2000. – 145 с. – С. 53 – 57.

2. *Мелкумян К.В., Вербицький М.А.* Узагальнений опис побудови інтелектуальної системи захисту інформації в розподілених автоматизованих системах / Захист інформації: Науково-технічний журнал. – Киев: КМУЦА, 2000, № 3. – 66 с. – С. 13 – 19.

3. *Грушо А.А., Тимонина Е.Е.* Теоретические основы защиты информации. – М: "Яхтсмен",1996.

4. *Искусственный интеллект:* Справочник/ Под ред. Д.А.Поспелова. – В 3-х кн. Кн. 2. Модели и методы. – М.: Радио и связь, 1990.

Надійшла 25.01.2006
Після доробки 16.05.2006

УДК 004.623 **Безмалый В.Ф.**

ПАРОЛЬНАЯ ЗАЩИТА: ПРОШЛОЕ, НАСТОЯЩЕЕ, БУДУЩЕЕ

Одним из важнейших процессов, создаваемых для соблюдения такого свойства информации, как конфиденциальность, является ограничение доступа. Наиболее распространен такой процесс аутентификации, как использование пароля. Практически с момента создания первых многопользовательских операционных систем для ограничения доступа используются пароли. Вспомним историю.

Операционные системы Windows 95/98 сохраняли пароль в PWL файле. PWL файлы хранились в каталоге Windows. Их имена, как правило, хранились как USERNAME.PWL. Вместе с тем стоит отметить, что PWL файл был зашифрован и извлечь из него пароли было не просто. Первый алгоритм шифрования версии Windows'95 был создан так, что позволял создать программы для расшифровки PWL файлов. Однако в версии OSR2 этот недостаток был устранен. Система защиты паролей в OSR2 была сделана профессионально и достоверно в терминах криптографии. Однако, несмотря на это, содержала несколько серьезных недостатков, а именно:

- все пароли преобразованы к верхнему регистру, это значительно уменьшает количество возможных паролей;
- используемые для шифрования алгоритмы MD5 и RC4 позволяют более быстрое шифрование пароля, но достоверный пароль Windows должен быть, по крайней мере, длиной в девять символов.

Система кэширования пароля по существу ненадежна. Пароль может быть сохранен только в том случае, если никакой персонал, не имеющий соответствующего разрешения, не может обращаться к вашему компьютеру.

В настоящее время рекомендуемая Microsoft длина пароля для рабочей станции Windows XP должна составлять не менее 8 символов, при этом в пароле должны встречаться большие и маленькие буквы, цифры и спецсимволы. При этом время жизни пароля должно составлять не более 42 дней. К тому же на пароль налагается требование неповторяемости. В дальнейшем эти требования будут только ужесточаться. К чему это приведет, вернее, увы, уже приводит? Чем сложнее пароли, чем больше приложений требуют ввод пароля, тем выше вероятность того, что ваши пользователи для всех приложений, в том числе и для аутентификации в ОС, будут использовать один и тот же пароль или они будут записывать его на бумагу. Хорошо это или плохо? Допустимо ли?

С одной стороны – явно не допустимо, так как резко вырастает риск компрометации пароля, с другой – слишком сложный пароль (типа PqSh*98+) весьма сложно удержать в голове, и пользователи явно будут либо выбирать простой пароль, либо постоянно забывать

его и звать администратора. Да добавим сюда еще и необходимость его постоянной смены, и требование неповторяемости паролей. Что делать? Где выход?

На самом деле уже на сегодня существует несколько вариантов, как помочь пользователю в решении этой нелегкой проблемы. Попробуем их кратко описать здесь.

Первый вариант. На видном месте в комнате (на стене, на столе) вывешивается (кладется) плакат с лозунгом. После этого в качестве пароля используется текст, содержащий, предположим, каждый третий символ лозунга, включая пробелы и знаки препинания. Не зная алгоритма выбора знаков, подобный пароль подобрать довольно сложно.

