АКТУАЛЬНЫЕ ВОПРОСЫ ЭКОНОМИКИ, УПРАВЛЕНИЯ И ТЕХНОЛОГИИ

УДК 004:57.087.1

Информационная безопасность и биометрия

Б.А. ШВЫРЕВ – начальник отдела исследования проблем обеспечения безопасности в учреждениях уголовно-исполнительной системы НИИ ФСИН России, кандидат физико-математических наук

В статье рассмотрены особенности несанкционированного доступа к информации, даны характеристики активной и пассивной атак. Определен один из перспективных способов защиты информации – использование биометрических признаков человека.

Ключевые слова: информационная безопасность; биометрия; клавиатурный подчерк; биометрический признак; несанкционированный доступ.

Information Security and Biometrics

B.A. SHVYREV – Head of the Department of Research of security issues in the penal system of the Research Institute of the Federal Penal Service of Russia, Phd. in Physic and Mathematic

The article describes the features of unauthorized access to information, there are given the characteristics of active and passive attacks. It is determined one of the most promising ways to protect information - the use of biometric features of man.

Key words: information security; biometrics; keyboard handwriting; biometric feature; unauthorized access.

Компьютеры, вычислительные системы и сети используются почти во всех отраслях деятельности. Решение многих задач частично или полностью возложено на компьютеры, при этом человек не подвергает сомнению результаты их работы. Такая ситуация привела к сильной зависимости от компьютера, широкомасштабной информатизации как на бытовом уровне, так и на производственном. Пластиковые банковские карты, электронная почта, терминалы оплаты услуг, электронные платежи и, конечно, Интернет гармонично вошли в жизнь современного общества. Количество вычислительных систем с каждым годом растет в геометрической прогрессии. Предприятия, организации и частные лица хранят на компьютерах и серверах уязвимую информацию: личные сведения, данные о производственном процессе, перспективных разработках, банковских счетах, кредитных историях и т.д. Использование этих сведений неавторизованными пользователями приводит к потере денежных средств, репутации, авторских прав и к другим нежелательным последствиям[1].

Получение несанкционированного доступа становится возможным при умышленном нарушении (атаке) системы информационной безопасности вычислительной системы и сети. Атаки делят на активные и пассивные[2].

При активной атаке используют изменение потока данных или создание мошеннического потока (подмену, воспроизведение, модификацию сообщения и отказ служб).

Пассивные атаки предполагают подслушивание или шпионаж при передаче данных по сети. Их задача получить доступ к передаваемой информации. К ним относятся

перехват электронного письма или файла с конфиденциальной информацией, анализ трафика и передаваемых сообщений в целях выявления данных о передаваемом узле, параметрах шифрования, паролей и т.д.

Пассивные атаки практически незаметны, их трудно обнаружить, однако существуют меры для борьбы с ними, а точнее, для их профилактики и предупреждения, например: использование длинного ключа шифрования, динамического изменения кода, передача пустых пакетов и т.д.[3] Борьба с пассивными атаками носит в основном профилактический характер. Активные атаки, наоборот, хорошо обнаруживаются, но их трудно предотвратить.

Компьютерная безопасность основывается на целостности, конфиденциальности и доступности[4]. Так, надежная защита конфиденциальной информации может строго ограничить разрешенным группам доступ к ней.

Целостность означает, что информация может быть изменена (заменена, удалена, добавлена) только разрешенными группами пользователей, прошедшими авторизацию. Конфиденциальность – доступность компьютера и компьютерных сетей только для разрешенных групп пользователей. Типы доступа и полномочия могут быть различными, например только чтение, копирование и чтение и т.д. Доступность означает, что информация открыта для разрешенных групп. Авторизованному пользователю нельзя препятствовать в доступе к разрешенной информации. Доступность относится и к данным, и к службам.

В вычислительных системах и сетях, где компьютер выступает отправителем и получателем информации, могут произойти следующие типы атак:

1) прерывание – это внесение изменений с последующей невозможностью доступа к информации и/или ее потерей. Является атакой на доступность. Результатом становится удаление файлов и программ, отключение систем управления файлами, сокращение линий связи и т.д.;

2) перехват – атака на конфиденциальность. Посторонний получает доступ к закрытой информации. Атакующей стороной может выступать человек, программа или компьютерная система;

3) модификация – это атаки на целостность, при которой несанкционированная сторона не только получает доступ к информации, но и вмешивается в нее. Результатом становятся изменения в отправляемых сообщениях, дополнительные действия существовавших программ и т.д.;

4) производство – атака на подлинность компьютерной системы и сети, при которой в систему вставляются поддельные объекты – побочные транзакции или записи в базы данных. При умелом исполнении обнаружить подобные изменения затруднительно.

Основная угроза многопользовательской системе – это возможность удаленного терминального доступа. Сложность контроля путей маршрутизации пакетов, множественных узлов, через которые они следуют, также повышают уязвимость системы. Удаленный доступ позволяет неограниченному числу пользователей, находящихся на различных расстояниях от системы и имеющих доступ к сети, пытаться пройти авторизацию и получить доступ.

