УДК 004.822:514

МОДЕЛИ АУТЕНИФИКАЦИИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ ДЛЯ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ С ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКОЙ ВЫБОРА

В.А. ВИШНЯКОВ, М.М. ГОНДАГ САЗ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 25 января 2017

Аннотация. Представлены шесть разновидностей математических моделей аутентификации при работе пользователей с мобильными приложениями в облачной среде. Для выбора модели аутентификации приведено трехфакторное символьное описание ее классификации. Для модели идентификация дан трехуровневый семифакторный подход к классификации идентификаторов. Предложен интеллектуальный подход для выбора системы идентификации и аутентификации (СИА) на основе базы правил экспертной системы (ЭС). Модель поддержки принятия решения в ЭС может базироваться как на экспертном подходе, так и в автоматическом режиме сервера.

Ключевые слова: аутентификация, идентификация, мобильные приложения, математическая модель, облачные вычисления.

Abstract. Six variants of mathematical models of authentification during users work with mobile applications in cloud area are represented: with application server, with applications forms, on sertification, with one-time parol, on accesses keys, and with tokens. Three factors simbol description for authentification classification for chois thear models is given. The three level seven factor approuch to identificators classification for model identification is given. The intelligence approach for choice of identification and authentification system (IAS) on the base of expert system (ES) knowledge base roles is proposed. The model of decision support system in ES may be based as on expert approach such as on automatic regime of server.

Keywords: authentification, identification, cloud computing, mobile applications, mathematical models.

Doklady BGUIR. 2017, Vol. 103, No. 1, pp. 82-86
Authentification models in cloud computing for mobile applications with intellectual support of choice
U.A. Vishniakou, M.M. Ghondagh Saz

Введение

Важное и актуальное направление исследований и разработок в области защиты информации представляют модели и средства идентификации и аутентификации пользователей в корпоративных информационных системах (КИС) и системах облачных вычислений. Идентификация (Identification) − процедура распознавания пользователя по его идентификатору. Аутентификация (Authentication) − процедура проверки подлинности заявленного пользователя, процесса или устройства. Фундаментальные основы вопросов идентификации и аутентификации представлены в работе [1]. Отдельные новые результаты разработок представлены в диссертациях [2, 3]. В монографии обобщены отдельные результаты российских исследований по моделям и средствам аутентификации [4, с. 228–254]. В последнее время быстрыми темпами развиваются мобильные приложения и сервисы. Вопросы, связанные с аутентификацией веб-приложений обсуждаются в работах [5–7]. В данной статье авторы представили модели аутентификации и идентификации пользователей при работе с

мобильными приложениями. Рассматриваются также модели классификации в системе аутентификации и идентификации пользователей (СИА), на основании которых строятся интеллектуальные системы для поддержки принятия решения по выбору варианта СИА.

Модели аутентификации

Аутентификация по паролю с сервером приложений. Эта модель основывается на том, что пользователь должен предоставить серверу приложений username − U_n и password − P_s для успешной идентификации и аутентификации в системе. Опишем эту модель: пусть X − пользователь, B − браузер, S_p − сервер приложений, A − признак аутентифицирован, n − уникальное значение, H − хэш-функция, С − процесс шифрования, P_k − k-е приложение. Тогда базовая модель аутентификации будет иметь вид: $X\,(U_n, P_s) \rightarrow B \rightarrow S_p$; $S_p(A) \rightarrow B \rightarrow X$.

Вторая разновидность этой модели отличается от простой (U_n, P_s передаются в открытом виде), зашифрованным вариантом (базовая модель с шифрованием), выглядит так: $X\,(C(U_n), P_s(U_n)) \rightarrow B \rightarrow S_p$; $S_p(A) \rightarrow B \rightarrow X$.

