УДК 004.056.53

ИССЛЕДОВАНИЕ СИСТЕМ АУТЕНТИФИКАЦИИ

Е.В. Сухаревская

студент кафедры информационной безопасности

Волгоградский государственный университет

Аннотация: В современном мире очень остро стоит вопрос обеспечения информационной безопасности любых информационных систем, так как в них хранится и обрабатывается очень большой объем информации ограниченного доступа. Одновременно с развитием информационных технологий очень быстро развиваются и злоумышленные действия над информацией. Поэтому в данной статье была очень подробно рассмотрена и проанализирована такая актуальная проблема современного общества, как обеспечение защиты информации в современных информационных системах. В основе защиты информации в информационных системах лежит базовый принцип защиты - разграничение доступа в систему. Разграничение доступа подразумевает собой проведение таких трех процессов, как идентификация, аутентификация и авторизация. В этой статье очень подробно описываются существующие современные системы аутентификации. Учитывая их разнообразие и многофункциональность, были также рассмотрены принципы и алгоритмы их работы, области их применения, преимущества и недостатки каждой системы аутентификации. В итоге были сформулированы качественные и количественные критерии для оценки систем аутентификации, была разработана математическая модель для исследования систем аутентификации, на основе которой был сделан вывод о наилучшей системе аутентификации в настоящее время.

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

THE RESEARCH OF AUTHENTICATION SYSTEMS

E.V. Sukharevskaya

Student of the Department of Information Security

Volgograd State University

Annotation: In the modern world it is an issue of information security of all information systems, as they are stored and processed a lot of information of limited access. Simultaneously with the development of information technologies the malicious acts over the information develop very quickly. So this article was very thoroughly reviewed and analyzed such a topical problem of modern society, as the protection of information in modern information systems. The basis of information protection in information systems is the basic principle of protection - control of access to the system. Access control involves the holding of such three processes as identification, authentication and authorization. In this article in great detail describes the existing modern system of authentication. Given their diversity and versatility were also considered principles and algorithms, their applications, advantages and disadvantages of each authentication system. In the end, there was formulated qualitative and quantitative criteria for evaluating authentication systems, developed a mathematical model for the analysis of authentication systems on the basis of which the conclusion was made about the authentication system is currently.

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

В настоящее время информационные технологии стали неотъемлемой частью всех сфер деятельности человека. Наравне с развитием технологий усиливаются и злоумышленные действия над информацией. Так как в информационных системах хранится и обрабатывается большой объем информации ограниченного доступа, очень остро стоит вопрос обеспечения безопасности этой информации [1, С. 42].

С помощью ИС 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 [2, С. 238]. Идентификация: субъект сообщает информацию о себе, идентифицируя себя (имя и др.). Аутентификация: система проверяет, действительно ли субъект тот, за кого себя выдает [3, С. 135]. Авторизация: система проверяет права пользователя на доступ к ресурсам [4, С. 127].

Процесс аутентификации является основой предоставления защищенного доступа, установления доверительных отношений между информационной системой 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, С. 174].

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 пароля с клавиатуры, так как существует еще графический пароль помимо текстового.

Для исследования систем аутентификации предлагается использовать следующие критерии:

1. Стоимость установки и обслуживания (К1) – это показатель затрат, который включает в себя затраченное время, усилия и средства администратора системы на её установку и обслуживание, а также время, затраченное пользователем на создание или изменения своей учётной записи.

2. Удобство использования (К2) – подразумевает простоту использования для пользователей, портативность систем аутентификации и универсальность.

3. Наличие открытого интерфейса (К3) – критерий отражает возможность интеграции и совместимости с уже существующими приложениями и для будущего использования для новых приложений.

4. Подверженность атакам (К4) – показатель, отражающий существующие уязвимости в реализации и конфигурации. Данный критерий можно разделить на три составляющие:

4.1. Возможность подмены (К4.1);

4.2. Возможность полного перебора (К4.2);

4.3. Возможность оптимизированного перебора (К4.3);

5. Возможность возникновения ошибок (К5) – 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 (К6).

В таблице 1 представлено сравнение систем аутентификации.

Таблица 1

Качественные значения критериев

Система аутентификации	**Критерии оценки**							
	К1	**К2**	**К3**	**К4.1**	**К4.2**	**К4.3**	**К5**	**К6**

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

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 $K = (K_1, K_2, K_3, K_4, K_5, K_6)$.