Управление доступом осуществляется посредством использования идентификатора и защиты прав доступа пользователей. Последняя реализуется на системном уровне и позволяет изменять права только авторизованным администраторам. Идентификатор пользователя, как правило, состоит из имени и пароля, а также может включать криптографические типы аутентификации[5].

Для идентификации пользователя обычно используются:

– пароль и имя;

– явный или скрытый индивидуальный ключ (карта);

– биометрические характеристики.

Наличие индивидуального ключа, прокси-карты или RFID-метки значительно повышает достоверность идентификации, особенно при применении тактики скрытого расположения. Эффективным является использование индивидуальных биометрических характеристик – анатомических, физиологических, психологических и поведенческих.

С начала XX в. психологи и математики исследовали человеческие поступки. Они утверждали, что поведение человека предсказуемо при выполнении повторных и стандартных задач. Медики и биологи отмечают уникальность папиллярного узора пальцев, рисунка сетчатки глаза, размера черепа человека, динамики отправки телеграфных сообщений, нажатия клавиш, почерка[6].

Использование биометрических характеристик для идентификации стало возможно благодаря стремительному росту вычислительных возможностей компьютеров и развитию полупроводниковой электроники.

Для регистрации каждого биометрического признака требуется высокочувствительный и точный датчик, высокопроизводительная вычислительная техника и программа, реализующая оптимальный алгоритм обработки экспериментальных данных.

ПРИМЕЧАНИЯ

[1] См.: Алгулиев Р.М., Рагимов Э.Р. Об одном методе оценки информационной безопасности корпоративных сетей в стадии их проектирования // Информационные технологии. 2005. № 7. С. 35–39; Швырев Б.А. Перспективы применения системы электронного мониторинга в отношении осужденных, отбывающих наказания в колониях-поселениях // Ведомости уголовно-исполнительной системы. 2011. № 11. С. 26–27.

[2] См.: Кухарев Г.А. Биометрические системы: методы и средства идентификации личности человека. СПб., 2001; Pfleeger C.P. Security in Computing, Prentice Hall. Upper Saddle River. NY., 1997.

[3] См.: Мао В. Современная криптография. Теория и практика. Вильямс, 2005. С. 768; Швырев Б.А. Перспективы применения системы биометрической идентификации при исполнении наказаний в виде лишения свободы // Ведомости уголовно-исполнительной системы. 2011. № 9 (112). С. 10–13.

[4] См.: Шнайер Б. Прикладная криптография: Протоколы, алгоритмы и исходные тексты на языке Си. М., 2005. С. 610; Pfleeger C.P. Security in Computing, Prentice Hall. Upper Saddle River.

[5] См.: Кухарев Г.А. Биометрические системы: методы и средства идентификации личности человека. СПб., 2001; IEEE Computer. 2010. Vol. 43.

[6] IEEE Computer. 2010. Vol. 43; Bleha S., Obaidat M.S. Computer User Verification Using the Perceptron // IEEE Trans. Systems Man and Cybernetics. 1993. Vol. 23. № 3. P. 900–902.

[1] Sm.: Alguliev R.M., Ragimov Je.R. Ob odnom metode ocenki informacionnoj bezopasnosti korporativnyh setej v stadii ih proektirovanija // Informacionnye tehnologii. 2005. № 7. S. 35–39; Shvyrev B.A. Perspektivy primenenija sistemy jelektronnogo monitoringa v otnoshenii osuzhdennyh, otbyvajushhih nakazanija v kolonijah-poselenijah // Vedomosti ugolovno-ispolnitel'noj sistemy. 2011. № 11. S. 26–27.

[2] Sm.: Kuharev G.A. Biometricheskie sistemy: metody i sredstva identifikacii lichnosti cheloveka. SPb., 2001; Pfleeger C.P. Security in Computing, Prentice Hall. Upper Saddle River. NY., 1997.

[3] Sm.: Mao V. Sovremennaja kriptografija. Teorija i praktika. Vil'jams, 2005. S. 768; Shvyrev B.A. Perspektivy primenenija sistemy biometricheskoj identifikacii pri ispolnenii nakazanij v vide lishenija svobody // Vedomosti ugolovno-ispolnitel'noj sistemy. 2011. № 9 (112). S. 10–13.

[4] Sm.: Shnajer B. Prikladnaja kriptografija: Protokoly, algoritmy i ishodnye teksty na jazyke Si. M., 2005. S. 610; Pfleeger C.P. Security in Computing, Prentice Hall. Upper Saddle River.

[5] Sm.: Kuharev G.A. Biometricheskie sistemy: metody i sredstva identifikacii lichnosti cheloveka. SPb., 2001; IEEE Computer. 2010. Vol. 43.

[6] IEEE Computer. 2010. Vol. 43; Bleha S., Obaidat M.S. Computer User Verification Using the Perceptron // IEEE Trans. Systems Man and Cybernetics. 1993. Vol. 23. № 3. P. 900–902.