УДК 004.732.056(075.8)

МОДЕЛИ И СРЕДСТВА АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В КОРПОРАТИВНЫХ СИСТЕМАХ УПРАВЛЕНИЯ И ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

В.А. ВИШНЯКОВ, М.М. ГОНДАГ САЗ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220600, Беларусь

Поступила в редакцию 15 декабря 2015

Приведены элементы анализа работы пользователей в корпоративных информационных системах. Математическая модель социальной аутентификации в таких системах позволяет по заданному числу неудовлетворительных оценок вычислить вероятность успешной аутентификации с использованием расчета времени модерации. Это позволяет восстанавливать пароль пользователя как при его утере, так и при смене злоумышленником. Представлен модифицированный алгоритм на базе этой модели, позволяющий выполнять аутентификацию пользователей с привлечением поручителей. Приведен подход для безопасной работы пользователей в среде облачных вычислений.

Ключевые слова: защита информации, аутентификация, пользователи, корпоративная информационная система, облачные вычисления.

Введение

Идентификация позволяет субъекту, процессу, действующему от имени определенного пользователя назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. Аутентификация бывает односторонней (клиент доказывает свою подлинность серверу) и двусторонней [1, 2]. Субъект может подтвердить свою подлинность, предъявив одну из следующих сущностей: что он знает (пароль, личный идентификационный номер, криптографический ключ и т. п.); чем он владеет (личную карточку или иное устройство аналогичного назначения); нечто, что есть часть его самого (голос, отпечатки пальцев и т. п., то есть свои биометрические характеристики) [1, 2].

В основе одного протокола аутентификации (секретный ключ) лежит принцип, применяемый во многих протоколах: одна сторона посылает другой случайное число, которое другая сторона преобразует особым образом и возвращает результат. Второй протокол, позволяющий не встречавшимся ранее людям устанавливать общий секретный ключ, называется протоколом обмена ключами Диффи−Хеллмана (Diffie−Hellman key exchange). Третий подход состоит в организации доверительного центра распространения ключей (KDC, key distribution center). При такой схеме у каждого пользователя всего один ключ, общий с KDC. Взаимная аутентификация также может выполняться с помощью шифрования с открытым ключом [1, 2].

В работе протокола Kerberos, помимо рабочей станции (PC), принимают участие еще три сервера [3]: сервер аутентификации (AS, Authentication Server): проверяет личность пользователей при входе в сеть; сервер выдачи билетов (TGS, Ticket Granting Server): выдает «билеты, подтверждающие подлинность»; сервер, предоставляющий услуги PC [1, 2].

1. Использование стандартных паролей. Эта схема является наиболее уязвимой с точки зрения безопасности − пароль может быть перехвачен и использован другим лицом.

2. Одноразовые пароли. Преимуществом при использовании одноразовых паролей является невозможность их использования повторно, даже если пароль был перехвачен. Для генерации одноразовых паролей используются как программные, так и аппаратные генераторы.

3. Контрольные суммы используются при создании резюме фиксированной длины для представления длинных сообщений.

4. Электронные подписи создаются шифрованием контрольной суммы и дополнительной информации при помощи личного ключа отправителя.

Если рассматривать аутентификацию пользователя с точки зрения возможности реализации угрозы по перехвату и использованию «ключа» злоумышленником, получено распределение и значение весомости по риску реализуемости угрозы [3]: перехват стандартных паролей 0,5 − возможность реализации угрозы средняя $0,3 < Y < 0,6$; перехват S/key паролей 0,35 − возможность реализации угрозы средняя $0,3 < Y < 0,6$; контрольные суммы 0,75 − возможность реализации угрозы высокая $0,6 < Y < 0,8$; перехвата электронной цифровой подписи 0,25 − возможность реализации угрозы низкая $0 < Y < 0,3$. Весомости каждого показателя: использование стандартных паролей − 0,27; S/Key (одноразовые пароли) − 0,18; контрольная сумма − 0,41; электронная подпись − 0,14.