Третьей разновидностью является двухсторонняя модель с использованием хэш-функции, когда сервер приложений посылает браузеру уникальное значение n, браузер передает значение хэш-пароля пользователя, вычисленное с использованием указанного n. Она имеет вид: $X \rightarrow B \rightarrow S_p$; $S_p(n) \rightarrow B \rightarrow X$; $X\,(U_n, H(n, P_s) \rightarrow B \rightarrow S_p$; $S_p(A) \rightarrow B \rightarrow X$.

Аутентификация с приложениями. Эта модель основывается на том, что пользователь должен предоставить приложению username − U_n и password − P_s для успешной идентификации и аутентификации в системе. Она имеет следующий вид: $X\,(U_n, P_s) \rightarrow B \rightarrow P_k\,(S_p)$; $P_k\,(S_p(A)) \rightarrow B \rightarrow X$.

Аутентификация по сертификату. В эту модель аутентификации введем обозначения: сервер аутентификации − CA, сертификат пользователя − $C_a(к)$, включающий $к$ атрибутов и подписанный CA − $C_a(к, CA)$, секретный ключ − K_s. Тогда она выглядит: $X(C_a(к), K_s) \rightarrow CA$; $CA(C_a(к, CA) \rightarrow X$; $X(C_a(к, CA) \rightarrow S_p$; $S_p \rightarrow CA$; $S_p(A) \rightarrow B \rightarrow X$. Модель более надежная, однако трудности с распространением и поддержкой сертификатов делают эту модель аутентификации сложно реализуемой.

Аутентификация по одноразовым паролям. Аутентификация по одноразовым паролям обычно применяется дополнительно к аутентификации по паролям для реализации *two-factor authentication* (2FA). В этой концепции пользователю необходимо предоставить данные двух типов для входа в систему: что-то, что он знает (например, пароль), и что-то, чем он владеет (например, устройство для генерации одноразовых паролей). Наличие двух факторов позволяет в значительной степени увеличить уровень безопасности, что востребовано для определенных видов веб-приложений (перевод денег, изменение настроек, паролей и т. д.). Введем токены, которые могут генерировать одноразовые пароли на основании секретного ключа, введенного в них, текущего времени − $T\,(K_s, t)$ и запроса одноразового пароля − R. Модель представляется в следующем виде: $X\,(U_n, P_s) \rightarrow B \rightarrow P_k\,(S_p)$; $P_k\,(S_p, R) \rightarrow X$; $X\,(T\,(K_s, t))) \rightarrow B \rightarrow P_k\,(S_p)$.

Аутентификация по ключам доступа. Эта модель используется для аутентификации устройств, сервисов или других приложений при обращении к веб-сервисам − *WS*, хранящимся на облачном сервере − S_{ws}, средством аутентификации является ключ доступа − K_a (произвольная строка символов, генерируемая сервером S_{ws}). Модель имеет вид: $X\,(U_n, P_s) \rightarrow B \rightarrow S_{ws}$; $S_{ws}(K_a) \rightarrow X$; $X\,(K_a) \rightarrow P_k\,(S_{ws})$. Более сложная модель аутентификации по ключам для незащищенных соединений включает два ключа: открытый − K_o и секретный − K_s. K_o используется для идентификации клиента, K_s позволяет сгенерировать подпись. Эта модель выглядит таким образом: $X\,(K_o) \rightarrow B \rightarrow S_{ws}$; ; $S_{ws}\,(n) \rightarrow B \rightarrow X$; $X\,(H(n, K_s) \rightarrow B \rightarrow S_{ws}$.

Сервер S_{ws} после установки соединения посылает клиенту уникальное значение n, а клиент возвращает хэш этого значения, вычисленный с использованием K_s. Это позволяет избежать передачи всего ключа в оригинальном виде и повышает надежность соединения.

Аутентификация по токенам. Данная модель аутентификации применяется при построении распределенных систем *Single Sign-On* (SSO), где одно приложение − *SP* (service provider) делегирует функцию аутентификации пользователей другому приложению − *IP* (identity provider). Примером является вход в приложения через учетную запись в социальных

сетях. Токен $T(P_i)$ генерируется $IP(P_i)$, где P_i − параметры токена. Модель имеет вид: $X(K_o) \rightarrow B \rightarrow IP$; $IP(n) \rightarrow B \rightarrow X$; $X(H(n, K_s) \rightarrow B \rightarrow IP$; $IP(T(P_i)) \rightarrow X$; $X(T(P_i)) \rightarrow SP$.

