КОНЦЕПЦИИ АУТЕНТИФИКАЦИИ

А.В. Ханкевич[1], З.М. Соловьева[2]

[1]- студент 1 курса, факультет ЭУТ, группы ДГТ, Белорусского государственного экономического университета

[2]- научный руководитель, старший преподаватель кафедры информационных технологий, Белорусского государственного экономического университета. Минск, 220672, Партизанский пр., 26, тел. (8017) 249-19-81. e-mail: solovjeva@bseu.minsk.by.

Аннотация. Проблема безопасности информационных систем существует, наверное, с тех самых пор, как появились подобные системы. Для ее решения в большинстве случаев применяются технологии, в том или ином виде использующие пароли. В данной же работе будут рассмотрены иные подходы в решении этой проблемы. Это такие методы аутентификации, как биометрия, основанная на физико-биологических характеристиках самого пользователя, шифрование PKI, смарткарты, которые характеризуются портативностью и широким спектром функций, технология электронных ключей, выполненных в виде брелка и по размеру сопоставимы с ключами дома. Также в работе будут выявлены положительные и отрицательные стороны по использованию приведенных выше методов аутентификации.

1.Введение

В настоящее время быстрые темпы развития информационных технологий делают крайне актуальными вопросы безопасности) в сетях Internet/Intranet. Если не так давно эти темы волновали, по большей части, лишь корпоративных пользователей, то в последние годы в связи с массовым развитием сетей они начинают интересовать и пользователей индивидуальных (по крайней мере, в тот момент, когда те решают совершить оплату через Internet с помощью банковской карточки).

Если раньше угрозой номер один считались компьютерные вирусы, то сейчас на первый план выходят безопасное хранение данных и их передача по Сети, защищенные финансовые трансакции и конфиденциальность электронно-цифровой подписи (ЭЦП), которая уже 30 июня 2000г. была приравнена к чернильной в США. Кроме того вместе с этой основной проблемой встают еще и две другие, принципиально влияющих на выбор того или иного решения, — это соотношение цены/качества(связанный с затратами на поддержания именно того уровня безопасности, который необходим компании или частному лицу) и мобильность, позволяющая пользователю или корпорации легко защитить все компьютеры, используемые в работе.

В настоящее время для реализации основных функциональных компонент системы безопасности используют различные механизмы и методы:

- коммуникационные протоколы,
- средства криптографии,
- механизмы авторизации и аутентификации,
- средства контроля доступа к рабочим местам сети и из сетей общего пользования,
- антивирусные комплексы,
- программы обнаружения атак и аудита,
- средства централизованного управления контролем доступа пользователей, и безопасного обмена пакетами данных и сообщениями любых приложений по открытым IP-сетям.

В данной работе мы будем рассматривать механизмы аутентификации и частично авторизации.

2.Основные концепции аутентификации

В переводе с латыни «аутентификация» означает «установление подлинности». Аутентификацию следует отличать от идентификации. Идентификаторы пользователей применяются с теми же целями, что и идентификаторы любых других объектов, файлов, процессов, структур данных, но они не связаны непосредственно с обеспечением безопасности. Идентификация заключается в сообщении пользователем системе своего идентификатора. При процедуре аутентификации пользователь доказывает, что он именно тот, за кого себя выдает.

В процессе участвуют две стороны: одна доказывает свою аутентичность, а другая (аутентификатор) проверяет эти доказательства и принимает решение. Легальность пользователя устанавливается по отношению к различным системам. Так, работая в сети, пользователь может проходить процедуру аутентификации и как локальный пользователь, претендующий на использование ресурсов только данного компьютера, и как пользователь сети, желающий получить доступ ко всем сетевым ресурсам. При локальной аутентификации пользователь вводит свой идентификатор и пароль, которые автономно обрабатываются операционной системой, установленной на данном компьютере. При логическом входе в сеть идентификатор и пароль передаются на сервер, где хранятся учетные записи обо всех пользователях сети. Многие приложения имеют свои средства определения, является ли пользователь законным. В этом случае приходится проходить дополнительные этапы проверки.