Идентификация пользователей компьютерных систем по динамике подсознательных движений с использованием альтернативных сценариев авторизации состоит из 2-х этапов: ввод парольной фразы на клавиатуре и ввод подписи при помощи графического планшета [4]. Алгоритм подразумевает 4 варианта окончания процедуры идентификации: 1) авторизация в соответствии с правами учетной записи пользователя (пользователь «свой» и он идентифицирован); 2) авторизация с правами ограниченной учетной записи, предусмотренной для таких случаев (пользователь «свой», но есть сомнения в том, кем он является); 3) отказано в доступе (есть сомнения, что пользователь «свой» и/или кем он является, либо уже на первом этапе очевидно, что пользователь – «чужой»); 4) «обманный» доступ (нет сомнений, что субъект является нарушителем). Механизмы аутентификации можно рассмотреть по приоритету их использования: основные − при штатном входе в систему, резервные (почтовый ящик) − при потере пароля либо взломе учетной записи, последние (last resort) − при вмешательстве администрации ИС. Наибольшие результаты в проблему социальной идентификации внесли три коллектива исследователей: RSA Laboratories, Microsoft, Fasebook [5].

Методика и алгоритм аутетификации в КИС

Современные корпоративные информационные системы (КИС) могут включать использование сред облачных вычислений (ОВ), так называемые интегрированные КИС (ИКИС). Вопросы исследования работы пользователей в ИКИС являются актуальными [6]. Потому рассмотрим два подхода аутентификации. В работе [5] представлена модель аутентификации, базирующаяся на трех классах объектов: *S* − ИС с подсистемой разграничения доступа, реализующей технологию аутентификации с помощью доверенных лиц, назовем ее СА; User − пользователь, имеющий учетную запись в *S*; Voucher − поручитель, способный подтвердить личность пользователя. В процессе аутентификации поручители должны подтвердить личность пользователя в СА. Выбор модели обусловлен ее простотой реализации в ИКИС.

Рассмотрим модификацию этой модели. Она включает КИС, пользователей, поручителей и множества аутентификаторов. Обозначим: $a_i = \{e^i_0,\ e^i_1 \ldots e^i_n\}$ − аутентификатор, где e_0 − владелец; $\{e_1, \ldots e_n\}$ − множество лиц, которым известен этот аутентификатор. $A = \{a^1, \ldots,\ a^N\}$; $Pr(x)\ \{x = e^i_0\}$ − функция, определяющая аутентификаторы, для объекта x; $Kn(x)$ − функция, определяющая аутентификаторы, известные объекту x, но не принадлежащие ему. Обозначим неизвестные величины: P_v − вероятность успешной аутентификации на основании оценок v.

В качестве входа примем идентификатор пользователя, в качестве выхода − либо новый пароль, либо отказ в восстановлении доступа. Определим функцию аутентификации F, определяющей подобие аутентификатора, имеющегося у пользователя и k-го поручителя:

$$F(User, Voucher_k, a_i) = \{1, if\ (User(a_i), Voucher_k(a_i)) \in [k_{min}, k_{max}]\},$$

$$F(User, Voucher_k, a_i) = \{0, if\ (User(a_i), Voucher_k(a_i)) \in\neq [k_{min}, k_{max}]\}.$$

Модифицированный алгоритм аутентификации имеет следующий вид.

1. Пользователь проходит проверку с вероятностью p_1, после чего посылает в центр аутентификации (ЦА) идентификатор своей учетной записи, которую надо восстановить $User\{Log\} \rightarrow CA$.

2. ЦА генерирует временную учетную запись (ВрУЗ), передает пользователю логин N_s и пароль P_{at}. В качестве логина выступает номер восстановления пароля (НВП) путем добавления числа в диапазоне [2−5] к предыдущему НВП: $N_s = N_s + ran\ [2–5];\ CA \rightarrow \{\ N_s,\ P_{at}\ \} \rightarrow User$;

User − пользователь; $Voucher_k$ − *k*-ый поручитель, способный подтвердить личность пользователя; $Z_k = (Pr(User) \cup Kn(User)) \cap (Pr(Voucher_k) \cup Kn(Voucher_k))$ − множество аутентификаторов, которые используются для проверки пользователя *k*-м поручителем.