Интеллектуальный подход выбора моделей аутентификации и идентификации

Модели идентификации (МИ). Они могут базироваться на трехуровневом семифакторном подходе классификации идентификаторов [8]: (1) как характеристики принадлежности − универсальный (U), корпоративный (C); личный (P); (2) для распознавания личности владельца − анонимный (N), персональный (I); (3) доступа владельца к ресурсам − одноразовый (O) или многоразовый (M). Тогда в электронном простанстве имеем разновидности идентификации, представленной семеркой МИ (*MCI*): *MCI* = {*UNM, UPO, UPM, CNO, CNM, CPM, IPM*}, где использованы 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). Возникает вопрос выбора той или иной модели аутентификации (МА) и модели идентификации (МИ), желательно с интеллектуальной поддержкой [4].

Рассмотрим подход к поддержке принятия решения по выбору МА и МИ. В работе [8] предложена классификация системы аутентификации по признакам выполнения целей и задач обеспечения ИБ. Процесс аутентификации состоит из последовательно выполняемых процедур двух классов: к первому относятся процедуры регистрации нового пользователя ИС и хранения аутентификационной информации (АИ), ко второму – процедуры предъявления АИ, протоколы обмена «претендент–проверяющая сторона», валидации и принятия решения о результате прохождения претендентом процесса аутентификации. Модель классификации аутентификации − *MCA* – представим тройкой: *MCF* = {*A, W, C*}, где *A* − доступность (accessibility), *T* − целостность (wholeness), *C* − конфиденциальность (confidelity). 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 АИ пользователя, *WPC* − целостность АИ пользователя в облачной среде; *CPP* − конфиденциальность учетных записей , *CAP* − конфиденциальность АИ пользователя, *CPC* − конфиденциальность АИ пользователя в облачной среде.

Интеллектуальный подход для выбора вариантов СИА. Данный подход базируется на составлении базы правил выбора, в качестве интеллектуального инструмента используются основанные на правилах экспертные системы (ЭС). ЭС в базе знаний содержит описание классификационных правил СИА, соответствующих профилям легальных пользователей. Эксперт (возможно 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 пользователей.

Заключение

Представлены шесть разновидностей математических моделей аутентификации: с сервером приложений, с приложениями, по сертификату, с одноразовыми паролями, по ключам доступа и с токенами. Дана модель классификации аутентификации в виде тройки *MCF* = {*A, W, C*}, где *A* – доступность (accessibility), *T* – целостность (wholeness), *C* – конфиденциальность (confidelity).

Модель идентификации базируется на трехуровневом семифакторном подходе классификации идентификаторов: (1) как характеристик принадлежности − универсальный (U), корпоративный (C); личный (P); (2) для распознавания личности владельца − анонимный (N), персональный (I); (3) доступа владельца к ресурсам − одноразовый (O) или многоразовый (M). Для электронного пространства это дает семь видов идентификаторов.

Предложен интеллектуальный подход для выбора вариантов системы идентификации и аутентификации (СИА) на основе ИИ. Модель поддержки принятия решения 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 пользователей.