K_1 – стоимость установки и обслуживания принимает следующие значения:

$$K_1 = \begin{cases} 0, \text{высокая} \\ 0.5, \text{средняя} \\ 1, \text{низкая} \end{cases}$$

K_2 – удобство использования принимает следующие значения:

$$K_2 = \begin{cases} 0, \text{низкое} \\ 0.5, \text{среднее} \\ 1, \text{высокое} \end{cases}$$

K_3- наличие открытого интерфейса принимает следующие значения:

$$K_3 = \begin{cases} 0, \text{нет} \\ 1, \text{да} \end{cases}$$

K_4- подверженность атакам будет рассчитываться по формуле (1).

$$K_4 = \sum_i K_{4i}, \quad (1)$$

где

$$K_{41} = \begin{cases} 0, \text{есть возможность подмены} \\ \frac{1}{3}, \text{нет возможности подмены} \end{cases}$$

$$K_{42} = \begin{cases} 0, \text{есть возможность полного перебора} \\ \frac{1}{3}, \text{нет возможности полного перебора} \end{cases}$$

$$K_{43} = \begin{cases} 0, \text{есть возможность оптимизированного перебора} \\ \frac{1}{3}, \text{нет возможности оптимизированного перебора} \end{cases}$$

K_5- возможность возникновения ошибок аутентификации принимает следующие значения:

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

K_6 – требование наличия дополнительных программных и аппаратных средств принимает следующие значения:

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

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:

$$K^i = (K_1^i, K_2^i, K_3^i, K_4^i, K_5^i, K_6^i)$$

«Манхэттенское расстояние» рассчитывается по формуле (2).

$$P^i = \sum_{j=1}^{6} |K_j^* - K_j^i| \quad (2)$$

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

Применив формулу (2), получаем обобщенные оценки:

1. Аутентификация посредством электронно-цифровой подписи и интеллектуальных карт - 2,8333;

2. Аутентификация с использованием многоразовых паролей – 2,5;

3. Аутентификация с использованием одноразовых паролей - 3;

4. Биометрическая аутентификация – 2,5;

5. Аутентификация через географическое местоположение – 3,8333;

6. Графическая аутентификация – 4;

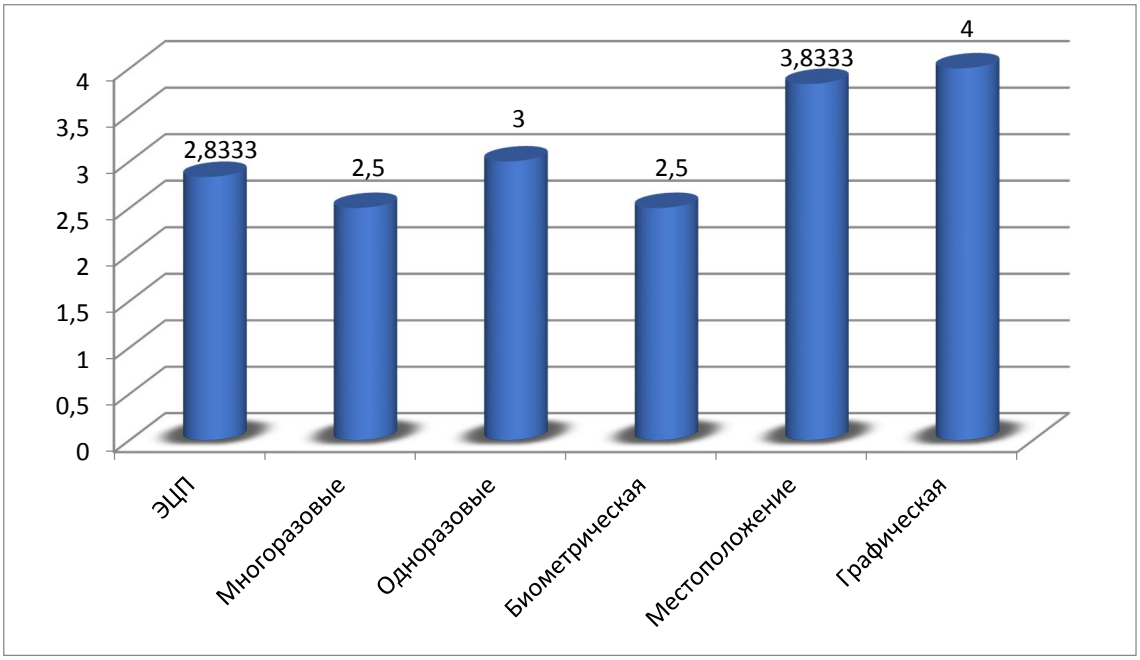

Рисунок 1 – Диаграмма обобщенных оценок систем аутентификации

Сравнив полученные результаты, можно прийти к выводу, что наиболее рациональными системами аутентификации является система с использованием многоразовых паролей и система биометрической аутентификации.

Достоинствами системы аутентификации с использованием многоразовых паролей являются низкая стоимость установки и обслуживания, отсутствие ошибок и отсутствие необходимости дополнительного аппаратного и программного обеспечения. Достоинствами системы биометрической аутентификации являются стойкость к атакам, высокое удобство использования для пользователей, совместимость и возможность к интеграции.

Библиографический список

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

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

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

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

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