DOI: https://doi.org/10.15688/jvolsu10.2017.3.3

УДК 004.056.53
ББК 51я73

РАЗРАБОТКА ФОРМАЛЬНОЙ МОДЕЛИ ИССЛЕДОВАНИЯ СИСТЕМ АУТЕНТИФИКАЦИИ

Сергей Александрович Македонский

Кандидат технических наук,
главный специалист по информационной безопасности службы безопасности,
Волгоградский филиал АБ «РОССИЯ»
abr@m-p.ru
ул. Калинина, 21, 400001 г. Волгоград, Российская Федерация

Екатерина Витальевна Сухаревская

Студент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В данной статье рассмотрена проблема обеспечения защиты информации в современных информационных системах. Описаны и проанализированы существующие системы аутентификации, принцип их работы, их преимущества и недостатки. Были сформулированы критерии для их оценки и разработана формальная модель исследования систем аутентификации.

Ключевые слова: аутентификация, система аутентификации, информация, информационная система, информационная безопасность, защита информации, биометрия, электронно-цифровая подпись, пароль.

В настоящее время наиболее важным ресурсом стала информация, а необходимый инструмент почти в любой сфере деятельности – это информационные системы (ИС) [1, с. 42]. С их помощью решается множество задач, это и привело к разнородности информационных систем и хранящейся в них информации. Очень важно обеспечить информационную безопасность любой ИС.

Обеспечить информационную безопасность ИС – значит организовать комплексную систему защиты доступа к конфиденциальной информации системы, чтобы исключить попытки несанкционированного доступа (НСД) к данным. Поэтому в современных ИС перед началом работы с системой пользователь обязан пройти идентификацию, аутентификацию и авторизацию [1, с. 238]. Идентификация: субъект сообщает информацию о себе, идентифицируя себя (имя и др.). Аутентификация: система проверяет, действительно ли субъект тот, за кого себя выдает [1, с. 135]. Авторизация – система проверяет права пользователя на доступ к ресурсам [1, с. 127].

Процесс аутентификации является основой предоставления защищенного доступа, установления доверительных отношений между сервером и пользователем. Поэтому актуальным является исследование систем аутентификации.

В современных ИС существует достаточно большое количество разнообразных систем аутентификации, но в данной статье будет рассмотрено 6 основных и наиболее часто используемых систем:

I. Аутентификация при помощи электронно-цифровой подписи (ЭЦП) и интеллектуальных карт.

ЭЦП помещается на аппаратные средства (интеллектуальные карты) и используется в качестве средства аутентификации. Сервер распознает подписанный ЭЦП идентификатор (или PIN пользователя) на карте и проверяет ее, проводя аутентификацию пользователя.

II. Многоразовые пароли.

В большинстве случаев пароли могут обеспечить необходимый уровень защиты системы, но в крупных предприятиях (организациях) применение паролей в политике безопасности информационной системы недостаточно. Они не обеспечивают нужной защиты системы на этапе проверки подлинности сотрудника. Пароли зачастую создаются очень простыми и легко угадываемыми; их не хранят в тайне (могут быть указаны в документации, хранятся на рабочем столе сотрудника), при вводе пароля его могут подсмотреть и др.

III. Одноразовые пароли.

Этот метод более надежен, чем применение многоразовых паролей, но и в нем есть минус – он уязвим. Злоумышленник может прослушать трафик, при этом перехватив логин и одноразовый пароль, который был послан пользователем. Блокируя компьютер сотрудника, он отправляет полученные данные от своего имени.

IV. Биометрическая аутентификация.

Аутентификация посредством биометрических данных является новым современным методом защиты доступа, который в дальнейшем будет только совершенствоваться. В свою очередь, биометрические системы доступа основаны на параметрах человека, которые всегда будут при нем, то есть проблема сохранности не возникает [5].

Несмотря на то, что биометрическая аутентификация является сравнительно новой технологией распознавания личности, она не является совершенной. Как и другие способы идентификации/аутентификации, биометрический метод также подвержен угрозам. К примеру, к устройству сканирования биометрических данных можно легко поднести муляж (запись голоса, муляжи пальцев из баллистического геля и др.).

