Розглядаються основні методи побудови систем двофакторної автентифікації. Аналізується система PassWindow, що забезпечує двухфакторную автентифікацію на унікальній здатності накладення фізичного шаблону знаків передбачуваного одержувача і шаблону штрих-коду, одержуваних через електронно-мережеві пристрої користувачів. Пропонується практичний алгоритм моніторингу даної системи, здатний отримати унікальний шаблон штрих-коду за фіксовану кількість перехоплень

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

Рассматриваются основные методы построения систем двухфакторной аутентификации. Анализируется система PassWindow, обеспечивающая двухфакторную аутентификацию на уникальной способности наложения физического шаблона знаков предполагаемого получателя и шаблона штрих-кода, получаемых через электронно-сетевые устройства пользователей. Предлагается практический алгоритм мониторинга данной системы, способный получить уникальный шаблон штрих-кода за фиксированное количество перехватов

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

УДК 621.391
DOI: 10.15587/1729-4061.2015.38779

АЛГОРИТМ МОНИТОРИНГУ МЕТОДА ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ СИСТЕМЫ PASSWINDOW

С. П. Евсеев
Кандидат технических наук, доцент
Кафедра информационных систем
Харьковский национальный экономический университет им. С. Кузнеца
пр. Ленина, 9-а, г. Харьков, Украина, 61166
E-mail: Evseev_Serg@inbox.ru
В. Г. Абдуллаев
Кандидат технических наук
Азербайджанская Государственная Нефтяная Академия (АГНА)
Институт Систем Управления НАНА
пр. Азадлыг, 20, г. Баку, Азербайджан, AZ1010
E-mail: abdulvugar@mail.com

1. Введение

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 [1]. Механизмы двухфакторной аутентификации, как правило, используют два независимых канала передачи конфиденциальных данных и только соединенные данные позволяют сгенерировать аутентификатор и подтвердить личность уполномоченного пользователя [1, 3–5].

2. Анализ литературных данных и постановка проблемы

Типичным примером двухфакторной аутентификации является работа банкомата. Чтобы получить доступ к услугам банкомата нужно иметь что-то (банковскую карту) и знать что-то (ПИН-код). Если злоумышленники украдут карту, они не смогут ей воспользоваться без ПИН кода (вот почему не стоит писать ПИН код на карте). Использование двух факторов для аутентификации является более надежной защитой.

Метод двухфакторной защиты работает в Интернет аналогично работе банкомата с картой и ПИН кодом. Вы можете использовать логин и пароль для доступа к онлайн аккаунтам. Однако, после успешного ввода пароля, сайт не предоставляет доступ к вашей учётной записи, а запрашивает второй фактор аутентификации, например, проверочный код или отпечатки пальцев [4, 5].

В основе механизмов обеспечения криптостойкости формируемого аутентификатора в протоколах двухфакторной аутентификации, как правило, используются криптографические алгоритмы формирования псевдослучайных последовательностей. Проведенные исследования гипотетических атак показывают, что практически все предлагаемые в коммуникационных системах способы формирования аутентификатора подвержены атакам и недостаткам [1, 6–8]. Кроме того,

дальнейшее развитие вычислительной техники позволяет рассматривать комбинированные атаки с использованием социальной инженерии, что значительно повышает успех реализации атаки.

3. Цели и задачи исследования

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 [1–4]. 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 [1, 2].

Целью работы 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.

Для достижения поставленной цели были поставлены следующие задачи:

– провести анализ способов построения протоколов двухфакторной аутентификации;

– исследовать протокол двухфакторной аутентификации на основе системы PassWindow;

– проанализировать известные гипотетические атаки на протоколы двухфакторной аутентификации;

– рассмотреть алгоритм мониторинга протокола двухфакторной аутентификации на основе системы PassWindow.

4. Способы построения протоколов двухфакторной аутентификации

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 подразделяются [3]:

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.

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. Принцип работы системы двухфакторной аутентификации фирмы VASCO представлен на рис. 1.