Список литературы

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / А.А. Афанасьев [и др.]. М.: Горячая линия–Телеком, 2012. 550 с.
2. Сулавко А.Е. Идентификация пользователей компьютерных систем по динамике подсознательных движений на основе статистической теории принятия решений : автореф. дис. канд. техн. наук. Омск: ФГБОУ ВПО СибАДИ, 2014. 19 с.
3. Малков А.А. Технология аутентификации с помощью доверенных лиц: автореф. дисс. канд. техн. наук. Уфа: ФГБОУ ВПО ПНИПУ, 2013. 16 с.
4. Вишняков В.А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения. Минск: Бестпринт, 2016. 276 с.
5. Ализар А. Главные уязвимости онлайн-банков: аутентификация, авторизация и Андроид [Электронный ресурс]. – Режим доступа: https://xakep.ru/2015 /05/21/online-bank/ – Дата доступа : 11.01.2017.
6. Вход в приложения для мобильных устройств или компьютеров [Электронный ресурс]. – Режим доступа : https://support.google.com/a/answer/ 1032419?hl=ru. – Дата доступа: 11.01.2017.
7. Как обеспечить аутентификацию на мобильных устройствах [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/security2014/articles/kak_obespechit_autentifikatsiyu_na_mobilnyh_ustrojstvah – Дата доступа: 11.01.2017.
8. Сабанов А.Г. Принципы классификации систем идентификации и аутентификации по признакам соответствия требованиям информационной безопасности // Электросвязь. 2014. № 2. С. 6–9.

References

1. Autentifikacija. Teorija i praktika obespechenija bezopasnogo dostupa k informacionnym resursam / A.A. Afanas'ev [i dr.]. M.: Gorjachaja linija–Telekom, 2012. 550 s. (in Russ.)
2. Sulavko A.E. Identifikacija pol'zovatelej komp'juternyh sistem po dinamike podsoznatel'nyh dvizhenij na osnove statisticheskoj teorii prinjatija reshenij : avtoref. dis. kand. tehn. nauk. Omsk: FGBOU VPO SibADI, 2014. 19 s. (in Russ.)
3. Malkov A.A. Tehnologija autentifikacii s pomoshh'ju doverennyh lic: avtoref. diss. kand. tehn. nauk. Ufa: FGBOU VPO PNIPU, 2013. 16 s. (in Russ.)
4. Vishnjakov V.A. Informacionnaja bezopasnost' v korporativnyh sistemah, jelektronnoj kommercii i oblachnyh vychislenijah: metody, modeli, programmno-apparatnye reshenija. Minsk: Bestprint, 2016. 276 s. (in Russ.)
5. Alizar A. Glavnye ujazvimosti onlajn-bankov: autentifikacija, avtorizacija i Android [Electronic resource]. – Access mode: https://xakep.ru/2015 /05/21/online-bank/ – Date of access: 11.01.2017.
6. Vhod v prilozhenija dlja mobil'nyh ustrojstv ili komp'juterov [Electronic resource]. – Access mode: https://support.google.com/a/answer/ 1032419?hl=ru. – Date of access: 11.01.2017.
7. Kak obespechit' autentifikaciju na mobil'nyh ustrojstvah [Electronic resource]. – Access mode: http://www.cnews.ru/reviews/security2014/articles/kak_obespechit_autentifikatsiyu_na_mobilnyh_ustrojstvah – Date of access: 11.01.2017.
8. Sabanov A.G. Principy klassifikacii sistem identifikacii i autentifikacii po priznakam sootvetstvija trebovanijam informacionnoj bezopasnosti // Jelektrosvjaz'. 2014. № 2. S. 6–9. (in Russ.)

Сведения об авторах

Вишняков В.А., д.т.н., профессор, профессор кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

Гондаг Саз М.М., аспирант кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, д. 6,
Белорусский государственный университет информатики и радиоэлектроники
тел. +375-17-245-75-69;
e-mail: vish2002@list.ru;
Вишняков Владимир Анатольевич

Information about the authors

Vishniakou U.A., D.Sci., professor, professor of information security department of Belarusian State University of Informatics and Radioelectronics.

Ghondagh Saz M.M., postgraduate student of information security department of Belarusian State University of Informatics and Radioelectronics.

Address for correspondence

220013, Republic of Belarus
Minsk, P. Brovka st., 6,
Belarusian State University
of Informatics and Radioelectronics
tel +375-17-245-75-69;
e-mail: vish2002@list.ru;
Vishniakou Uladzimir Anatolievich