [9]. Этот метод атаки является одним из наиболее эффективных. Стандартные методы одноразового пароля (OTP) не в состоянии обеспечить защиту, так как сам OTP просто передается злоумышленнику вместе с любой другой необходимой информации, такой как имя пользователя и пароль.

PassWindow решает эту проблему, предоставляя пассивную проверку на уровне транзакций, чтобы убедиться, что пользователь знает о подлинности транзакции, которую он выполняет до ввода OTP при завершении данной транзакции. Таким образом, PassWindow защищает от мошеннических атак MITM транзакций и обеспечивает аутентификацию в обоих направлениях – от пользователя к серверу и сервера к пользователю.

Атаки в области социнженирии.

В “атаках социальной инженерии” пользователя убеждают разгласить его личные данные, и в случае аппаратных маркеров – его одноразовые пароли.

Комбинации клавиш PassWindow не так легко передается в устной форме или через печатные символы, тем самым устраняя наиболее удобные телефонные атаки социальной инженерии, которые используются против электронных аппаратных маркеров, метод, который получил название “вишинг” [10]. Эти атаки используют человека, который звонит пользователю и выдает себя за уполномоченного представителя обслуживания. Устный запрос делается для чтения действительного кода авторизации с устройства аутентификации жертвы, что, якобы, позволит звонящему выявить, например, “важную конфиденциальную информацию”. Маловероятно, что злоумышленник попытается извлечь комбинацию клавиш PassWindow от клиента этим способом, так как трудно на словах объяснить визуальные характеристики сегмента PassWindow матрицы.

Человек в браузере или хакерское проникновение. Злоумышленник получает отчеты от вредоносных программ, установленных на компьютере жертвы и обнаруживает, что жертва обращается к сайту финансовой организации, программное обеспечение изменяет данные формы в браузере на такие, чтобы другой объем средств передавался на чужой счет – обычно гибридный. Владелец такого счета затем передает эти деньги злоумышленнику.

Проверка информации о проходящей сделке может быть закодирована в штрих-коде шаблона PassWindow. Это может заверить пользователя, к примеру, что средства переводятся на правильный счет.

Простая кража.

Единственным способом для открытия и копирования ключевого шаблона PassWindow является прямое копирование карты сразу после её получения. Эта возможность снижается путем введения оттенка, который можно распечатать поверх шаблона, что затруднит попытки фотографирования и ксерокопирования.

Однако, поскольку PassWindow используется в стратегии двухфакторной аутентификации, простое знание ключевого шаблона является недостаточным для мошеннической аутентификации без знания логина или пароля жертвы.

Подглядывание со спины. PassWindow защищён против "подглядывания со спины" – незаметного наблюдения за тем, как пользователь вводит свои данные. Поскольку ключ / штрих-код представляют собой одноразовый пароль, подглядывающий не может извлечь выгоду из его знания.

Опять же, оттенок, напечатанный поверх ключевого шаблона на карте делает шаблон невидимым никому, кроме пользователя.

Прямая атака на сервер аутентификации PassWindow. Злоумышленник может попытаться непосредственно атаковать сервер аутентификации PassWindow, чтобы нарушить целостность всей процедуры аутентификации PassWindow. Сервер аутентификации PassWindow использует очень простой и ограниченный протокол связи, и вся обработка аутентификации осуществляется на самом сервере. Его функциональность ограничена созданием данных изображения штрих-кода, и получения коротких кодов доступа и значения идентификаторов пользователей, и в конечном счете выдачи ответа (да/нет) на запрос проверки подлинности. Кроме этого, различные стратегии аутентификации управляют удовлетворительной скоростью запросов и сроков ответа. Эта базовая цифровая связь с сервером аутентификации дает небольшую возможность злоумышленнику непосредственно занять сервер любым эффективным способом, что может привести к успешному доступу.

Аналитическая атака на секретный ключ.

*З*лоумышленник может попытаться вывести печатную комбинацию клавиш пользователя через аналитическую (например, статистическую или алгебраическую) атаку. Это может быть осуществлено с использованием сложной программы "атака посредника" или вредоносных установленных локально программ на основе мониторинга, что позволит перехватывать и штрих-коды PassWindow и соответствующие ответы пользователя. Со временем, как у злоумышленника накапливаются эти пары запрос /ответ, он может потенциально получить некоторое представление о ключевом шаблоне PassWindow через анализ перехваченных данных.

В интересах тестирования уязвимости PassWindow к такому нападению, был построен алгоритм взлома, который пытается использовать эти принципы для выполнения указанного анализа.

Сам алгоритм использует технику грубой силы. Он начинается с генерации всех комбинаций, в результате чего, цифры, являющиеся результатом могут быть размещены в шаблоне.

Например, шестизначный результат в шаблоне из 14-колонок дает следующие возможные варианты (среди прочих):

2 – 5 – 7 – 2 – 4 – 3 – – –

2 – 5 – 7 – 2 – 4 – – 3 – –

2 – 5 – 7 – 2 – 4 – – – 3 –

2– – 5– – 7 – 2 – 4 – – 3

Каждая комбинация оценивается по известному штрих-коду для расчёта может ли он представить цифру в запросе или нет.

Сегменты могут либо присутствовать, если они необходимы для построения решения, либо нет, если они должны отсутствовать для него, либо могут быть неизвестными, если сегмент находится далеко от цифры, или налагается на бит штрих-кода.

После отдельного набора комбинаций для каждого перехвата, алгоритм ищет несовместимости между комбинациями. Он берёт первую комбинацию первого набора, сравнивая его, в свою очередь с каждой комбинаций второго комплекта. Если она несовместима с каждой комбинацией во второй группе, комбинация отбрасывается.