3. ЦА определяет время модерации t_p и разницу между последней сменой пароля пользователем T_r и моментом создания новой записи ВрУЗ T_0. Если $T_0 > t_p + T_r$, ЦА высылает пользователю сообщение об этом, ждет ответа о прекращении процедуры восстановления пароля, получив его, прекращает работу с ним.

4. Если ответа пользователя не последовало или $t_p + T_r \geq T_0$, то ЦА передает пользователю перечень ников из списка поручателей, содержащий имена, каналы связи, отношения с пользователем и объем общения с поручателем.

5. ЦА рассылает всем поручителям из списка сообщение связаться с пользователем и получить его НВП и методику проверки личности пользователя.

6. Получив список поручителей, пользователь пытается связаться с ними, передав НВП и необходимую для установления личности информацию.

7. Получив данные от пользователя, поручитель пытается с помощью шкалы Харрингтона сравнить полученную информацию аутентификаторов с имеющейся у него, и высылает в ЦА оценку E_t, номер НВП и способ проверки.

8. Получив эту информацию, ЦА вычисляет компетентность *k*-го поручителя η_k, (выступает экспертом), которая зависит от перечня вопросов для проверки пользователя. В ЦА имеется множество нечетких количественных мер ψ, учитывающих компетентность поручителей. Эта мера используется для борьбы с атаками злоумышленников.

9. Общая оценка равна $E = \min \psi$. Если общая компетентность поручителей (сумма их оценок) превышает минимальный (η_{gr}) вес поручителей $\sum \eta_i > \eta_{gr}$, и общая оценка компетенции превышает границу доверия $E > E_{gr}$, аутентификация успешно пройдена. ЦА высылает пользователю его ВрЗУ, новый пароль учетной записи $CA \rightarrow \{Pass_{new}\} \rightarrow User$.

Аутентификация пользователей в среде облачных вычислений

В работе [7] представлены элементы подхода для безопасной работы пользователей в среде ОВ. Участники взаимодействий: пользователь (пользователями могут быть физические лица и организации), аутентификатор подлинности (Trusted Authenticator − TA), облачный провайдер услуг (Cloud Service Provider − CSP), цифровая подпись (Digital Signature − DS), агент CSP's. Ниже представлены функции элементов данного подхода.

1. Пользователь имеет ограниченный доступ к услугам из облака предлагаемых услуг, он запрашивает облачные ресурсы у CSPs.

2. TA устанавливает соединение с органом аутентификации. Задача TA в облачной среде − обеспечить пользователю безопасный доступ к облачным сервисам через поставщика услуг.

3. Облачный провайдер услуг (CSP). Облачный сервис может динамически масштабироваться для удовлетворения потребностей пользователей, потому что поставщик услуг предоставляет необходимое для обслуживания оборудование и программное обеспечение.

4. Цифровая подпись (DS), является электронной подписью, которая идентифицирует личность отправителя сообщения или подписавшего документ, и удостоверяет, что оригинальное содержание посланного сообщения или документа не изменилось.

5. Агенты CSP's способны принимать решения на выполнение задач от имени своих пользователей. Агенты имеют право взаимодействовать с другими агентами путем переговоров, сотрудничества и координации. В CSP, агент работает для предоставления услуг, обслуживания переговоров, услуг сотрудничества и их координации.

Расширим эту модель: *X* − пользователь, *У* − аутентификатор подлинности. Для описания введем обозначения: t_x − временная метка, r_x, r_y − случайные числа *X* и *У* соответственно; S_x, S_y − подписи, сгенерированные *X* и *У*; $C_{кох}$, $C_{коу}$ − сертификаты открытого ключа *X* и *У*. Приведем алгоритмы аутентификации.

1. Односторонняя аутентификация с применением меток времени: $X \rightarrow У$: $C_{кох}$, t_x, I_x, $S_x(t_x, I_x)$.

