ВЕСТНИК ЮЖНОГО НАУЧНОГО ЦЕНТРА РАН, Том 1, № 3, 2005, стр. 95–99

ЗАЩИТА ИНФОРМАЦИИ

УДК 681.31

БИОМЕТРИЧЕСКИЕ КРИПТОСИСТЕМЫ. ПУТЬ К ЗАЩИЩЕННОЙ БИОМЕТРИИ

© 2005 г. Л.К. Бабенко[1], О.Б. Макаревич[1], Е.П. Тумоян[1]

В статье рассматривается новое направление в защите информации – биометрическая криптография. Биометрические криптосистемы позволяют решить основные проблемы безопасности биометрических систем аутентификации. Одной из ведущих организаций в данной области является кафедра БИТ ТРТУ. На кафедре БИТ в течение нескольких лет ведутся работы по разработке биометрических криптосистем, в частности, систем генерации криптографических ключей по голосу. Один из разработанных методов приведен в данной статье.

Расширение рынка биометрических систем управления доступом свидетельствует об интересе пользователей к решениям такого рода. Однако необходимо отметить, что область практического применения биометрических систем не выходит за пределы круга задач, связанных с управлением доступом к объектам и помещениям и компьютерным системам. Основными пользователями биометрических систем по-прежнему являются крупные государственные учреждения и частные корпорации, т.е. биометрические системы управления доступом практически не используются массовыми пользователями. Среди причин сложившейся ситуации можно назвать проблемы, связанные с безопасностью биометрических систем.

Рассмотрим общую схему биометрической аутентификации и идентификации применительно к управлению доступом. Одна из реализаций данной схемы приведена на рисунке 1 (по материалам [1]). Многие исследователи отмечают, что данная классическая схема обеспечивает надежную защиту от случайных атак, но является весьма нестойкой к целенаправленным атакам [2, 3]. Основная проблема данных систем заключается в том, что программное обеспечение системы не сможет использоваться за пределами контролируемой зоны и должно быть хорошо защищено как от модификации, так и от исследования. Существует достаточно обширный класс задач, например, криптографическая аутентификация мобильных пользователей, использование биометрии для доступа к ключам шифрования в персональных компьютерах и т.д., для которых необходима разработка метода, обеспечивающего хранение и управление ключевой информацией без использования дорогостоящих аппаратных средств, а также выделенных удаленных серверов аутентификации. По мнению исследователей [4, 5], одним из наиболее перспективных решений может стать применение биометрических криптосистем.

На основе [4, 5] можно сформулировать следующее определение биометрической криптосистемы. Биометрическая криптосистема – это система, обеспечивающая хранение криптографических ключей в таком виде, что они могут быть извлечены и использованы только в том случае, когда пользователь обладает некоторым заданным на этапе регистрации биометрическим параметром.

ТЕКУЩЕЕ СОСТОЯНИЕ ОБЛАСТИ

В настоящее время биометрическая криптография является одним из наиболее новых направлений в защите информации. Основные работы в данной области были опубликованы начиная с 1998 г. Одной из первых является работа C. Soutar и др. [5]. Авторы предложили алгоритм генерации криптографического ключа на основе отпечатков пальцев с применением цифрового фильтра и кодов с коррекцией ошибки. G.I. Davida и др. [6] в 1998 и 1999 гг. предложили алгоритм генерации криптографического ключа на основе бинарного представления сетчатки глаза (IrisCode). В предлагаемом авторами методе используется несколько сканирований сетчатки глаза и применение кодов с коррекцией ошибки для компенсации вариабельности биометрического признака.

Коллектив исследователей под руководством F. Monrose [7] предложил алгоритм для усиления клавиатурного пароля путем добавления в него

[1] Таганрогский государственный радиотехнический университет, г. Таганрог.