Однако при компрометации систем аутентификации пароли, как одноразовые, так и многоразовые, можно сменить, цифровые сертификаты или USB-ключи можно аннулировать, но биометрику человек заменить не сможет. Поэтому если биометрические данные сотрудников будут скомпрометированы, то организация будет вынуждена производить полную модернизацию всей системы.

V. Аутентификация через географическое местоположение.

Данный метод – новейшее направление аутентификации, которое устанавливает подлинность пользователя на основе его местонахождения. Этот механизм использует систему космической навигации – GPS (Global Positioning System): подсистема определяет с точностью до метра месторасположение пользователя.

Основным достоинством такого метода аутентификации является то, что аппаратура GPS надежна в использовании и относительно недорога. Ее использование необходимо в тех случаях, когда удаленный пользователь должен находиться в нужном месте для авторизации. Так как координаты спутников меняются постоянно, то вероятность перехвата этих координат равна нулю.

VI. Графическая аутентификация.

Суть такой аутентификации заключается в том, что пользователю предоставляется несколько коллекций изображений, которые, в свою очередь, разбиты по темам. Пользователь должен выбрать определенный набор изображений, при этом введя дополнительный текстовый пароль (многоразовый).

Такая аутентификация устойчива к перехвату: программа-шпион не отследит ввод графического пароля с клавиатуры, так как кроме графического пароля существует текстовый пароль.

Для исследования систем аутентификации предлагается использовать следующие критерии:

1. Стоимость установки и обслуживания ($К_1$) – это показатель затрат, который вклю-

чает в себя затраченное время, усилия и средства администратора системы на ее установку и обслуживание, а также время, затраченное пользователем на создание или изменения своей учетной записи.

2. Удобство использования ($К_2$) – подразумевает простоту использования для пользователей, портативность систем аутентификации и универсальность.

3. Наличие открытого интерфейса ($К_3$) – критерий отражает возможность интеграции и совместимости с уже существующими приложениями и для будущего использования для новых приложений.

4. Подверженность атакам ($К_4$) – показатель, отражающий существующие уязвимости в реализации и конфигурации. Данный критерий можно разделить на три составляющие:

4.1. Возможность подмены ($К_{4.1}$);

4.2. Возможность полного перебора ($К_{4.2}$);

4.3. Возможность оптимизированного перебора ($К_{4.3}$).

5. Возможность возникновения ошибок ($К_5$) – подразумевает возможность системы аутентификации допускать ошибки, а именно: допустить к системе незарегистрированного пользователя и, наоборот, не допустить к системе зарегистрированного пользователя.

6. Требование наличия дополнительных программных и аппаратных средств ($К_6$).

В таблице представлено сравнение систем аутентификации.

Так как ни одна из систем аутентификации не обладает наилучшим набором значений критериев, необходимо разработать формальную модель для выбора наиболее рациональной системы аутентификации.

Сформируем вектор критериев К = ($К_1$, $К_2$, $К_3$, $К_4$, $К_5$, $К_6$).

$К_1$ – стоимость установки и обслуживания – принимает следующие значения:

$$К_1 = \begin{cases} 0, \text{высокая} \\ 0.5, \text{средняя} \\ 1, \text{низкая} \end{cases}$$

$К_2$ – удобство использования – принимает следующие значения:

$$К_2 = \begin{cases} 0, \text{низкое} \\ 0.5, \text{среднее} \\ 1, \text{высокое} \end{cases}$$

$К_3$ – наличие открытого интерфейса – принимает следующие значения:

$$К_3 = \begin{cases} 0, \text{нет} \\ 1, \text{да} \end{cases}$$

$К_4$ – подверженность атакам – будет рассчитываться по формуле (1).

