УДК 004.822:514

ИНТЕЛЛЕКТУАЛЬНОЕ УПРАВЛЕНИЕ ВЫБОРОМ ДЛЯ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К МОБИЛЬНЫМ ПРИЛОЖЕНИЯМ

В.А. ВИШНЯКОВ, М.М. ГОНДАГ САЗ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 01 ноября 2019

Аннотация. Предложена модель интеллектуального выбора метода аутентификации пользователей мобильных приложений, основанная на экспертном подходе. Разработана структура такой экспертной системы и приведены детали ее программной реализации.

Ключевые слова: метод аутентификации, интеллектуальный выбор, экспертная система.

Введение

Вопросы надежного доступа к инфокоммуникационным ресурсам – это основной момент защиты. Контроль доступа, системы шифрования, фаейрволы, виртуальные частные сети – все основано на аутентификации пользователей и выдачи прав доступа к программам, с которым устанавливается соединение, если этого недостаточно, то упомянутые средства защиты не эффективны [1]. Данные исследований безопасности отражают факт, что более частыми являются атаки, с загрузкой паразитических программ или подключение атакующего [1, 2]. Использование аутентификации с многоразовым паролем не совсем надежны и плохо влияют на обеспечение информационной защиты локальных сетей и мобильных приложений. Для предотвращения предоставления атакующим возможности для нарушения конфиденциальности, доступности и целостности в мобильных приложениях, следует выполнять рекомендации по частому изменению многоразового пароля и использовать варианты строгой аутентификации [1]. Но это требует больших вычислительных ресурсов и относительно дорого. Поэтому требуется реализация интеллектуального выбора вида доступа в зависимости от ряда факторов.

Контроль доступа в локальных сетях и облачных средах

Аутентификации пользователей – один из основных компонентов организации информационной безопасности в локальных сетях. В многочисленных работах рассматриваются средства аутентификации [1, 2]:

– применение многоразовых паролей. Этот подход используется часто, но является наиболее уязвимым − код пароля может быть прочитан атакующим;

– использование одноразовых паролей. Достоинством является невозможность их использования при перехвате, поскольку пароль уже не будет действовать. Хорошей реализацией этого подхода является схема S/Key;

– контрольные суммы используются при вычислении значения для проверки сообщений переменной длины, но, возникает проблема передачи их второй стороне. Решением является шифрование контрольной суммы или включение их в цифровую подпись.

– электронная подпись, созданная хешированием сообщения с дополнительной информацией (контрольной суммы, ключа), шифрованием полученного кода при помощи личного ключа отправителя. Пользователь может расшифровать это послание, используя открытый ключ, вычислив хэш от кода сообщения и сравнив его с расшифрованным. Если они совпадут, все хорошо.

Аутентификация для организации облачных вычислений имеет особенности [3]:

– для удобства пользователей должны использоваться механизмы однократной удаленной аутентификации при доступе к различным облачным сервисам;

– для обеспечения взаимодействия облачных сервисов с сервисом аутентификации должны использоваться распространенные протоколы, стандарты и модели контроля доступа;

– должна обеспечиваться информационная безопасность сервисов аутентификации.

Способы и протоколы аутентификации в мобильных приложениях

Основные способы аутентификации, их применение и соответствующие протоколы приведены в табл. 1.

Таблица 1. **Способы и протоколы аутентификация пользователей МП [4–6]**

Способ	Основное применение	Протоколы
По паролю	Аутентификация клиентов	HTTP, Forms
По сертификатам	Аутентификация клиентов в безопасных приложениях; аутентификация сервисов	SSL/TLS
По одноразовым паролям	Дополнительная аутентификация клиентов (двухразовая проверка – TFA)	Forms
По ключам доступа	Аутентификация сервисов и приложений	SSL/TLS
По знакам (токенам)	Предоставляемая аутентификация клиентов; предоставляемая авторизация программ	SAML, WS-Federation, OAuth, OpenID Connect

Для выбора того или другого вида аутентификации, нужно понимать, как различия технологий при их использовании, так и затраты на реализацию. Выбрав ряд критериев, можно провести сравнительную оценку различных технологии аутентификации при том или ином решении. Критерии, по которым вычисляется интегральная оценка вида аутентификации, можно определить следующим образом: разновидность способа ввода кода; тип считывающего устройства; стойкость; затраты на разработку и внедрение; трудность использования для клиента; применимость удаленного доступа; множественность настроек; степень стойкости от настроек; срок хранения аутентифицирующей информации; вероятность ошибок. Данные положения были положены в основу работы системы по интеллектуальному выбору вида доступа пользователей к мобильным приложениям.