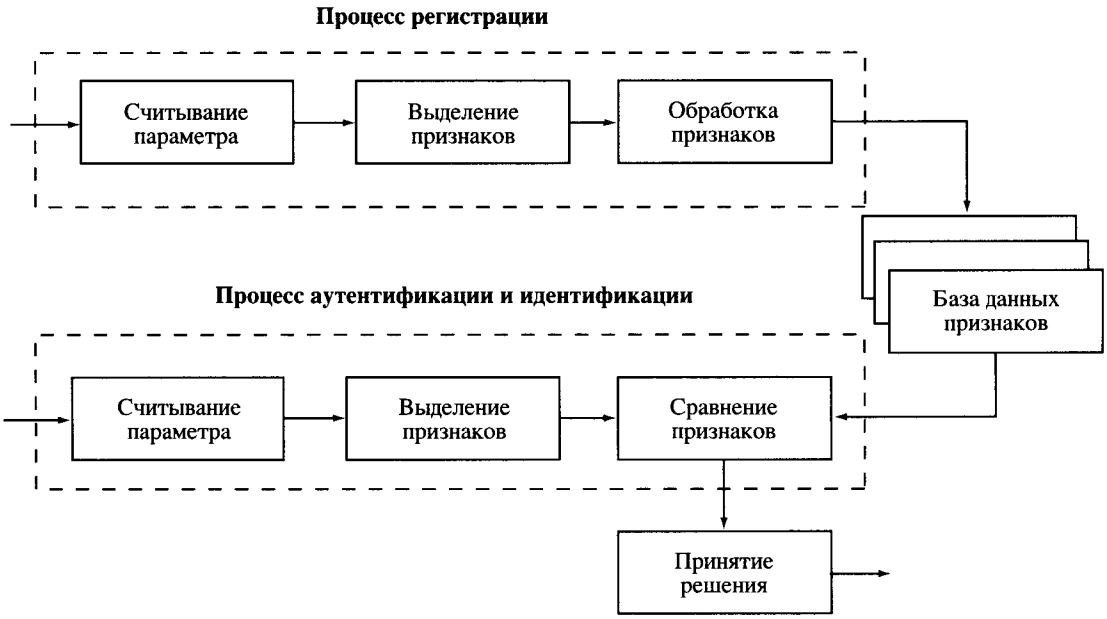

Рис. 1. Функционирование биометрических методов управления доступом

Рис. 2. Сохранение и восстановление криптографического ключа

характеристик динамики набора и создания т.н. hardened password. При этом также используются коды с коррекцией ошибки и таблица инструкций для восстановления ключа. В настоящее время данная схема считается наиболее практичной, поскольку подтверждена экспериментальными данными, в то время как остальные исследователи остановились на теоретическом обосновании своих методов. Другие зарубежные исследователи, например, P. Tuyls [8], A. Juels и M. Wattenberg [9] и др., также используют методы генерации ключей с коррекцией ошибок, возникающих в проверяемых данных. Одно из наиболее интересных исследований было проведено А.И. Ивановым в работе [10]. Автор предлагает использовать для генерации криптографических ключей расширяющиеся нейронные сети, в частности, сети на ядрах Вольтера. Применение искусственных нейронных сетей при генерации криптографического ключа позволяет достичь ряда преимуществ, недоступных при использовании методов фильтрации и коррекции ошибок. Основные достоинства – высокая сложность анализа нейронной сети, поскольку закономерности преобразования биометрического ключа содержатся в большом количестве весов нейронной сети.

С 2002 г. исследования в области интеграции биометрических технологий и криптографии ведутся на также кафедре безопасности информационных технологий Таганрогского радиотехнического университета (БИТ ТРТУ). В настоящее время ТРТУ является одним из немногих в мире и одним из двух в России центров развития данной технологии. На кафедре БИТ создана целевая лаборатория, занимающаяся исследованием проблем биометрической криптографии, выполнено и ведется несколько научно-исследовательских работ, защищена кандидатская диссертация. Основное направление исследований связано с безопасной генерацией криптографических ключей по голосовому паролю.

ГЕНЕРАЦИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ ПО ГОЛОСОВОМУ ПАРОЛЮ

Голос является одним из наиболее привлекательных с практической точки зрения биометрических признаков по следующим причинам:

– распознавание по голосу – один из наиболее естественных типов распознавания, он является гигиеничным, не считается опасным для здоровья и не вызывает у пользователей криминальных ассоциаций;

– подсистемы записи звука компактны, дешевы и в настоящее время встраиваются в большое количество вычислительных и бытовых приборов (компьютеры, PDA, мобильные телефоны и т.д.);

– содержание голосового пароля является неизвестным фактором для злоумышленника.

Метод, разработанный на кафедре БИТ, состоит из двух этапов: сохранение криптографического ключа пользователя и восстановление криптографического ключа. На рисунке 2 показаны схемы сохранения и восстановления криптографического ключа. Как видно, при выполнении этих этапов используются одинаковые функциональные элементы: запись и оцифровка голосового пароля, выделение голосовых признаков, наиболее полно отражающих особенности голосового пароля диктора, стабилизация признаков, обучение нейронной сети и т.д.

