Бобрышева Г.В., Мещерякова Е.С. Анализ систем аутентификакции. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVIII Междунар. научно-техн. конф. – Пенза: ПДЗ, 2018. – С. 117-123.

УДК 004.056.53

АНАЛИЗ СИСТЕМ АУТЕНТИФИКАЦИИ

Г.В. Бобрышева, Е.С. Мещерякова

ANALYSIS OF AUTHENTICATION SYSTEMS

G.V. Bobrysheva, E.S. Meshcheryakova

Аннотация. Рассматривается безопасное хранение и передача конфиденциальной и персональной информации в вычислительных системах и сетях, обеспечиваемое применением различных моделей защиты информации от несанкционированного доступа третьих лиц. Это позволяет надежно проводить идентификацию и аутентификацию пользователей, а также реализовывать конкретные системы разграничения доступа аутентифицированных пользователей к ресурсам вычислительной системы или сети.

Ключевые слова: конфиденциальная информация, несанкционированный доступ, идентификация пользователя, аутентификация пользователя.

Abstract. We consider the safe storage and transfer of confidential and personal information in computer systems and networks, provided by the use of various models of information protection from unauthorized access of third parties. This allows reliable identification and authentication of users, as well as implement specific systems of access control of authenticated users to the resources of the computer system or network.

Keywords: confidential information, unauthorized access, user identification, user authentication.

В настоящее время информационные технологии стали неотъемлемой частью всех сфер деятельности человека. Однако с развитием информационных технологий возрастает проблема защиты информации от злоумышленных действий нарушителей. При этом особенно остро стоит вопрос обеспечения безопасного хранения и передачи конфиденциальной и персональной информации в вычислительных системах и сетях.

Эффективное решение вопроса обеспечения безопасного хранения и передачи конфиденциальной и персональной информации в вычислительных системах и сетях обеспечивается за счет реализации конкретных моделей защиты информации от несанкционированного доступа (НСД) с применением технических средств и проведением соответствующих административных мероприятий, направленных на:

идентификацию и аутентификацию пользователей;

формирование конкретных систем разграничения доступа аутентифицированных пользователей к ресурсам вычислительной системы или сети, реализуемых в виде методов контроля доступа.

Идентификация пользователя вычислительной системы или сети заключается в установлении и закреплении за каждым из них уникального идентификатора в виде:

- персонального идентификационного номера PIN (Personal

Identification Nuber);

- социального безопасного номера SSN (Socia1 Security Nutber);
- личного номера;
- кода безопасности и т.д.

Данные идентификаторы используются при построении различных систем разграничения доступа и защиты информации [1].

Аутентификация пользователей заключается в проверке подлинности пользователя по предъявленному им идентификатору при входе в вычислительную систему или сеть, которая позволяет исключить фальсификацию пользователей в системе и их компрометацию.

Процесс аутентификации является основой предоставления защищенного доступа, установления доверительных отношений между вычислительной системой или сетью и пользователями [2].

Аутентификация пользователей в вычислительной системе или сети может осуществляться различными методами и средствами, наиболее популярными среди которых являются следующие системы:

1) аутентификация с помощью карт идентификации;
2) парольная аутентификация;
3) биометрическая аутентификация;
4) аутентификация через географическое местоположение;
5) графическая аутентификация.

Аналитический анализ используемых на практике систем аутентификации проведен по следующим критериям:

- стоимость установки и обслуживания, К1;
- удобство использования, К2;
- возможность подмены, К3;
- возможность полного перебора, К4;
- возможность оптимизированного перебора, К5;
- возможность возникновения ошибок, К6;
- требование наличия дополнительных программных и аппаратных средств, К7.

Результаты аналитического анализа систем аутентификации приведены в таблице.

Значения полученных характеристик позволяют сделать вывод, что наиболее рациональными системами аутентификации являются системы с использованием паролей, что объясняется их простотой, низкой стоимостью установки и обслуживания, отсутствием необходимости дополнительного аппаратного и программного обеспечения.

Парольная система аутентификации является одной из первых и самой популярной системой аутентификации. Аутентификация пользователя в данном случае осуществляется по «логину» и многоразовому или одноразовому паролю [3].

Характеристики систем аутентификации

Система аутентификации	Критерии оценки						
	К1	К2	К3	К4	К5	К6	К7
Аутентификация с помощью карт идентификации	высокая	среднее	нет	нет	нет	нет	требуется
Парольная аутентификация	низкая	среднее	да	да	нет	нет	не требуется
Биометрическая аутентификация	высокая	высокое	да	нет	нет	да	требуется
Аутентификация через географическое местоположение	средняя	низкое	да	нет	нет	да	требуется
Графическая аутентификация	высокая	высокое	нет	да	да	да	не требуется

Главной угрозой парольной аутентификации является взлом или компрометация пароля, которая может быть реализована с помощью:

- полного перебора паролей;
- атаки с помощью словаря;
- атаки с помощью радужных таблиц;
- метода социальной инженерии, основанного на предположении, что пользователь использовал в качестве пароля личные сведения: имя или фамилию, дату рождения и т.п.;
- установки вредоносных программ для перехвата пароля;
- подмены доверенного объекта сети (IP-spoofing);
- перехвата пакетов (sniffing).

Аутентификация с помощью карт идентификации заключается в том, что идентификационные данные пользователя заносятся на карту в зашифрованном виде. При этом ключ шифрования может быть дополнительным идентифицирующим параметром, который известен только пользователю и вводится им каждый раз при обращении к вычислительной системе или сети. Информация, находящейся на карте идентификации, может быть записана и считана различными способами или комбинацией нескольких способов в зависимости от используемого устройства аутентификации пользователя.