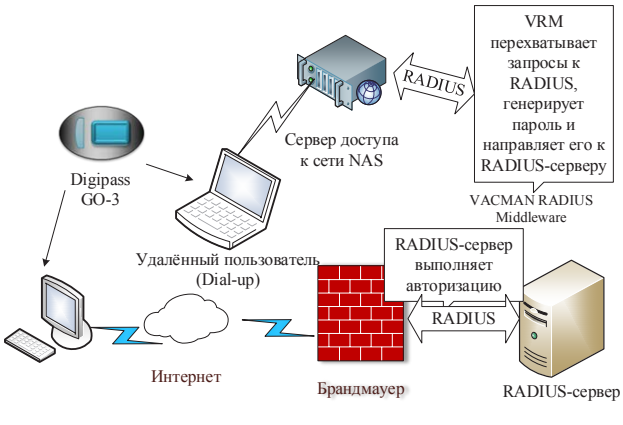


Рис. 1. Принцип работы системы двухфакторной аутентификации фирмы VASCO

Для ее реализации используются различные виды генераторов OTP. Генератор OTP представляет собой автономный портативный электронный прибор, способный генерировать и отображать на встроен-

ном 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 [4]. 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.

5. Аутентификация на основе PassWindow

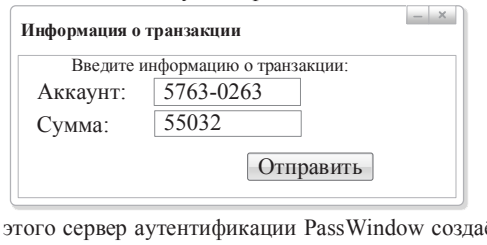
PassWindow является способом обеспечения двухфакторной аутентификации в онлайн среде. Она включает в себя две части матрицы – физический ключ с печатным рисунком на переносной пластиковой пластине и цифровой шаблон штрих-кода представленный в виде изображения на обычном электронном экране, например, 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)) [4].

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.

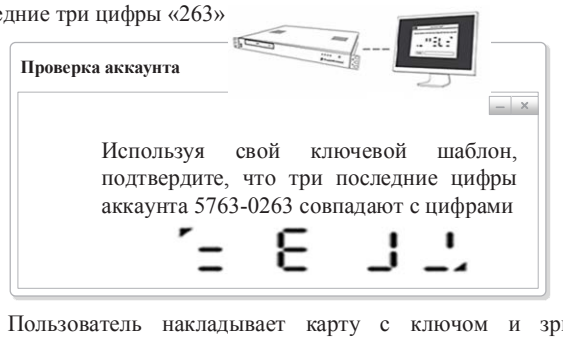
Шаблоны штрих-кода PassWindow могут существовать в виде уникальных статических изображений последовательности символов или в виде более расширенной анимационной версии, которая является основной темой этого документа. Эти анимированные штрих-коды состоят из последовательности статических шаблонов, каждый 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. Основные этапы системы PassWindow представлены на рис. 2.

1.Пользователь вводит информацию об транзакции для аутентификации



2. После этого сервер аутентификации PassWindow создаёт штрих-код с одноразовым ключом и также специфическую информацию: последние три цифры «263»



3. Пользователь накладывает карту с ключом и зрительно проверяет совпадения информации о транзакции, после этого он вводит одноразовый пароль, чтобы провести аутентификацию транзакции

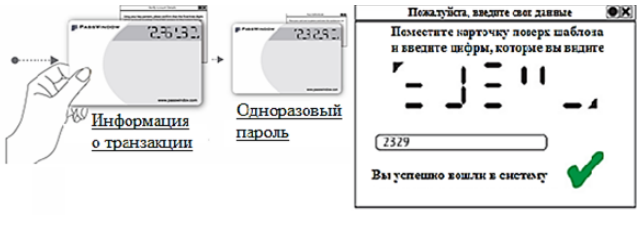


Рис. 2. Основные этапы работы PassWindow

Любое вмешательство или подделка шаблона штрих-кода будет пассивно представлена пользователю в виде появления комбинаций, не приводящих к появлению цифр аутентификатора. При этом могут появляться случайно размещенные сегменты, которые не содержат никаких символов, или случайные цифры, недостающие или избыточные цифры, появляющиеся в пределах одного шаблона, не относящиеся 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. 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 [1–4]. 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 обманывают с 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.

Обозначение SMS-систем или систем двухфакторной аутентификации на основе мобильных телефонов является ошибочным, более точный термин – это “внеполосная” аутентификация. Тем не менее, с распространением 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 [6], но и путем перехвата и дешифрования данных, передаваемых через сеть GSM-телекоммуникаций [8].

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 [9]. 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 [10].

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” [7]. 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 поль-

зователи 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 [1, 11].

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.

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.

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.

6. 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 [12].

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 [13]. 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" [14].

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.

Злоумышленник 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.

