УДК 004.492.2

СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ АУТЕНТИФИКАЦИИ ДЛЯ ПРОТИВОДЕЙСТВИЯ АТАКАМ В СОЦИОТЕХНИЧЕСКИХ СИСТЕМАХ.

С.А. Брич, Н.Е. Губенко
Донецкий национальный технический университет
multik88@mail.ru

Совершенствование методов аутентификации для противодействия атакам в социотехнических системах. В данной статье предлагаются методы усложнения процесса парольной аутентификации путем передачи секретного ключа по другому каналу, а так же использование мобильной связи для передачи ключей шифрования.

Социотехническая система – сложная система, состоящая из технической подсистемы, подсистемы персонала, внешней среды, взаимодействующей с организацией, и организационного дизайна.

Стремительное развитие информационных технологий и их применение в науке, технике, технологиях промышленного производства сложных изделий и систем выдвигает на передний план задачу управления доступом пользователей к информационным ресурсам различного назначения, имеющих, как правило, гетерогенную структуру. Одной из базовых задач этого направления является задача установления подлинности субъектов и объектов информационных отношений, то есть задача аутентификации. [1]

В конце обычного послания или документа исполнитель или ответственное лицо обычно ставит свою подпись. Подобное действие как правило преследует две цели. Во-первых, получатель имеет возможность убедиться в истинности письма, сличив подпись с имеющимся у него образцом. Во-вторых, личная подпись является юридическим гарантом авторства документа. Последний аспект особенно важен при заключении разного рода торговых сделок, составлении доверенностей, обязательств и т.д.

Электронные системы требуют похожего алгоритма подтверждения авторства, кроме того, сохранения целостности то есть невмешательства в текст послания. Для обеспечения этих требований необходимо гарантировать (реализовать) правовое регулирование доступа к информационным документам, для чего широко используется механизм аутентификации.

Существует несколько видов аутентификации:

- Парольная аутентификация
- Многофакторная идентификация
- Биометрическая аутентификация
- Аутентификация с использованием криптографии
- Аутентификация с нулевой передачей знаний.

Рассмотрим типовую схему аутентификации, применяемую во многих системах. Для каждого субъекта доступа существует аутентифицирующий объект, представляющий собой пару (ID_i, K_i):

- ID_i – идентификатор, позволяющий однозначно выделить i-й субъект доступа из множества всех субъектов, зарегистрированных в системе.
- K_i – аутентифицирующая информация, подтверждающая подлинность i-го субъекта доступа.

В целях безопасности аутентифицирующий объект не хранится в системе в открытом виде, вместо этого используется объект-эталон, хранящий данные в защищенном формате. Объект-эталон представляет собой пару (ID_i, E_i), где $E_i = F(ID_i, K_i)$. Трудоемкость определения K_i по E_i должна быть выше некоторого порогового значения T_0. Для пары Ki и Kj возможно совпадение соответствующих значений E, что может привести к ложной аутентификации с некоторой вероятностью P0. Для практического применения задают $T_0 = 10^{20}…10^{30}$, $P_0 = 10^{-7}…10^{-9}$. [2]

В общем виде механизм аутентификации выглядит следующим образом:

- Субъект доступа предъявляет свой идентификатор.
- Система управления доступом запрашивает его аутентификатор.
- Система управления доступом проводит сравнение значений. При совпадении значений устанавливается, что данный субъект прошел аутентификацию.

Рассмотрим парольную аутентификацию. Разрешив доступ зарегистрированным пользователям, невозможно удостовериться, что именно сам пользователь проходит аутентификацию. Потому как наибольшим недостатком этого метода является возможность перехвата пароля при передаче по сети. Поэтому для большей уверенности предлагается усложнить процесс аутентификации. Методом рассылки одноразового пароля на email.

Идея аутентификации с помощью email не нова. Классический метод предполагает посылку статического пароля на email. [3] В данный методе предполагается посылка через email одноразовый пароль, генерируемый при каждой аутентификации.