В качестве объектов, требующих аутентификации, могут выступать не только пользователи, но и различные устройства, приложения, текстовая и другая информация. Так, например, пользователь, обращающий с запросами к корпоративному серверу и доказывающий ему свою легальность, должен сам убедиться, что ведет диалог действительно с сервером своего предприятия. Другими словами, сервер и клиент проходят процедуру взаимной аутентификации. Здесь мы имеем дело с аутентификацией на уровне приложений. При установке сеанса связи между двумя устройствами также часто предусматриваются процедуры взаимной аутентификации на более низком, канальном уровне. Примером такой процедуры является **аутентификация по протоколу** PAP(Password Authentication Protocol-протокол аутентификации пароля), входящему в семейство в семейство протоколов PPP(протоколы связи между терминалом и маршрутизатором).

Аутентификация данных является доказательством целостности этих данных, а также того, что они поступили именно от человека, который объявил об этом. В этом случае используется механизм **электронной подписи.**

В вычислительных сетях процедуры аутентификации часто реализуются теми же программными средствами, что и процедуры авторизации. В отличие от аутентификации, распознающей легальных и нелегальных пользователей, система авторизации имеет дело только с легальными пользователями, которые уже успешно прошли процедуру аутентификации. Цель подсистем авторизации состоит в том, чтобы предоставить каждому легальному пользователя именно те виды доступа к ресурсам, которые были для него определены администратором системы.

Средства авторизации контролируют доступ легальных пользователей к ресурсам системы, предоставляя каждому из них именно те права, которые были определены администратором. Кроме того предоставления прав доступа пользователей к каталогам, файлам и принтерам, система авторизации может контролировать возможность выполнения пользователями различных системных функций, таких, как локальный доступ к сервер, установка системного времени, создание резервных копий данных, выключение сервера и т.д.

Системы аутентификации и авторизации совместно выполняют одну задачу, поэтому к ним необходимо предъявлять одинаковый уровень требований. Ненадежность одного звена здесь не может быть компенсирована высокой надежностью другого. Если при аутентификации используются пароли, то требуются чрезвычайные меры по их защите. Однажды украденный пароль открывает двери ко всем приложениям и данным, к которым пользователь имел легальный доступ.

Но, так как, технология авторизации работает уже с идентифицированными пользователями, а аутентификация предоставляет именно возможность идентификации, то мы решили глубже рассмотреть проблему аутентификации, раскрыть механизмы и способы ее осуществления.

Первым шагом в обеспечении безопасности стало изобретение пароля и логина. Этот простейший метод аутентификации всем хорошо знаком и не нуждается в отдельном представлении. Очевидны и их недостатки: помимо того что пользователь вынужден запоминать множество паролей для входа в различные программы и системы, использование пароля давно уже не считается достаточной гарантией безопасности:пароль не сложно подсмотреть,

подобрать или расшифровать, если он кодируется стандартными средствами операционной системы. Кроме того, несмотря на кажущуюся простоту управление паролями требует немалых затрат. Так, по некоторым оценкам, замена пароля только лишь у одного сотрудника крупной компании обходится приблизительно в $200.

Следующим шагом в обеспечении защиты информации стало использование различных средств и способов шифрования. Широко распространено использование Инфраструктуры Открытых Ключей(Public Key Infrastructure— PKI). В одних случаях используется то, что системы, основанные на PKI, генерируют два отдельных ключа шифрования. А в других удобным также оказывается использование цифровых сертификатов, выполняющих роль своеобразного виртуального паспорта. При этом проверкой занимается организация, выпустившая сертификат(Certification Authority-CA).

Однако хранение ключей шифрования на жестких дисках компьютеров становится дополнительным фактором , поскольку появляется опасность их копирования с дальнейшими попытками подбора парольной фразы и получения несанкционированного доступа к ключам. Таким образом, хотя PKI и обеспечивает не только аутентификацию на и защиту информации, ее использование лишь на программном уровне вызывает немало трудностей.