Второй вариант. В качестве пароля выбирается (генерируется с помощью специального ПО) случайная последовательность букв, цифр и специальных символов. Полученный пароль распечатывается на матричном принтере на специальных конвертах, которые нельзя вскрыть, не нарушив целостности. Примером такого конверта может служить PIN-конверт к платежной карте. Далее такие конверты хранятся в сейфе начальника подразделения или сейфе службы информационной безопасности. Единственной сложностью при таком способе хранения является необходимость немедленной смены пароля сразу после вскрытия конверта и изготовления другого подобного конверта с новым паролем, а также организация учета конвертов. Однако если учесть сбережение времени администраторов сети и приложений, то эта цена не является чрезмерной.

Третий вариант – использование двухфакторной аутентификации на базе новейших технологий аутентификации. Основным преимуществом двухфакторной аутентификации является наличие физического ключа и PIN -кода к нему, что обеспечивает дополнительную устойчивость к взлому. Ведь утрата аппаратного ключа не влечет за собой компрометации пароля, так как кроме ключа для доступа к системе нужен еще и PIN -код к ключу.

Отдельно стоит рассмотреть системы с применением разовых паролей, которые получают все большее распространение в связи с широким развитием Интернет-технологий и системы биометрической аутентификации.

В настоящее время основным способом защиты информации от несанкционированного ознакомления (модификации, копирования) является внедрение так называемых средств AAA (authentication, authorization, administration – аутентификация, авторизация, администрирование).

При использовании этой технологии пользователь получает доступ к компьютеру лишь после того, как успешно прошел процедуры идентификации[1] и аутентификации[2].

Стоит учесть, что на мировом рынке ИТ-услуг традиционно растет сегмент AAA. Эта тенденция подчеркивается в аналитических обзорах IDC, Gartner и других фирм.

То есть в дальнейшем мы с вами все чаще будем встречаться именно с программно-аппаратными средствами аутентификации, которые постепенно придут на смену традиционным паролям.

Классификация средств идентификации и аутентификации

Современные программно-аппаратные средства идентификации и аутентификации по виду идентификационных признаков можно разделить на электронные, биометрические и комбинированные. В отдельную подгруппу в связи с их специфическим применением можно выделить системы одноразовых паролей, входящие в состав электронных (рис. 1).

В электронных системах идентификационные признаки представляются в виде кода, хранящегося в памяти идентификатора (носителя). Идентификаторы в этом случае бывают следующие: контактные смарт-карты; бесконтактные смарт-карты; USB-ключи (USB-token); iButton.

---

[1] Идентификация – процесс распознавания пользователя по его идентификатору (имени).

[2] Аутентификация – проверка соответствия идентификационного признака (например, пароля) пользователю, т.е. проверка соответствия пользователя его идентификатору (имени).