$$К_4 = \sum_i К_{4i}, \qquad (1)$$

где

$$К_{4.1} = \begin{cases} 0, \text{есть } \textit{возможность подмены} \\ \frac{1}{3}, \text{нет } \textit{возможности подмены} \end{cases}$$

$$К_{4.2} = \begin{cases} 0, \text{есть } \textit{возможность полного перебора} \\ \frac{1}{3}, \text{нет } \textit{возможности полного перебора} \end{cases}$$

$$К_{4.3} = \begin{cases} 0, \text{есть } \textit{возможность оптимизированного перебора} \\ \frac{1}{3}, \text{нет } \textit{возможности оптимизированного перебора} \end{cases}$$

$К_5$ – возможность возникновения ошибок аутентификации – принимает следующие значения:

$$K_5 = \begin{cases} 0, \text{да} \\ 1, \text{нет} \end{cases}$$

$К_6$ – требование наличия дополнительных программных и аппаратных средств – принимает следующие значения:

Качественные значения критериев систем аутентификации

Система аутентификации	Критерии оценки							
	$К_1$	$К_2$	$К_3$	$К_{4.1}$	$К_{4.2}$	$К_{4.3}$	$К_5$	$К_6$
ЭЦП и интеллектуальные карты	Высокая	Среднее	Да	Да	Нет	Нет	Нет	Требуется
Многоразовые пароли	Низкая	Среднее	Нет	Да	Да	Да	Нет	Не требуется
Одноразовые пароли	Низкая	Низкое	Нет	Да	Да	Нет	Нет	Только ПО
Биометрическая аутентификация	Средняя	Высокое	Да	Да	Нет	Нет	Да	Требуется АО
Аутентификация через географическое местоположение	Средняя	Низкое	Нет	Да	Нет	Нет	Да	Требуется
Графическая аутентификация	Высокая	Высокое	Нет	Нет	Да	Да	Да	Только ПО

$$K_6 = \begin{cases} 0, \text{ требуется} \\ \frac{1}{3}, \text{ требуется аппаратное обеспечение} \\ \frac{2}{3}, \text{ требуется программное обеспечение} \\ 1, \text{ не требуется} \end{cases}$$

Существует наилучший вектор K* , в котором все значения критериев соответствуют максимальным значениям. Для всех критериев это значение 1.

$$K^* = (1, 1, 1, 1, 1, 1).$$

Для оценки качества систем аутентификации вводится скалярная величина, равная расстоянию городских кварталов, или «манхэттенскому расстоянию», между наилучшим вектором и вектором критериев, полученным для *i*-го оцениваемой системы:

$$K^i = \left(K_1^i, K_2^i, K_3^i, K_4^i, K_5^i, K_6^i\right).$$

«Манхэттенское расстояние» рассчитывается по формуле (2).

$$p^i = \sum_{j=1}^{6} \left| K_j^* - K_j^i \right|. \qquad (2)$$

Систему, для которой расстояние до наилучшего вектора окажется наименьшим, можно считать наиболее рациональной системой аутентификации.

Основной целью разработанной формальной модели является выбор наиболее рациональной системы аутентификации. Преимущество данной модели заключается в том, что даже при изменении качественных характеристик системы аутентификации или при добавлении новой системы к сравнению мы получим адекватный ответ. По сути, расстояние городских кварталов отражает геометрическое расстояние в многомерном пространстве, поэтому применение данной формальной модели дает нам комплексный, учитывающий все критерии результат при выборе наилучшей системы аутентификации.

СПИСОК ЛИТЕРАТУРЫ

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. – М. : Горячая линия – Телеком, 2012. – 552 с.

2. Динамические методы биометрической аутентификации / А. А. Островский, Д. Н. Жариков, В. С. Лукьянов, Д. С. Попов // Известия Волгоградского государственного технического университета. – 2010. – Т. 6, № 8. – С. 72–76.

3. Кусков, Н. А. Исследование способов несанкционированного доступа к информации / Н. А. Кусков // Научный вестник Московского государственного технического университета гражданской авиации. – 2013. – № 6 (192). – С. 127–129.

4. Сабанов, А. Г. Об уровнях строгости аутентификации / А. Г. Сабанов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. – № 2-1 (26). – С. 134–139.

