Автор:

Швейкин Владислав Витальевич

студент

ФГАОУ ВО «Самарский национальный исследовательский

университет им. академика С.П. Королева»

г. Самара, Самарская область

АУТЕНТИФИКАЦИЯ, ОСНОВАННАЯ НА ФАКТОРЕ ВЛАДЕНИЯ

Аннотация: *в данной статье рассматриваются основные принципы аутентификации, основанной на факторе владения, а также меры повышения защиты от компрометации.*

Ключевые слова: *аутентификация, информационная безопасность, защита, фактор владения, ключ, пароль.*

Аутентификация, основанная на факторе владения, широко используется в повседневной жизни. Самым простым примером является ключ от замка. Во время зарождения данных систем аутентификации их надёжность основывалась на сложности воспроизведения физического объекта. Технология и в настоящее время широко используется, несмотря на существенный прорыв технологий воспроизведения физических предметов. В роли предметов, позволяющих аутентифицировать владельца, используют электронные ключи, смарт-карты.

Основной проблемой, возникающей при использовании аутентификации, основанной на факторе владения, является то, что аутентифицирующий предмет может быть скомпрометирован (похищен, утерян и т. д.). Многие современные информационные системы используют комплексную процедуру аутентификации, состоящую из двух этапов. Первым этапом является предъявление пользователем системы уникального предмета: ключа, смарт-карты или токена, которые вводятся в специальное считывающее устройство. На втором этапе вводится персональный индикационный номер пользователя (PIN), который является до-

казательством того, что данный пользователь действительно является владельцем предмета и имеет право доступа к определённым ресурсам информационной системы.

Для защиты от атак полного перебора вводятся дополнительные организационные меры. Например, блокировка пользователя при нескольких неудачных попытках ввода номера. В этом случае информация, которая позволяет идентифицировать и аутентифицировать пользователя, хранится на внешнем носителе информации. При входе в систему пользователь подключает носитель ключевой информации к компьютеру, и система считывает с него идентификатор и соответствующий ключ.

Так как ключ, который хранится на внешнем носителе, может иметь длину большую, чем пароль, подобрать такой ключ практически невозможно. Но угроза компрометации ключевой информации все ещё остаётся актуальной. Если процедура аутентификации не предполагает дополнительных средств защиты, любой обладатель носителя ключевой информации имеет доступ к системе с правами пользователя, которому принадлежит носитель. Поэтому в большинстве случаев ключевая информация на носителе хранится в зашифрованном виде. Пользователь при входе в систему должен не только подключить носитель ключевой информации, но и ввести пароль, соответствующий носителю, что делает практически невозможным использование ключа случайным обладателем.

Основной угрозой при использовании описываемой технологии является кража носителя ключевой информации с последующим его копированием и подбором пароля для доступа к ключу. Если ключ генерируется случайным образом и не содержит проверочных полей, то подбор пароля на доступ к ключу не атакуемой системы невозможен, потому что нет критерия, благодаря которому можно отличить правильно расшифрованный ключ от неправильно расшифрованного. Для защиты от атак подобного рода используются следующие меры:

1. Защита от копирования ключевой информации с носителя.

2. Блокировка или уничтожение ключевой информации после нескольких неудачных попыток ввода пароля.

Однако при использовании в качестве носителя ключевой информации ключевых дискет, электронных ключей или пластиковых карт, данные меры защиты неприменимы. Поскольку проверку ввода правильного пароля для доступа к ключу производит операционная система то, если пароль подбирается злоумышленником при помощи специальной программы, подсчитывать количество неудачных попыток невозможно.

Отличительной особенностью интеллектуальных пластиковых карт от перечисленных носителей является наличие микропроцессора, способного выполнять криптографические преобразования информации. Таким образом, интеллектуальные пластиковые карты имею возможность самостоятельно проверять правильность пароля для доступа к ключевой информации. Интеллектуальную карту можно запрограммировать на стирание хранимой ключевой информации после превышения допустимого количества неправильных попыток ввода пароля, что не допускает подбор пароля без частого копирования карты, что приводит к большим затратам ресурсов.

В заключении следует отметить, что при использовании для аутентификации пользователей внешних носителей информации и паролей позволяет значительно повысить эффективность защиты информационной системы.

Список литературы

1. Смирнов С.Н. Безопасность систем баз данных. – М.: Гелиос АРВ, 2007. – 352 с.

2. Дейт К.Дж. Введение в системы баз данных. – 8-е изд. – М.: Вильямс, 2005. – 1328 с.