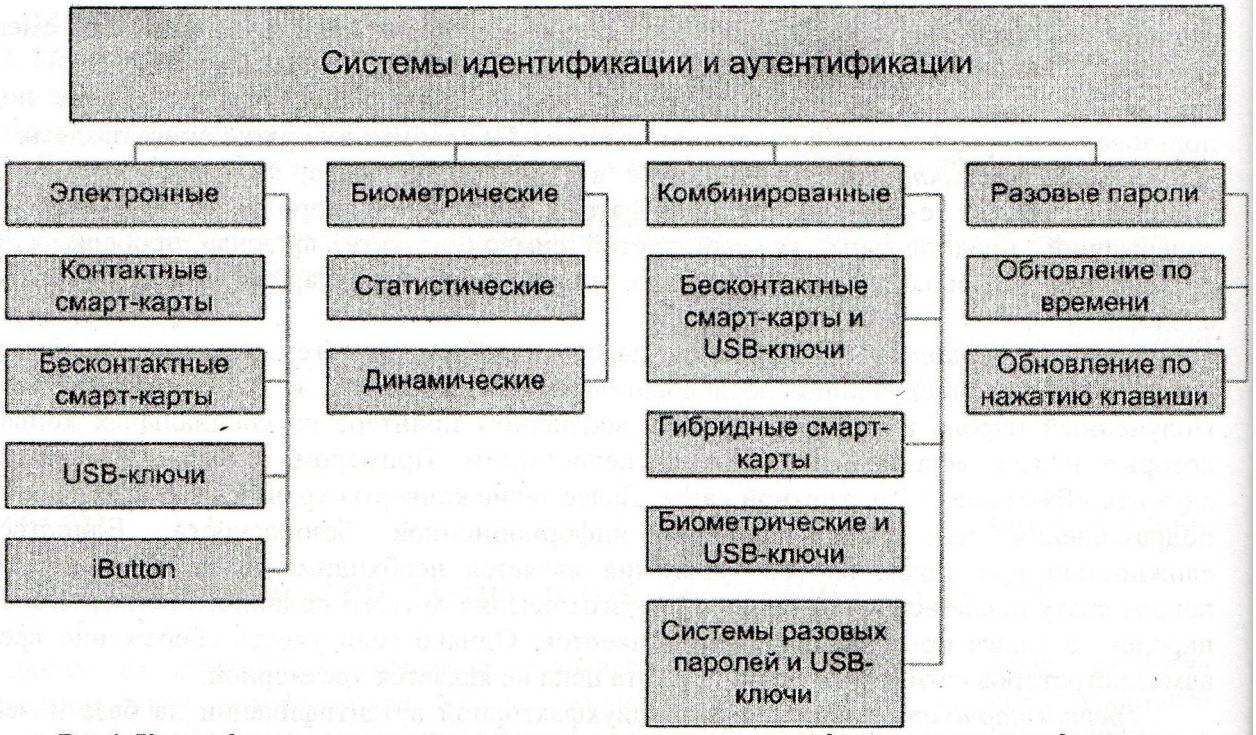

Рис.1. Классификация программно-аппаратных систем идентификации и аутентификации

В биометрических системах идентификационными являются индивидуальные особенности человека, которые в данном случае называются биометрическими признаками. Идентификация производится за счет сравнения полученных биометрических характеристик и хранящихся в базе шаблонов. В зависимости от характеристик, которые при этом используются, биометрические системы делятся на статические и динамические.

Статическая биометрия основывается на данных (шаблонах), полученных из измерений анатомических особенностей человека (отпечатки пальцев, узор радужки глаза и т.д.).

Динамическая основывается на анализе действий человека (голос, параметры подписи, ее динамика).

В комбинированных системах используется одновременно несколько признаков, причем они могут принадлежать как системам одного класса, так и разным.

Особенности электронных систем идентификации и аутентификации

В состав электронных систем идентификации и аутентификации входят контактные и бесконтактные смарт-карты и USB-token. Что такое USB-ключ, мы рассмотрим на примере eToken от компании Aladdin Software.

eToken – персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронными цифровыми подписями (ЭЦП). eToken может быть выполнен в виде USB-ключа или стандартной смарт-карты.

eToken поддерживает работу и интегрируется со всеми основными системами и приложениями, использующими технологии смарт-карт или PKI (Public Key Infrastructure).

Основное назначение:

- строгая двухфакторная аутентификация пользователей при доступе к защищенным ресурсам (компьютерам, сетям, приложениям);
- безопасное хранение закрытых ключей цифровых сертификатов, криптографических ключей, профилей пользователей, настроек приложений и пр. в энергонезависимой памяти ключа;
- аппаратное выполнение криптографических операций в доверенной среде (генерация ключей шифрования, симметричное и асимметричное шифрование, вычисление хэш-функции, формирование ЭЦП).

eToken как средство аутентификации поддерживается большинством современных операционных систем, бизнес-приложений и продуктов по информационной безопасности.

Возможности применения:

- строгая аутентификация пользователей при доступе к серверам, базам данных, разделам Web-сайтов;
- безопасное хранение секретной информации: паролей, ключей шифрования, закрытых ключей цифровых сертификатов;
- защита электронной почты (цифровая подпись и шифрование, доступ);
- системы электронной торговли, «клиент-банк», «домашний банк»;
- защита компьютеров;
- защита сетей, VPN;
- клиент-банк, home-банк.

eToken обеспечивает:

