Л. С. Носов, А. С. Попов

ДВУХФАКТОРНАЯ АВТОРИЗАЦИЯ В LINUX

Контроль доступа к ресурсам компьютера является неотъемлемой составляющей обеспечения информационной безопасности [1]. Однако, прежде чем контролировать, необходимо удостовериться в легальности пользователя. В этом процессе можно выделить несколько этапов.

В самом начале необходимо определить того, с кем имеем дело. Иными словами, провести идентификацию пользователя. Такой процесс происходит при входе пользователя в систему. У каждого пользователя в системе есть имя (логин), который отождествляется с конкретным человеком. На следующем этапе пользователя попросят предъявить уникальную «вещь» — токен. Традиционно таковым является пароль пользователя, однако некоторые системы требуют предоставить физическую вещь (USB-ключ) или используют биометрические параметры. Токен позволяет отличить легального пользователя от злоумышленника. Такой процесс называется аутентификацией. Аутентификация — процедура проверки подлинности данных и субъектов информационного взаимодействия исключительно на основе внутренней структуры самих данных [1].

В некоторых системах защиты информации от НСД, таких как Secret Net [2], возможен вариант, когда внешний ключ используется не для аутентификации, а для идентификации. А иногда USB-ключ используется для хранения имени и пароля пользователя, как это сделано в электронных ключах e-Token от Aladdin, при этом пользователю достаточно знать более короткий, чем пароль, уникальный пин-код [3].

Завершающая стадия осуществляет контроль доступа пользователя к ресурсам компьютера в течение всего сеанса работы. Многопользовательские системы разграничивают права доступа к различным объектам: одним пользователям позволено почти все, другим — только разрешенное. В переводе с английского термин authorization (авторизация) означает:

1) санкционирование, разрешение, уполномочивание;

2) санкция, утверждение, одобрение, разрешение.

Другими словами, пользователю запрещено все, что не разрешено. Разница между пользователями заключается только в количестве разрешенных действий.

Изначально в операционной системе Linux пользователи, желающие войти в систему, были вынуждены пообщаться с программой-охранником, гордо именуемой login. Она спрашивала ваше имя, затем пароль шифровала известным алгоритмом и сличала получившийся результат с записью в файле /etc/passwd. Если все совпадало, то вам разрешалось войти, если нет — предлагалось начать все сначала [4].

Через некоторое время наученные горьким опытом системы перестали хранить зашифрованные пароли в файле /etc/passwd, открытом на всеобщее обозрение, и переместили эту тайную информацию в файл /etc/shadow, читать который было дозволено только обладателям прав суперпользователя. Программа login была переписана заново: теперь она умела и читать из нового файла, и шифровать по более серьезному алгоритму [4].

Неизвестно, сколько еще раз пришлось бы переписывать эту программу, да и не только ее (с паролированием в системе связаны еще и passwd, и su), если бы не пришла кому-то в голову мысль отделить программы от механизма аутентификации. Эта система получила название PAM (Pluggable Authentication Modules), что переводится как «подгружаемые модули аутентификации» (ПМА) [4].

Теперь, если программа (в частности, login) желает произвести аутентификацию пользователя, она больше не занимается этим, а обращается к PAM с соответствующей просьбой.

Все заботы о выборе алгоритма и особенностях аутентификации теперь лежат на PAM. Формально PAM выполнен в виде разделяемых библиотек-модулей, комфортно расположившихся в каталоге /lib/security/. Каждый модуль по-особому пропускает через себя пользователя, реализуя свой особенный механизм аутентификации. Сценарии авторизации находятся в каталоге /etc/pam.d. Имя каждого сценария в этом каталоге совпадает с именем программы, для которого он предназначен. Например, сценарий для login находится по адресу /etc/pam.d/login [4].

Модуль USB, который может быть использован для двухфакторной авторизации, разрабатывается отдельно от основного приложения PAM и пока считается незавершенным, хотя на самом деле полностью функционален. Называется он Pam_usb, и его можно найти на сайте разработчиков [5]. Последняя версия работает с ядрами 2.6 и современными дистрибутивами [5, 6].

Однако модуль Pam_usb по сути реализует стандартную схему «логин/пароль» [5, 6]. Реализовывать стандартную схему не имеет смысла. Поэтому можно придумать нечто новое. Назовем этот модуль pam_enigma.so. Будем спрашивать у пользователя загадки: правильный ответ позволит войти в систему, а ошибочный запросит стандартный пароль при соответствующей настройке стека модулей PAM. База загадок и отгадок будет храниться непосредственно в модуле (хотя возможно настроить и отдельное хранение). Загадки выбираются случайным образом. После написания и сборки модуля скопируем файл pam_enigma.so в /lib/security/ и добавим соответствующую запись в стек модулей PAM. Пример использования модуля приведен ниже:

sasha$su test

Что это такое: синий, большой, с усами и полностью набит зайцами?

троллейбус

test$

Таким образом, в работе рассмотрена возможность создания средств двухфакторной авторизации для операционной системы Linux. Кроме того, рассмотрен вариант замены стандартной авторизации типа «логин/пароль».

СПИСОК ЛИТЕРАТУРЫ:

1. *Малюк А. А., Пазизин С. В., Погожин Н. С.* Введение в защиту информации в автоматизированных системах. М.: Горячая линия — Телеком, 2001. — 148 с.
2. Secret Net. Продукты компании Код безопасности. URL: http://www.securitycode.ru/products/secret_net (дата обращения: 18.11.2009).
3. Aladdin: краткое описание eToken. URL: http://www.aladdin.ru/catalog/etoken/etoken.php (дата обращения: 18.11.2009).
4. Начала PAM // Linux SoftWare Library — Российский портал Linux программ. URL: http://www.linuxsoft.ru/info/lib/lib/secur/pam.htm (дата обращения: 18.11.2009).
5. PAM-usb. URL: http://www.pamusb.org (дата обращения: 18.11.2009).
6. Linux PAM. URL: http://www.kernel.org/pub/linux/libs/pam/ (дата обращения: 18.11.2009).

Д. Ю. Персанов

МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В работе освещены вопросы управления инцидентами информационной безопасности на предприятии. Рассмотрены аспекты классификации событий и инцидентов информационной безопасности.