Именно это и заставило специалистов искать выход на стыке программных средств. Для тех организаций, перед которыми не стоит задача кодирования информации, ряд производителей предлагает обратиться к биометрии, когда идентификатор пользователя всегда находится при нем и нет необходимости запоминать логины и пароли. Биометрические технологии, в общем-то, тоже предполагают применение своего рода паролей, однако эти пароли уникальны и невоспроизводимы — отпечатки пальцев, подписи, радужная оболочка глаза, голос, лицо и даже мимика пользователя. Возможно также объединение традиционных паролей с биометрическими методами — в частности, в 2001 году компании Musicrypt.com и Net Nanny Software представили технологию BioPassword, идентифицирующую пользователей по технике набора ключевой последовательности символов.

Среди основных областей биометрии можно считать идентификацию по радужной оболочке глаза. Здесь стоит отметить компанию IrisScan, предлагающую на рынке специальные сканеры, в том числе и подключаемые к компьютерам. Подобные устройства стоят заметно дороже (например, цена системы для защиты доступа к ПК PCIris составляет около $1000, в то время как сканер отпечатков пальцев доступен за $100—200), однако они и обеспечивают гораздо более высокий уровень безопасности. Также стоит упомянуть фирму Viisage, разработавшую технологию идентификации пользователей, правда, не по радужной оболочке, а по чертам лица.

Активно ведутся разработки и в области голосовой аутентификации. Соответствующая технология VeriVoice Security Lock была создана компанией VeriVoice, причем она позволяет идентифицировать пользователей не только при "непосредственном контакте", но и по телефону. Интересно отметить, что голосовое распознавание поддерживается последней операционной системой от Apple.

Но, пожалуй, самым распространенным методом, использующим биометрические функции, на данный момент является идентификация пользователей по отпечаткам пальцев — в этом направлении работает большинство фирм. Например, Identix в сотрудничестве с Motorola разработала технологию распознавания отпечатков пальцев Identicator, нашедшую применение в аппаратных и программных продуктах целого ряда производителей, в том числе Unisys, Compaq, IBM, Dell Computer и NEC. Компания Ethentica, ранее называвшаяся Who?Vision System, за спиной которой стоит, среди прочих, Philips Electronics, предлагает сканеры для считывания отпечатков пальцев и соответствующее ПО. Разработку аналогичных продуктов ведут также Digital Persona, спонсируемая Intel и Kensington Technology, а также Veridicom, поддерживаемая Lucent Technologies и AT&T. А вот фирма AuthenTec (в числе ее инвесторов Harris Semiconductor) создала отдельную микросхему с сенсором,

реализующую функции защиты по отпечаткам пальцев, под названием FingerLoc.

Внешне решение выглядит достаточно красиво, однако и у него есть свои минусы. С одной стороны, данный метод аутентификации вызывает понятную настороженность у людей, которые не хотят, чтобы их отпечатки пальцев хранились у компании. Речь идет о защите частных прав. Помните, какой шум поднялся, когда Intel решила встроить в свои процессоры идентификационные номера? А тут открываются такие возможности по сбору персональной информации о пользователях без их ведома! Вдобавок, как показывает практика, возможно использование ложных отпечатков на негативах; экраны и поверхности устройств требуют частой очистки и при интенсивной эксплуатации могут порядить немалые проблемы. С другой стороны, такое решение нельзя назвать дешевым. Хотя мышки с распознаванием отпечатков пальцев можно приобрести у отечественных компаний по цене, колеблющейся от 70$ до 150$, к ним необходимо еще и соответствующее программное обеспечение. Клавиатуры и сканеры стоят еще дороже.

И, наконец, едва ли не главный минус биометрии — это невозможность освобождения пользователя от остальных проблем, кроме аутентификации—от конфиденциальности ЭЦП до применения различных методов шифрования в сетях. Таким образом, переходя к биометрии, компания решает только одну задачу и нередко оказывается вынужденной устанавливать дополнительные системы безопасности.