- **строгую аутентификацию** пользователей за счет использования криптографических методов;
- **безопасное хранение ключей шифрования и ЭЦП**, а также закрытых ключей цифровых сертификатов для доступа к защищенным корпоративным сетям и информационным ресурсам;
- **мобильность пользователя** и возможность безопасной работы с конфиденциальными данными в недоверенной среде (например, на чужом компьютере) за счет того, что ключи шифрования и ЭЦП генерируются ключом eToken аппаратно и не могут быть перехвачены;
- **безопасное использование** – воспользоваться ключом eToken может только его владелец, знающий PIN-код ключа;
- **реализацию как западных, так и российских стандартов на шифрование и ЭЦП**, сертифицированных ФАПСИ (ФСБ);
- **удобство работы** – ключ выполнен в виде брелка со световой индикацией режимов работы и напрямую подключается к USB-портам, которыми сейчас оснащены 100% компьютеров, не требует специальных считывателей, блоков питания, проводов и т.п.;
- **использование одного ключа для решения множества различных задач** – входа в компьютер, входа в сеть, защиты канала, шифрования информации, ЭЦП, безопасного доступа к защищенным разделам Web-сайтов, информационных порталов и т.п.

Таблица 1.
Радиочастотные идентификаторы

Характеристика	Proximity	Смарт-карты	
		ISO/IEC 14443	ISO/IEC 15693
Частота радиоканала	125 кГц	13,56 МГц	13,56 МГц
Дистанция чтения	До 1 м	До 10 см	До1 м
Встроенные типы чипов	Микросхема памяти, микросхема с жесткой логикой	Микросхема памяти, микросхема с жесткой логикой, процессор	Микросхема памяти, микросхема с жесткой логикой
Функции памяти	Только чтение	Чтение-запись	Чтение-запись
Емкость памяти	8-256 байт	64 байт – 64 кбайт	256 байт – 2 кбайт
Алгоритмы шифрования и аутентификации	Нет	Технология MIRAGE, DES, 3DES, AES, RSA, ECC	DES, 3DES
Механизм антиколлизии	Опционально	Есть	Есть

Бесконтактные смарт-карты разделяются на идентификаторы Proximity и смарт-карты, базирующиеся на международных стандартах ISO/IEC 15693 и ISO/IEC 14443. В основе большинства устройств на базе бесконтактных смарт-карт лежит технология радиочастотной идентификации.

Основными компонентами бесконтактных устройств являются чип и антенна. Идентификаторы могут быть как активными (с батареями), так и пассивными (без источника питания). Идентификаторы имеют уникальные 32/64 разрядные серийные номера.

Системы идентификации на базе Proximity криптографически не защищены, за исключением специальных заказных систем.

USB-ключи работают с USB-портом компьютера. Изготавливаются в виде брелков. Каждый ключ имеет прошиваемый 32/64 разрядный серийный номер.

Таблица 2.
Характеристики USB-ключей

Изделие	Емкость памяти, кБ	Разрядность серийного номера	Алгоритмы шифрования
iKey 20xx	8/32	64	DES (ECB и CBC), DESX, 3DES, RC2, RC5, MD5, RSA-1024/2048
eToken R2	16/32/64	32	DESX (ключ 120 бит), MD5
eToken Pro	16/32	32	RSA/1024, DES, 3DES, SHA-1
ePass 1000	8/32	64	MD5, MD5-HMAC
ePass 2000	16/32	64	RSA, DES, 3DES, DSA, MD5, SHA-1
ruToken	8/16/32/64/128	32	ГОСТ 28147-89, RSA, DES, 3DES, RC2, RC4, MD4, MD5, SHA-1
uaToken	8/16/32/64/128	32	ГОСТ 28147-89

USB-ключи, представленные на рынке:

- eToken R2, eToken Pro – компания Aladdin Knowledge Systems;
- iKey10xx, iKey20xx,iKey 3000 – компания Rainbow Technologies;
- ePass 1000 ePass 2000 – фирма Feitian Technologies;
- ruToken – разработка компании «Актив» и фирмы «АНКАД»;
- uaToken – компания ООО «Технотрейд».

USB-ключи – это преемники смарт-карт, в силу этого структуры USB-ключей и смарт-карт идентичны.

Комбинированные системы

Внедрение комбинированных систем существенно увеличивает количество идентификационных признаков и тем самым повышает безопасность.

На сегодня существуют комбинированные системы следующих типов:

- системы на базе бесконтактных смарт-карт и USB-ключей;
- системы на базе гибридных смарт-карт;
- биоэлектронные системы.