Поскольку в данной работе нет возможности описать все функциональные элементы метода, остановимся на основном элементе, определяющем безопасность и точность предлагаемого метода – искусственной нейронной сети. Нейронная сеть может находиться в двух состояниях: в режиме обучения (для сохранения ключа) и в режиме классификации (для восстановления ключа). В режиме обучения нейронная сеть обучается сопоставлять биометрические параметры одного пользователя (или нескольких пользователей с одинаковым ключом) (F_1, F_2, ..., F_N) с их секретным криптографическим ключом (*PPK*). Кроме того, сеть обучается связывать параметры незарегистрированных дикторов (U_1, U_2, ..., U_N) со случайным битовым набором (*RBS*). Операционные возможности искусственной нейронной сети полностью определяются ее весами (W). Таким образом, цель обучения нейронной сети состоит в нахождении значений W, которые минимизируют ошибку между желаемыми и актуальными выходными значениями. Обучение продолжается до тех пор, пока ошибка E_t не достигнет необходимого минимального порога P_t. После обучения параметры нейронной сети (число слоев сети, размер каждого слоя, значения весов) сохраняются; для восстановления функциональности нейронной сети необходимо загрузить сохраненные параметры и создать нейронную сеть в соответствии с ними. В процессе восстановления ключа нейронная сеть получает биометрические параметры зарегистрированного пользователя или пользователей (F_i) и продуцирует на выходах сохраненный секретный ключ (*PPK*). В том случае, если полученные параметры не принадлежат зарегистрированному пользователю, сеть продуцирует некоторый случайный битовый набор (*RBS*), определяемый внутренними весами сети.

ЭКСПЕРИМЕНТАЛЬНЫЕ ОЦЕНКИ

В соответствии с предложенным методом коллективом разработчиков кафедры БИТ ТРТУ была реализована программная система преобразования голосового пароля в криптографический ключ. В экспериментах по тестированию данной системы участвовало 20 дикторов различных возрастов без явных отклонений в произношении. При тестировании голосовые образы записывались в обычных офисных условиях. В качестве *PPK* используется случайно сгенерированный криптографический ключ размерностью 32 бит. В качестве *RBS* используются случайным образом сгенерированные битовые наборы размерностью 32 бит. Полученная обучающая выборка используется для обучения трехслойного MLP. Для обучения сети использована одна из модификаций метода обратного распространения ошибки – resilent backpropagation. В процессе экспериментов контролировались такие параметры, как вероятность неправильного восстановления ключа при правильных голосовых данных (false rejection rate, FRR), вероятность правильного восстановления ключа при неверных голосовых параметрах (false acceptance rate, FAR), время обучения и время тестирования в секундах. Общее число экспериментов составило более 10^6. Подробно результаты экспериментов приведены в работе [14] и частично [15, 16]. Коротко результаты можно охаракте-