Интеллектуальный выбор аутентификации и идентификации

Естественно, возникает вопрос выбора той или иной модели аутентификации (МА) и модели идентификации (МИ). Рассмотрим детально модели для поддержки принятия решения по выбору МА и МИ. В [7] были приведены символьные описания видов моделей аутентификации клиента и было предложено выбирать вид аутентификации по ряду критериев для реализации обеспечения информационной безопасности.

Алгоритм аутентификации состоит из ряда выполняемых проверок двух видов: к первому относятся процедуры входа и идентификации нового пользователя ИС, ко второму – процедуры предъявления аутентификационных признаков (АП), протоколы обмена претендент – контролирующая сторона, проверка и принятие решения о результате прохождения клиентом процесса аутентификации. Модель классификации аутентификации − *MCA* представим тройкой:

$$MCA = \{A, W, C\},$$

где A − доступность (accessibility), W − целостность (wholeness), C − конфиденциальность (confidently). Детализацию модели классификации выразим таким образом:

$$A = \{GA, DA, CA, PA\} : W = \{WS, WRR, WAP, WPC\}; C = \{CPP, CAP, CPC\},$$

где GA − гарантия обработки запросов пользователей на аутентификацию, DA − разделение доступа пользователей, CA − контроль доступа, PA − персонификация доступа; WS −

целостность ПО, WRR − целостность учетных записей, WAP − целостность АП пользователя, WPC − целостность АП пользователя в облачной среде; CPP − конфиденциальность учетных записей, CAP − конфиденциальность АП пользователя, CPC − конфиденциальность АП пользователя в облачной среде.

МИ базируется на трехуровневом семифакторном подходе классификации идентификаторов:

– как характеристик принадлежности − универсальный (U), корпоративный (C); личный (P);

– для распознавания личности владельца − анонимный (N), персональный (I);

– доступа владельца к ресурсам − одноразовый (O) или многоразовый (M). Тогда в электронном пространстве имеем разновидности идентификации, представленной семеркой МИ (MCI):

$$MCI = \{UNM, UPO, UPM, CNO, CNM, CPM, IPM\},$$

где следующие идентификаторы: UNM − универсальный анонимный многоразовый (пользователь Интернета), UPO − универсальный персональный одноразовый (генератор одноразовых паролей), UPM − универсальный персональный, содержащийся в реестре (электронный паспорт), CNO − корпоративный анонимный одноразовый (электронный билет), CNM − корпоративный анонимный многоразовый (банковская карта), CPM − корпоративный персональный многоразовый (пропуск – смарт-карта) анонимный многоразовый идентификатор, IPM − личный персональный многоразовый (биометрия на карте или сервере).

Интеллектуальный подход для выбора вариантов СИА базируется на составлении базы правил выбора, в качестве интеллектуального инструмента используются основанные на правилах, экспертные системы (ЭС). ЭС в базе знаний содержат описание классификационных правил СИА, соответствующие профилям легальных пользователей. Эксперт (с инженером по знаниям) формирует базу правил для выбора варианта СИА. Работа такой ЭС может базироваться как на экспертном подходе, так и в автоматическом режиме сервера. Для первого варианта организуется диалог, в ходе которого выявляются пожелания или требования пользователя, или администратора КИС. На основании результатов опроса формируется вариант СИА. В автоматическом режиме сервера вариант СИА формируется по профилям легальных клиентов.

Структура экспертной системы для выбора модели аутентификации

На базе критериев, перечисленных выше, будет происходить оценка пяти различных разновидностей аутентификации: использованием многоразового пароля; одноразового пароля; код по персональному; графический пароль; биометрическая аутентификация.