Таблица 3.
Основные функции комбинированных систем

Функция	Комбинированные системы		
	На базе бесконтактных смарт-карт и USB-ключей	На базе гибридных смарт-карт	Биоэлектронные системы
Идентификация и аутентификация компьютеров	Есть	Есть	Есть
Блокировка работы компьютеров и разблокирование при предъявлении персонального идентификатора	Есть	-	Есть
Идентификация и аутентификация сотрудников при их доступе в здание, помещение (из него)	Есть	Есть	-
Хранение конфиденциальной информации (ключей шифрования, паролей, сертификатов и т.д.)	Есть	Есть	Есть
Визуальная идентификация	-	Есть	Есть

Бесконтактные смарт-карты и USB-ключи

В корпус брелка USB-ключа встраиваются антенна и микросхема для создания бесконтактного интерфейса. Это позволит организовать управление доступом в помещение и к компьютеру, используя один идентификатор. Данная схема использования идентификатора может исключить ситуацию, когда сотрудник, покидая рабочее место, оставляет USB-ключ в разъеме компьютера, что позволит работать под его идентификатором. В случае же, когда нельзя выйти из помещения, не используя бесконтактный идентификатор, данной ситуации удастся избежать.

На сегодня наиболее распространены два идентификатора подобного типа:

- RfiKey – компания Rainbow Technologies;
- eToken PRO RM – компания Aladdin Software Security R.D.

Изделие RfiKey поддерживает интерфейс USB 1.1/2.0 и функционирует со считывателями HID Corporation (PR5355, PK5355, PR5365, MX5375, PP6005) и российской компании Parsec (APR-03Hx, APR-05Hx, APR-06Hx, APR-08Hx, H-Reader).

eToken RM – USB-ключи и смарт-карты eToken PRO, дополненные пассивными RFID-метками.

Интеграция eToken с RFID-метками

RFID-технология (*Radio Frequency Identification*, радиочастотная идентификация) является наиболее популярной на сегодня технологией бесконтактной идентификации. Радиочастотное распознавание осуществляется с помощью закрепленных за объектом так называемых RFID-меток, несущих идентификационную и другую информацию.

Из семейства USB-ключей eToken RFID-меткой может быть дополнен только eToken PRO/32K. При этом надо учитывать ограничения, обусловленные размерами ключа: RFID-метка должна быть не более 1,2 см в диаметре. Такие размеры имеют метки, работающие с частотой 13.56 МГц, например, производства Ангстрем или HID.

Гибридные смарт-карты

Гибридные смарт-карты содержат разнородные чипы. Один чип поддерживает контактный интерфейс, другой – бесконтактный. Как и в случае гибридных USB-ключей, гибридные смарт-карты решают две задачи: доступ в помещение и доступ к компьютеру. Дополнительно на карту можно нанести логотип компании, фотографию сотрудника или магнитную полосу, что делает возможным полностью заменить обычные пропуска и перейти к единому "электронному пропуску".

Смарт-карты подобного типа разрабатывают многие компании: HID Corporation, Axalto, GemPlus, Indala, Aladdin Knowledge Systems и др.

В России компанией Aladdin Software Security R.D. разработана технология производства гибридных смарт-карт eToken Pro/SC RM. В них микросхемы с контактным интерфейсом eToken Pro встраиваются в бесконтактные смарт-карты. Смарт-карты eToken PRO могут быть дополнены пассивными RFID-метками производства HID/ISOProx II, EM-Marine (частота 125 кГц), Cotag (частота 122/66 кГц), Ангстрем /КИБИ-002 (частота 13,56 МГц), Mifare и других компаний. Выбор варианта комбинирования определяет заказчик.

Биоэлектронные системы

Как правило, для защиты компьютерных систем от несанкционированного доступа применяется комбинация из двух систем – биометрической и контактной на базе смарт-карт или USB-ключей.

Наиболее часто в качестве биометрических систем применяются системы распознавания отпечатков пальцев. При совпадении отпечатка с шаблоном разрешается доступ.

К недостаткам такого способа идентификации можно отнести возможность использования муляжа отпечатка.

Генераторы разовых паролей

Идентификаторы на базе генераторов разовых паролей применяются чаще всего для организации web-доступа или систем типа e-banking.