7. Практический алгоритм мониторингу системы PassWindow

Проведенный анализ угроз системы PassWindow показал, что наиболее эффективной угрозой является аналитическая атака на секретной ключ (штрих-код карты). Для успешной работы алгоритма следует сделать от трех до пяти сессий мониторинга (передачи клиентом OTP банка). Алгоритм мониторинга пластиковых карт PASSWINDOW приведен на рис. 3.

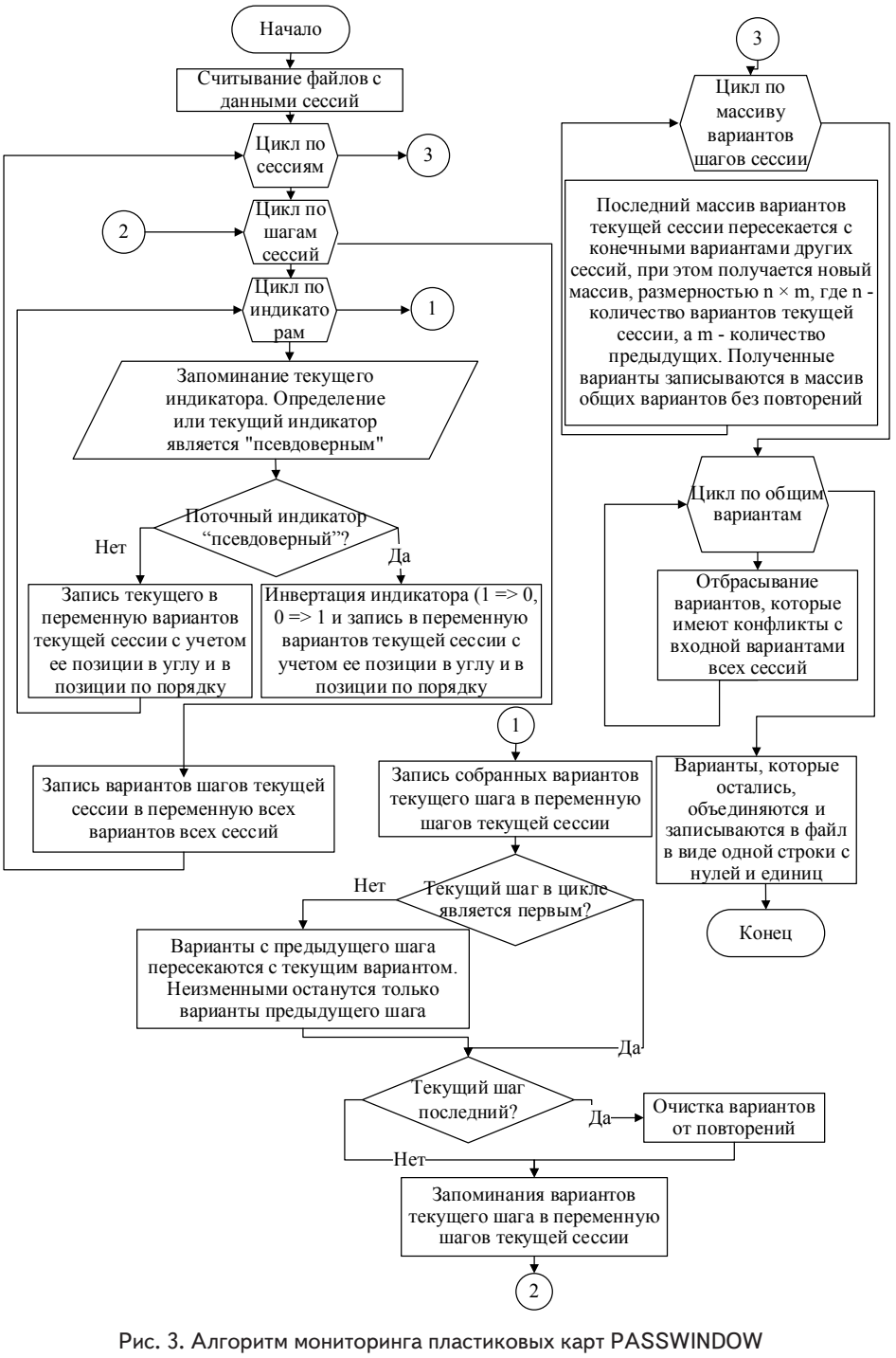


Рис. 3. Алгоритм мониторинга пластиковых карт PASSWINDOW

В интересах тестирования уязвимости PassWindow к такому нападению, был построен алгоритм взлома, который пытается использовать эти принципы для выполнения указанного анализа, который подтверждает практическую составляющую предложенного алгоритма, вне зависимости от количества передаваемых цифр.