Для подбора наиболее оптимального вида аутентификации эксперту нужно ввести следующую информацию:

– ряд вопросов $Q = \{q_1, ..., q_N\}$, где $q_1, ..., q_N$ – вопросы пользователю;

– ряд ответов $A = \{a_1, ..., a_G\}$, где $a_1, ..., a_G$ – ответы на вопросы Q;

– несколько критериев $C = \{c_1, ..., c_K\}$, где $c_1, ..., c_K$ варианты критериев.

– соответствие вопросов и критериев $W = A \times C$;

– виды аутентификации $S = \{s_1, ..., s_M\}$;

– соответствие методов и критериев $R = S \times C$.

Ряд вопросов будет состоять из десяти заранее подготовленных вариантов, с двумя выборами ответа «ДА/НЕТ».

Разработана структура экспертной системы для выбора модели аутентификации, включающая интерфейс клиента, базу знаний по описанию видов аутентификации, процессор вывода лучшего варианта аутентификации. Клиент сам формирует желаемый вариант доступа, отвечая на ряд вопросов. Предусмотрен режим автоматического выбора вариантов доступа в зависимости от доступных ресурсов.

Процесс разработки физической структуры разрабатываемого программного продукта инструментами Visual Studio начинается с формирования пользовательского интерфейса

и разработки кода и различных рабочих форм с учетом эргономичности, эстетичности, минимализма. При разработке программы использовано два вида форм:

– формы, которые создаются при запуске программы и затем, при открытии или закрытии, просто прорисовываются либо скрываются;

– диалоговые окна, уведомляющие пользователя о произошедшем событии. При работе с такими окнами нельзя начать работу с какими-либо другими формами, пока это окно не будет закрыто.

События, использованные на форме FormTest:

– private void private void init_test() – метод инициализации формы, где объявляются основные переменные;

– private void private void load_questions() – обработчик загрузки вопросов для прохождения опроса;

– private void show_question() – обработчик события отображения вопроса и вариантов ответа;

– private void button_next_Click – обработчик события клика по кнопке далее, где сохраняется ответ пользователя;

– private void show_result() – обработчик события отображения результата.

При запуске программы пользователю показывается страница с вопросом и двумя вариантами ответа, отвечая на которые выбирается лучшая форма аутентификации.

Заключение

1. Представлены символьные модели на основе теории множеств для поддержки принятия решения по выбору видов идентификации и аутентификации пользователей мобильных приложений в конкретной ситуации, которые позволяют по ряду критериев выбрать лучший вариант. Для реализации данных моделей предложен экспертный подход.

2. Разработана структура экспертной системы для выбора модели идентификации и аутентификации, включающая интерфейс, базу знаний, процессор вывода. Клиент формирует желаемый вариант доступа, отвечая на ряд вопросов. Предусмотрен режим автоматического выбора вариантов доступа в зависимости от доступных ресурсов. Приведены детали программной реализации экспертной системы с использованием инструментариев системы Visual Studio.

INTELLIGENT MANAGEMENT OF CHOICE FOR USER ACCESS TO MOBILE APPLICATIONS

U.A. VISNIAKOU, M.M. GHONDAGH SAS

Abstract. The model of intelligent choice of authentication method for mobile application user on expert approach was proposed. The structure of such expert system and its details of software realization was shown.

Keywords: authentication method, intelligent choice, expert system.

Список литературы

1. Смит Р.И. Аутентификация: от паролей до открытых ключей. М.: Вильямс, 2002.
2. Бобов М.Н., Конопелько В.К. Основы аутентификации в телекоммуникационных системах. Уч. пособие. Минск: БГУИР, 2009.
3. Вишняков В.А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения. Монография. Минск: Бестпринт, 2016.
4. Вход в приложения для мобильных устройств или компьютеров [Электронный ресурс]. URL: https://support.google.com/a/answer/ 1032419?hl=ru. (дата доступа: 12.10.2019).
5. Выростков Д. Обзор способов и протоколов аутентификации в веб-приложениях [Электронный ресурс]. URL: https://habrahabr.ru/ company/dataart/blog/262817/. (дата доступа: 12.10.2019).
6. Как обеспечить аутентификацию на мобильных устройствах [Электронный ресурс]. URL: http://www.cnews.ru/reviews/security2014/ articles/. (дата доступа: 12.10.2019).
7. Вишняков В.А., М.М. Гондаг Саз. // Докл. БГУИР. 2017. № 1. С. 82–86.