Проверка совместимости продолжается таким образом, что каждая комбинация в каждом наборе сравнивается с комбинациями каждого другого набора. Если комбинация отбрасывается, тогда каждый последующий набор необходимо пересмотреть. Путем перебора и анализа достаточного количества перехватов алгоритм способен вывести ключевой шаблон с достаточной степенью достоверности.

Однако, данная атака требует значительного количества перехватов взломщиком: от 20 – 30 в случае малых шаблонов, сотен для больших шаблонов, нескольких тысяч в случае использования метода в анимационном режиме повышенной безопасности.

Таким образом, безопасность PassWindow состоит не столько в сложности алгоритма, необходимого для ее решения, как в системной трудности извлечения достаточного количества информации от цели. Если PassWindow используется правильно, то есть высокая вероятность того, что необходимая информация может быть недоступна даже для самых опытных хакеров.

Подделанные (ослабленные) штрих-коды

Злоумышленник может попытаться ослабить защиту PassWindow, изменяя частоту кадров из настоящего (перехваченного) штрих-кода, прежде чем доставить ослабленный (упрощенный) штрих-код пользователю. Этот метод уменьшает энтропию штрих-кода, чтобы изменить детали, которые могли бы упростить анализ перехвата запросов / ответов. Однако, явно поврежденный штрих-код, пассивно предупреждает пользователя о попытке нападения, вызывая его подозрения об использовании вычислительной техники и коммуникационных каналов.

Вывод. Проведенный анализ методов двухфакторной аутентификации показал, что практически все системы в своей основе используют криптографические алгоритмы (таблицы) и подвержены как традиционным атакам на

криптографические процедуры, так и атакам, на основе социальной инженерии, и не в полном объеме обеспечивают безопасность их использования в банковских системах. Особое место среди них занимает система двухфакторной аутентификации PassWindow, основанная на использовании штрих-кодов для формирования аутентификатора эффективнее других противостоит современным онлайн-атакам.

Список литературы

1. Chickowski, Ericka (5 Oct. 2010) – "'Man In The Mobile' Attacks Highlight Weaknesses In Out-Of-Band Authentication"

2. Elad Barkan -Eli Biham -Nathan Keller — "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Computer Science Department Technion -Israel Institute of Technology

3. Brett Winterford — "$45k stolen in phone porting scam", 6 Dec. 2011

4. Schwartz, Mathew J. (13 Jul. 2011) — "Zeus Banking Trojan Hits Android Phones"

5. Christian Zeitz, Tobias Scheidat, Jana Dittmann, Claus Vielhauer, Elisardo González Agulla, Enrique Otero Muras, Carmen García Mateo, José L. Alba Castro, Dpt. of Computer Science, Univ. of Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany, Signal and Communications Processing Dpt., Univ. of Vigo, Campus Universitario, 36310 Vigo,Spain — "Security issues of Internet-based biometric authentication systems: risks of Man-in-the-Middle and BioPhishing on the example of BioWebAuth"

6. Dunn, John E (3 Jul. 2010) — "Trojan Writers Target UK Banks With Botnets"

7. Het Belang Van Limburg, (24 Jul. 2010) — "Belgian court found fraud in Internet banking"

8. NETRESEC Network Security. (27 Mar. 2011) — "Network Forensic Analysis of SSL MITM Attacks"

9. Metropolitan Police Service. (3 Jun. 2005) — "Internet Banking Targeted Phishing Attack"

10. Brian Krebs, (20 Jun. 2010) — "Spike in phone phishing attacks" — http://krebsonsecurity.com/2010/06/a-spike-in-phone-phishing-attacks/

11. Двухфакторная Аутентификация [Электронный ресурс]. – Режим доступа: http://www.aladdin-rd.ru/solutions/authentication/

12. Настройка двухфакторной аутентификации [Электронный ресурс]. – Режим доступа: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-two-factor-authentication-gransden.html?locale=ru

13. Семь методов двухфакторной аутентификации [Электронный ресурс]. – Режим доступа: http://www.infosecurityrussia.ru/news/29947

14. Двухфакторная аутентификация при удаленном доступе [Электронный ресурс]. – Режим доступа: http://itc.ua/articles/dvuhfaktornaya_autentifikaciya_pri_udalennom_dostupe_23166/

Рецензент: *д.т.н., проф. Хорошко В.А., Национальный Авиационный университет, Киев.*

Автори:

ЕВСЕЕВ Сергей Петрович

Харьковский национальный экономический университет имени Семена Кузнеца, Харьков, к.т.н., с.н.с, доцент кафедры информационных систем.Тел. 095-360-66-13, E-mail: evseev_serg@inbox.ru.

КОРОЛЬ Ольга Григорьевна

Харьковский национальный экономический университет имени Семена Кузнеца, Харьков, преподаватель кафедры информационных систем.

Раб. тел. – 702-18-31, E-mail: korol_o@mail.ru

ANALYSIS METHODS TWOFACTOR AUTHENTICATION

S. Evseev, O. Korol

Analysis the basic methods for constructing two-factor authentication systems, risk is assessed various methods of online attacks against two-factor authentication PassWindow. A comparative analysis of the different systems with two-factor authentication system PassWindow in opposition to various Internet attack scenario.

Keywords: two-factor authentication, online attacks, social engineering.

ДОСЛІДЖЕННЯ МЕТОДІВ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ

Євсеєв С.П., Король О.Г.,

Досліджені основні методи побудови систем двофакторній автентифікації, оцінюється ризик різних методів онлайн-атак проти системи двофакторній автентифікації PassWindow. Проводиться порівняльний аналіз різних систем двофакторній автентифікації з системою PassWindow у сфері протистояння різним інтернет-сценаріями атак.

Ключові слова: двофакторна автентифікація, онлайн-атаки, соціальна інженерія