Алгоритм мониторинга пластиковых карт на основе системы PassWindow состоит из следующих шагов:

1. Мониторинг канала связи и получения данных с сессиями.

2. Перевод данных в класс индикатора (в виде бинарного кода), с которым есть возможность оперировать как с объектом (класс индикатора представляет из себя массив из 7-ми единиц/нулей).

3. Проверка возможности формирования "цифр" в каждой позиции карточки (цикл по всем сессиям). Внутри цикла начинается цикл по каждой последовательности – поочередно каждый индикатор представляется "верным" (считаем, что в нем была цифра).

Внутри цикла проводится проверка – если текущая позиция "верной", тогда создается вариант, в который записывается инвертированный индикатор генератора, если это "неверная" позиция может записывается индикатор. После каждого цикла внутри одной последовательности идет пересечение с вариантами прошлой последовательности, т. е. N * N (Ni & Nj), если все последовательности в текущей сессии были пересечены – высвобождаем их, то есть конечные листья (варианты) просматриваются и выбрасываются копии.

4. Просмотр всех последовательностей во всех сессиях. Пересечение всех писем между сессиями поочередно (первая сессия со второй, результат их пересечения с третьей сессией и т. д.). После каждого пересечения листьев смежной сессии - листья "чистятся" от копий.

5. Пересечение писем всех сессий между собой. Цикл по всем письмам – каждый вариант (он же лист) проверяется на входных данных – на данных генератора, если он имеет конфликт с каким индикаторов, то такое письмо (вариант) отбрасывается. В результате останется только один вариант, который не имеет конфликтов ни с одной из последовательностей всех сессий.

6. Вывод конечного варианта в файл output.txt в формате бинарного строки.

8. Выводы

В роботе выполнено теоретическое обобщение основных принципов повышения целостности и аутентичности пакетов данных в протоколах безопасности банковских транзакций, на основе методов двухфакторной аутентификации, основным отличием является использование двух каналов формирования аутентификатора и использование двух независимых его составляющих, что значительно повышает его безопасность. Проведенные исследования показали, что механизмы двухфакторной аутентификации, основанные на криптографических алгоритмах при использовании комплексных атак с использованием методов социальной инженерии и методов криптоанализа не обеспечивают уполномоченному пользователю требуемый уровень безопасности. Предложенная в 2010 году система PassWindow из-за отсутствия в своем протоколе криптографических алгоритмов и основанная на формировании уникального штрих-кода позволяет устранить основные гипотетические атаки на протоколы двухфакторной аутентификации, включая атаки социальной инженерии, что является преимуществом по отношению к другим протоколам аутентификации. Предложенный авторами алгоритм мониторинга системы PassWindow позволяет за 3–5 сессий передачи OTP-паролей сформировать уникальный штрих-код карты пользователя и получить полный доступ к банковским счетам пользователя.

Литература

1. Slyman, M. An evaluation of hypothetical attacks against the PassWindow authentication method [Electronic resource] / M. Slyman, S. O'Neil, G. H. Nicolae, B. van der Merwe // The PassWindow method. – 2009. – Available at: http://www.passwindow.com/evaluation_of_hypothetical_attacks_against_passwindow.pdf
2. Двухфакторная Аутентификация [Электронный ресурс] / Aladdin, 2014. – Режим доступа: http://www.aladdin-rd.ru/solutions/authentication
3. Настройка двухфакторной аутентификации [Электронный ресурс] / Citrix, 2012. – Режим доступа: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-two-factor-authentication-gransden.html?locale=ru
4. Семь методов двухфакторной аутентификации [Электронный ресурс] / ITC.ua, 2007. – Режим доступа: http://www.infosecurityrussia.ru/news/29947
5. Двухфакторная аутентификация при удаленном доступе [Электронный ресурс] / Infosecurity, 2006. – Режим доступа: http://itc.ua/articles/dvuhfaktornaya_autentifikaciya_pri_udalennom_dostupe_23166
6. Man In The Mobile Attacks Highlight Weaknesses In Out-Of-Band Authentication [Electronic resource] / Information week, 2010. – Available at: http://www.darkreading.com/risk/man-in-the-mobile-attacks-highlight-weaknesses-in-out-of-band-authentication/d/d-id/1134495
7. Zeitz, C. Security issues of Internet-based biometric authentication systems: risks of Man-in-the-Middle and BioPhishing on the example of BioWebAuth [Electronic resource] / C. Zeitz, T. Scheidat, J. Dittmann, C. Vielhauer, E. G. Agulla, E. O. Muras, C. G. Mateo, J. L. Alba Castro // Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 2008. – 12 p. – Available at: http://spie.org/Publications/Proceedings/Paper/10.1117/12.767632 doi: 10.1117/12.767632
8. Barkan, E. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication [Text] / E. Barkan, E. Biham, N. Keller // Journal of Cryptology. – 2008. – Vol. 21, Issue 3. –P. 392–429. – Available at: http://dl.acm.org/citation.cfm?id=1356689 doi: 10.1007/s00145-007-9001-y