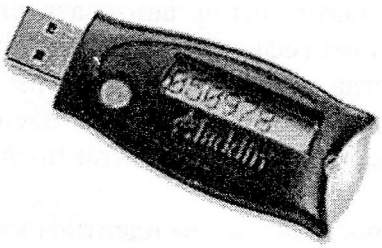

Рис. 2. eToken NG

eToken NG – функциональный аналог eToken PRO, имеющий встроенный генератор одноразовых паролей.

eToken NG-OTP предназначен для аутентификации пользователей при их подключении к защищенным информационным ресурсам (в том числе при недоступности USB-портов, к примеру – доступ с мобильных устройств, интернет-кафе), а также для безопасного хранения ключевой информации, профилей пользователей и других конфиденциальных данных, для аппаратного выполнения криптографических вычислений и работы с асимметричными ключами и сертификатами X.509.

Выпускается в двух модификациях: с 64 Кб и 32 Кб памяти (внутри защищенного чипа смарт-карты).

Имеет аппаратно реализованные алгоритмы RSA/1024, DES, 3DES, SHA-1 и аппаратный генератор одноразовых паролей.

Если необходимо получить соединение с сетью, пользователь вводит PIN-код, затем генерирует разовый пароль, нажимая кнопку на eToken NG. При этом пароль равен PIN-код+Token-код.

На стороне сети этот пароль проверяется с помощью специального серверного ПО.

Второй вариант реализован в продуктах компании RSA Security.

RSA SecurID for Microsoft Windows – это программное решение для проверки подлинности пользователей в вычислительных средах Microsoft Windows.

С точки зрения конечного пользователя разница между обычной процедурой регистрации в системе Windows и аутентификацией в системе RSA SecurID состоит лишь в том, что вместо стандартного пароля требуется ввести составной код доступа, состоящий из личного PIN-кода и комбинации цифр, которая в данный момент отображается на экране жетона-аутентификатора. Затем этот код доступа отсылается серверу RSA Authentication Manager, который и выполняет проверку подлинности пользователя.

RSA SecurID for Microsoft Windows обеспечивает прозрачную интеграцию с контролерами доменов Windows и каталогами Active Directory. База данных пользователей и групп сервера аутентификации RSA Authentication Manager синхронизирована с каталогом Active Directory. Поэтому, когда пользователь успешно проходит аутентификацию, сервер RSA Authentication Manager отправляет его пароль клиентской системе. Затем этот пароль отсылается контролеру домена для завершения аутентификации.

Отличие между этими двумя технологиями заключается в том, что разовый пароль в RSA SecurID изменяется через заранее заданные промежутки времени, а в продукте eToken NG смена разового пароля производится по нажатию кнопки (т. е. по мере надобности).

Вывод

Таким образом, рассмотрев различные технологии аппаратно-программной и парольной аутентификации, можно сделать вывод, что в дальнейшем по мере роста вычислительных мощностей все более востребованным будет именно применение двухфакторной аутентификации, что позволит избежать человеческих ошибок, связанных с применением слабых паролей, и ужесточить требования к парольной аутентификации.

Поступила 29.03.2006

УДК 681.03

Спирягин М.И., Спирягин В.И., Белозеров Е.В., Клюев С.А., Поляков А.С.

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ ПУТЕМ ИСПОЛЬЗОВАНИЯ JAVA CARD ТЕХНОЛОГИИ

Постановка проблемы

Для обеспечения более эффективной защиты информации необходимо обеспечить аутентификацию пользователя, на уровне одного документа (студенческий, читательский билет) для доступа к электронным ресурсам (библиотека, комплект учебно-методической документации и т.д.), услуг Интернет, а также обеспечение целостности информации в процессе передачи и приема данных через Интернет. Проведенный анализ показывает, что одним из наиболее рациональных средств обеспечения безопасности при аутентификации пользователей является использование смарт-карт.

Основная часть

Смарт-карта является на сегодняшний день одним из самых маленьких вычислительных устройств без источника питания, дисплея и клавиатуры. Тем не менее существует ряд задач, которые решают с помощью смарт-карт. Существуют два основных типа смарт-карт: *интеллектуальные карты*, содержащие микропроцессор, позволяющие читать и записывать информацию, а также производить вычисления, и *карты памяти*, у которых нет микропроцессора и которые могут быть использованы только для хранения информации. Доступ к информации на картах памяти защищен.