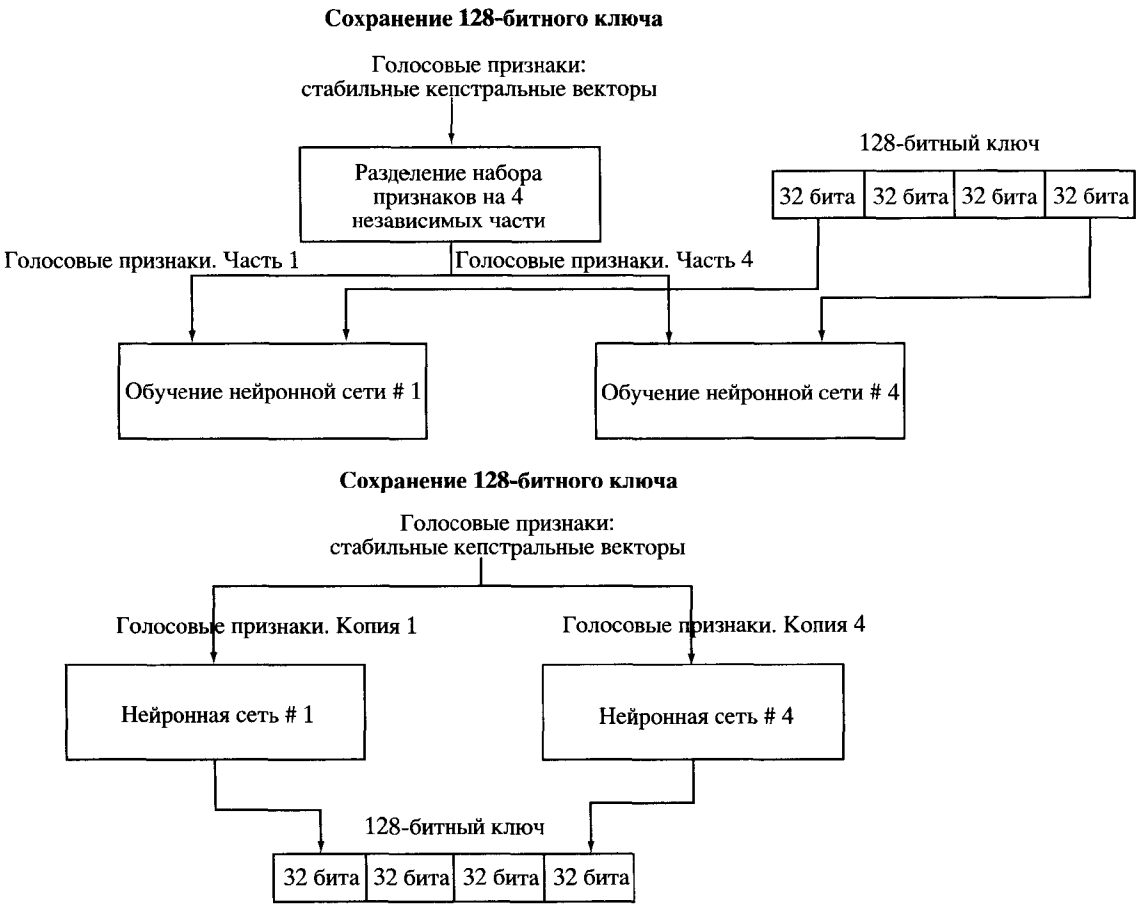

Рис. 3. Метод сохранения 128-битного ключа

ризовать следующим образом. Среднее значение FAR = 0.00125, среднее значение FRR порядка 0.20, вероятность двукратного ложного отказа FRR около 0.1, а трехкратного менее 0.04. Объем памяти для хранения параметров нейронных сетей менее 40 Кб для одного пользователя. Время восстановления ключа около 2 с. Эксперименты проводились с криптографическими ключами длиной 32 бит. Ключи такой длины не применяются на практике, поэтому для хранения практически значимых ключей длиной 128 бит была разработана схема 4-кратной репликации метода, как показано на рисунке 3.

Схема имеет ряд особенностей по сравнению с базовой. При сохранении ключа каждая из нейронных сетей обучается ставить в соответствие параметры голосового пароля пользователя и одну из 32-битных частей 128-битного ключа. Нужно обратить внимание, что обучающие выборки для каждой из искусственных нейронных сетей создаются так, чтобы гарантировать взаимную статистическую независимость возникновения ошибок FAR и FRR для каждой сети. При восстановлении ключа каждая из сетей восстанавливает одну из частей большего криптографического ключа.

Эксперименты с данной схемой показали следующие результаты: среднее значение FAR = $= 2 \cdot 10^{-13}$, среднее значение FRR порядка 0.20. Объем памяти для хранения четырех нейронных сетей менее 160 кб. Время восстановления 128-битного ключа менее 9 с.

ЗАКЛЮЧЕНИЕ

Биометрическая криптография позволяет решить основные проблемы безопасности, возникающие при практической эксплуатации систем биометрической идентификации. В частности, разработанный на кафедре БИТ ТРТУ метод позволяет использовать для проведения процессов аутентификации незащищенную вычислительную среду, предусматривает хранение биометрических параметров без дополнительных средств защиты, позволяет выполнять построение системы биометрической аутентификации поверх уже существующих протоколов сетевой аутентификации или шифрования. Использование предложенного метода значительно расширяет круг устройств, которые могут быть включены в защищенную информационную систему, например, для

случая голосовой аутентификации в состав системы могут быть включены не только рабочие станции, терминалы, портативные компьютеры, но также и PDA, смартфоны и мобильные телефоны. Развитием представленных исследований станет внедрение разработанного метода в распределенные информационные системы, в частности, в настоящее время ведутся разработки по реализации данной технологии для КПК PocketPC. Кроме того, ведутся исследования по использованию других биометрических признаков, например, отпечатков пальцев.