После принятия сообщения аутентификатор подлинности проверяет правильность метки времени t_x, полученный идентификатор I_x и, используя открытый ключ из сертификата $C_{кох}$, корректность цифровой подписи $S_x(t_x, I_x)$.

2. Односторонняя аутентификация с применением случайных чисел: $У \rightarrow X$, r_y $У$ (1); $X \rightarrow У$: $С_{кох}$, r_x, I_y, $S_x(r_x, r_y, I_x)$ $У$ (2).

Атентификатор подлинности направляет пользователю X случайное число r_y на основании сообщения от X. Используя открытый ключ X из сертификата $С_{кох}$, $У$ проверяет корректность подписи $S_x(r_x, r_y, I_x)$ под числом r_x, числом r_y, полученным в первом сообщении, и его идентификатором I_x.

3. Двухсторонняя аутентификация с применением случайных чисел: $У \rightarrow X$, r_y (1); $X \rightarrow У$, $С_{кох}$, r_x, I_y, $S_x(r_x, r_y, I_x)$ (2); $У \rightarrow X$: $С_{коу}$, I_x, $S_y(r_x, r_y, I_x)$ (3).

В этом алгоритме обработка сообщений 1 и 2 выполняется как и в предыдущем, а сообщение 3 обрабатывается аналогично сообщению 2.

Заключение

В КИС используются следующие средства аутентификации: стандартные пароли, одноразовые пароли, аутентификации с использованием S/Key, контрольные суммы (при создании резюме фиксированной длины для представления длинных сообщений), электронные подписи (создаются шифрованием контрольной суммы и дополнительной информации при помощи личного ключа отправителя). Механизмы аутентификации можно рассмотреть по приоритету их использования: основные − при штатном входе в систему, резервные (почтовый ящик) − при потере пароля либо взломе учетной записи, последние (last resort) − при вмешательстве администрации информационной системы. Наибольшие результаты в проблему социальной идентификации внесли три коллектива исследователей: RSA Laboratories, Microsoft, Fasebook. Математическая модель модифицированной аутентификации в КИС позволяет по заданному числу неудовлетворительных оценок вычислить вероятность успешной аутентификации с использованием метода вычисления времени премодерации, позволяющего восстанавливать пароль как при его утере, так и при смене злоумышленником. Представлен модифицированный алгоритм на базе этой модели, позволяющий выполнять аутентификацию пользователей с привлечением поручителей.

AUTHENTIFICATION USER TOOLS IN CORPORATIVE INFORMATION SYSTEMS AND CLOUD COMPUTING AREAS

U.A. VISHNIAKOU, M.M. GONGAG SAS

Abstract

Analysis elements of users work in information corporative systems (ICS) are done. The mathematical model of social authentification in ICS allows on given quality of unsatisfactory marks to calculate the probability of successful authentification with the use of time primoderatin calculating. It allows to restore the user password during losing and by villain exchanging. The modifying algorithm on this model base is reproduced which allows to execute user authentification on charger with attraction. The approach for save user activity in clouding computer area is done.

Список литературы

1. *Афанасьев А.А., Веденьев Л.Т., Воронцов А.А. и др.* Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. М., 2012.
2. *Коноплев А.С.* Метод контроля и управления доступом в распределенных вычислительных сетях: Автореф. дисс. … канд. техн. наук. СПб, 2014.
3. *Васильчук К.С.* // Молодой ученый. 2014. № 4.2. С. 118–121.
4. *Волокитина Е.С.* Метод и алгоритмы гарантированного обезличивания и реидентификации субъекта персональных данных в автоматизированных информационных системах: Автореф. дисс. … канд. техн. наук. СПб, 2014.
5. *Малков А.А.* Технология аутентификации с помощью доверенных лиц: Автореф. дисс. … канд. техн. наук. Уфа, 2013.
6. *Вишняков В.А.* Информационное управление и безопасность: методы, модели, программно-аппаратные решения. Минск, 2014.
7. *Гондаг С.М., Вишняков В.А.* // Тез. докладов XIII Бел.-росс. НТК «Технические средства защиты информации». Минск, 2015. С. 29.