Более универсальным является другой вариант— использование смарткарт (интеллектуальных карт), которые на настоящий момент предлагает целый ряд производителей (Schlumberger, Bull, Siemens, Solaic, Orga). Их основное удобство заключается в портативности и широком спектре функций, позволяющем компании, выбрав данную технологию, постепенно достраивать необходимые компоненты защиты в зависимости от текущих потребностей. При этом не придется испытывать тех сложностей, которые скажем , возникают при простом использовании систем, основанных на PKI. Смарткарты обеспечивают двухфакторную аутентификацию при доступе к защищенным ресурсам и выступают в качестве хранилища любой секретной информации — от закрытых ключей(например, для использования в системах аутентификации для LAW, WAN и VPN) до цифровых сертификатов, делая ее мобильной и не повергая угрозе копирования, как это может происходить с данными, расположенными на жестком диске. В качестве примера можно привести выпускаемую Orga линейку смарткарт Micardo—Standard, Public и Dual— с памятью EEPROM от 4 до 32 Кбайт, от 32 до 64 Кбайт ROM и криптоконтроллем (в зависимости от модели). Orga также поставляет специальные инструменты для интегрирования технологии в различное программное обеспечение.

Однако переход на смарткарты невозможен без приобретения специальных считывающих устройств и оснащения ими всех компьютеров, на которых ведется работа с защищенными данными. Подобные устройства стоят дороже 100$, а клавиатура со встроенными смарт-ридерами обычно попадают в ценовой диапазон свыше 150$.

Технология смарткарт обладает двумя недостатками— относительная дороговизна в использовании, если нет необходимости считывать данные с пластиковых карт, и неудобство в использовании с мобильными компьютерами, хотя решения на основе PCMCIA существуют.

В настоящее время существует достойная альтернатива смарткартам— более удобная технология электронных ключей (eToken), выполненный в виде брелка. Он напрямую подключается к компьютеру через USB порт, которым оснащены едва ли не все компьютеры, выпускаемые в последние годы, и не требует наличия дорогостоящих карт-ридеров либо других дополнительный устройств. Конкретные параметры устройства зависят от модели ключа; например, eToken R2 компании Aladdin имеет до 64 Кбайт энергозависимой памяти и встроенный криптопроцессор, реализующий алгоритм симметричного шифрования DES-X со 120-битным ключом.

eToken обеспечивает одно- и двухфакторную аутентификацию с использованием аппаратного брелка и PIN-кода. Каждый eToken имеет 32-битный уникальный номер, доступный только на чтение. Одной из отличительных черт является то, что этот метод аутентификации поддерживает большинство современных стандартов и API, легко встраивается как в существующие приложения, так и в новые. Например, в Windows 2000 и Windows XP его

поддержка встроена изначально. Поддержка PC/SC стандарта позволит без труда перейти от смарткарт к eToken.

Цена брелка e-Token колеблется от 25$ до 39$, Комплект состоящий из 2 eToken R2,подробная документация, CD-ROM для инсталляции eToken R2. CD-ROM с trial-версией CSP от КриптоПро стоит 149$.

Однако не существует универсальных решений: если у вас старый компьютер без порта USB, то вы все же столкнетесь с проблемой при использовании устройств от Aladdin.

Подводя итоги, следует сказать, что в настоящее время основными конкурирующими решениями аутентификации являются разработки на основе смарткарт и eToken. Но до тех пор, пока не произойдет существенное снижение их стоимости трудностей нам не избежать.

ЛИТЕРАТУРА

1. Сергей Воронов «Виртуальная безопасность»//CHIP 01/2002, стр.62-66.
2. Ольга Афанасьева «Виртуальная частная сеть: процедуры защиты данных»//CHIP 11/2001, стр. 80-87.
3. Алексей Гвозденко «Биометрические технологии: сам себе пароль»// http://www.itc.ua/article.phtml?ID=3098&IDw=43&pid=62
4. www.aladdin.ru
5. www.elvis.ru