Преимущества данного способа аутентификации заключаются в:

- универсальности применения;
- относительно низкой стоимости;
- высокой точности;
- легкости комплексирования (взаимодействия) с терминалом и персональной ЭВМ.

Основным недостатком аутентификации пользователей с помощью карт идентификации является наличие возможности потери или порчи карты.

Биометрическая аутентификация в последнее время начинает приобретать возрастающее значение и основана на измерении биометрических параметров человека и применении специальных систем идентификации (опознавания) пользователей по физиологическим признакам (биометрическим характеристикам). Процесс прохождения биометрической аутентификации называется процедурой биометрики [2].

Для аутентификации терминальных пользователей вычислительных систем и сетей по физиологическим признакам или биометрическим характеристикам наиболее приемлемыми считаются следующие способы:

1) аутентификация пользователей по отпечаткам пальцев;

2) аутентификация пользователей по форме кисти руки – по геометрии руки;

3) аутентификация пользователей с помощью автоматического анализа подписи;

4) аутентификация пользователей по манере ввода данных с клавиатуры:

5) аутентификация пользователей по характеру голоса;

6) аутентификация пользователей по лицу;

7) аутентификация пользователей по радужной оболочке глаза.

Другими примерами систем аутентификации пользователей по физиологическим признакам или биометрическим характеристикам, над которыми в настоящее время ведутся разработки, являются системы аутентификации по отпечаткам ног, почерку, тембру голоса, ферментам (органическим веществам, которые вырабатываются живой клеткой и содействуют различным химическим реакциям, происходящим в организме: бродильный фермент, фермент окисления, фермент гниения), динамики дыхания, инфракрасной картине капиллярных сосудов, запаху, формам ушей, зубам и ДНК.

Достоинства биометрической аутентификации заключаются в том, что:

- почти 100 % идентификация пользователей;

- решается проблема утраты паролей и личных идентификаторов пользователей.

Недостатками биометрической аутентификации являются:

1) сравнение биометрического шаблона (эталона) не с первоначальным, а конечным результатом обработки биометрических характеристик пользователя;

2) база шаблонов может быть изменена злоумышленником;

3) зависимость вероятности ошибочной аутентификации от места и условий применения процедуры биометрики;

4) требуется постоянное сопровождение и обновление базы биометрических шаблонов (эталонов), что создает определенные проблемы, как для пользователей, так и для администраторов;

5) возможна кража и компрометация биометрических данных пользователей;

6) биометрические характеристики являются уникальными идентификаторами пользователей, но их нельзя сохранить в секрете.

Аутентификация через географическое местоположение позволяет установить подлинность пользователя по его местонахождению. Данный метод для аутентификации пользователей использует спутниковую систему навигации GPS (Global Positioning System) и чаще всего применяется в тех случаях, когда необходимо авторизовать удаленного пользователя при условии, что он должен находиться в нужном, конкретном месте. При этом месторасположение пользователя определяется с точностью до метра. Основным требованием для реализации метода является наличие у пользователя аппаратуры GPS [2].

Основными достоинствами метода аутентификации через географическое местоположение являются:

- высокая надежность: определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно, и, кроме того, координаты спутников постоянно меняются, что сводит на нет возможность их перехвата;
- сравнительно невысокая стоимость реализации: объясняется тем, что аппаратура GPS проста, надежна в использовании и сравнительно недорога;
- сложность взлома: состоит в том, что аппаратура беспроводной (спутниковой) связи передает оцифрованный сигнал спутника, не производя никаких вычислений, а все вычисления о местоположении пользователя производятся на сервере аутентификации.

Графическая аутентификация 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).

Достоинством такой аутентификации является устойчивость к перехвату: например, программа-шпион не может отследить ввод пароля с клавиатуры, так как существует еще графический пароль помимо текстового.

Выбор системы аутентификации для реализации конкретных моделей защиты информации от несанкционированного доступа (систем безопасности) должен осуществляться на основании:

- установленных требований к системе аутентификации пользователей;
- требуемой степени защищенности систем безопасности;
- стоимости построения системы аутентификации пользователей;
- необходимости обеспечения мобильности пользователя.

Правильный выбор системы аутентификации во многом определяет эффективность используемой системы безопасности и соответственно обеспечивает информационную безопасность ресурсов вычислительной системы или сети.

Библиографический список

1. Афанасьев А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учебное пособие для вузов / под ред. А. Шелупанова, С. Груздева, Ю. Нахаева. М.: Горячая Линия – Телеком, 2009. 552 с.

2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие для вузов. М.: Горячая Линия – Телеком, 2011. 320 с.

3. Брянцев А.В. Разработка программного модуля аутентификации внешних пользователей компьютерной системы / А.В. Брянцев, В.Е. Дихнов, А.Г. Качурин, А.А. Адодин // Молодой ученый. 2018. №23. с. 195-197. URL: https://moluch.ru/archive/209/51198/ (дата обращения: 24.09.2018).

Бобрышева Галина Владимировна
Пензенский государственный университет,
г. Пенза, Россия
E-mail: g_bobr@mail.ru

Bobrysheva G.V.
Penza State University,
Penza, Russia

Мещерякова Елена Сергеевна
Пензенский государственный университет,
г. Пенза, Россия

Meshcheryakova E.S.
Penza State University,
Penza, Russia