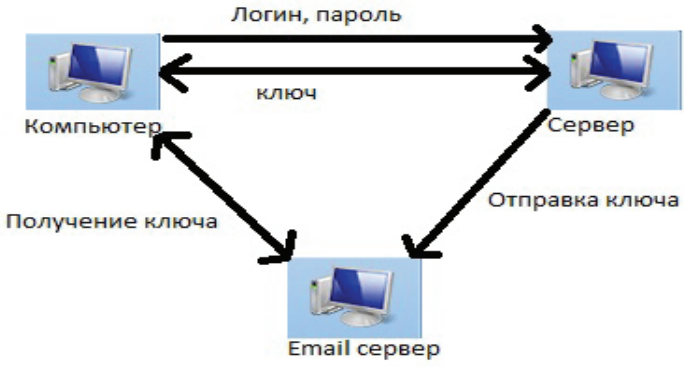

Рисунок 1 – Аутентификация с помощью email

Преимуществом данного метода является то, что на e-mail пользователя можно выслать ключи довольно большого размера и сложности, но это требует от пользователя дополнительного времени, а также запоминания дополнительного пароля от email.

- Методом рассылки sms.

В наше время мобильные телефоны являются очень распространенным средством связи и являются наиболее личным и достоверным идентификатором пользователя. Отправлять посредством sms можно не только коды подтверждения аутентификации, но и персональные данные, ключи необходимые для расшифровки сообщений.

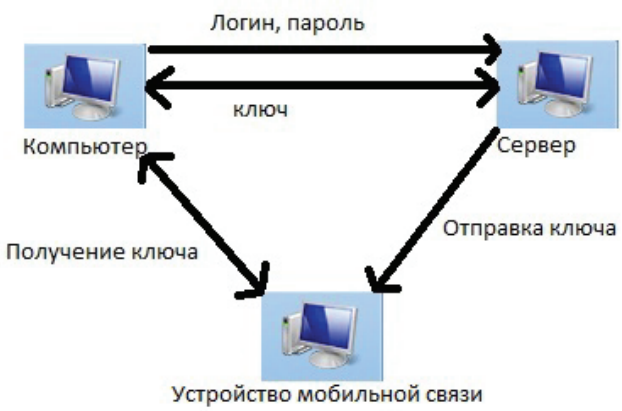

Рисунок 2 – Аутентификация с помощью sms

Большим преимуществом предложенных методов является использование другого канала передачи секретного ключа, что усложняет процесс его перехвата. При передаче одноразовых паролей перехват и вовсе перестает иметь смысл. Использование мобильной связи увеличивает защищенность информации, что делает возможным

передачу секретных ключей шифрования. Если для коротких сообщений подойдет простой мобильный телефон и пользователь самостоятельно введет полученные данные. Но для больших паролей или ключей этот метод введения данных вручную становиться неудобным. Для упрощения процедуры аутентификации предполагается подключение устройства мобильной связи к компьютеру с предустановленным программным обеспечением, которое сможет открыть сообщение и упростить ввод секретного ключа, самостоятельно передав его серверу или же сделав ключ доступным для копирования. Для реализации приведенных методов разрабатывается программное обеспечение, предназначенное для установки на компьютеры сервера и клиента.

У приведенных выше методов также существуют недостатки. Логин и пароль от email могут быть перехвачены при передаче по сети, а также оба метода увеличивают время аутентификации. Отправка sms - более защищенный метод для передачи кодов авторизации, секретных ключей и другой важной информации. Утечка информации с мобильного телефона может произойти путем его кражи, взлома сети оператора, установки вредоносного программного обеспечения (которое будет передавать злоумышленнику информацию, полученную и переданную мобильным телефоном в незаметном для его владельца режиме). Но так как все из вышеперечисленных методов атаки на мобильное устройство чрезвычайно сложны и ресурсоемки, отправка кодов путем пересылки их по sms является наиболее предпочтительным методом.

Список литературы

1. Смыслов В.Ю. Разработка методов управления доступом в трехуровневых распределенных СУБД. Интернет ресурс. - Режим доступа: www/URL: www.referun.com/n/razrabotka-metodov-upravleniya-dostupom-v-trehurovnevyh-raspredelennyh-relyatsionnyh-subd
2. Созыкин А.В. Семантическая интеграция управления доступом к сервисам. Интернет ресурс. - Режим доступа: www/URL: http://asozykin.ru/sites/default/files/sozykin.pdf
3. Mozilla предложила новую систему авторизации на сайтах. Интернет ресурс. - Режим доступа: www/URL: http://xakep.ru/post/56252/default.asp

Получено 09.09.2011