ЛИТЕРАТУРА

1. *Jain A.K., Bolle R.M., Pankanti S.* Biometric: Personal identification in networked society. Kluwer Academic Publishers, Norvell, Maas, 1999. 441 p.
2. *Schneier B.* // Comm. ACM, 1999. V. 42. N 8. P. 136.
3. *Ratha N.K., Connell J.H., Bolle R.M.* // Proc. AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication. 2001. P. 223–228.
4. *Uludag U., Pankanti S., Prabhakar S., Jain A.K.* // Proceedings of the IEEE. 2004. V. 92. N 6. P. 948–960.
5. *Soutar C., Roberge D., S. Stojanov A., Gilroy R., Vijaya Kumar B.V.K.* // Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II. 1998. V. 3314. P. 178–188.
6. *Davida G.I., Frankel Y., Matt B.J.* // Proc. 1998 IEEE Symp. Privacy and Security. 1998. P. 148–157.
7. *Monrose F., Reiter M.K., Wetzel S.* // Proc. 6th ACM Conf. Computer and Communications Security / Ed. by G. Tsudik. 1999. P. 73–82.
8. *Linnartz J.-P., Tuyls P.* // Proc. 4th Int. Conf. Audio- And Video-Based Biometric Person Authentication. 2003. P. 393–402.
9. *Juels A., Wattenberg M.* // Proc. 6th ACM Conf. Computer and Communications Security/ Ed. by G. Tsudik. 1999. P. 28–36.
10. *Иванов А.И.* Биометрическая идентификация личности по динамике подсознательных движений. Пенза: Изд-во ПГУ, 2000. 188 с.
11. *Макаревич О.Б., Тумоян Е.П.* // Известия ТРТУ. Таганрог: Изд-во ТРТУ, 2003. № 4. С. 132–141.
12. *Makarevich O.B., Babenko L.K., Tumoyan E.P.* // Proc. IEEE AIS'04 and CAD -2004. 2004. P. 61–66.
13. *Makarevich O.B., Babenko L.K., Tumoyan E.P.* // Proc. Intern. Scientific Workshop "High-performance computing systems". 2004. P. 214–218.

BIOMETRICAL CRYPTOSYSTEMS. A WAY TO SECURED BIOMETRICS

L.K. Babenko, O.B. Makarevitch, E. P. Tumoian

A new area of information security, the biometric cryptography, is considered in the article. Biometric cryptography allow to solve basic problems of biometric authentication systems. The department of IT-security of TSURE is one of the leading organizations in this area. The department has been carrying out various researches on biometric cryptography systems within the last several years; particular attention is paid to the generation of cryptography keys based on voice features. One of the developed methods is described in the article.

REFERENCES

1. Jain A.K., Bolle R.M., Pankanti S. 1999. *Biometric: Personal identification in networked society*. Kluwer Academic Publishers, Norvell, Maas: 441 p.
2. Schneier B. 1999. *Comm. ACM*. 42(8): 136.
3. Ratha N.K., Connell J.H., Bolle R.M. 2001. In: *Proc. AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication*. P. 223–228.
4. Uludag U., Pankanti S., Prabhakar S., Jain A.K. 2004. *Proceedings of the IEEE*. 92(6): 948–960.
5. Soutar C., Roberge D., S. Stojanov A., Gilroy R., Vijaya Kumar B.V.K. 1998. In: *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II*. Vol. 3314. P. 178–188.
6. Davida G.I., Frankel Y., Matt B.J. 1998. In: *Proc. 1998 IEEE Symp. Privacy and Security*. P. 148–157.
7. Monrose F., Reiter M.K., Wetzel S. 1999. In: *Proc. 6th ACM Conf. Computer and Communications Security*. (Ed. by G. Tsudik). P. 73–82.
8. *Linnartz J.-P., Tuyls P.* 2003. In: *Proc. 4th Int. Conf. Audio- And Video-Based Biometric Person Authentication.* P. 393–402.
9. *Juels A., Wattenberg M.* 1999. In: *Proc. 6th ACM Conf. Computer and Communications Security*. (Ed. by G. Tsudik). P. 28–36.
10. Ivanov A.I. 2000. *Biometricheskaya identifikatsiya lichnosti po dinamike podsoznatel'nykh dvizheniy*. [*Biometric identification on the dynamics of subconscious movements*]. Penza, Penza State University: 188 p. (In Russian).
11. Makarevich O.B., Tumoyan E.P. 2003. *Izvestiya TRTU*. (4): 132–141.
12. Makarevich O.B., Babenko L.K., Tumoyan E.P. 2004. In: *Proc. IEEE AIS'04 and CAD-2004*. P. 61–66.
13. Makarevich O.B., Babenko L.K., Tumoyan E.P. 2004. In: *Proc. Intern. Scientific Workshop "High-performance computing systems"*. P. 214–218.