5. Технология усиленной аутентификации пользователей информационных процессов / И. А. Ходашинский, М. В. Савчук, И. В. Горбунов, Р. В. Мещеряков // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2011. – № 2-3 (24). – С. 236–248.

6. The analysis of methods and approaches for modeling components of the complex organizational and technical systems “smart city” / Yu. S. Bakhracheva, A. A. Kadyrov, A. A. Kadyrova, E. A. Maksimova // Вестник Волгоградского государственного университета. Серия 10, Инновационная деятельность. – 2017. – Т. 11, № 2. – С. 6–10. – DOI: https://doi.org/10.15688/jvolsu10.2017.2.1.

REFERENCES

1. Shelupanova A.A., Gruzdeva S.L., Nakhaeva Yu.S., eds. *Autentifikatsiya. Teoriya i praktika obespecheniya bezopasnogo dostupa k informatsionnym resursam* [Authentication. The Theory and Practice of Providing Safe Access to Information Resources]. Moscow, Goryachaya liniya – Telekom Publ., 2012. 552 p.

2. Ostrovskiy A.A., Zharikov D.N., Lukyanov V.S., Popov D.S. Dinamicheskie metody biometricheskoy autentifikatsii [Dynamic Methods of Biometric Authentication]. *Izvestiya Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta*, 2010, vol. 6, no. 8, pp. 72-76.

3. Kuskov N.A. Issledovanie sposobov nesanktsionirovannogo dostupa k informatsii [The Study of the Ways of Unauthorized Access to Information]. *Nauchnyy vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta grazhdanskoy aviatsii*, 2013, no. 6 (192), pp. 127-129.

4. Sabanov A.G. Ob urovnyakh strogosti autentifikatsii [About the Levels of Rigor

Authentication]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki*, 2012, no. 2-1 (26), pp. 134-139.

5. Khodashinskiy I.A., Savchuk M.V., Gorbunov I.V., Meshcheryakov R.V. Tekhnologiya usilennoy autentifikatsii polzovateley informatsionnykh protsessov [Technology of Enhanced Authentication of Information Processes User]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki*, 2011, no. 2-3 (24), pp. 236-248.

6. Bakhracheva Yu.S., Kadyrov A.A., Kadyrova A.A., Maksimova E.A. The analysis of methods and approaches for modeling components of the complex organizational and technical systems "smart city". *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 10, Innovatsionnaya deyatelnost* [Science Journal of Volgograd State University. Technology and Innovations], 2017, vol. 11, no. 2, pp. 6-10. DOI: https://doi.org/10.15688/jvolsu10.2017.2.1.

THE FORMAL MODEL OF RESEARCH ON AUTHENTICATION SYSTEMS

Sergey Aleksandrovich Makedonskiy

Candidate of Technical Sciences, Chief Specialist for Information Security of Security Service,
Volgograd Branch of ROSSIYA JS Bank
abr@m-p.ru
Kalinina St., 21, 400001 Volgograd, Russian Federation

Ekaterina Vitalyevna Sukharevskaya

Student, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. Currently, the information systems are the most important resource and necessary tool in almost any field. They help to solve various problems, and this led to the heterogeneity of information systems and information stored in them. It is very important to maintain the security of any information system.

Providing information security means organizing a comprehensive system of protection of access to information system, to prevent unauthorized access to data. Therefore, before working with modern information systems, the user shall complete the identification, authentication and authorization. **Identification:** the subject reports identifying information about themselves (name, etc.). **Authentication:** the system checks whether the subject is who they claim to be. **Authorization:** the system checks the user's rights to access resources.

The authentication process is the basis for providing secure access, for establishing a trust relationship between the server and the user. So, it is important to study authentication systems.

The paper deals with the problem of information security in modern information systems. The authors describe and analyze existing authentication systems, the principles of their work, their advantages and disadvantages. The criteria for their evaluation have been formulated, and the formal model of research on authentication systems has been developed.

Key words: authentication, authentication system, information, information system, information security, protection of information, biometric, digital signature, password.