9. Winterford, B. $45k stolen in phone porting scam [Electronic resource] / B. Winterford // ITnews, 2011. – Available at: http://www.itnews.com.au/News/282310,45k-stolen-in-phone-porting-scam.aspx/0
10. Schwartz, M. J. Zeus Banking Trojan Hits Android Phones [Electronic resource] / M. J. Schwartz // Information week, 2011. – Available at: http://www.informationweek.com/mobile/zeus-banking-trojan-hits-android-phones/d/d-id/1098909
11. Trojan Writers Target UK Banks With Botnets [Electronic resource] / TechWorld, 2010. – Available at: http://news.techworld.com/security/3228941/trojan-writers-target-uk-banks-with-botnets
12. Network Forensic Analysis of SSL MITM Attacks [Electronic resource] / NETRESEC Network Security Police Service, 2011. – Available at: http://www.netresec.com/?page=Blog&month=2011-03&post=Network-Forensic-Analysis-of-SSL-MITM-Attacks
13. Internet Banking Targeted Phishing Attack [Electronic resource] // Metropolitan Police Service, 2005. – Available at: http://www.webcitation.org/5ndG8erWg
14. Krebs, B. Spike in phone phishing attacks [Electronic resource] / B. Krebs // KrebsOnSecurity – 2010. – Available at: http://krebsonsecurity.com/2010/06/a-spike-in-phone-phishing-attacks/

Розроблено інформаційну модель системи управління якістю промислової продукції на основі процесу оцінки та прогнозування показників якості з використанням інформаційних систем підтримки прийняття рішень. Модель дозволяє встановити і наочно представити взаємозв'язки між структурними елементами системи управління якістю для дослідження процесів будь-якої складності при розробці, виготовленні та експлуатації продукції різного цільового призначення

Ключові слова: інформаційна модель, система управління якістю, процес оцінки і прогнозування

Разработана информационная модель системы управления качеством промышленной продукции на основе процесса оценки и прогнозирования показателей качества с использованием информационных систем поддержки принятия решений. Модель позволяет установить и наглядно представить взаимосвязи между структурными элементами системы управления качеством и исследовать процессы любой сложности при разработке, изготовлении и эксплуатации продукции различного целевого назначения

Ключевые слова: информационная модель, система управления качеством, процесс оценки и прогнозирования

УДК 658.562:004.9
DOI: 10.15587/1729-4061.2015.40538

ИНФОРМАЦИОННАЯ МОДЕЛЬ СИСТЕМЫ ОЦЕНКИ, ПРОГНОЗИРОВАНИЯ И УПРАВЛЕНИЯ КАЧЕСТВОМ ПРОМЫШЛЕННОЙ ПРОДУКЦИИ

Н. А. Зубрецкая
Доктор технических наук, профессор
Кафедра метрологии,
стандартизации и сертификации
Киевский национальный университет
технологий и дизайна
ул. Немировича-Данченко, 2,
г. Киев, Украина, 01011
E-mail: zubr_27@mail.ru

1. Введение

Функционирование современных систем управления качеством промышленной продукции связано с необходимостью оперативного анализа больших объемов качественной и количественной информации. Деятельность промышленных предприятий и их взаимодействие с окружающей средой невозможно представить в виде традиционных формальных количественных взаимосвязей. В значительной степени эти взаимосвязи приходится описывать на качественном уровне, а последствия принятия организационно-технических решений часто оказываются неоднозначными или неопределенными.

Повышение эффективности управленческих процедур производства за счет упорядочения и синхронизации информационных потоков между структурно-функциональными элементами промышленного предприятия возможно на основе процесса оценки и прогнозирования качества. Однако реализация этого процесса в большинстве случаев не позволяет идентифицировать всю совокупность свойств продукции, процессов и их связей, вследствие чего для принятия управленческих решений необходимо создание и использования многофакторных структурно-параметрических моделей и современных технологий многомерного анализа данных.